Information Security and Privacy

DCAP309/DCAP513

LOVELY
PROFESSIONAL
UNIVERSITY

LOVELY PROFESSIONAL UNIVERSITY

INFORMATION SECURITY AND PRIVACY

Produced & Printed by
EXCEL BOOKS PRIVATE LIMITED
A-45, Naraina, Phase-I,
New Delhi-110028
for
Lovely Professional University
Phagwara

SYLLABUS

Information Security and Privacy

Objectives: To Impart the skills needed to provide security to the system. Student will learn: Various types of threats, Risk analysis, Physical security of infrastructure, Providing authorization using biometrics, Network security and cryptography techniques, Database security and Web security issues.

DCAP309 INFORMATION SECURITY AND PRIVACY

Sr. No.	Topics
1.	**Information Systems:** Meaning, importance, basics, changing nature and global information systems.
2.	**Threats:** New Technologies Open Door Threats, information Level Threats Vs Network Level Threats, information system security, Computer Viruses, Classifications of Threats and Assessing Damages and protecting information system security
3.	**Building Blocks of Information Security:** Basic Principles, Security related Terms, Three Pillars of Information Security. Information Classification, criteria for information and classification, data obfuscation
4.	**Information security Risk Analysis:** Introduction, Risk Management & Risk Analysis. Approaches and Considerations.
5.	**Physical Security:** Need, Meaning, Natural Disasters and control, basic tenets of physical security of information systems resources, physical entry controls.
6.	**Biometrics Controls for Security: Introduction,** Access Control, User Identification & Authentication. Meaning, Nature of Biometric identification/Authentication techniques, Biometric Techniques. Key Success factors and benefits.
7.	**Network security:** Need, Basic concepts, network security dimensions, establishing security perimeter for network protection. **Cryptography & Encryption:** Meaning, Applications of Cryptography, Digital Signature, Cryptographic Algorithms.
8.	**Databases Security:** Introduction, Need, federated databases, securing the contents of mobile databases, data integrity as a parameter for database security, database security policy.
9.	**Security Models & Frameworks:** Intro, Terminology. Methodologies for Information System Security
10.	**Privacy:** Meaning, direct marketing and impact on privacy, privacy invasion through data mining, privacy in outsourcing, privacy challenges in test environment. **Privacy Technological Impacts:** Implications of RFID. Use with Bio-Metrics. Smart Card Applications.

DCAP513 INFORMATION SECURITY AND PRIVACY

Sr. No.	Topics
1.	**Information Systems:** Meaning, Importance. Global Information Systems: Role of Internet and Web Service. Information System Security & Threats.
2.	**Threats:** New Technologies Open Door Threats. Level of Threats: Information, Network Level. Threats and Attacks. Computer Viruses. Classifications of Threats and Assessing Damages.
3.	**Building Blocks of Information Security:** Principles, Terms, Three Pillars of Information Security. Information Classification. **Risk Analysis:** Risk Management & Risk Analysis. Approaches and Considerations.
4.	**Physical Security:** Need, Meaning, Natural Disasters, Controlling Physical Access, Intrusion Detection System.. Controlling Visitors. Fireproof Sales, Security through cables and locks.
5.	**Biometrics Controls for Security:** Access Control, User Identification & Authentication. Meaning, Biometric Techniques. Key Success factors.
6.	**Network Security:** Intro, Network Types, Basic Concepts: Computer Security, Network Security, Trusted and UnTrusted Networks. Unknown Attacks.
7.	**Cryptography & Encryption:** Meaning, Applications of Cryptography, Digital Signature, Cryptographic Algorithms. **Firewalls:** Meaning, Demilitarized Zone. Proxy Servers. Packet Filtering, Screening Routers. Application Level Firewalls, Hardware Level Firewalls.
8.	**Databases Security:** Introduction, Need, Mobile Databases Security, Enterprise Database Security. Database Security Policy. **Security Models & Frameworks:** Intro, Terminology. Intro to ISO 27001. COBIT, SSE-CMM. **Methodologies for Information System Security:** IAM, IEM, SIPES.
9.	**Security Metrics:** Intro, Basic, Security Matrix, Classification. **Privacy:** Meaning, Business Issue, Privacy Vs. Security, Related Terms. Information Privacy Principles.
10.	**Privacy Technological Impacts:** Implications of RFID. Use with Bio-Metrics. Smart Card Applications. **Web Services and Privacy:** Privacy on Internet, Web Services, Privacy Aspects of SOA.

CONTENTS

Notes

Unit 1: Information Systems

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand meaning and importance of information systems
- Discuss Global Information Systems
- Recognize role of internet and web service
- Explain the concept of information system security & threats

Introduction

Information System is a particular discipline or branch of learning that is concerned with the application of information to organizational needs. The scope of information system includes manual, computer-based and other forms of automated procedures and applications of information technology generally.

In order for organizations to use information technologies effectively, information systems must be designed, developed, implemented and managed in ways that fit with the specific work processes and organizational contexts. A thorough understanding of information systems development and management concepts together with skills in desktop computing enables the manager to develop end user systems and provide the business perspective to participate in the creation and management of major information systems. Management Information System (MIS) concepts also provide a foundation on which to base expertise in information systems for specialized work processes such as marketing, accounting and international business.

Any system designed to provide Information with above-discussed qualities to the managers in an organization for decision-making is called an 'Information System.' But before formalizing the word 'Information System', we need to understand the meaning of the term 'System' in more detail and then look into the 'Management Information System' which is an important subset of the overall information system in an organization.

1.1 Information Systems: Meaning

The word 'System' is a common term that we use in daily life. Literally speaking, a system is a set of components that interact to accomplish some purpose or in other words, a system is a set of interrelated components or objects that work together for the overall objective.

The term, system, is taken from the word *'Systema'* which means an organized relationship among its components. The system can be defined as orderly grouping of interdependent components linked together according to plan to achieve a specific objective or goal. Therefore, a system is designed to achieve one or more objectives. The components/parts of a system refer to sub-system. A 'sub-system' is a system which is an element of a larger system. The large system is called a super system or supra system.

Although the word, system, is used in many diverse areas, all systems have some common properties—they have elements, environments, and communication between their elements and with the environment. A system is designed to achieve a predefined objective. Also, interrelation and interdependence must exist amongst the components.

So, broadly we can define a system as an organized collection of people, machines, procedures, documents, data or any other entities such that they interact with each other as well as with the environment to reach a predefined goal.

Now, it is time to see the real meaning and concept of Information Systems. Too often you hear someone say, "Oh yeah, I know how to use a computer. I can surf the Web with the best of them and I can play Solitaire for hours. I'm really good at computers." Okay. So that person can pound a keyboard, use a mouse at lightning speed, and has a list of favorite Web sites a mile long. But the real question is "Is that person's information literate?" Just because you can pound the keyboard it doesn't necessarily mean that you can leverage the technology to your advantage or the advantage of your organization. An organization can gather and keep all the data on its customers that a hard drive can hold. You can get all the output reports that one desk can physically hold. You can have the fastest Internet connection created to date. But if the organization doesn't take advantage of customer data to create new opportunities, then all it has is useless information. If the output report doesn't tell the management that it has a serious problem on the factory floor, then all that's been accomplished is to kill a few more trees. If you don't know how to analyze the information from a Website to take advantage of new sales leads, then what have you really done for yourself today?

Task Make distinction between sub-system and super system.

Self Assessment

Fill in the blanks:

1. Any system designed to provide Information with above-discussed qualities to the managers in an organization for decision-making is called an ....

Notes

2. A .... is a set of components that interact to accomplish some purpose.
3. A '.......................' is a system which is an element of a larger system.

1.2 Importance of Information Systems

Information system is the study of information production, flows and use within organizations. Information system makes extensive use of information technology means. But it is very important to appreciate that its scope encompasses systems in their entirety, including manual activities, the interface between manual and automated components of systems, design aspects of IT means, and economic, legal, organizational, behavioral and social aspects of systems.

Information systems overlap with both the computer science and business management disciplines.

Example: Software engineering and database management and some aspects of application software development overlap with computer science, and systems analysis and organisational behaviour overlap with the business-related disciplines.

The information system of an organization may be defined as a system that serves to provide information within the organization when and where it is needed at any managerial level. An information system is a set of people, procedures and resources that interact to satisfy the information processing needs of an organization. During the processing, the data is collected, stored, transformed and distributed in an organization. Such a system must take the information received and store, retrieve, transform, process, and communicate it using the computer system or some other means. It is not necessary that an information system cannot function in the absence of computers. An information system is a logically interrelated set of business processes that accomplish organizational goals.

Management Information System is mainly dependent upon information, which is a vital ingredient of any Management Information System. Information is the most critical resource of Management Information System. We all know that information is a vital factor for our existence. Just as our body needs air, water and clothes, we are as much dependent upon information. To make life more interesting and to achieve the feeling of being a part of the social system, we want to know our surroundings and for that we need information. Information is an important input for achieving our goals such as learning to help each other and to become integral part of society.

Actually, information system is not a new concept; it is as old as the hills. From biblical times, humans have been making the use of information generated through information systems in all times. There have been systems that generated and communicated information. Kings and rulers had their own ways of designing information systems to retrieve information. The main objective of these information systems was to ascertain the well being of their people in the kingdom and to effectively and efficiently manage the kingdom. The church had its own information system. In India, Tainali Rama, Akbar and many others had impressive management information systems in operation. Similarly, the merchants of Venice had their own fully functional appropriate management information system in place.

Most of us think only of hardware and software when we think of an Information System. There is another component of the triangle that should be considered, and that's the people side, or "liveware."

We talk about the input, processing, output and feedback processes. Most important is the feedback process; unfortunately it's the one most often overlooked. Just as we discussed above, the hardware (input and output) and the software (processing) receive the most attention. With

Notes

those two alone, you have computer literacy. But if you don't use the "liveware" side of the triangle to complete the feedback loop, you don't accomplish much. Add the "liveware" angle with good feedback and then you have the beginnings of information literacy.

An information system differs from other kinds of systems in that its objective is to monitor/document the operations of some other system, which we can call a target system. An information system cannot exist without such a target system.

Example: Production activities would be the target system for a production scheduling system, human resources in the business operations would be the target system of a human resource information system, and so on.

It is important to recognize that within a vending machine there is a component/sub-system that can be considered an information system. In some sense, every reactive system will have a subsystem that can be considered an information system whose objective is to monitor and control such a reactive system.

Need for Information Systems

Ask managers to describe their most important resources and they'll list money, equipment, materials, and people – not necessarily in that order. It's very unusual for managers to consider information an important resource and yet it is.

Competitive Business Environment

For many years computer technology was relegated to the backrooms or basements of a corporation. Only the "techies" worried about it and were often the only ones who really knew how it all worked. Now computers are all over the organization — one on every desk. It's not enough for you to know how to pound a keyboard or click a mouse. It is not even enough for you to know how to surf the Web. Now every employee, including you, must know how to take advantage of Information Systems to improve your organization and to leverage the available information into a competitive advantage for your company.

Did u know? **What is Management Information System?**

Management information system is a refined orientation of available sources of information which enables managers to tie planning and control procedures to operational systems of implementation.

Self Assessment

Fill in the blanks:

4. The information system of an organization may be defined as a system that serves to provide information within the organization when and where it is needed at any .... level.

5. During the ...., the data is collected, stored, transformed and distributed in an organization.

6. An information system differs from other kinds of systems in that its objective is to monitor/document the operations of some other system, which we can call a .... system.

1.3 Global Information Systems: Role of Internet and Web Services

Notes

Understanding information infrastructures requires a holistic perspective – an infrastructure is more than the individual components. Successful development and deployment of information infrastructures requires more than a combination of traditional approaches and strategies for development of telecommunications solutions and information systems.

The infrastructures up to some extent can be seen as information systems as they contain everything you find in an information system. But an infrastructure is something more than an information system. Current information infrastructures are combination of traditional information systems and telecommunication technology.

Traditional approaches to information systems development are implicitly based on assumptions where the information systems are closed, stand-alone systems used within closed organizational limits.

They are assumed developed within a hierarchical structure – a project (managed by a project leader and a steering group) – which is a part of a larger hierarchical structure - the user organization (or the vendor organization in case of a commercial product).

Telecommunication systems, on the other hand, are global. The most important design work – or decisions at least – are taken care of by standardization bodies (CCITT and ITU). When developing infrastructures, the focus on closed, stand-alone systems has to be replaced by one focusing on the infrastructures as open and global as is the case for development of telecommunication technologies. However, there are other parts of the telecommunication approach which is more problematic.

Characteristic for traditional telecommunication solutions have been their stability. This is in particular true for their functionality and user interface. To put it simply, the basic functionality has been stable for more than hundred years. A telephone service has one function: the user can dial a number, talk to the person at the other end, and hand up when finished.

As telecommunication got "informational zed," however, this started to change and new functions (for instance, you can transfer your phone "virtually" to another number, you may use it as an alarm clock, etc.) have been added. But the stability of the functionality is a basic precondition for how the approaches and strategies followed for developing telecommunication technologies.

What has been in focus has been the improvement of the technologies invisible to the users. At the national level, the telecommunication infrastructures have been built and operated by national monopolies since about the turn of the century. Monopolies have dominated this technology as its size and interconnectedness makes this "natural," and most investments have been made based on long time horizons, usually 30 years.

All technologies are designed and specified as global (universal) standards. Such standards have been seen as absolutely required to enable smooth operation and use of the infrastructure. However, the development of such standards takes time – usually about ten years for each standard. And under the existing conditions – the simple user interface – one (or may be three: dial, talk, hang up) operation not being modified for 100 years, the long term planning of the infrastructure, and the limited number of actors – one for each country – this approach has worked pretty well.

Information systems development, however, has very different – or rather opposite – characteristics. While the telephone functionality and user interface has been extremely stable and simple, information systems are characterized by very rich and highly dynamic functionality.

Information systems are closely tied to the working processes they support. These processes are inscribed into the systems making them unique and local - not universal. The environments of

Notes

information systems are highly dynamic. And the information systems are in themselves a driving force in changing the very work practices and other environmental elements they are designed to support.

In the case of telecommunication technologies the stability of the functionality and user interface has made users irrelevant in the design process. The user interface has been given, and one could concentrate only on technological issues.

For information systems the situation is the opposite. As the links between the technology and the users are so rich and dynamic, dealing with the interaction between technological and human, social, and organizational issues has been of utmost importance.

Future information infrastructures will be just as dynamic as our information systems have been so far. They will be very heterogeneous (i.e. the combined vertical and horizontal integration of information systems).

So, can we find an approach to infrastructure development which account for the dynamics and non-technical elements of information systems at the same time as the standards enabling the required integration – an approach which works for more heterogeneous and dynamic technologies that telephone services up to now? This is a too big question.

However, that is the question we want to inquire into. Our main focus is the tension between standardization and flexibility, which we believe is an important element in the bigger question.

Caution Although traditional approaches and telecommunications solutions approaches complement each other, they also contain important contradictions and accordingly brand new approaches are required.

Task Differentiate between traditional information systems and telecommunication technology.

1.4 Role of Internet and Web Service

Internet is considered as one of the most significant things for people these days. All the systems and spheres are incompletely or completely dependent on the Internet. Let us consider the world's banking system, for instance. People do not generally think of how all the financial functions in the world are executed out. Actually, all the financial functions and transfers would be unworkable without the influence of Internet. If Internet stops functioning, everything fails and the whole system stops too. If Internet stopped working all over the world one day, it would be a real disaster and many companies, organizations and enterprises would be recuperating years long. Therefore, Internet and computers are very significant element of people's life and the part of the life movement of people.

Certainly, we can make a simpler instance here. What do you typically feel, when your private computer is broken? You most likely feel the deficiency of information and are concerned regarding all the materials and documents, accumulated in it. You think that they can be just damaged and you do not know, what you will do, if they vanish. Now visualize the same problem, but when it is concerned with the billions of dollars, concerning dissimilar people and deposited with banks. Problems with Internet and computers can cause the problems with money transfers, conclusions of contracts and many other significant processes all through the world. All these probable problems make all establishments have their own support services, programmers, web designers, etc. If they have some difficulty, this difficulty must be right away solved, or else, it can have random consequences and cause extraordinary money losses. So, Internet and computers are very significant for both vast corporations and the regular people. We all depend on the Internet uniformly and cannot deny it. But do we think of the manner in which Internet works and offers us with all his functional information? Most people never have a consideration of it and take Internet for granted.

The function of the World Wide Web is offered and assured by the web-hosting organizations. These organizations are the groups of people, who have rooms, full of prevailing computers, named host servers. The function of each host server offers the work of one, tens, hundreds or even thousands of websites.

Free and sovereign nature of Internet provides security for information system. Internet has developed communication and hence its contribution to information sharing. With use to a computer and an association to Internet, anyone can communicate with others worldwide. Web is intended to exchange unstructured information. Humans are included when conducting business over web. Web services plays a significant and dominant role in constructing global IS. "Web services are self-incorporated, modular applications that can be described, published, situated and invoked over a network, usually WWW". Web services execute functions varying from simple requests and complex business procedures. A deployed web service can be located and invoked by other applications and other web services via Universal Description, Discovery and Integration (UDDI). 'Services' points to components and the services provided that can be used to construct larger application services.

Web services make information obtainable from computer systems to other applications means of well-defined standards. A series of standards have included web services discovery, security, transactions and coordination. Web Services Interoperability Organization (WS-I) overlooks the establishment and promulgation of standards such as:

1. Simple Object Access Protocol (SOAP): formats messages between web services
2. Web Services Definition Language (WSDL): defines use of web services
3. UDDI and WSIL (web services inspection language): locates web services
4. WS-security: handles security across web services
5. WS-coordination: coordinates numerous web services into composite systems.

W3C (World Wide Web Consortium) & OASIS (Organization for the Advancement of Structured Information Standards) issue these standards.

Did u know? Someway or other, web hosting is a service, which makes Internet function and it will always be significant for the World Wide Web.

Notes The types of web-hosting plans, offered by the web-hosting companies, depend on the space client requirements for his or her website and the services, incorporated into a package. If you want to select the most luxurious plan, you will be offered with your own host server.

Notes

Self Assessment

Fill in the blanks:

7. Current information infrastructures are combination of traditional information systems and .... technology.
8. The function of the World Wide Web is offered and assured by the .... organizations.
9. All the systems and spheres are incompletely or completely dependent on the ....
10. .... is used to format messages between web services.
11. The function of each .... offers the work of one, tens, hundreds or even thousands of websites.

1.5 Information System Security and Threats

Security information management is a type of software that automates the collection of event log data from security devices, such as such as firewalls, proxy servers, intrusion-detection systems and anti-virus software.

The short form of Security information management is SIM. The SIM translates the logged data into correlated and simplified formats. Many SIM architecture provides security reporting, analysis and reporting for Sarbanes-Oxley, HIPAA, Basel II, FISMA and Visa CISP compliance audits.

A SIM automates collection and analysis of information from all the security components in a network. Rather than having to look at logs and alerts from firewall, IDS, anti-virus, VPN, and other security systems, a security manager can obtain all of this information from a single SIM console. Some SIMs simply aggregate reports from these various components; others correlate the information to improve the quality of overall security information.

Security Information Management (SIM) products (also referred to as Security Information and Event Management or Security Event Management) automate the manual process of collecting security-specific event-log data from file systems, security appliances and other network devices.

These products, which can be hardware, software, or a service, feature data-aggregation and network event-correlation features similar to those found in network management software. Information can be collected from firewalls, proxy servers, intrusion-detection systems, intrusion-prevention systems, routers and switches, and anti-spam, anti-virus and anti-spyware software.

In addition to being able to access a number of sources for this information, SIM products try to distinguish themselves by how quickly they can collect the information without missing an event, how well the can correlate specific security events with user identities, and how rich their reporting capabilities are to help managers.

Example: Distinguish a legitimate security event from a false-positive alert.

The main objective of Security Information Management is to prevent interruptions to business activities and ensure the correct and secure operation of computer and network facilities. It can be obtained by:

1. Minimizing the risk of systems failures (through use of appropriate operational procedures and plans).
2. Safeguarding the integrity of the organization's software and data.

3. Maintaining the integrity and availability of information services, networks and supporting infrastructure.

4. Preventing damage to assets by controlling and physically protecting computer media.

1.6 Importance of Security Information Management

With a high incidence of severe threats and attacks on information assets, IT security has become a priority at organizations' highest levels. In addition to mitigating threats to mission-critical network systems, enterprises must also comply with a wide range of federal and industry regulations that require them to implement — and verify the effectiveness of — security information management controls.

In a network of any size, the Security Information Management will be dealing with a large quantity of data. Precisely where and how the data is processed will be the key to know whether a particular Security Information Management can keep up with the data generated by your network.

Almost all Security Information Managements have two primary components for the creation and presentation of information: the Security Information Management appliance itself and a dashboard application running on a remote workstation. If all the information is processed in either the appliance or the dashboard workstation, performance can become an issue when either network traffic or incidents become high in density.

⚠

Caution Delayed security information can result in falling victim to an attack that you might have survived.

1.7 How Security Information Management Works?

All Security Information Managements gather information from the sources within the network. Some will gather information from external sources as well, ranging from public threat identification services to proprietary correlation networks. A Security Information Management, to a great extent, adds value with its capability of finding patterns in network traffic.

This activity requires two primary traits: the capability of gathering data from a various places and the intelligence to turn all that data into meaningful information. Both are critical. Just as the Security Information Management must draw information from all of the important components of your network, the correlation data must come from sources you trust.

1.8 Advantages of Information Management Security

The benefits of a Security Information Management (SIM) product can be difficult to justify. SIMs don't provide a direct security benefit in the way that anti-malware products do. Users don't touch them, like a new SSL VPN concentrator. And unlike a firewall, it's not a foregone conclusion that everyone large or small needs one.

However, a SIM can bring tremendous value by providing total visibility into your security posture, and by leveraging security products you already have. Regulatory compliance has been a top driver for SIM purchases, but there are a number of less obvious advantages that should be considered when selecting a product. The key to realizing the full value of a SIM is to understand all of its advantages and leveraging the product in a way that brings maximum benefit.

Notes

In the panoply of functions a SIM can provide, perhaps the foremost is absorbing the bulk of log data from IDS sensors, IPS devices and firewalls. In this sense, a SIM can act as an IDS console, helping navigate through what is normally an overwhelming amount of IDS data. That's easy enough, but that function alone often doesn't provide enough purchase value for organizations that already have an IDS console.

For a greater benefit we can look beyond analysis of IDS events and focus on the SIM product's alerting and analysis capabilities. These features are appreciated by the security team, but other IT staff can find them useful as well.

Example: Most IDSes have a subset of signatures that help track virus-infected or Trojan-controlled systems. You can use SIM alerts to immediately send infected system data to the organization's help desk, enabling a more proactive approach to tracking and resolving these issues.

A SIM also collects firewall data, which can also be advantageous. Your SIM knows who the top talkers and listeners are on the network, and can probably help identify hot spots and hot protocols where some network engineering or bandwidth controls might be useful.

When deploying a SIM, bring the network engineering team on board by sharing reports and dashboards that focus on bandwidth usage. A SIM might be the only system in your organization that can give this level of visibility into the network, irrespective of security concerns.

Thinking outside of the traditional security box is a good way to leverage a SIM's correlation engine and normalization capabilities. While SIMs might be focused on the security implications of the data they collect, every log message tells a story - one that is generally buried in a pile of unrelated minutiae.

Example: Most devices can emit log messages that presage future failures, such as bad power supplies, fans or failing hard drives. Find those messages using your SIM and you can turn a future emergency failure into a planned maintenance window.

Another potential bonus lies in the piles of typically unexamined logs from Windows and Unix servers. Not every SIM specializes in Windows, but all the good ones are happy to accept Windows event logs, even if they require a conversion to the System log, log-forwarding standard using a tool like Snare. While most system managers have already developed their own local methods for watching logs, a SIM provides a place to collect these logs, rules, and alerts in a single management console.

When leveraging a SIM this way, you can reduce deployment time by eliminating the steps of installing and configuring local log watch tools. And, by cross-correlating events from multiple systems, you may gain greater security visibility than by considering each log one system at a time.

A SIM has to stand or fail on its own merits and for the task you bought it to handle. But taking advantage of the opportunities to leverage a SIM for greater network and system visibility and control will ensure your organization makes the most of its investment.

It's one thing to be notified that unauthorized activities are happening on the network. It's another thing entirely to convince less security-savvy network management to do anything about it. Security Information Management is capable of generating reports to support your call for action and to generate them quickly. If the product comes with prepackaged reports that you can modify to provide the information specific to your organization and incident, then you're way ahead of the game. Prepackaged reports are critically important time-savers when it comes to regulatory-compliance audits.

Notes

1.9 Disadvantages of Information Management Security

Security Information Managements (SIM) is by its very nature a heterogeneous product, and thus SIM rollouts involve complex technical integration and political negotiations. The architecture of the SIM tool doesn't seem to make a whole lot of difference either.

Even if a solution doesn't require an installed agent to get information from a system, it still usually requires a configuration change or privileged account to get the data it needs – and system owners aren't likely to let that happen without good reason.

As threats become more targeted and sophisticated, there is often no single tool that can detect the telltale signs of an attack. Many modern attacks manifest themselves in policy violations like privilege escalations or changes to critical files rather than specific vulnerabilities being exploited or well-known malware being downloaded.

You cannot simply throw the SIM in the system and assume that it will tell you what you need to know about your security or network posture. You have to be willing to actually look deep into what you really care about and either write or activate rules that will make the SIM product work.

Industry watchers and IT managers alike say that SIM won't protect environments from all threats, but the technology can go a long way toward identifying the risk present in any environment.

Notes To be certain SIM is able to adequately streamline the "processes of gathering, analyzing and reporting log, vulnerability and configuration data," it is essential to identify the critical systems in your environment before choosing a SIM technology.

Self Assessment

Fill in the blanks:

12. The .... translates the logged data into correlated and simplified formats.

13. With a high incidence of severe threats and attacks on information assets, IT security has become a priority at organizations' .... levels.

14. Thinking outside of the .... security box is a good way to leverage a SIM's correlation engine and normalization capabilities.

15. Security Information Managements (SIM) is by its very nature a .... product, and thus SIM rollouts involve complex technical integration and political negotiations.

Caselet

Tool to Track BPO Transport Fleet

A LOCAL IT company has come out with a software that integrates the functioning of three key components of Geographical Information System (GIS), Global Positioning.

System (GPS) and Short Messaging Service (SMS) to provide a complete management solution for a virtual fail-safe system for the BPO companies in managing their transportation of their employees to the place of work.

Contd...

Notes

An automated solution converging the three systems Proficio Geo Technologies on Thursday announced the launch of its product that provides complete employee logistics from design to security by helping them route planning and tracking of vehicles and system-activated SMS for end-user reception to ensure security confidentiality and optimum use of the vehicles, said Mr Shashidhar Joshua, Vice-President, Business Development. Profico is the second company to announce a complete solution for the BPO company to deal with their transportation logistics and employee security issues.

The system not only helps in bringing down the time taken for designing of logistics planning considerably, it also provides a voice-cum- automatic alert facility in the cars for the both the driver and the passenger to reach the automate help desk for quick relief at times of emergencies.

Source: http://www.proficio.in/resources/press/http___www.thehindubusinessline.pdf

1.10 Summary

- A system is defined as an organized collection of people, machines, procedures, documents, data or any other entities such that they interact with each other as well as with the environment to reach a predefined goal.
- Information system is the study of information production, flows and use within organizations. Information system makes extensive use of information technology means.
- The information system of an organization may be defined as a system that serves to provide information within the organization when and where it is needed at any managerial level.
- An information system is a logically interrelated set of business processes that accomplish organizational goals.
- Telecommunication systems are considered as global. When developing infrastructures, the focus on closed, stand-alone systems has to be replaced by one focusing on the infrastructures as open and global as is the case for development of telecommunication technologies.
- The function of the World Wide Web is offered and assured by the web-hosting organizations. These organizations are the groups of people, who have rooms, full of prevailing computers, named host servers.
- Security information management is a type of software that automates the collection of event log data from security devices, such as such as firewalls, proxy servers, intrusion-detection systems and anti-virus software.
- A Security Information Management, to a great extent, adds value with its capability of finding patterns in network traffic.
- Security Information Managements (SIM) is by its very nature a heterogeneous product, and thus SIM rollouts involve complex technical integration and political negotiations.

1.11 Keywords

Information System: An information system is a logically interrelated set of business processes that accomplish organizational goals.

Notes

Security Information Management: It is a type of software that automates the collection of event log data from security devices, such as such as firewalls, proxy servers, intrusion-detection systems and anti-virus software.

System: A system is defined as an organized collection of people, machines, procedures, documents, data or any other entities such that they interact with each other as well as with the environment to reach a predefined goal.

1.12 Review Questions

1. What is information system? Also explain the importance of information system.
2. Elucidate the concept of global information system.
3. Explain the function of internet and web services in global information system.
4. Discuss the necessity of information system security for an organization.
5. Explain the working of information system security.
6. Illustrate the advantages and disadvantages of information system security.
7. Scrutinize the trait for traditional telecommunication solution.
8. Information systems overlap with both the computer science and business management disciplines. Comment.
9. Discuss the assumptions on which traditional approaches to information systems are based upon.
10. Identify the standards defined by web services.

Answers: Self Assessment

1. Information System
2. system
3. Sub-system
4. managerial
5. processing
6. target
7. telecommunication
8. web-hosting
9. internet
10. Simple Object Access Protocol (SOAP)
11. host server
12. Security information management (SIM)
13. highest
14. traditional
15. heterogeneous

1.13 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Notes

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide, 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online links

www.gissite.com

www.internetworldstats.com

Unit 2: Threats

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of threats
- Discuss new technologies open door threats
- Recognize level of threats
- Explain threats and attacks
- Understand classification of threats and assessing damages

Introduction

Any person, act, or object that poses a danger to computer security is called a threat. Any kind of policy, procedure, or action that recognizes, minimizes, or eliminates a threat or risk is called a countermeasure.

Threat, is considered as constant. Any kind of asset that is not working optimally and is mission-critical or essential to the organization, such as data that are not backed-up, is called a vulnerability, while anything imperfect is called a weakness. Any kind of counter measure that becomes fairly automated and meets the expectations of upper management is called a control, and there are many types of controls in a computer security environment, as well as threats.

Notes

The invalid access to the host can be prevented to a certain extent in case of conventional host to terminal as there is number of terminals connected is limited. The situation is entirely different in case of Internet where Internet allows access from any terminal connecting on a network. Therefore this requires proper security measures. In this unit, we will discuss some of the threats happening frequently in the network.

2.1 New Technologies Open Door Threats

For modern period companies, particularly those occupied in electronic business, it is increasingly imperative to be conscious of the online threats since more and more people are using the internet to obtain information concerning their business partners, customers, and other business associated links. Nowadays, almost all business organizations have IS that use incorporated technologies like the networks of computers, company intranets or internet access to converse and broadcast information for quick business decisions, thus opening the organization to the outside world like never before. Under the situations, threats from outside the organization must be addressed, since the damages from non-secured information system can effect in disastrous consequences for the organization.

Caution Organizations must examine and estimate the aspect that could be a threat to the reliability of the information system.

Self Assessment

Fill in the blanks:

1. Any kind of policy, procedure, or action that recognizes, minimizes, or eliminates a threat or risk is called a ....
2. Any kind of asset that is not working optimally and is mission-critical or essential to the organization, such as data that are not backed-up, is called a ....
3. Nowadays almost all business organizations have IS that use incorporated technologies like the networks of computers, company intranets or internet access to converse and broadcast information, thus opening the organization to the .... world like never before.

2.2 Level of Threats Information Level and Network Level Threats

It is significant to differentiate 'information-level threats' from 'network-level threats'. By network-based threats we signify that to be effective, latent attackers need network access to corporate computer systems or to networks accessed by corporate computer systems.

Example: For network dependent threats are hacking of computer systems and initiating of DoS attacks in addition to spreading malicious code, like viruses.

Other security concerns included when data are broadcasted over networks are confidentiality, authentication, integrity, and non-repudiation.

Information-level threats also make important utilization of network but at the key level is the content of a message and not its form. Transferring false inquiries to service accounts to eat up resources would qualify as an information-based attack. It is the content of the messages that would offer a foundation for the attack.

Other **examples** of information-based threats are setting up revenge websites and disseminating on biased information as in the case of the false acquisition. Such attacks can cause considerable damage to the goodwill of the organization against which they may be launched, and customer loyalty is too good to lose.

Propagation of information that is expected to trigger particular counter-reactions as in the case of say some threadbare job advertisement also considered as information-based threat. Fundamentally a DoS attack that is dependent on flooding accounts with large quantities of e-mail is a network-based attack as it is the size and the magnitude of the email that is significant and not the content of the e-mail.

Task Discuss information-level and network level threats with examples.

Self Assessment

Fill in the blanks:

4. In case of .... threat, latent attackers need network access to corporate computer systems or to networks accessed by corporate computer systems.

5. Transferring false inquiries to service accounts to eat up resources would qualify as an .... attack.

2.3 Threats and Attacks

Attacks can be represented by relation among threat, vulnerability, and damage. To avoid attacks from viruses and worms, a latest version of anti virus software should be used. Security threats related to computer crime or abuse include:

2.3.1 Computer Viruses

The term virus refers specifically to malware inserting malicious code into existing documents or programs. It spreads itself by various means. Still viruses are considered the most common type of network security threat. Almost 90 percent of viruses are spread through attachments on e-mails. However, a cautious user action may prevent the spread of virus because virus requires a user action to insert itself into a computer. It is therefore suggested that never open an email attachment, which is not expected, even though the sender appears to be known. However, this preventive measure will do little to stop worms from infecting the network because worms do not need a host file and they propagate themselves.

Did u know? When worms infect a computer, they often make quick copies of it and infect an entire network within a few hours.

2.3.2 Trojan Horses

This malware attack disguises itself as something innocent like a computer game or a search results page. Once installed on a computer, the Trojan horse may download and install a keylogger onto the infected computer to record every keystroke by a computer’s user, thus stealing vital details of the users. They usually hide themselves in a downloadable free software on a website.

The users should detest themselves from downloading freeware. It is often observed that organizations block free download software to prevent themselves from the attack of Trojan horses.

Notes Sometimes, a computer infected with Trojan horse are required to be reformatted, therefore, it is suggested that preventive steps need to enforced effectively than curing the infected computer system.

2.3.3 Spam

Spam constitutes 70 to 84 percent of daily emails sent throughout the world that demands an ever increasing need for IT resources to filter out this irritating and potentially malicious menace. Spam email comprises of unsolicited emails promoting products and coordinated spam attacks to consume so much bandwidth on a network so as to cause it to crash. Spam may use techniques "news service" spam, which uses legitimate news headlines to trick recipients into opening spam emails. Good email filters are used to filter the spams. And much of what slips through can be avoided by staying away not to trick with the emails. There should be check for signing of any online service or freebie.

Caution The naming system for creating email accounts should not be easily guessable because spammers are increasingly going through common name lists in order to harvest emails to spam.

2.3.4 Phishing

Emails with titles such as, "URGENT: Update Account Status" are all attempts by a spammer to "phish" the account details. The Phishing refers to spam emails to trick recipients into clicking on a link to an insecure website and provide details considering the website as genuine one. Typically, phishing attempts are carried out to steal account information for e-commerce sites such as banks, eBay or regular financial institutions' websites. A phishing email tricks the user to click a link, which will take the user to a page where the user is asked to re-enter all his or her account details including credit card number(s) and/or passwords. These websites are not actual site, even though they look like it.

Notes To protect the network, users should be vigilant and detest themselves to opening and providing vital details requested by any financial institutions. They should confirm the integrity before supplying such details. Financial institution should also educate their employees about the most common ways in which hackers try to phish the account information.

2.3.5 Password Attacks

A 'Password Attack' includes a number of techniques used by hackers to steal passwords. Some of them are listed as follows:

Brute-force: It is method in which a hacker tries to guess a password by repeatedly entering in new combinations of words and phrases compiled from a dictionary to steal the password. Developing difficult to guess usernames and passwords can prevent it.

Packet sniffers: Packet sniffers are the technique used to capture data streams over a network to obtain sensitive data like usernames, passwords, credit card numbers, etc. Thus, packet sniffers are more malicious forms of threats to the network security. Packet sniffers monitor and record details that are coming from and going to a computer over a compromised network. To get access to a network, packet sniffer use honeypots. They are simply unsecured wi-fi access points that hackers create to trap users who are using them. Making users aware about the threat of packet sniffers is best prevention policy. Falling to packet sniffers technique will lead to compromise with sensitive network data. In addition, the user should use a variety of different sign on names and passwords to access various levels of network security. This helps at the instance when login information is compromised, the damage can at least be limited in scope.

Caution A user should be aware not to access the Internet through an unsecured connection.

IP-spoofing: Like honeypots, IP spoofing involves the interception of data packets by a computer successfully pretending to be a trusted server/resource.

2.3.6 Zombie Computers and Botnets

'Zombie' computer is a computer under seize of a spammer who has infected the computer attached to a network with malware so that it acts as a tool of a spammer by silently sending out thousands of emails from the owner's email address. Thus, an innocent user's computer sends thousands of spam messages without the knowledge of the user. The spammers organize zombie computers into small groups called 'botnets'. These 'botnets' then transmits spam including phishing attempts, viruses and worms.

Task What are Zombie computers? Discuss.

Did u know? The botnets normally send spamming and phishing attacks.

2.3.7 Denial-of-Service Attack (DoS)

Denial-of-Service attack (DoS) is an attack method to deny the access to webpages of a website or network to the legitimate users.

Self Assessment

Fill in the blanks:

6. The term .... refers specifically to malware inserting malicious code into existing documents or programs.

7. It is often observed that organizations block free download software to prevent themselves from the attack of ....

Notes

8. Spam may use techniques "......................." spam, which uses legitimate news headlines to trick recipients into opening spam emails.

9. The .... refers to spam emails to trick recipients into clicking on a link to an insecure website and provide details considering the website as genuine one.

10. The spammers organize zombie computers into small groups called '.......................'.

11. .... is an attack method to deny the access to webpages of a website or network to the legitimate users.

12. .... involves the interception of data packets by a computer successfully pretending to be a trusted server/resource.

Caselet

US Drones Hit by Virus

America's remote controlled kill machines, the Predator and Reaper drones which fly hunt missions over Pakistan, Afghanistan and Yemen, have been hit by a computer virus and network specialist can't seem to get rid of it.

The virus has infected Creech Air Force base in Nevada from where the robotic machines fly globally, Los Angeles Times reported. But, media report said so far the virus hasn't hindered global missions of the drones and there's been no leak of classified information.

The infection, first reported by Wired magazine two weeks back is allegedly logging pilots' every keystroke as they carry out the missions.

The virus has remained on the drones' computer system despite multiple efforts to remove it. "We keep wiping it off, and it keeps coming back... We think it's benign," Wired magazine reported.

"Military network security specialists aren't sure whether the virus and its so-called 'keylogger' payload were introduced intentionally or by accident; it may be a common piece of malware that just happened to make its way into these sensitive networks," the magazine said.

The specialists don't know exactly how far the virus has spread. Something is going on, but it has not had any impact on the missions overseas.

Source: http://www.thehindubusinessline.com/industry-and-economy/article2520670.ece

2.4 Classification of Threats and Assessing Damages

Any kind of asset that is not working optimally and is mission-critical or essential to the organization, such as data that are not backed-up, is called a vulnerability, while anything imperfect is called a weakness. Any kind of counter measure that becomes fairly automated and meets the expectations of upper management is called a control, and there are many types of controls in a computer security environment, as well as threats, some of which are given below:

Table 2.1: Malicious Threats

Category	Threat	OSI Layer	Definition	Typical Behaviors	Vulnerabilities	Prevention	Detection	Assessing damages
Malicious Software	Virus	Application	Malicious software that attaches itself to other software. For example, a patched software application in which the patch's algorithm is designed to implement the same patch on other applications, thereby replicating.	Replicates within computer system, potentially attaching itself to every software application Behavior categories ➢ Innocuous ➢ Humorous ➢ Data altering ➢ Catastrophic	All computers Common categories ➢ Boot sector ➢ Terminate and Stay Resident (TSR) ➢ Application software ➢ Stealth (or Chameleo) ➢ Mutation engine ➢ Network ➢ Mainframe	Limit connectivity. Limit downloads Use only authorized media for loading data and software Enforce mandatory access controls. Viruses generally cannot run unless host application is running	Changes in file sizes or date/time stamps Computer is slow starting or slow running Unexpected or frequent system failures Change of system date/time Low computer memory or increased bad blocks on disks	Contain, identify and recover Antivirus scanners- look for known viruses Antivirus monitors- look for virus related application behaviors Attempt to determine source of infection and issue alert
	Worm	Application Network	Malicious software which is a stand alone application	Often designed to propagate through a network, rather than just a single computer	Multitasking computers, especially those employing open network standards	Limit connectivity, employ firewalls Worms can run even without a host application	Computer is slow starting or slow running Unexpected or frequent system failures	Contain, identify and recover Attempt to determine source of infection and issue alert
	Trojan Horse	Application	A Worm which pretends to be a useful program or a Virus which is purposely attached to a useful program prior to distribution	Same as Virus or Worm, but also sometimes used to send information back to or make information available to perpetrator	Unlike Worms, which self propagate, Trojan Horses require user cooperation Untrained users are vulnerable	User cooperation allows Trojan Horses to bypass automated controls User training is best prevention	Same as Virus and Worm	Same as Virus and Worm Alert must be issued, not only to other system admins, but to all network users
	Time Bomb	Application	A Virus or Worm designed to activate at a certain date/time	Same as Virus or Worm, but widespread throughout organization upon trigger date	Same as Virus and Worm Time Bombs are usually found before the trigger date	Run associated anti-viral software immediately as available	Correlate user problem reports to find patterns indicating possible Time Bomb	Contain, identify and recover Attempt to determine source of infection and issue alert
	Logic Bomb	Application	A Virus or Worm designed to activate under certain conditions	Same as Virus or Worm	Same as Virus and Worm	Same as Virus and Worm	Correlate user problem reports indicating possible Logic Bomb	Contain, identify and recover Determine source and issue alert
	Rabbit	Application Network	A Worm designed to replicate to the point of exhausting computer resources	Rabbit consumes all CPU cycles, disk space or network resources, etc.	Multitasking computers, especially those on a network	Limit connectivity, employ firewalls	Computer is slow starting or running Frequent system failures	Contain, identify and recover Determine source and issue alert
	Bacterium	Application	A Virus designed to attach itself to the OS in particular (rather than any application in general) and exhaust computer resources, especially CPU cycles	Operating System consumes more and more CPU cycles, resulting eventually in noticeable delay in user transactions	Older versions of operating systems are more vulnerable than newer versions since hackers have had more time to write Bacterium	Limit write privileges and opportunities to OS files System administrators should work from non-admin accounts whenever possible	Changes in OS file sizes, date/time stamps Computer is slow in running Unexpected or frequent system failures	Antivirus scanners: look for known viruses Antivirus monitors: look for virus related system behaviors.

Contd...

Notes

Spoofing	Spoofing	Network Data Link	Getting one computer on a network to pretend to have the identity of another computer, usually one with special access privileges, so as to obtain access to the other computers on the network	Spoofing computer often doesn't have access to user level commands so attempts to use automation level services, such as email or message handlers, are employed	Automation services designed for network interoperability are especially vulnerable, especially those adhering to open standards	Limit system privileges of automation services to minimum necessary Upgrade via security patches as they become available	Monitor transaction logs of automation services, scanning for unusual behaviors If automating this process do so off-line to avoid "tunneling" attacks	Disconnect automation services until patched or monitor automation access points, such as network sockets, scanning for next spoof, in attempt to trace back to perpetrator
	Masquerade	Network	Accessing a computer by pretending to have an authorized user identity	Masquerading user often employs network or administrator command functions to access even more of the system, e.g., by attempting to download password, routing tables	Placing false or modified login prompts on a computer is a common way to obtain user IDs, as are Snooping, Scanning and Scavenging	Limit user access to network or administrator command functions Implement multiple levels of administrators, with different privileges for each	Correlate user identification with shift times or increased frequency of access Correlate user command logs with administrator command functions	Change user password or use standard administrator functions to determine access point, then trace back to perpetrator
Scanning	Sequential Scanning	Transport Network	Sequentially testing passwords/authentication codes until one is successful	Multiple users attempting network or administrator command functions, indicating multiple Masquerades	Since most login prompts have a time delay built in to foil automated scanning, accessing the encoded password table and testing it off-line is a common technique	Enforce organizational password policies. Make even system administrator access to password files cumbersome	Correlate user identification with shift times Correlate user problem reports relevant to possible Masquerades	Change entire password file or use baiting tactics to trace back to perpetrator
	Dictionary Scanning	Application	Scanning through a dictionary of commonly used passwords/authentication codes until one is successful	Multiple users attempting network or administrator command functions, indicating multiple Masquerades	Use of common words and names as passwords or authentication codes (so called "Joe Accounts")	Enforce organizational password policies	Correlate user identification with shift times Correlate user problem reports relevant to possible Masquerades	Change entire password file or use baiting tactics to trace back to perpetrator
Snooping (Eavesdropping)	Digital Snooping	Network	Electronic monitoring of digital networks to uncover passwords or other data	Users or even system administrators found online at unusual or off-shift hours Changes in behavior of network transport layer	Example of how COMSEC affects COMPUSEC Links can be more vulnerable to snooping than nodes	Employ data encryption Limit physical access to network nodes and links	Correlate user identification with shift times Correlate user problem reports. Monitor network performance	Change encryption schemes or employ network monitoring tools to attempt trace back to perpetrator
	Shoulder Surfing	Physical	Direct visual observation of monitor displays to obtain access	Authorized user found online at unusual or off-shift hours, indicating a possible Masquerade Authorized user attempting administrator command functions	"Sticky" notes used to record account and password information Password entry screens that do not mask typed text "Loitering" opportunities	Limit physical access to computer areas Require frequent password changes by users	Correlate user identification with shift times or increased frequency of access Correlate user command logs with administrator command functions	Change user password or use standard administrator functions to determine access point, then trace back to perpetrator
Scavenging	Dumpster Diving	All	Accessing discarded trash to obtain passwords and	Multiple users attempting network or administrator	"Sticky" notes used to record account and password	Destroy discarded hardcopy	Correlate user identification with shift times	Change entire password file or use baiting tactics to trace back to

Contd...

			other data	command functions, indicating multiple Masquerades	information System administrator printouts of user logs		Correlate user problem reports relevant to possible Masquerades	perpetrator
	Browsing	Application Network	Usually automated scanning of large quantities of unprotected data (discarded media or online "finger" type commands) to obtain clues as to how to achieve access	Authorized user found online at unusual or off-shift hours, indicating a possible Masquerade Authorized user attempting administrator command functions	"Finger" type services provide information to any and all users. The information is usually assumed safe but can give clues to passwords (e.g., spouse's name)	Destroy discarded media When on open source networks especially, disable "finger" type services	Correlate user identification with shift times or increased frequency of access Correlate user command logs with administrator command functions	Change user password or use standard administrator functions to determine access point, then trace back to perpetrator
Spamming	Spamming	Application Network	Overloading a system with incoming message or other traffic to cause system crashes	Repeated system crashes, eventually traced to overfull buffer or swap space	Open source networks especially vulnerable	Require authentication fields in message traffic	Monitor disk partitions, network sockets, etc. for overfull conditions	Analyze message headers to attempt trace back to perpetrator
Tunneling	Tunneling	Network	Any digital attack that attempts to get "under" a security system by accessing very low level system functions (e.g., device drivers, OS kernels)	Bizarre system behaviors such as unexpected disk accesses, unexplained device failures, halted security software, etc.	Tunneling attacks often occur by creating system emergencies to cause system reloading or initialization	Design security and audit capabilities into even the lowest level software, such as device drivers, shared libraries, etc.	Changes in date/time stamps for low level system files or changes in sector/block counts for device drivers	Patch or replace compromised drivers to prevent access Monitor suspected access points to attempt trace back to perpetrator

Table 2.2: Unintentional Threats

Category	Threat	OSI Layer	Definition	Typical Behaviors	Vulnerabilities	Prevention	Detection	Assessing damages
Malfunction	Equipment Malfunction	All	Hardware operates in abnormal, unintended mode	Immediate loss of data due to abnormal shutdown Continuing loss of capability until equipment is repaired	Vital peripheral equipment is often more vulnerable than the computers themselves	Replication of entire system including all data and recent transactions	Hardware diagnostic systems	On-site replication of hardware components for quick recovery
	Software Malfunction	Application	Software behavior is in conflict with intended behavior	Immediate loss of data due to abnormal end Repeated system failure when re-fed "faulty" data	Software developed using ad hoc rather than defined formal processes	Comprehensive testing procedures and software designed for graceful degradation	Software diagnostic tools	Backup software and robust operating systems facilitate quick recovery
Human Error	Trap Door (Back door)	Application	System access for developers inadvertently left available after software delivery	Unauthorized system access enables viewing, alteration or destruction of data or software	Software developed outside defined organizational policies and formal methods	Enforce defined development policies Limit network and physical access	Audit trails of system usage, especially user identification logs	Close Trap Door or monitor ongoing access to trace back to perpetrator
	User/Operator Error	All	Inadvertent alteration, manipulation or destruction of programs, data files or hardware	Incorrect data entered into system or incorrect behavior of system	Poor user documentation or training	Enforcement of training policies and separation of programmer/operator duties	Audit trails of system transactions	Backup copies of software and data On-site replication of hardware

Notes

Table 2.3: Physical Threats

Category	Threat	OSI Layer	Definition	Typical Behaviors	Vulnerabilities	Prevention	Detection	Assessing damages
Physical Environment	Fire Damage	N/A	Physical destruction of equipment due to fire or smoke damage	Physical destruction of systems and supporting equipment	Systems located near potential fire hazards, e.g., fuel storage tanks	Off-site system replication, while costly, provides backup capability	On-site smoke alarms	Halon gas or FM200 fire extinguishers mitigate electrical and water damage
	Water Damage	N/A	Physical destruction of equipment due to water (including sprinkler) damage	Physical destruction of systems and supporting equipment	Systems located below ground or near sprinkler systems	Off-site system replication	Water detection devices	Computer rooms equipped with emergency drainage capabilities
	Power Loss	N/A	Computers or vital supporting equipment fail due to lack of power	Immediate loss of data due to abnormal shutdown, even after power returns Continuing loss of capability until power returns	Sites fed by above ground power lines are particularly vulnerable Power loss to computer room air conditioners can also be an issue	Dual or separate feeder lines for computers and supporting equipment	Power level alert monitors	Uninterruptible Power Supplies (UPS) Full scale standby power facilities where economically feasible
	Civil Disorder Vandalism	N/A	Physical destruction during operations other than war	Physical destruction of systems and supporting equipment	Sites located in some overseas environments, especially urban environments	Low profile facilities (no overt disclosure of high value nature of site)	Physical intrusion detection devices	Physical access restrictions and riot contingency policies
	Battle Damage	N/A	Physical destruction during military action	Physical destruction of systems and supporting equipment	Site located in theater	Off-site system replication OPSEC and low profile to prevent hostile targeting	Network monitoring systems	Hardened sites

Self Assessment

Fill in the blanks:

13. .... threat is a virus or worm designed to activate at a certain date/time.

14. .... threat leads to physical destruction of equipment due to fire or smoke damage.

15. In .... threat, hardware operates in abnormal, unintended mode.

Caselet

Ethical Hacking for CYBER Security

Investment in Business Process Outsourcing (BPO) and Information Technology services are estimated to grow by 16.6 per cent during 2011, to reach ₹ 43,600 crore in 2012. Expenditure on software is projected to scale by 19.5 per cent during the period, to reach ₹ 18,800 crore. The rate of cyber crimes is also bound to grow exponentially in the coming years.

Contd...

Notes

As most sophisticated cyber criminals prefer targeting banks and government organisations, there is an urgent need to revamp the security system for Internet activities and to put in place effective internal controls. As the hackers' prime objective is to find secure IDs for accessing networks for cyber burglary, authentication procedures should be made secure and foolproof from hacking.

The rapidly-increasing use of mobile-banking technologies augments risks and increases vulnerability. When a large number of customers prefer using wireless technology, iPhones, iPads, and Android-enabled smart phones for financial services, the cyber criminal may use the opportunity to phish with an application, and gain access to their secure credentials.

Ethical hackers are in greater demand to counter cyber crimes which are growing at an alarming speed.

Experts specialised in different aspects of cyber policing, ranging from the relatively inexperienced greenhorns to seasoned cyber security greybeards need to visualise the big picture, anticipate potential attacks to the organisation and mitigate risks from cyber hacking.

An ethical hacker is not a cyber criminal though he knows well the art and science of hacking. He exercises his hacking expertise prudently for ethical concerns and deploys the cyber tools effectively to counter hacking and to identify the loopholes in order to safeguard the system from lethal cyber criminals.

Cyber Security

Ethical hacking must be encouraged for detection and prevention of automated application attacks, because hackers are becoming adept at automating attacks by intensifying computerised attacks at smaller, vulnerable and largely homogenous targets.

For this, IT security professionals should monitor and analyse attack data, extract relevant information, share information for enlarging the knowledge base for identifying attacks and select appropriate mitigation tools.

They must ensure that controls are in place at all times to deter automated attacks. Securing data confidentiality, and availability in the cyber realm is becoming an increasingly challenging objective for the government and private sectors. Organisations must engage competent, well-trained, skilled, information security professionals to continuously monitor and manage cyber threats and secure sensitive organisational information assets.

Source: http://www.thehindubusinessline.com/features/mentor/article2356616.ece

2.5 Summary

- Any person, act, or object that poses a danger to computer security is called a threat.
- Any kind of asset that is not working optimally and is mission-critical or essential to the organization, such as data that are not backed-up, is called a vulnerability, while anything imperfect is called a weakness.
- Threats from outside the organization must be addressed, since the damages from non-secured information system can effect in disastrous consequences for the organization.
- By network-based threats we signify that to be effective, latent attackers need network access to corporate computer systems or to networks accessed by corporate computer systems.

Notes

- Information-level threats also make important utilization of network but at the key level is the content of a message and not its form.
- Attacks can be represented by relation among threat, vulnerability, and damage. To avoid attacks from viruses and worms, a latest version of anti virus software should be used.
- The term virus refers specifically to malware inserting malicious code into existing documents or programs. It spreads itself by various means.
- Any kind of counter measure that becomes fairly automated and meets the expectations of upper management is called a control, and there are many types of controls in a computer security environment, as well as threats, some of which are Malicious Threats, Unintentional Threats, and physical threats.

2.6 Keywords

Authentication: It is a process used to ascertain the identity of a person or the integrity of specific information. For a message, authentication involves ascertaining its source and that it has not been modified or replaced in transit.

Botnets: The spammers organize zombie computers into small groups called 'botnets'. These 'botnets' then transmits spam including phishing attempts, viruses and worms. The botnets normally send spamming and phishing attacks.

Brute-force: It is method in which a hacker tries to guess a password by repeatedly entering in new combinations of words and phrases compiled from a dictionary to steal the password. Developing difficult to guess usernames and passwords can prevent it.

Countermeasure: Any kind of policy, procedure, or action that recognizes, minimizes, or eliminates a threat or risk is called a countermeasure.

Denial-of-Service Attack (DoS): Denial-of-Service attack (DoS) is an attack method to deny the access to webpages of a website or network to the legitimate users.

Dynamic Packet Filter: A dynamic packet filter firewall is capable of monitoring the state of active connections and decides which network packets should be allowed through the firewall.

Firewalls: A firewall is a combination of software and hardware components to control the traffic that flows between a secure network and an insecure network using rules defined by the system administrator.

IP-spoofing: Like honeypots, IP spoofing involves the interception of data packets by a computer successfully pretending to be a trusted server/resource.

Packet Sniffers: Packet sniffers are the technique used to capture data streams over a network to obtain sensitive data like usernames, passwords, credit card numbers, etc.

Password Attacks: A 'Password Attack' includes a number of techniques used by hackers to steal passwords.

Phishing: Emails with titles such as, "URGENT: Update Account Status" are all attempts by a spammer to "phish" the account details.

Spam: Spam constitutes 70 to 84 percent of daily emails sent throughout the world that demands an ever-increasing need for IT resources to filter out this irritating and potentially malicious menace.

Static Packet Filter: The packet filtering mechanism examines only the protocol and the address detail each TCP/IP packet and ignores its data contents and context.

Threat: Any person, act, or object that poses a danger to computer security is called a threat.

Trojan Horses: This malware attack disguises itself as something innocent like a computer game or a search results page.

Viruses: The term virus refers specifically to malware inserting malicious code into existing documents or programs.

Vulnerability: Any kind of asset that is not working optimally and is mission-critical or essential to the organization, such as data that are not backed-up, is called a vulnerability.

Zombie Computers: 'Zombie' computer is a computer under seize of a spammer who has infected the computer attached to a network with malware so that it acts as a tool of a spammer by silently sending out thousands of emails from the owner's email address.

2.7 Review Questions

1. How do we keep our own and other people's computers safe from hackers? Explain with the help of a hypothetical situation.
2. How do we keep viruses from attacking all our computers if we get connected to the Internet?
3. Make distinction between information level threat and network level threat.
4. Explain the techniques used by hackers to steal passwords.
5. What does the term packet filtering firewall mean? Where would such a device be used and for what purpose?
6. Illustrate briefly two kinds of security attacks, which can be directed against an Internet-connected computer system.
7. Explain the security threats of information systems.
8. Describe the physical threats of information systems.
9. Discuss various Malicious Threats with their accessing damages respectively.
10. Threats from outside the organization must be addressed, since the damages from non-secured information system can effect in disastrous consequences for the organization. Comment.

Answers: Self Assessment

1. countermeasure
2. vulnerability
3. outside
4. Network level
5. Information-based
6. virus
7. trojan horses
8. News service
9. Phishing
10. Botnets
11. Denial-of-Service attack (DoS)
12. IP spoofing
13. Time Bomb
14. Fire damage
15. Hardware malfunction

Notes

2.8 Further Readings

Books

Andrew S. Tannenbaum, *Computer Networks*, published by Prentice Hall.

Behrouz A. Forouzan, Sophia Chung, *Data Communications and Networking*, Fegan published.

Burton, Bill, *Remote Access for Cisco Networks*, published by McGraw-Hill Osborne Media McGraw-Hill Osborne Media.

Gary Halleen/Greg Kellogg, *Security Monitoring with Cisco Security MARS*, Cisco Press, Jul. 6, 2007.

Dale Tesch/Greg Abelar, Cisco Press, *Security Threat Mitigation and Response: Understanding CS-MARS*, Sep. 26, 2006.

Web Tutorials on HTML and Front Page.

Online links

www.kaspersky.com

www.engr.colostate.edu/.

Notes

Unit 3: Building Blocks of Information Security

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of information security
- Discuss principles of information security
- Recognize various terms related to information security
- Explain three pillars of information security
- Understand information classification

Introduction

Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for instance, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks.

Precision in estimating information security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system.

This unit will help you to understand some of the security pillars and principles. In many ways, information security is almost a statistical game. You can reduce but not eliminate the chance that you may be penetrated by an intruder or virus.

3.1 Information Security

Information security can be very complex and may be very confusing to many people. It can even be a controversial subject. Network administrators like to believe that their network is secure and those who break into networks may like to believe that they can break into any network.

Information security is the prevention and protection of computer assets from unauthorized access, use, alteration, degradation, destruction, and other threats. There are two main sub-types: physical and logical.

Physical information security involves tangible protection devices.

Example: Locks, cables, fences, safes or vaults.

Logical information security involves non-physical protection.

Example: Protection provided by authentication or encryption schemes.

Make a point of noting that the physical versus non-physical (logical) distinction runs through a number of areas in computer science, despite minor differences in definition.

Task What are the two sub-types of information technology? Illustrate.

3.1.1 Need for Information Security

Information security is as much a business process as it is a technical one. No longer can security be viewed as a backroom operation, separate from the essential activity of an organization.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction. Governments, military, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status.

Information assets are critical to any business and vital to the survival of any organization in today's globalize digital economy. Information leak is therefore intolerable. Confidential information about a businesses customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business.

An information leak often indicates that security measures were not properly implemented. Improper information security hurts both customer and merchant. A security breach isn't good for anyone.

Information security is the only thing that keeps electronic commerce running. Security breach can break the confidence of the customer. It may take long time to rebuild that trust. Information security is required for the goodwill of the business. Therefore companies are thinking about prioritize information security on the basis of a possible breach. There just always seems like there's too much to do in the here-and-now to worry about possibilities.

For that reason the major credit card companies came together and developed the PCI DSS (or Payment Card Industry Data Security Standard). Any company that transmits, processes, or stores sensitive credit card information is required to be PCI compliant.

Information security is absolutely essential as we move deeper and deeper into the digital age, and a merchant has a couple of choices.

Information security is required because most organizations can be damaged by hostile software or intruders. There may be several forms of damage which are obviously interrelated. These include:

1. Damage or destruction of computer systems.
2. Damage or destruction of internal data.
3. Loss of sensitive information to hostile parties.
4. Use of sensitive information to steal items of monetary value.
5. Use of sensitive information against the organization's customers which may result in legal action by customers against the organization and loss of customers.
6. Damage to the reputation of an organization.
7. Monetary damage due to loss of sensitive information, destruction of data, hostile use of sensitive data, or damage to the organization's reputation.

⚠

Caution The methods used to accomplish these unscrupulous objectives are many and varied depending on the circumstances.

Did u know? Security is a key to the success of all operations.

Self Assessment

Fill in the blanks:

1. .... is the prevention and protection of computer assets from unauthorized access, use, alteration, degradation, destruction, and other threats.
2. .... information security involves tangible protection devices, such as locks, cables, fences, safes or vaults.
3. .... information security involves non-physical protection, such as that provided by authentication or encryption schemes.

Notes

4. .... is a key to the success of all operations.

5. An information .... often indicates that security measures were not properly implemented.

3.2 Basic Principles of Information Security

The major technical areas of information security are usually represented by the initials CIA: confidentiality, integrity, and authentication or availability. Confidentiality means that information cannot be access by unauthorized parties.

Maintaining access control means not only that users can access only those resources and services to which they are entitled, but also that they are not denied resources that they legitimately can expect to access. Non-repudiation implies that a person who sends a message cannot deny that he sent it and, conversely, that a person who has received a message cannot deny that he received it. In addition to these technical aspects, the conceptual reach of information security is broad and multifaceted.

While confidentiality, integrity, and authenticity are the most important concerns of an information security manager, privacy is perhaps the most important aspect of information security for everyday Internet users. Although users may feel that they have nothing to hide when they are registering with an Internet site or service, privacy on the Internet is about protecting one's personal information, even if the information does not seem sensitive.

3.2.1 Secrecy

Information security, in many ways, is about secrecy, not in the sense of being mysterious or clandestine, but because of the fact that you are always dealing with authorization and Authenticity.

Information security touches draws from disciplines as ethics and risk analysis.

Example: It is concerned with topics such as computer crime; the prevention, detection, and remediation of attacks; and identity and anonymity in cyberspace.

3.2.2 Authenticity

Authentication means that users are who they claim to be. Availability means that resources are accessible by authorized parties; "denial of service" attacks, which are sometimes the topic of national news, are attacks against availability. Other important concerns of information security professionals are access control and Non-repudiation.

Authorization refers to the power you have over distinguishing authorized users from unauthorized users, and levels of access in-between. Authenticity refers to the constant checks you have to run on the system to make sure sensitive areas are protected and working properly.

3.2.3 Confidentiality

Confidentiality is also known as secrecy or privacy; breaches of confidentiality range from the embarrassing to the disastrous. Confidentiality is discussed in detail in next section.

3.2.4 Integrity

Integrity means that information is protected against unauthorized changes that are not detectable to authorized users; many incidents of hacking compromise the integrity of databases and other resources. Integrity is discussed in detail in next section.

3.2.5 Accuracy

The accuracy and completeness of information systems and the data maintained within the systems should be a management concern. Information which has been inappropriately modified or destroyed (by outsiders or employees) can adversely impact the organization. Each organization must establish controls to ensure that data entered into and stored in its automated files and data bases are complete and accurate, as well as ensure the accuracy of disseminated information.

> *Notes* Depending upon the nature of the information being protected and the threats to which it is subjected, additional measures may be required to ensure the integrity and security of automated files and databases can range from password protection to encryption.

Self Assessment

Fill in the blanks:

6. Maintaining .... means not only that users can access only those resources and services to which they are entitled, but also that they are not denied resources that they legitimately can expect to access.

7. .... refers to the power you have over distinguishing authorized users from unauthorized users, and levels of access in-between.

8. .... on the Internet is about protecting one’s personal information, even if the information does not seem sensitive.

9. The .... and completeness of information systems and the data maintained within the systems should be a management concern.

3.3 Terms

Alert: Warning that a particular attack has been directed at the information system of an organization.

Attack: Deliberate act of trying to bypass one or more computer or network.

Authenticate: To authenticate the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized alteration in an information system, or to institute the authority of a transmission.

Authentication: Security measure intended to begin the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to obtain particular categories of information.

Back Door: Hidden software or hardware mechanism used to avoid security controls. It is identical to trap door.

Card Skimmers: An unlawful electronic device that can capture all of the personal information from a credit card or debit card.

Countermeasures: Action, device, procedure, method or other measure that decreases the vulnerability of an information system.

Data Driven Attack: A form of attack that is encoded in apparently inoffensive data, which is executed by a user or a process to execute an attack. A data driven attack is a concern for firewalls, as it may get through the firewall in data form and begin an attack against a system at the back of the firewall.

Denial of Service: Effect of any action or series of actions that averts any part of an information system from functioning.

Dictionary Attack: An attack that accesses a brute-force technique of successively attempting all the words in some large, comprehensive list.

DNS Spoofing: Assuming the DNS name of another system by either humiliating the name service cache of a victim system, or by compromising a domain name server for a valid domain.

Firewall: A firewall is a hardware or software solution to implement security policies.

Flooding: Type of incident including insertion of a large volume of data effecting in denial of service.

Hacker: Unauthorized user who tries to or gains access to an information system and the data it supports.

Intrusion: Unauthorized act of bypassing the security techniques of a system.

Malicious Code: Software efficient of performing an unauthorized process on an information system.

Mobile Code: Software modules received from remote systems, transferred across a network, and then downloaded and implemented on a local system without explicit installation or execution by the recipient.

Packet: A block of data sent over the network broadcasting the identities of the sending and receiving stations, error-control information, and message.

Packet Filtering: A feature included into routers to restrict the flow of information based on predetermined communications like source, destination, or type of service being provided by the network.

Packet Sniffer: A machine or program that observes the data traveling within computers on a network.

Phishing: A type of scam with the intention of obtaining personal information like online banking user identification numbers, debit and credit card account numbers, and passwords.

Probe: An effort to collect information about an information system for the apparent reason of circumventing its security controls.

Proxy: Software agent that carries out a function or operation on behalf of another application or system while hiding the details involved.

Replicator: Any program that acts to generate copies of itself. Examples include; a program, a worm, or virus.

Retro-virus: A retro-virus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state.

Rootkit: A hacker security tool that obtains passwords and message traffic to and from a computer.

Smurfing: Software that mounts a denial of service attack by destroying IP broadcast addressing and ICMP ping packets to cause flooding.

Spam: Haphazardly sending unsolicited, unwanted, irrelevant or inappropriate messages, particularly commercial advertising in mass quantities, is measured spam. Another term used to portray spam is "electronic junk mail."

Spoofing: Impersonating another person or computer, generally by providing a false email name, URL or IP address.

Spyware: Software that gathers information about a person or organization without their knowledge or informed consent and reports such data back to a third party.

Threat: Any situation or event with the potential to unfavorably impact an information system via unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Virus: Self-replicating, malicious code that links itself to an application program or other executable system component and leaves no noticeable signs of its presence.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be destroyed.

Worm: Autonomous program that replicates from machine to machine across network connections generally clogging networks and information systems as it spreads.

Self Assessment

Fill in the blanks:

10. .... is a hacker security tool that obtains passwords and message traffic to and from a computer.

11. Haphazardly sending unsolicited, unwanted, irrelevant or inappropriate messages, particularly commercial advertising in mass quantities, is measured ....

3.4 Three Pillars of Information Security

There are three pillars of information security; that is confidentiality, integrity and availability that are important to guaranteeing the effective safety of information. Each of these pillars will be discussed as below.

3.4.1 Confidentiality

The first pillar, confidentiality, is related with guaranteeing that information of a particular classification is not disseminated to persons outside the group for which it is classified. It makes sure that only those individuals who have access permissions will be able to inspect certain information. The group for which the information is classified could be a particular organization, department or a specific individual.

Confidentiality means that sensitive information must be prohibited from being revealed to illegal parties. There are usually two methods, or an amalgamation of these, in the course of which confidentiality can be provided. One method is to limit access to the information that must be kept undisclosed. The other method is to encrypt the secret information. Confidentiality is at times also known as secrecy.

3.4.2 Integrity

The second pillar is known as integrity of the information. This is related with the eminence and dependability of information; like management can be guaranteed that the information on which decisions are relied has not been tailored dishonestly or else when the data is transferred, captured and accumulated. One method of offering integrity is to link a particular indicator or message digest at the end of the message that is going to be sent. If this digest remains undamaged during transit then the integrity has been conserved. Integrity signifies that an asset or information can only be tailored by authorized parties or only in authorized manners.

3.4.3 Availability

The third pillar is the availability of the information. When systems or data are unavailable, opportunities may be vanished, deadlines missed or commitments evaded. Work progress could be weakened if the information is not available when it is needed. Even if the information is precisely what is required to fulfill business requirements, if it is not available when required to accomplish a task, it turns out to be useless.

Confidentiality, integrity and availability are broadly acknowledged as the three vital pillars of information security. Without sufficient safety in place to avert illegal activities, an organization's most significant asset, namely its information, is at risk. Thus, it is significant that this asset be secluded and secured by means of these three pillars. There, are additional support structures of information security that could be used in combination with the three main pillars to balance them, namely; identification and authentication, access control/authentication and non-denial.

> *Notes* Information security is tremendously significant to the well-being of any organization and, therefore, it is necessary to guarantee the pillars of confidentiality, integrity and availability. There are, however, many troubles or false opinions encountered when making sure that information security is a part of an organization.

Self Assessment

Fill in the blanks:

12. .... means that sensitive information must be prohibited from being revealed to illegal parties.

13. .... signifies that an asset or information can only be tailored by authorized parties or only in authorized manners.

3.5 Information Classification

We can categorize the information on the basis of the purpose for which the information is utilized. Broadly, we can categories information as following:

1. ***Strategic Information:*** Strategic information is the information needed for long range and strategic decisions. Strategic decisions are taken by the top management people. Strategic information is required for planning and policy formulation of the business. Strategic information includes information concerned with new technologies, market availability, raw-material costs, new product developments, manpower planning and competitors, etc.

2. ***Tactical Information:*** Tactical information is needed to take medium range decisions and usually the time period it covers is around one year. Tactical information includes sales analyses and forecasts, financial projections, production resource requirements and the annual financial statements. Usually, the data for this type of information is generally based on current activities and transactions. This requires immediate generation and processing of data. Tactical decisions require information from several sources, both internal and external, before making decisions.

3. ***Operational Information:*** Operational information is required for routine operations of a business organization. This information applies to very short-term period, which may vary from an hour to a few days. It includes information about current stocks-in-hand, outstanding purchase orders, inventory reorder level, and customers' outstanding orders etc. Almost all the operational information is generated internally.

Caution Depending upon the different types of decisions made by the management, information is supplied to them according to the needs of their decision.

Task Make distinction between strategic, tactical, and operational information.

Did u know? Operational information is derived from current activity data.

Self Assessment

Fill in the blanks:

14. .... information is the information needed for long range and strategic decisions.

15. .... information applies to very short-term period, which may vary from an hour to a few days.

3.6 Summary

- Information security is the prevention and protection of computer assets from unauthorized access, use, alteration, degradation, destruction, and other threats.
- No longer can security be viewed as a backroom operation, separate from the essential activity of an organization.
- Information assets are critical to any business and vital to the survival of any organization in today's globalize digital economy. Information leak is therefore intolerable.
- Information security is required because most organizations can be damaged by hostile software or intruders.
- The major technical areas of information security are usually represented by the initials CIA: confidentiality, integrity, and authentication or availability.
- Maintaining access control means not only that users can access only those resources and services to which they are entitled, but also that they are not denied resources that they legitimately can expect to access.

- Confidentiality is related with guaranteeing that information of a particular classification is not disseminated to persons outside the group for which it is classified.
- Integrity is related with the eminence and dependability of information; like management can be guaranteed that the information on which decisions are relied has not been tailored dishonestly or else when the data is transferred, captured and accumulated.
- The third pillar is the availability of the information. When systems or data are unavailable, opportunities may be vanished, deadlines missed or commitments evaded.
- We can categorize the information on the basis of the purpose for which the information is utilized. Depending upon the different types of decisions made by the management, information is supplied to them according to the needs of their decision.

3.7 Keywords

Accuracy: The accuracy and completeness of information systems and the data maintained within the systems should be a management concern.

Authenticity: It refers to the constant checks you have to run on the system to make sure sensitive areas are protected and working properly.

Authorization: It refers to the power you have over distinguishing authorized users from unauthorized users and levels of access in-between.

Confidentiality: It means that information cannot be access by unauthorized parties.

Information Security: It is the prevention and protection of computer assets from unauthorized access, use, alteration, degradation, destruction and other threats.

Integrity: It means that information is protected against unauthorized changes that are not detectable to authorized users; many incidents of hacking compromise the integrity of databases and other resources.

Logical Computer Security: It involves non-physical protection, such as that provided by authentication or encryption schemes.

Physical Computer Security: It involves tangible protection devices, such as locks, cables, fences, safes or vaults.

3.8 Review Questions

1. What do you mean by information security?
2. Enlighten the various principles of information security.
3. What do you mean by "loss of integrity" in database security issue?
4. How accuracy and completeness of information systems can adversely impact the organization?
5. Make distinction between physical computer security and logical computer security.
6. Explain the concept of confidentiality. Also illustrate why confidentiality is required in information system.
7. How to ensure the safety, integrity and privacy of corporate information?
8. How data security breaches in an organization?
9. How database of an organization can be damaged?

10. Categorize the information on basis of the purpose for which the information is utilized.

11. Without sufficient safety in place to avert illegal activities, an organization's most significant asset, namely its information, is at risk. Comment.

Answers: Self Assessment

1. Information security
2. Physical
3. Logical
4. Security
5. leak
6. access control
7. Authorization
8. Privacy
9. accuracy
10. Rootkit
11. spam
12. Confidentiality
13. Integrity
14. Strategic
15. Operational

3.9 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, by IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online links

www.key.com

http://adminguide.stanford.edu/63.pdf

Notes

Unit 4: Risk Analysis

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of risk management
- Explain the concept of risk assessment
- Discus various approaches and considerations to risk analysis

Introduction

Most of us hate the idea of risk. While we collectively spend a great deal of time and money to reduce it, we can never hope to eliminate it. The reason is that some amount of uncertainty is "built in" to all aspects of the world around us. In fact, at the smallest level of physical reality, quantum physicists must deal only in probabilities, as they cannot predict with certainty which events will occur, or where or when they might occur. The very word "risk" tends to make us nervous, as it portends the probability that something bad may happen to us. The word "happen" is also a clue to our deep concerns about risk, because it indicates events that are out of our control.

In this unit we will discuss the concept of risk analysis and risk management.

4.1 Risk

Risk is virtually anything that threatens or limits the ability of an organization to achieve its mission. Risk Management should be a set of continuous and developing processes that are applied throughout an organization's strategy and should methodically address all the risks surrounding past, present and future activities.

The information security risks confronting an organization will vary with the nature of the processing performed by the organization and the sensitivity of the information processed. An understanding of risk and the application of risk assessment methodology is essential to being able to efficiently and effectively create a secure computing environment.

Unfortunately, this is still a challenging area for information professionals due to the rate of change in technology, the relatively recent advent and explosive growth of the Internet, and perhaps the prevalence of the attitude (or reality) that assessing risk and identifying return on investment is simply too hard to do.

This has kept information systems and information systems security in the undesirable position of being unable to systematically identify and monetarily quantify security risks. This in turn has led to inconsistent and inappropriate applications of security solutions as well as either excessive or insufficient funding for such activities.

Did u know? Risk Management is primarily concerned with reducing the potential of any internal or external events to detrimentally affect a business.

Self Assessment

Fill in the blanks:

1. .... is virtually anything that threatens or limits the ability of an organization to achieve its mission.

2. An understanding of risk and the application of risk assessment methodology is essential to being able to efficiently and effectively create a .... computing environment.

4.2 Risk Management

Risk management is a process to identify and then manage threats which could severely impact or bring down the organization. As per the CISA Review Manual 2006 the definition of risk management – it is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization. Successful risk management needs the involvement of all levels of employers of an organization.

There are two main areas of focus for risk management, each with its own set of objectives.

4.2.1 Internal Factors

1. To reassure management that the business is aware of, and in control of, current and future business risks.

2. To safeguard business assets and reputation.

3. To help improve the business's operating performance and shareholder value.
4. To improve efficiency by reducing risk exposure inherent in the business processes.
5. To support the achievement of strategic goals.

4.2.2 External Factors

1. To ensure compliance with regulatory requirements.
2. To deliver competitive advantage.
3. To reassure stakeholders and interest groups that the business is actively managing risk.

4.2.3 Steps involve in Risk Management

Risk management involves the following steps:

1. Reviewing operations of the organization.
2. Identifying potential threats to the organization.
3. The likelihood of their occurrence.
4. Adopting appropriate actions to address the most likely threats.

Risk management is not a matter of getting the right insurance. Previously, people were not serious about risk management. Nowadays the impression of risk management has changed dramatically. With the recent increase in rules and regulations, employee-related lawsuits and reliance on key resources, risk management is becoming a management practice that is every bit as important as financial or facilities management.

Information security, availability and confidentiality only address some of the components of an organization's information security. Therefore, we are moving beyond the concept of just information security.

Task Discuss the process of identifying risk.

Caution To successfully manage their risk in the future, organizations need to develop an enterprise-wide risk management framework.

Self Assessment

Fill in the blanks:

3. .... is a process to identify and then manage threats which could severely impact or bring down the organization.
4. Successful risk management needs the involvement of all levels of .... of an organization.
5. To successfully manage their risk in the future, organizations need to develop an .... risk management framework.

6. The two main areas of focus for risk management, each with its own set of objectives are internal and ....

4.3 Risk Analysis

Organizations should regularly undertake comprehensive, focused assessment of potential risks to the organization. The way of risk assessment process may vary from one organization to other but the outline of the assessment work flow is as below:

1. ***Establish the Risk Assessment Team:*** The risk assessment team will be responsible for the collection, analysis, and reporting of the assessment results to management. It is important that all aspects of the activity work flow be represented on the team, including human resources, administrative processes, automated systems, and physical security.

2. ***Set the Scope of the Project:*** The assessment team should identify at the outset the objective of the assessment project, department, or functional area to be assessed, the responsibilities of the members of the team, the personnel to be interviewed, the standards to be used, documentation to be reviewed and operations to be observed.

3. ***Identify Assets covered by the Assessment:*** Assets may include, but are not limited to, personnel, hardware, software, data (including classification of sensitivity and criticality), facilities and current controls that safeguard those assets. It is the key to identify all assets associated with the assessment project determined in the scope.

4. ***Categorize Potential Losses:*** Identify the losses that could result from any type of damage to an asset. Losses may result from physical damage, denial of service, modification, unauthorized access or disclosure. Losses may be intangible, such as the loss of the organizations' credibility.

5. ***Identify Threats and Vulnerabilities:*** A threat is an event, process, activity, or action that exploits a vulnerability to attack an asset. Include natural threats, accidental threats, human accidental threats, and human malicious threats. These could include power failure, biological contamination or hazardous chemical spills, acts of nature, or hardware/software failure, data destruction or loss of integrity, sabotage, or theft or vandalism. Vulnerability is a weakness which a threat will exploit to attack the assets. Vulnerabilities can be identified by addressing the following in your data collection process: physical security, environment, system security, communications security, personnel security, plans, policies, procedures, management, support, etc.

6. ***Identify existing Controls:*** Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.

7. ***Analyze the Data:*** In this phase, all the collected information will be used to determine the actual risks to the assets under consideration. A technique to analyze data includes preparing a list of assets and showing corresponding threats, type of loss and vulnerability. Analysis of this data should include an assessment of the possible frequency of the potential loss.

8. ***Determine Cost-effective Safeguards:*** include in this assessment the implementation cost of the safeguard, the annual cost to operate the safeguard, and the life cycle of the safeguard.

9. ***Report is to be Submitted:*** The type of report to make depends on the audience to whom it is submitted. Typically, a simple report that is easy to read, and supported by detailed analysis, is more easily understood by individuals who may not be familiar with your

organization. The report should include findings a list of assets, threats, and vulnerabilities; a risk determination, recommended safeguards, and a cost benefit analysis.

Notes This focused assessment should occur at least twice a year by a team of staff members representing all the major functions of the organization. The assessment should be carefully planned, documented and methodically carried out.

Task How to identify existing controls?

4.3.1 Basic Principles of Risk Assessment

IT security failures may cause loss of information confidentiality, integrity, or availability. Information assets or electronic resources management units should assess to determine what information resources exist that require protection. They should conduct formal risk assessments to understand and document potential risks. Full support of senior management is required for successful risk assessments.

The basic principles of risk assessment are given below:

1. The assessment should have clear objective(s) reflecting the informational needs of decision makers and determined in an iterative dialogue between the assessor(s) and the decision maker(s).

   Risk assessment is always linked to decision-making. In particular, it can help prioritize actions, provide objective and defensible means to distinguish between alternative courses of action, and enable a choice to be made. Ultimately, the risk assessment process can help in deciding whether risk can be tolerated or whether further controls are justified. It is important to establish clearly why a particular risk assessment is initiated: what decision depends on the outcome?

   The risk assessor and decision maker (also referred to as risk manager) may be the same person or be in the same organization, but other situations are also common.

   Some applications of risk assessment are proactive in nature, i.e. they are aimed at future or potential risks; in other cases, a reactive assessment is aimed at concrete products that have been involved in incident, found to fail a standard, or otherwise suspected of being unsafe.

2. The scope and content should be based on the objectives of the assessment and best professional judgment, considering the benefits and costs of acquiring additional information before undertaking the assessment.

   The scope of the assessment includes at least:

   (a) The product (type) that is the subject of the assessment;

   (b) The hazard(s) of concern;

   (c) The affected entities (population(s), subpopulation(s), individuals, or other) that are the subject of the assessment;

   (d) The exposure/event scenarios relevant to the objectives of the assessment;

Example: It is necessary to clarify whether the risk manager needs estimates of population or individual risk, or both.

3. The type of risk assessment shall be responsive to the nature of the potential hazard, the available data, and the decision needs.

Example: If the objective is to decide whether a particular incident requires a product recall, the risk assessment will focus on that incident and not on the complete risk profile of the product.

On the other hand, the risk profile should be determined as completely as possible in the design stage.

Different risk assessment methods or tools are available for these different types of risk assessment. Selecting the type of risk assessment also means selecting the right methods and tools.

4. The level of effort put into the risk assessment shall be commensurate with the importance of the decisions to be made.

This principle is linked with principles 2 and 3 and emphasizes that risk assessments may vary considerably in scale. The time frame available for decision making may also influence the scale of the risk assessment.

5. The assessment shall be objective, systematic, structured and – as far as practically possible – evidence based.

This means that the processes used for risk assessment should be methodical and use recognized methods to ensure that the results are repeatable and reliable.

An evidence based assessment also implies that efforts are necessary to ensure the availability of suitable data. Data are necessary at the start to picking up any signals that may call for a risk assessment, and later in the risk assessment itself. Therefore, an organization that wants to perform risk assessments needs to prepare itself by establishing a system for collecting relevant data of good quality or to know where such information already exists.

6. The risk shall be characterized qualitatively and, whenever possible, quantitatively.

7. Risk Assessment should explicitly describe its own uncertainty and the causes of the uncertainty.

This may include: providing a range of plausible risk estimates with a quantitative characterization of risk; for critical assumptions, whenever possible, include a quantitative evaluation of reasonable alternative assumptions and their implications for the key findings of the assessment; documenting and disclosing the nature and quantitative implications of model uncertainty, and the relative plausibility of different models based on scientific judgment; where feasible, performing a sensitivity analysis; and providing a quantitative distribution of the uncertainty.

The primary purpose of risk assessment should always be to deal with those aspects of decision making that are uncertain. If the outcomes of actions or decisions are completely certain in terms of what will occur, when and its extent and nature, then there is less need to assess the risks but just manage them and monitor the results. Decision makers need help understanding where uncertainty lies and how it is best treated and managed.

Notes

To the extent possible, discussion should be provided of the nature, difficulty, feasibility, cost and time associated with undertaking research to resolve the key scientific limitations and uncertainties.

8. Risk Assessment should be multidisciplinary and therefore transparent and understood by all involved and/or interested parties through their inclusion and involvement in the process.

   This implies the need of reflection at the start of the risk assessment, on who should be involved in the risk assessment process. Risk assessment is usually not a one man show. Different parties are involved.

   Example: The executive party (the team which actually perform the risk assessment), the manager or organization taking decisions based on the risk assessment and parties influenced by these decisions.

   Good communication between these parties is vital for the risk assessment process.

   Furthermore, risk assessment exists of different assignments for which different kind of expertise is necessary. Therefore, risk assessment needs a multidisciplinary involvement and view on the process.

9. Appropriate procedures for peer review and public participation should be used in the process of preparing the risk assessment.

   These procedures will contribute to scientific objectivity, transparency and acceptance of the conclusions.

   Peer review may include: issuing a draft risk assessment report; considering comments received on this draft; issuing a "response-to-comment" document that summarizes the significant comments received and the risk assessor's responses to those comments; and providing a rationale for why the risk assessor has not adopted the position suggested by commenter.

   Involvement also ensures that their views are properly represented and are taken into account. It is particularly important that any risk criteria used adequately reflect the perceptions and views of the relevant interested parties because risk evaluation must determine what level of risk is tolerable to them and where and when further treatment is required. Of course, during risk identification the involvement of a representative group with a large and diverse experience base always ensures the most comprehensive of analyses. Finally, those held accountable for the monitoring of control measure benefit greatly from involvement in the risk assessment that lead to those controls.

10. Risk Assessment should be dynamic, iterative and responsive to change.

    Risks change with time. New risks emerge and others decline. As events occur and control activities take place, knowledge changes and increases. It is therefore important that risk assessment is not a 'one pass' process and that there is a 'monitor and review' element to ensure that risk assessment and controls reflect the current situation.

    Involvement of interested parties and, in particular, decision makers in the risk assessment process are essential to ensure it remains relevant and up to date.

    As relevant and scientifically plausible information becomes available, the risk assessor shall, considering the resources available, consider: revising the risk assessment to incorporate such information; and updating or replacing the assumptions to reflect new data or scientific understandings.

Did u know? **What is the purpose of risk management?**

The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets.

Notes Risk assessments must be conducted by teams that include both functional managers and information technology administrators. Business operations, workflow, or technologies change, periodic reviews should be conducted to analyze these changes. The affect of new threats and vulnerabilities created by these changes has to be determined. A thorough checking of the effectiveness of existing controls also required.

Self Assessment

Fill in the blanks:

7. A threat is an event, process, activity, or action that exploits a .... to attack an asset.
8. .... are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset.
9. A technique to .... data includes preparing a list of assets and showing corresponding threats, type of loss and vulnerability.
10. The primary purpose of risk assessment should always be to deal with those aspects of .... that are uncertain.
11. As events occur and control activities take place, ... changes and increases.

4.4 Approaches and Considerations

Risks that are worthy of attention are managed and risks not worthy of consideration are accepted. A risk treatment plan should be identified for all risks identified. Identified risk can be and is usually managed by a variety of approaches: Risk transfer, risk avoidance, risk reduction and risk acceptance.

4.4.1 Acceptance

Risk acceptance is also known by the name of risk retention. It is simply accepting the identified risk without taking any measures to prevent loss or the probability of the risk happening. It involves a decision by management to accept a given risk without further mitigation or transfer, for a period of time. This happens in two classes of circumstances. For risks that are too low to bother protecting against or for which insurance and due diligence are adequate, risk is accepted. For risks that are to be mitigated but where mitigation cannot be done instantaneously or for which rapid mitigation is too expensive to warrant, risks are accepted for periods during which mitigation is undertaken. This approach is ideal for those risks that will not create a high amount of loss if they occur. These risks in fact would be considered more costly to manage than to allow.

4.4.2 Avoidance

Risk avoidance is exactly as it sounds. It is a business strategy in which certain classes of activities or business processes are not undertaken because the risks are too high to justify the return on investment. A risk may be avoided by not accepting or entering into the event which has hazards. This method has severe limitations because such a choice is not always possible, or if possible, it may require giving up some important advantages. Nevertheless, in some situations risk avoidance is both possible and desirable.

4.4.3 Transfer

Risk transfer involves transferring the weight or the consequence of a risk on to some other party. There are many ways that risk transfer can take place. Insurance is a commonly used method of risk transfer; the insurance company accepts the risk of another. Another form of risk transfer can happen in the way that a contract is laid out. Risk transfer for low consequences is usually affordable and reasonable if some level of reasonable and prudent controls are in place. This meets due diligence standards for low risk systems. Risk transfer for medium and high consequences is rare, expensive, and only justified in cases where the worst case loss is not sustainable and an adequate outside insurance capacity is willing to take on the risk.

Caution Risk Transfer is a strategy that loses in the long run for medium and high risks.

4.4.4 Reduction

Risk reduction reduces the potential loss associated with that risk. Risks can be reduced by implementation of standard operating procedures, education and training, limiting the numbers or types of participants, establishing security methodologies, duplication of records, selecting appropriate venues, preventive maintenance, etc.

Self Assessment

Fill in the blanks:

12. .... is simply accepting the identified risk without taking any measures to prevent loss or the probability of the risk happening.

13. .... is a business strategy in which certain classes of activities or business processes are not undertaken because the risks are too high to justify the return on investment.

14. .... involves transferring the weight or the consequence of a risk on to some other party.

15. Risks can be .... by implementation of standard operating procedures, education and training, limiting the numbers or types of participants, etc.

Caselet

Operational Risk Management — How Banks can Manage the Unknown

WHAT if suddenly ATMs stopped vending crisp notes, bank branches closed for few days, the data centre of major banks shut down, busy operations in dealing rooms of major banks come to a halt and banking personnel don't reach their offices.

This is not a doomsday scenario but what actually happened during the Mumbai floods. Uncertainty has crept into our lives. In technical parlance, we can call the risk involved in running daily operations "operational risk", or op-risk, for short.

In the banking industry, op-risk is as old as banking itself. The banking landscape has undergone a sea change and is becoming more complex in terms of volume of business, product innovation, financial engineering, new market practices, fast and rapid technology innovation, deregulation, consolidation of banks and increasing competition among banks.

This has increased probability of failure or mistakes from the operations point of view; it has increased the focus on managing op-risk.

The new BIS guidelines, generally known as "Basel II Accord", recognises this and places increased emphasis on op-risk management. The Basel committee defines op-risk as the risk "of loss resulting from inadequate or failed internal processes, people and systems or from external events". This definition includes legal risk, but excludes strategic and reputation risk. As banks move towards implementing Basel II norms, they need to evolve an internal framework for effective management of op-risk.

Depending on the size, complexity and organisational structure of bank, a five-step approach can be used for building a robust op-risk framework:

(a) Identification of operational risk through event framework

(b) Analysing the causes of events

(c) Risk mapping

(d) Risk measurement and control

(e) Management of operational risk and, thereby, capital management.

To start with, banks, as part of identification, should classify and capture all operational losses in the form of "events". Events are nothing but "occurrences" or "happenings". Banks should start accumulating data on events that have occurred in the past and also identify potential events.

All events should be defined with attributes, such as, frequency of event, severity, loss amount, reason for loss, date of discovery of loss and date of occurrence.

Banks can adopt the seven type of events suggested by Risk Management Group (RMG) of Basel committee for one of their quantitative studies (QIS-2) which includes internal fraud, external fraud, employment practices and work safety, client products and business services, damages to physical assets, business disruption and system failures and execution delivery.

Contd...

The second step involves doing a causal analysis to understand the exact cause for the above events and estimate the actual loss as well as potential loss in case the events are repeated. This analysis on cause of events can make the bank understand the level of exposure and the op-risk management strategy it needs to adopt.

Once banks have developed an event database and done the causal analysis, they can start risk mapping. Risk mapping is a tool wherein banks can map the above risk events and losses to any specified set of business lines.

Basel has come out with eight set of business lines — corporate finance, trading and sales, retail banking, commercial banking, payment and settlement, agency and custody services, asset management and retail brokerage — to which the events collected by bank can be mapped.

Op-risk measurement is still evolving in terms of tools and techniques that can be used for effective measurement and management. Banks can follow either or both of qualitative risk measurement or quantitative risk measurement:

The generic ways of measuring op-risk include qualitative risk measurement techniques such as critical assessment method, which involves questionnaire format and interviews with all line managers to identify the op-risk events.

Another widely used approach, which is a combination of qualitative as well as quantitative approaches, is the Key Risk Indicators (KRI) approach, which involves identifying indicators, which convey good idea about the scope of business and thereby the risk involved.

For instance, portfolio size, volume of transactions traded, volume of deals routed through payment and settlement systems, etc., form one set of predictive indicators. KRI is more a predictive model than a cause-and-event approach.

A common quantitative approach used is Loss Distribution Approach (LDA), which involves arriving at a right fit distribution of historical loss events and, thereby, at quantitative results like expected loss and finally operational value at risk.

Another forward-looking scenario generation approach for op-risk measurement is Loss Scenario Modelling, which involves generating simulations for loss scenarios based on the events and losses captured in the first step.

Basel II norms suggest three approaches for measurement of op-risk. The simplest approach, best suited for less sophisticated and small balance-sheet banks, is the Basic Indicator Approach (BIA). BIA requires banks to allocate capital based on a single indicator of operational risk, which in this case will be average gross income of past three years multiplied by factor called alpha, which is set at 15 per cent.

The second approach is the Standardised Approach (SA), which involves mapping the bank's business lines to the set of eight business lines and use multiplier (Beta) of average gross income to compute capital charge.

Also, there is the Alternative Standardised Approach (ASA), which uses loans and advances, instead of gross income, for retail banking and commercial banking business lines multiplied by fixed factor which results in capital charge to be set aside.

The most sophisticated approach suggested is advanced measurement approach (AMA). Under the AMA, the regulatory capital requirement will equal the risk measures generated by the bank's internal operational risk measurement system using quantitative and qualitative criteria for the AMA. Internal data used must be based on a minimum historical observation period of five years. However, when a bank first moves to AMA, a three-year period is acceptable.

Contd...

Banks need to employ the quantitative approaches like Internal Measurement Approach (IMA) or Loss distribution Approach (LDA) or Balance Scorecard Approach (BSA) for adopting AMA. All AMA approaches compute the expected and unexpected loss. The most significant aspect for a bank to graduate from Basic Indicator Approach (BIA) to Advanced Measurement Approach (AMA) is the potential benefit of less capital allocation for operational risk.

As op-risk involves failures during operations in daily business, the key steps in op-risk management involve improving internal control environment, designing and developing procedures to implementing the risk management processes and employing risk transfer techniques, such as insurance, to mitigate the loss arising from operational risk. Credit rating agencies have started rating banks based on their risk control and management frameworks. Investor awareness has also increased to the extent that banks with robust risk management frameworks are able to attract strategic investments with less effort.

Given the known benefits of implementing the provisions of the Basel II accord, banks should prioritise their strategy towards op-risk management. A constructive approach in this direction could be to automate the suggested five-step approach and, as a first step, to start developing a loss event database.

Source: http://www.thehindubusinessline.in/2006/01/19/stories/2006011900991000.htm

4.5 Summary

- Risk is virtually anything that threatens or limits the ability of an organization to achieve its mission.
- Risk management is a process to identify and then manage threats which could severely impact or bring down the organization.
- Successful risk management needs the involvement of all levels of employers of an organization.
- To successfully manage their risk in the future, organizations need to develop an enterprise-wide risk management framework.
- Organizations should regularly undertake comprehensive, focused assessment of potential risks to the organization. This focused assessment should occur at least twice a year by a team of staff members representing all the major functions of the organization.
- The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets.
- Risk acceptance is also known by the name of risk retention. It is simply accepting the identified risk without taking any measures to prevent loss or the probability of the risk happening.
- Risk avoidance is a business strategy in which certain classes of activities or business processes are not undertaken because the risks are too high to justify the return on investment.
- Risk reduction reduces the potential loss associated with that risk.

4.6 Keywords

Control: Any kind of counter measure that becomes fairly automated and meets the expectations of upper management is called a control.

Notes

Risk: Any kind of analysis that ties-in specific threats to specific assets with an eye toward determining the costs and/or benefits of protecting that asset is called risk, or risk assessment.

Risk Acceptance: It is simply accepting the identified risk without taking any measures to prevent loss or the probability of the risk happening.

Risk Avoidance: It is a business strategy in which certain classes of activities or business processes are not undertaken because the risks are too high to justify the return on investment.

Risk Control: It is the entire process of policies, procedures and systems an institution needs to manage prudently all the risks.

Risk Management: It is a process to identify and then manage threats which could severely impact or bring down the organization.

Risk Reduction: It reduces the potential loss associated with that risk.

Risk Transfer: It involves transferring the weight or the consequence of a risk on to some other party.

Vulnerability: Any kind of asset that is not working optimally and is mission-critical or essential to the organization, such as data that are not backed-up, is called a vulnerability.

4.7 Review Questions

1. What is risk? How it results in reducing the potential of any internal or external events to detrimentally affect a business.
2. What is risk management? Discuss the main areas that have been focused for risk management.
3. Enlighten the steps involved in risk management.
4. Explain the risk control measure for an organization.
5. How to reduce the risk?
6. Make distinction between risk acceptance and risk avoidance.
7. Explain the process of risk transfer.
8. Explain the basic principles of risk assessment.
9. Describe the various approaches involved in identifying risk.
10. The purpose of a risk assessment is to help management create appropriate strategies and controls for stewardship of information assets. Comment.

Answers: Self Assessment

1. Risk
2. secure
3. Risk management
4. employers
5. enterprise-wide
6. external
7. vulnerability
8. Controls
9. analyze
10. decision making
11. knowledge
12. Risk Acceptance

Notes

13. Risk Avoidance

14. Risk transfer

15. reduced

4.8 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online links

www.drj.com

www.security-risk-analysis.com

Notes

Unit 5: Physical Security

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the need and meaning of physical security
- Discuss the process of natural disasters, controlling physical access
- Understand the concept of intrusion detection system
- Discuss controlling visitors, fireproof sales, and security through cables and locks.

Introduction

Protection against intrusions into the computer system by outsiders is an essential element of the security policy. But it's not just intrusion via the Internet that you need to guard against. The following issues relate to physical safety of the computer equipment on which your information is stored, the premises in which they are stored, and staff who have physical and electronic access to systems and information. Some of the most effective advances in security technologies during the past few decades have been in the area of physical security — i.e., protection by tangible means.

In this unit we'll discuss about the physical threats and physical securities.

5.1 Need for Physical Security

Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including data security. Physical security refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders. Risk assessment process identifies the organization's vulnerabilities. Then use the vulnerabilities list to set priorities on resources needed. Every enhancement of an identified vulnerability in the current system will generally provide more security than previously. Enhance the system to the extent possible, and keep a list of improvements still needed.

Task Write the importance of physical security.

Self Assessment

Fill in the blanks:

1. .... refers to the protection of building sites and equipment from theft, vandalism, natural disaster, man-made catastrophes, and accidental damage.
2. .... process identifies the organization's vulnerabilities.

5.2 Physical Security: Meaning

Physical security is defined as the security of personnel, hardware, programs, networks, and data from physical situations and events that could provide severe losses or harm to an enterprise, agency, or organization. This involves security from fire, natural disasters, robbery, theft, destruction, and terrorism.

Physical security is frequently unobserved (and its significance undervalued) in support of more technical and dramatic concerns like hacking, virus, such as, Trojans, and spy ware. Though, breaches of physical security can be carried out with small or no technical information regarding an attacker. Furthermore, accidents and natural disasters are a part of everyday life, and in the long term, are unavoidable.

Physical security should take care of the following elements:

1. Unauthorized access may result in lost data, altered data, altered equipment configurations (having a wide variety of negative results), physical damage or theft of equipment, or even the disclosure of private information. So, hardware should protect against internal and external intruders by using authentication factor. Security lock may be used.
2. Minimize external access. Secure rooms should only have one or two solid, fireproof, and lockable doors. The doors should be observable by security staff. Doors to secure areas should never be left open. Windows should be small and have locks.
3. Maintain appropriate locks. Keep doors locked when room is not in use. Maintain secure system for keys and combinations. If there is a breach, each compromised lock should be changed.

4. Alternative physical security strategies should be implemented. When appropriate, consider the use of window bars, anti-theft cabling (with alarm when cable is disconnected from system), magnetic key cards, and motion detectors.

5. Be prepared for fire emergencies with appropriate automatic non water fire fighting equipment, and provide appropriate staff training in its use.

6. Maintain reasonable climate control in secured rooms, with temperature ranges between 50 and 80 degrees Fahrenheit, with a humidity range of 20 - 80%.

7. Minimize nonessential materials that could jeopardize a secure room.

Example: Non-essential items include: coffee, food, cigarettes, curtains, reams of paper, and other flammables.

8. Dispose of confidential waste carefully and adequately to maintain confidentiality.

9. Label confidential information appropriately and ensure suitable security procedures from common carriers when shipping or receiving confidential information.

10. Keep critical systems separate from general systems.

11. Store computer equipment in places that cannot be seen or reached from windows and doors, and away from radiators, heating vents, air conditioners, or other work. Workstations that do not routinely display sensitive information should stored in open, visible spaces to prevent covert use.

12. Protect cabling, plugs, and other wires from foot traffic.

13. Keep a secure inventory of equipment and peripheral equipment, with up-to-date logs of manufacturers, models, and serial numbers. Consider videotaping the equipment for insurance purposes.

14. Hardware (servers, workstations, network devices) must be replaced or upgraded within reasonable timeframes to keep the network functional. However, once a workstation gets to be four to five years old, its processing power diminishes in relation to the requirements of newer software.

15. Consider the use of maintenance contracts. Keep equipment information, contact and tech support numbers readily available at the computers.

16. When computers containing sensitive information are being maintained or repaired, be sure that sensitive data is properly passworded, encrypted, or removed from the computer before maintenance or repair.

17. Proper annual maintenance and repairing of computer equipment is required.

18. Backup media should be more secured. Some hardware techniques provide a higher level of security than non-secure media such as backup tapes, floppy diskettes, or smart cards, since the latter can be easily removed or copied. Backup on internet may be used for that.

19. Proper procedure to be used to backup system information and applications.

20. Establish a procedure and schedule of system backup.

21. Establish overall system backup responsibilities and assign them.

22. Individuals who use the computers should also have backup responsibilities.

23. Use a rotation of media (using different disks at each backup and rotating every X days or weeks).

Notes

24. Both onsite and offsite backup storage should be considered and used.
25. Regulate power supplies to the extent possible.
26. Prepare for electrical power fluctuations by using surge suppressors or electrical power filters and using uninterruptible power sources to serve as auxiliary electrical supplies as backup to critical systems.
27. Design electrical systems to better withstand fires, floods, and other disasters.
28. Ensure distributed use of outlets by all equipment.
29. Use anti-static carpeting and pads, and use anti-static sprays whenever possible.
30. Get appropriate insurance, even if your business is a very small concern.

Self Assessment

Fill in the blanks:

3. Physical security is frequently .... in support of more technical and dramatic concerns like hacking, virus, such as, Trojans, and spy ware.
4. Hardware should protect against internal and external intruders by using .... factor.

5.3 Physical Threats to the Information System

Physical threat to a computer system could be as a result of loss of the whole computer system, damage of hardware, damage to the computer software, theft of the computer system, vandalism, natural disaster such as flood, fire, war, earthquakes etc. Acts of terrorism such as the attack on the world trade centre is also one of the major threats to computer which can be classified as physical threat.

Natural hazards, civil unrest and terrorism all comes under disaster. A disaster is defined as a sudden misfortune that is ruinous to an undertaking. This means that there is little time to react at the time of the misfortune. Preparations have to have been made in advance. The focus should, therefore, be on disaster planning.

Did u know? **What is disaster?**

A disaster is defined as a sudden misfortune that is ruinous to an undertaking.

5.3.1 Natural Disasters

Certain natural disasters could either severely damage the computer system directly, or prevent its operations.

These include:

1. Local flooding including fracture of air conditioning or water cooling equipment,
2. Local landslide, earth quake, subsidence and so on,
3. Exceptional weather conditions.

Notes

Civil Unrest

Electronic system might be popular targets for attack by politically motivated groups and individuals as well as by mobs. It is undesirable that an electronic system site should be in vicinity with:

1. Unusually high risk of mob violence,
2. Unusually high incidence of criminal and malicious damage,
3. Unusually high risk terrorist activity.

If such a site is unavoidable, additional levels of physical security may be appropriate.

Computer Terrorism

Computer terrorism is the act of destroying or of corrupting computer systems with an aim of destabilizing a country or of applying pressure on a government. It is the act of doing something intended to destabilize a country or to apply pressure on a government by using methods classified in the category of computer crimes.

It is possible to carry out three types of actions against an information system, a physical, syntactic attack and semantic attack:

1. The physical attack consists of damaging equipment in a "traditional" way, bomb, fire, etc.
2. The syntactic attack consists of modifying the logic of the system in order to introduce delays or to make the system unpredictable. An attack by means of a virus or of a Trojan horse is included in this category.
3. The semantic attack is more perfidious. It exploits the confidence that the users have in their system. It consist of modifying information that is entering or exiting the system, without the users' knowledge, in order to induce errors.

Table 5.1: Physical Threats

Category	Threat	OSI Layer	Definition	Typical Behaviors	Vulnerabilities	Prevention	Detection	Countermeasures
Physical Environment	Fire Damage	N/A	Physical destruction of equipment due to fire or smoke damage	Physical destruction of systems and supporting equipment	Systems located near potential fire hazards, e.g., fuel storage tanks	Off-site system replication, while costly, provides backup capability	On-site smoke alarms	Halon gas or FM200 fire extinguishers mitigate electrical and water damage
	Water Damage	N/A	Physical destruction of equipment due to water (including sprinkler) damage	Physical destruction of systems and supporting equipment	Systems located below ground or near sprinkler systems	Off-site system replication	Water detection devices	Computer rooms equipped with emergency drainage capabilities
	Power Loss	N/A	Computers or vital supporting equipment fail due to lack of power	Immediate loss of data due to abnormal shutdow, even after power returns Continuing loss of capability until power returns	Sites fed by above ground power lines are particularly vulnerable Power loss to computer room air conditioners can also be an issue	Dual or separate feeder lines for computers and supporting equipment	Power level alert monitors	Uninterruptible Power Supplies (UPS) Full scale standby power facilities where economically feasible

Contd...

Notes

	Civil Disorder Vandalism	N/A	Physical destruction during operations other than war	Physical destruction of systems and supporting equipment	Sites located in some overseas environments, especially urban environments	Low profile facilities (no overt disclosure of high value nature of site)	Physical intrusion detection devices	Physical access restrictions and riot contingency policies
	Battle Damage	N/A	Physical destruction during military action	Physical destruction of systems and supporting equipment	Site located in theater	Off-site system replication OPSEC and low profile to prevent hostile targeting	Network monitorin g systems	Hardened sites

Self Assessment

Fill in the blanks:

5. A .... is defined as a sudden misfortune that is ruinous to an undertaking.

6. .... is the act of destroying or of corrupting computer systems with an aim of destabilizing a country or of applying pressure on a government.

5.4 Controlling Physical Access

Access controls protect against improper access of equipment, data files, and software. To restrict physical access, a security system must be able to differentiate among authorized and unauthorized individuals. Physical access can be restricted by means of three general techniques.

Identification: Identification depends on comparing the physical traits of the individual with previously accumulated information.

Example: An individual's signature, personnel number, code, voice print, palm print, fingerprint, teeth print, or other personal characteristic could be verified before permitting access.

Secondary authentication, like the user's place of birth, may be needed for highly sensitive information.

User's Name and Passwords: Passwords depends on some memorized mixture of letters or numbers. There should be no logic to the password, so it cannot be simply presumed; Individuals are authorized depending on what they know. Passwords should be changed within a fixed period of time. Inactive passwords (like., more than 4 months old) should be removed. Passwords should be modified and confidential data taken from terminated employees. If a user alters a password, controls must appear to ensure the user does not access his old password. Passwords should not be shared. Access control software may be used to have a minimum password time period in which a new password cannot be modified or a new password comparing an old one will be not accepted.

Cards/Keys: Access can also be restricted by the use of cards, keys, or badges; individuals are authorized depending on what they own. Improper use may be signaled by an alarm, and unauthorized access patterns should be examined. A smart card, which is a small electronic device regarding the size of a credit card that includes electronic memory, may be used in which the user enters both his or her identification number and a random generated code which modifies each time the card is used or over a specified time period. Smart cards are used for a numerous purposes, involving: accumulating a patient's medical records, accumulating digital cash, and generating network IDs (identical to a token).

Notes

Inside the plant, areas including sensitive data should be accessible only to authorized personnel. These areas, involving the computer room, should have only a single entry door, which can be functioned by an appropriate encoded magnetic-strip ID card. Physical controls might involve having a librarian keep a log. A lockout should appear with repeated faults. Logs should automatically be kept of the ID number, time of access, and function executed. Further, data dictionary software offers an automated log of access to software and file information. Intrusion detection devices like cameras and motion detectors should be accessed to observe sensitive and high-risk areas against unauthorized individuals.

Every individual function (such as., accounts receivable, payroll) may have its own password so that users have access to restricted areas of the database. The computer can keep an internal record of the date and time each file was last updated, and this internal record contrasted against the log. The hours to use "key" microcomputer files can be restricted, to avert unauthorized access after usual working hours. Files should be displayed in terms of diverse levels of confidentiality and security like top secret, confidential, internal use only, and unrestricted. Confidential information should not be appeared on the screen.

Notes To control access to sensitive data, there should be a mapping of access needs to the system components. Access rights should depend on job function, and there should occur an appropriate segregation of duties. Temporary employees should be limited to a particular project, activity, system, and time period.

Self Assessment

Fill in the blanks:

7. To restrict ...., a security system must be able to differentiate among authorized and unauthorized individuals.

8. .... software may be used to have a minimum password time period in which a new password cannot be modified or a new password comparing an old one will be not accepted.

5.5 Intrusion Detection System

Intrusion Detection System (IDS) technology is an important component in designing a secure environment. It is a type of security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions and misuse.

It is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees.

An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses and worms).

An IDS can be composed of several components: Sensors which generate security events, a Console to monitor events and alerts and control the sensors, and a central Engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received.

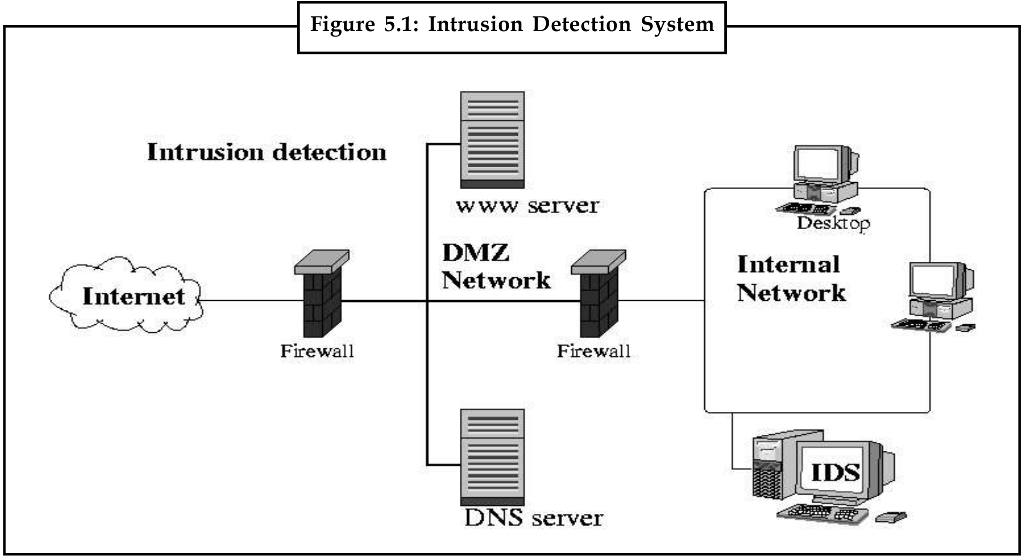
Caution In many simple IDS implementations all three components are combined in a single device or appliance.

There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. While there are several types of IDSs, the most common types work the same. They analyze network traffic and log files for certain patterns. What kind of patterns you may ask? While a firewall will continually block a hacker from connecting to a network, most firewalls never alert an administrator.

The administrator may notice if he/she checks the access log of the firewall, but that could be weeks or even months after the attack. This is where an IDS comes into play. The attempts to pass through the firewall are logged, and IDS will analyze its log. At some point in the log there will be a large number of request-reject entries.

An IDS will flag the events and alert an administrator. The administrator can then see what is happening right after or even while the attacks are still taking place. This gives an administrator the advantage of being able to analyze the techniques being used, source of attacks, and methods used by the hacker.

Figure 5.1: Intrusion Detection System



Caution An IDS cannot directly detect attacks within properly encrypted traffic.

5.5.1 Types of Intrusion-Detection Systems

In a Network-based Intrusion-detection System (NIDS), the sensors are located at choke points in network to be monitored, often in the Demilitarized Zone (DMZ) or at network borders. The sensor captures all network traffic and analyzes the content of individual packets for malicious traffic.

In systems, PIDS and APIDS are used to monitor the transport and protocols illegal or inappropriate traffic or constructs of language (say SQL). In a host-based system, the sensor usually consists of a software agent, which monitors all activity of the host on which it is installed. Hybrids of these two systems also exist.

1. A network intrusion detection system is an independent platform which identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap.

   An **example** of a NIDS is Snort.

2. A Protocol-based Intrusion Detection System (PIDS) consists of a system or agent that would typically sit at the front end of a server, monitoring and analyzing the communication protocol between a connected device (a user/PC or system). For a web server this would typically monitor the HTTPS protocol stream and understand the HTTP protocol relative to the web server/system it is trying to protect. Where HTTPS is in use then this system would need to reside in the "shim" or interface between where HTTPS is un-encrypted and immediately prior to it entering the Web presentation layer.

3. An Application Protocol-based Intrusion Detection System (APIDS) consists of a system or agent that would typically sit within a group of servers, monitoring and analyzing the communication on application specific protocols.

Example: In a web server with database this would monitor the SQL protocol specific to the middleware/business-login as it transacts with the database.

4. A Host-based Intrusion Detection System (HIDS) consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state.

   An **example** of a HIDS is OSSEC.

5. A hybrid intrusion detection system combines two or more approaches. Host agent data is combined with network information to form a comprehensive view of the network.

   An **example** of a Hybrid IDS is Prelude.

Self Assessment

Fill in the blanks:

9. An .... gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions and misuse.

10. A .... system is an independent platform which identifies intrusions by examining network traffic and monitors multiple hosts.

5.6 Intrusion Prevention System

An Intrusion Prevention System is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.

Network-based IPS, for example, will operate in-line to monitor all network traffic for malicious code or attacks. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass. Intrusion prevention technology is considered by some to be an extension of intrusion detection (IDS) technology.

Intrusion Prevention Systems (IPS) evolved in the late 1990s to resolve ambiguities in passive network monitoring by placing detection systems in-line. Early IPS was IDS that were able to implement prevention commands to firewalls and access control changes to routers. This technique fell short operationally for it created a race condition between the IDS and the exploit as it passed through the control mechanism.

Inline IPS can be seen as an improvement upon firewall technologies (snort inline is integrated into one), IPS can make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done.

However, in order to improve performance and accuracy of classification mapping, most IPS use destination port in their signature format. As IPS systems were originally a literal extension of intrusion detection systems, they continue to be related.

Intrusion prevention systems may also serve secondarily at the host level to deny potentially malicious activity. There are advantages and disadvantages to host-based IPS compared with network-based IPS. In many cases, the technologies are thought to be complementary.

An Intrusion Prevention System must also be a very good Intrusion Detection System to enable a low rate of false positives. Some IPS systems can also prevent yet to be discovered attacks, such as those caused by a Buffer overflow.

The role of an IPS in a network is often confused with access control and application-layer firewalls. There are some notable differences in these technologies. While all share similarities, how they approach network or system security is fundamentally different.

An IPS is typically designed to operate completely invisibly on a network. IPS products do not typically claim an IP address on the protected network but may respond directly to any traffic in a variety of ways. (Common IPS responses include dropping packets, resetting connections, generating alerts, and even quarantining intruders.) While some IPS products have the ability to implement firewall rules, this is often a mere convenience and not a core function of the product.

Moreover, IPS technology offers deeper insight into network operations providing information on overly active hosts, bad logons, inappropriate content and many other network and application layer functions.

Application firewalls are a very different type of technology. An application firewall uses proxies to perform firewall access control for network and application-layer traffic. Some application-layer firewalls have the ability to do some IPS-like functions, such as enforcing RFC specifications on network traffic. Also, some application layer firewalls have also integrated IPS-style signatures into their products to provide real-time analysis and blocking of traffic.

Application firewalls do have IP addresses on their ports and are directly addressable. Moreover, they use full proxy features to decode and reassemble packets. Not all IPS perform full proxy-like processing. Also, application-layer firewalls tend to focus on firewall capabilities, with IPS capabilities as add-on. While there are numerous similarities between the two technologies, they are not identical and are not interchangeable.

Unified Threat Management (UTM), or sometimes called "Next Generation Firewalls" are also a different breed of products entirely. UTM products bring together multiple security capabilities on to a single platform.

A typical UTM platform will provide firewall, VPN, anti-virus, web filtering, intrusion prevention and anti-spam capabilities. Some UTM appliances are derived from IPS products such as 3Com's X-series products.

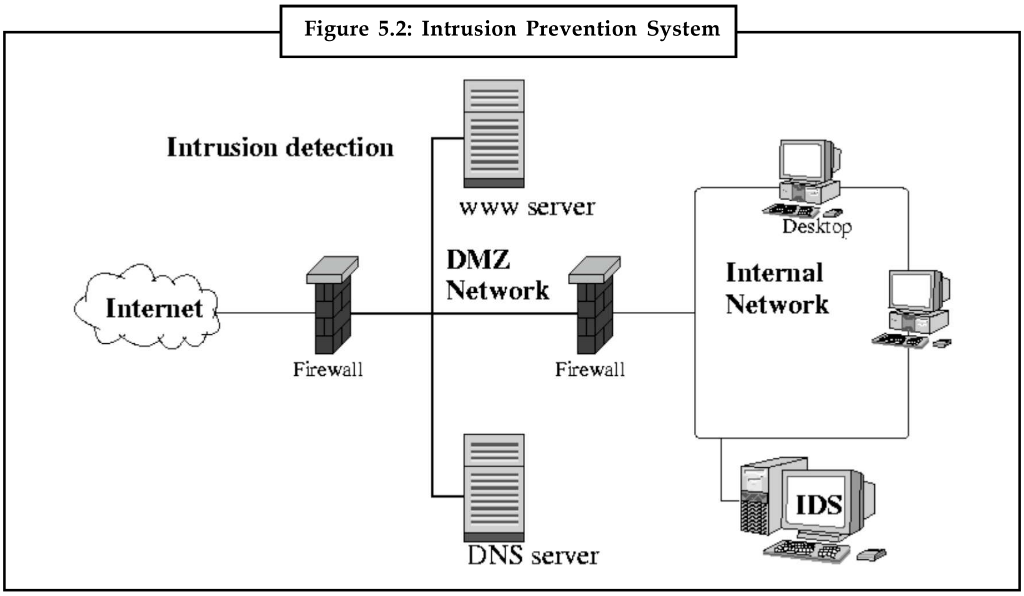
Notes

Others are derived from a combination with firewall products, such as Juniper's SSG or Cisco's Adaptive Security Appliances (ASA). And still others were derived from the ground up as a UTM appliance such as Fortinet or Astero. The main feature of a UTM is that it includes multiple security features on one appliance. IPS is merely one feature.

Access Control is also an entirely different security concept. Access control refers to general rules allowing hosts, users or applications access to specific parts of a network. Typically, access control helps organizations segment networks and limit access.

While an IPS has the ability to block access to users, hosts or applications, it does so only when malicious code has been discovered. As such, IPS does not necessarily serve as an access control device. While it has some access control abilities, firewalls and Network Access Control (NAC) technologies are better suited to provide these features.

Figure 5.2: Intrusion Prevention System



Did u know? The term "Intrusion Prevention System" was coined by Andrew Plato who was a technical writer and consultant for *NetworkICE.

5.6.1 Types of Intrusion Prevention System

Host-based IPS (HIPS)

A host-based IPS is one where the intrusion-prevention application is resident on that specific IP address, usually on a single computer. HIPS compliments traditional finger-print-based and heuristic anti-virus detection methods, since it does not need continuous updates to stay ahead of new malware. As ill-intended code needs to modify the system or other software residing on the machine to achieve its evil aims, a truly comprehensive HIPS system will notice some of the resulting changes and prevent the action by default or notify the user for permission.

Extensive use of system resources can be a drawback of existing HIPS, which integrate firewall, system-level action control and sandboxing into a coordinated detection net, on top of a traditional AV product.

This extensive protection scheme may be warranted for a laptop computer frequently operating in untrusted environments (e.g., on cafe or airport Wi-Fi networks), but the heavy defenses may take their toll on battery life and noticeably impair the generic responsiveness of the computer as the HIPS protective component and the traditional AV product check each file on a PC to see if it is malware against a huge blacklist.

Alternatively if HIPS is combined with an AV product utilizing whitelisting technology then there is far less use of system resources as many applications on the PC are trusted (whitelisted). HIPS as an application then becomes a real alternative to traditional anti-virus products.

Network-based IPS (NIPS)

A network-based IPS is one where the IPS application/hardware and any actions taken to prevent an intrusion on a specific network host(s) is done from a host with another IP address on the network (This could be on a front-end firewall appliance.)

Network intrusion prevention systems are purpose-built hardware/software platforms that are designed to analyze, detect, and report on security related events. NIPS are designed to inspect traffic and based on their configuration or security policy, they can drop malicious traffic.

Content-based IPS (CBIPS)

A content-based IPS (CBIPS) inspects the content of network packets for unique sequences, called signatures, to detect and hopefully prevent known types of attack such as worm infections and hacks.

Protocol Analysis

A key development in IDS/IPS technologies was the use of protocol analyzers. Protocol analyzers can natively decode application-layer network protocols, like HTTP or FTP. Once the protocols are fully decoded, the IPS analysis engine can evaluate different parts of the protocol for anomalous behavior or exploits.

Example: The existence of a large binary file in the User-Agent field of an HTTP request would be very unusual and likely an intrusion.

A protocol analyzer could detect this anomalous behavior and instruct the IPS engine to drop the offending packets.

Not all IPS/IDS engines are full protocol analyzers. Some products rely on simple pattern recognition techniques to look for known attack patterns. While this can be sufficient in many cases, it creates an overall weakness in the detection capabilities. Since many vulnerabilities have dozens or even hundreds of exploit variants, pattern recognition-based IPS/IDS engines can be evaded.

Example: Some pattern recognition engines require hundreds of different signatures (or patterns) to protect against a single vulnerability. This is because they must have a different pattern for each exploit variant.

Protocol analysis-based products can often block exploits with a single signature that monitors for the specific vulnerability in the network communications.

Rate-based IPS (RBIPS)

Rate-based IPS (RBIPS) are primarily intended to prevent Denial of Service and Distributed Denial of Service attacks. They work by monitoring and learning normal network behaviors. Through real-time traffic monitoring and comparison with stored statistics, RBIPS can identify abnormal rates for certain types of traffic e.g. TCP, UDP or ARP packets, connections per second, packets per connection, packets to specific ports etc. Attacks are detected when thresholds are exceeded. The thresholds are dynamically adjusted based on time of day, day of the week, etc., drawing on stored traffic statistics.

Unusual but legitimate network traffic patterns may create false alarms. The system's effectiveness is related to the granularity of the RBIPS rulebase and the quality of the stored statistics.

Notes Once an attack is detected, various prevention techniques may be used such as rate-limiting specific attack-related traffic types, source or connection tracking, and source-address, port or protocol filtering (blacklisting) or validation (whitelisting).

Task Compare and contrast between NIDS and PIDS.

Self Assessment

Fill in the blanks:

11. An .... is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.

12. A .... is one where the intrusion-prevention application is resident on that specific IP address, usually on a single computer.

13. A .... inspects the content of network packets for unique sequences, called signatures, to detect and hopefully prevent known types of attack such as worm infections and hacks.

5.7 Controlling Visitors

Visitors can be controlled through the following process:

1. If the company consists of more than about 15-20 people, issue visitor badges and encourage staff to challenge unaccompanied visitors.

2. Escort all visitors – don't let them wander around unsupervised.

3. Keep a visitor book and log the times when visitors enter and leave the premises. Keep another signing-in/out list for sensitive areas, such as computer rooms.

4. Consider CCTV in critical IT areas (e.g., server rooms) and reception areas.

5.8 Fireproof Safes and Security through Cables and Locks

Notes

To maintain physical security, following points should be considered:

1. Structural protection should be maximized. Secured rooms should have full height walls and fireproof ceilings.
2. Secure rooms should only have one or two solid, fireproof, and lockable doors.

Many modern PC cases comprise a "locking" trait. Generally this will be a socket on the front of the case that permits you to turn an incorporated key to a locked or unlocked location. Case locks can help avoid someone from stealing your PC, or opening up the case and directly influencing/stealing your hardware. They can also sometimes avert someone from rebooting your computer from their own floppy or other hardware.

These case locks do unrelated things as per the support in the motherboard and how the case is constructed. On many PC's they make it so you have to rupture the case to get the case open. On some others, they will not allow you plug in new keyboards or mice. Check your motherboard or case directions for more information. This can at times be a very useful feature, although the locks are regularly very low-quality and can simply be beaten by attackers with locksmithing.

If you put a cable through the machine, attackers would have to cut the cable or smash the case to get into it. Just putting a padlock or combo lock via these can be a good prevention to someone robbing your machine.

Cable locks deter out-in-public, broad-daylight thefts (but not in private places, like your hotel room; bolt cutters slice through cables like butter). Most laptops, some desktop PCs, and even some flat-panel monitors are designed with standard cable-lock slots.

Self Assessment

Fill in the blanks:

14. If the company consists of more quantity of people, issue .... and encourage staff to challenge unaccompanied visitors.
15. A "....................." trait is considered as a socket on the front of the case that permits you to turn an incorporated key to a locked or unlocked location.

Caselet

Business Value of Security

BULLETPROOF your systems before you are hacked! That's the simple message of Roberta Bragg's *Hardening Windows Systems*, from Tata McGraw-Hill Publishing Co Ltd. So, "mount your hardening, securing campaign in at least two directions," says chapter 1, titled `an immediate call to action'. One, the big picture, and two, the intimate reality of day-to-day work.

Hardening takes time and cultural change in organisations is slow. For this, you would need "evangelists and disciples, leaders and doers, talkers and strong, silent types". You can effect significant changes in the security posture and actual security status of your networks right now by doing things that are under your control, goads Bragg.

Contd...

Among the tips is this: keep secrets. "Learn to shut your mouth. It's not rude, but a good practice, to refuse to talk about those things that might compromise security." That doesn't mean you turn non-communicative because: "It's one thing to share a security-hardening tip, or to alert someone to a bad practice that can be corrected. It's another thing to reveal your own system's security weaknesses by talking about them to others."

If there are high-risk systems in your organisation, requiring extra physical security, you may consider the following at workstation level: "a BIOS password; a required syskey Windows boot password; a smart-card, token, and/or biometric for administrator logon; removal of floppy, CD-ROM, or other removable drives; disabling of USB, serial, and other communications ports in the BIOS; hardware locks on cables and drives; physical locks that prevent theft of the workstation; and alarms that warn of computer movement."

'Harden WetWare' says the last chapter. WetWare? That's "the people part of an information system," explains the author. An important lesson for techies is to learn to speak business, because "management is not going to learn to speak geek." So, express security concerns in the context of business value, advises Bragg. "If you have trouble thinking what the business value is, just think money."

Ignorance of law is no excuse, and there are laws beyond Moore's and Murphy's. In the US context, there is the Gramm-Leach Bliley Act that requires financial institutions to implement a security program that safeguards customer info. HIPAA or the Health Insurance Portability and Accountability Act requires the protection of health-related personal information that is maintained electronically. Sarbanes-Oxley Act or SOX emphasises on internal controls. The Computer Fraud and Abuse Act "seeks to punish people whose unauthorised access to computer causes harm." Likewise, there are laws on wiretap, economic espionage, and electronic communications privacy.

It's hard to think of hardening if you trust too much in the goodness of the world. So, first harden your heart before bulletproofing your systems, because there are those with guns outside!

Source: http://www.thehindubusinessline.in/ew/2004/09/27/stories/2004092700160200.htm

5.9 Summary

- Physical security is an essential part of a security plan. It forms the basis for all other security efforts, including data security.
- Physical threat to a computer system could be as a result of loss of the whole computer system, damage of hardware, damage to the computer software, theft of the computer system, vandalism, natural disaster such as flood, fire, war, earthquakes, etc.
- Certain natural disasters could either severely damage the computer system directly, or prevent its operations.
- To restrict physical access, a security system must be able to differentiate among authorized and unauthorized individuals.
- Intrusion Detection System (IDS) technology is an important component in designing a secure environment. It is a type of security management system for computers and networks.
- An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions and misuse.

- In a Network-based Intrusion-detection System (NIDS), the sensors are located at choke points in network to be monitored, often in the Demilitarized Zone (DMZ) or at network borders.
- A Protocol-based Intrusion Detection System (PIDS) consists of a system or agent that would typically sit at the front end of a server, monitoring and analyzing the communication protocol between a connected device.

5.10 Keywords

Application Protocol-based Intrusion Detection System: it consists of a system or agent that would typically sit within a group of servers, monitoring and analyzing the communication on application specific protocols.

Computer Terrorism: It is the act of destroying or of corrupting computer systems with an aim of destabilizing a country or of applying pressure on a government.

Disaster: It is defined as a sudden misfortune that is ruinous to an undertaking.

Host-based Intrusion Detection System: It consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state.

Hybrid Intrusion Detection System: It combines two or more approaches, like host agent data is combined with network information to form a comprehensive view of the network.

Intrusion Detection System: It gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions and misuse.

Intrusion Prevention System: It is a network security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities.

Network Intrusion Detection System: It is an independent platform which identifies intrusions by examining network traffic and monitors multiple hosts.

Protocol-based Intrusion Detection System: It consists of a system or agent that would typically sit at the front end of a server, monitoring and analyzing the communication protocol between a connected device (a user/PC or system).

5.11 Review Questions

1. What is physical security? Discuss the elements that should be considered for physical security.
2. Explain the various physical threats to the information system.
3. Discuss the concept of natural disasters.
4. Explain the techniques used for controlling physical access.
5. What are the various types of intrusion-detection systems?
6. Why intrusion detection system is important?
7. Write short note on application protocol-based intrusion detection system.
8. Describe host-based intrusion detection system.

9. What do you mean by intrusion prevention systems? Why IPS is required?
10. How intrusion prevention systems can be categorized?

Answers: Self Assessment

1. Physical security
2. Risk assessment
3. unobserved
4. authentication
5. disaster
6. Computer terrorism
7. physical access
8. Access control
9. Intrusion Detection System (IDS)
10. Network intrusion detection
11. Intrusion Prevention System
12. Host-based IPS
13. Content-based IPS (CBIPS)
14. visitor badges
15. Locking

5.12 Further Readings

Books

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

An Introduction to Computer Security: The NIST Handbook

Risk Management Guide for Information Technology Systems

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online link

www.wbdg.org

Unit 6: Biometric Controls for Security

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand access control
- Discuss user identification and authentication
- Explain biometrics techniques
- Understand key success factors

Introduction

A biometric is a dimension of a natural trait like fingerprint, iris pattern, retina image, face or hand geometry; or a behavioral trait such as voice, gait or signature. Biometric technology uses these traits to recognize individuals automatically. Biometric systems are usually used in combination with other authentication resources in environments requiring high security.

In this unit we will discuss access control, biometrics techniques and key success factors.

6.1 Access Control

The meaning of access control has changed over the last several years. Originally, access control usually refereed to restricting physical access to a facility, building or room to authorized persons. This used to be enforced mainly through a physical security guard. Then, with the advent of electronic devices, access control has evolved into the use of physical card access systems of a wide variety including biometric activated devices.

As computers evolved the meaning of access control began to change. Initially "access control lists" evolved specifying the user identities and the privileges granted to them in order to access a network operating system or an application.

Access control further evolved into the authentication, authorization and audit of a user for a session. Access control authentication devices evolved to include id and password, digital certificates, security tokens, smart cards and biometrics.

Access control authorization meanwhile evolved into Role based Access Control (RBAC). This normally involves "mandatory access control".

RBAC is commonly found in government, military and other enterprises where the role definitions are well defined, the pace of change is not that fast and the supporting human resource environment is capable of keeping up with changes to an identity re their roles and privileges.

Access control is the process by which users are identified and granted certain privileges to information, systems, or resources. Understanding the basics of access control is fundamental to understanding how to manage proper disclosure of information.

Access control is the ability to permit or deny the use of a particular resource by a particular entity. Access control mechanisms can be used in managing physical resources (such as a movie theater, to which only ticketholders should be admitted), logical resources (a bank account, with a limited number of people authorized to make a withdrawal), or digital resources

Example: Digital resources includes a private text document on a computer, which only certain users should be able to read.

Today, in the age of digitization, there is a convergence between physical access control and computer access control. Modern access control (more commonly referred to in the industry as "identity management systems") now provide an integrated set of tools to manage what a user can access physically, electronically and virtually as well as providing an audit trail for the lifetime of the user and their interactions with the enterprise.

Modern access control systems rely upon:

1. Integrated enterprise user and identity databases and Lightweight Directory Access Protocol (LDAP) directories.

2. Strong business processes pertaining to the provisioning and de-provisioning of a user.
3. Provisioning software integrated with the business provisioning and de-provisioning process.
4. Site, building and room based access control systems that are LDAP enabled or, able to be integrated into a virtual enterprise LDAP directory.
5. A global enterprise id for each user to integrate the user's identity between many applications and systems.
6. A strong end to end audit of everywhere the physical person went as well as the systems, application and information systems they accessed.

With many portions of an enterprise now outsourced, the challenges to access control have increased. Today it is becoming common to have contractual agreements with the enterprise's outsource partners that:

1. Automatically provision and de-provision users.
2. Build trusted authentication and authorization mechanisms.
3. Provide end to end user session audit.
4. Integrate with the remote user's physical access, e.g., to a call center operating on the enterprise's behalf.

Controlling how network resources are accessed is paramount to protecting private and confidential information from unauthorized users. The types of access control mechanisms available for information technology initiatives today continues to increase at a breakneck pace.

Most access control methodologies are based on the same underlying principles. If you understand the underlying concepts and principles, you can apply this understanding to new products and technologies and shorten the learning curve so you can keep pace with new technology initiatives.

Access control devices properly identify people, and verify their identity through an authentication process so they can be held accountable for their actions. Good access control systems record and timestamp all communications and transactions so that access to systems and information can be audited at later dates.

Reputable access control systems all provide authentication, authorization, and administration. Authentication is a process in which users are challenged for identity credentials so that it is possible to verify that they are who they say they are.

Notes Once a user has been authenticated, authorization determines what resources a user is allowed to access. A user can be authenticated to a network domain, but only be authorized to access one system or file within that domain. Administration refers to the ability to add, delete, and modify user accounts and user account privileges.

Did u know? **What is Mandatory access control?**

Mandatory access control is access control policies that are determined by the system and not the application or information owner.

6.1.1 Access Control Objectives

The primary objective of access control is to preserve and protect the confidentiality, integrity, and availability of information, systems, and resources. Many people confuse confidentiality with integrity. Confidentiality refers to the assurance that only authorized individuals are able to view and access data and systems.

Integrity refers to protecting the data from unauthorized modification. You can have confidentiality without integrity and vice versa. It's important that only the right people have access to the data, but it's also important that the data is the right data, and not data that have been modified either accidentally or on purpose.

Availability is certainly less confusing than confidentiality or integrity. While data and resources need to be secure, they also need to be accessible and available in a timely manner. If you have to open 10 locked safes to obtain a piece of data, the data is not very available in a timely fashion. While availability may seem obvious, it is important to acknowledge that it is a goal so that security is not overdone to the point where the data is of no use to anyone.

Self Assessment

Fill in the blanks:

1. .... is the process by which users are identified and granted certain privileges to information, systems, or resources.
2. .... refers to protecting the data from unauthorized modification.
3. .... refers to the assurance that only authorized individuals are able to view and access data and systems.

6.2 User Identification and Authentication

Authentication is any process by which you verify that someone is who they claim they are. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints. Authentication is equivalent to showing your drivers license at the ticket counter at the airport.

Authorization is finding out if the person, once identified, is permitted to have the resource. This is usually determined by finding out if that person is a part of a particular group, if that person has paid admission, or has a particular level of security clearance. Authorization is equivalent to checking the guest list at an exclusive party, or checking for your ticket when you go to the opera.

Finally, access control is a much more general way of talking about controlling access to a web resource. Access can be granted or denied based on a wide variety of criteria, such as the network address of the client, the time of day, the phase of the moon, or the browser which the visitor is using.

Access control is analogous to locking the gate at closing time, or only letting people onto the ride who are more than 48 inches tall - its controlling entrance by some arbitrary condition which may or may not have anything to do with the attributes of the particular visitor.

Because these three techniques are so closely related in most real applications, it is difficult to talk about them separate from one another. In particular, authentication and authorization are, in most actual implementations, inextricable.

If you have information on your web site that is sensitive, or intended for only a small group of people, the techniques in this tutorial will help you make sure that the people that see those pages are the people that you wanted to see them.

Determining if a user is authorized to use an IT system includes the distinct steps of identification and authentication. Identification concerns the manner in which a user provides his unique identity to the IT system. The identity may be a name (e.g., first or last) or a number (e.g., account number). The identity must be unique so that the system can distinguish among different users. Depending on operational requirements, one "identity" may actually describe one individual, more than one individual, or one (or more) individual's only part of the time.

Example: An identity could be "system security officer," which could denote any of several individuals, but only when those individuals are performing security officer duties and not using the system as an ordinary user. The identity should also be non-forcible so that one person cannot impersonate another.

Additional characteristics, such as the role a user is assuming (for example, the role of database administrator), may also be specified along with an identity. Authentication is the process of associating an individual with his unique identity, that is, the manner in which the individual establishes the validity of his claimed identity. There are three basic authentication means by which an individual may authenticate his identity.

1. Something an individual KNOWS (e.g., a password, Personal ID Number (PIN), the combination to a lock, a set of facts from a person's background).
2. Something an individual POSSESSES (e.g., a token or card, a physical key to a lock).
3. Something an individual IS (e.g., personal characteristics or "biometrics" such as a fingerprint or voice pattern).

These basic methods may be employed individually, but many user login systems employ various combinations of the basic authentication methods.

> *Notes* An important distinction between identification and authentication is that identities are public whereas authentication information is kept secret and thus becomes the means by which an individual proves that he actually is who he claims to be. In addition, identification and authentication provides the basis for future access control.

Self Assessment

Fill in the blanks:

4. .... is finding out if the person, once identified, is permitted to have the resource.
5. .... concerns the manner in which a user provides his unique identity to the IT system.
6. .... is the process of associating an individual with his unique identity, that is, the manner in which the individual establishes the validity of his claimed identity.

Notes

6.3 Biometric Devices

Biometric devices authenticate users to access control systems through some sort of personal identifier such as a fingerprint, voiceprint, iris scan, retina scan, facial scan, or signature dynamics. The nice thing about using biometrics is that end-users do not lose or misplace their personal identifier. It's hard to leave your fingers at home. However, biometrics have not caught on as fast as originally anticipated due to the false positives and false negatives that are common when using biometric technologies.

Biometric authentication systems employ unique physical characteristics (or attributes) of an individual person in order to authenticate the person's identity. Physical attributes employed in biometric authentication systems include fingerprints, hand geometry, hand -written signatures, retina patterns and voice patterns. Biometric authentication systems based upon these physical attributes have been developed for computer login applications.

Self Assessment

Fill in the blank:

7. .... devices authenticate users to access control systems through some sort of personal identifier such as a fingerprint, voiceprint, iris scan, retina scan, facial scan, or signature dynamics.

6.4 Biometric Techniques

The various biometrics techniques are discussed below:

6.4.1 Face Recognition

The biometric system can robotically identify a person by the face. This technology functions by analyzing particular traits in the face such as - the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin ,unique shape, pattern etc. These systems include dimensions of the eyes, nose, mouth, and other facial features for identification. To rise accuracy these systems also may measure mouth and lip movement. Face recognition captures traits of a face either from video or still image and converts unique traits of a face into a set of numbers. These data gathered from the face are mixtured in a single unit that uniquely recognizes identifies each person. Sometime the traits of the face are examined like the ongoing modifications in the face while smiling or crying or reacting to dissimilar situation, etc. The whole face of the person is taken into consideration or the other part of the face is taken into consideration for the recognition of a person. It is very complicated technology. The data capture by means of video or thermal imaging. The user identity is assured by looking at the screen. The primary advantage to using facial recognition as a biometric authenticator is that people are adapted to presenting their faces for identification and rather than ID card or photo identity card this method will be beneficial in recognizing a person.

⚠ *Caution* As the person faces alters by the age or person goes for plastic surgery, in this case the facial recognition algorithm should gauge the relative position of ears, noses, eyes and other facial traits.

6.4.2 Hand Geometry

Hand geometry is a method that captures the physical traits of a user's hand and fingers. It examines finger image ridge endings, branches made by ridges. These systems gauge and record the length, width, thickness, and surface area of an individual's hand. It is accessed in applications like access control and time and attendance etc. It is easy to use, relatively not costly and broadly accepted. A camera captures a three dimensional image of the hand. A verification template is formed and accumulated in the database and is compared to the template at the time of confirmation of a person. Fingerprint identification. Presently fingerprint readers are being constructed into computer memory cards for use with laptops or PCs and also in cellular telephones, and personal digital assistants. It is successfully executed in the area of physical access control.

6.4.3 Eye Recognition

This method includes scanning of retina and iris in eye. Retina scan method maps the capillary pattern of the retina, a thin nerve on the back of the eye. A retina scan gauges patterns at over 400 points. It examines the iris of the eye, which is the colored ring of tissue that surrounds the pupil of the eye. This is a very mature technology with a proven track record in a number of application areas. Retina scanning captures individual pattern of blood vessels where the iris scanning captures the iris. The user must focus on a point and when it is in that position the system accesses a beam of light to capture the unique retina traits. It is broadly secure and accurate and used heavily in controlled environment. However, it is expensive, secure and needs perfect alignment and generally the user must look in to the device with proper focus. Iris recognition is one of the most reliable biometric recognition and verification methods. It is accessed in airports for travellers. Retina scan is used in military and government organization. Organizations use retina scans initially for authentication in high-end security applications to control access.

Example: Government buildings, military operations or other limited quarters, to authorized personnel only.

The unique pattern and traits in the human iris remain unchanged during one's lifetime and no two persons in the world can have the same iris outline.

6.4.4 Voice Biometrics

Voice biometrics, accesses the person's voice to verify or recognize the person. It confirms as well as identifies the speaker. A microphone on a standard PC with software is needed to examine the unique traits of the person. It is mainly used in telephone-based applications. Voice verification is simple to use and does not need a great deal of user education. To enroll, the user speaks a provided pass phrase into a microphone or telephone handset. The system then forms a template based on various traits, including pitch, tone, and shape of larynx. Generally, the enrollment procedure takes less than a minute for the user to accomplish. Voice verification is one of the least intrusive of all biometric methods. Moreover, voice verification is simple to use and does not need a great deal of user education.

Task Discuss the functioning of voice biometrics.

6.4.5 Signature Verification

Signature verification technology is the examination of an individual's written signature, involving the speed, acceleration rate, stroke length and pressure applied during the signature. There are diverse methods to capture data for analysis i.e. a special pen can be used to identify and examine analyze various movements when writing a signature, the data will then be obtained within the pen. Information can also be captured among a special tablet that gauges time, pressure, acceleration and the duration the pen touches it. As the user writes on the tablet, the movement of the pen produces sound against paper an is used for verification. An individual's signature can modify over time, though, which can effect in the system not identifying authorized users. Signature systems depend on the device such as special tablet, a special pen etc. When the user signs his name on an electronic pad, instead of merely comparing signatures, the device instead compares the direction, speed and pressure of the writing instrument as it moves across the pad.

Task Explain the process of signature verification.

6.4.6 Keystroke

This technique depends on the fact that each person has her/his own keyboard-melody, which is examined when the user types. It gauges the time taken by a user in pressing a specific key or looking for a particular key.

Other biometric techniques are:

1. *Vein/vascular patterns:* Analyses the veins in, for example, the hand and the face.
2. *Nail identification:* Analyses the tracks in the nails.
3. *DNA patterns:* it is a very expensive technique and it takes a long time for verification/identification of a person.
4. *Sweat pore analysis:* Analyses the way pores on a finger are located.
5. *Ear recognition:* Shape and size of an ear are unique for every person.
6. *Odour detection:* Person is verified or identified by their smell.
7. *Walking recognition:* It analyses the way the person walks.

Self Assessment

Fill in the blanks:

8. .... method captures traits of a face either from video or still image and converts unique traits of a face into a set of numbers.
9. .... is a method that captures the physical traits of a user's hand and fingers. It examines finger image ridge endings, branches made by ridges.
10. .... biometrics accesses the person's voice to verify or recognize the person.
11. .... technology is the examination of an individual's written signature, involving the speed, acceleration rate, stroke length and pressure applied during the signature.
12. .... technique depends on the fact that each person has her/his own keyboard-melody, which is examined when the user types.

6.5 Key Success Factors

For any effectual biometrics system, there are a some significant factors related with it: accuracy, speed and throughput rate, acceptance by users, exclusiveness of biometrics organ and action, reliability, data storage needs, enrolment time, intrusiveness of data collection, etc.

Effective performance of biometrics system would rely on these factors as discussed below.

6.5.1 Accuracy

It is the most important trait of a biometric identification verification system. If the system cannot correctly separate an authentic person from an imposter, it should not be considered a biometrics identification system. There are two concerns that occurs-false rejection rate (FRR) and false acceptance rate (FAR):

1. ***FRR:*** This rate is usually articulated as a percentage. It is the rate at which authentic, enrolled persons are discarded as anonymous persons by a biometrics system. It is also called Type 1 error. When FRR increase, it may be fine if it is a tight security area such as defense or medical foundation but not fine if it is a retail business. FAR is a reverse condition. This is the rate at which unenrolled persons are established as authentic, enrolled persons by a biometrics system. FAR is also called Type II error.
2. ***Crossover Error Rate (CER):*** It is the rate at which FAR and FRR compares. It is also called EER and is specified as a percentage. This is the most significant measure of biometrics system accuracy. ERR or CER displays the accuracy level at which the probability of a false non-match.

Did u know? **Full form of ERR**

Equal Error Rate.

6.5.2 Speed and Throughput Rate

For biometrics system classification, speed and throughput are imperative. Data-processing ability of the biometrics system decides the speed; it is declared as how fast the accept or reject decision is articulated. It associates to the authentication procedure; the system setup, card input or PIN; inputting the physical data by inserting the hand or finger, aligning the eye speaking access words or signing a name processing and matching of data files, etc. A system speed of 5s of start up via decision enunciation is good as per usually accepted standards. Another standard is a portal throughput rate of 6-10 per min, which is equal to 6-10 s per person through the door.

Caution Regardless of great strides in the biometrics research, it is not simple for most biometrics systems to meet these standards.

6.5.3 Acceptability by Users

User acceptability to-date is a big confront for enveloping deployment of biometrics systems, this is mainly owing to the social sigma linked to the biometrics system provided their nature and lack of adequate responsiveness on biometrics identification system. Biometric system acceptance appears when those who must access the system, that is, management and unions concerned in the organizations, need to come to an agreement that biometrics should be deployed for the protection of organizational assets. Also consider the social sigma factor mentioned as well as the lack of awareness; fingerprinting is a chiefly sensitive topic, given that it is linked with criminals. Eye retina scanning requires users to trust that the system will not harm their eyes, a feeling they carry perhaps owing to rumors and insufficient information concerning how the retinal scanning technology functions.

6.5.4 Uniqueness of Biometrics Organ and Action

The intention of biometrics system is positive identification of the personnel- specified this, it is significant that the systems are based on unique traits of the employees. So when the base is exclusive trait, a file match is a positive identification instead of a statement of high probability that it is the right person. Out of the many physical traits that can be used, only three can actually be considered unique enough for recognition: the fingerprint, the retina of the eye and the iris of the eye.

6.5.5 Reliability of Biometrics

When using biometrics verification systems, it is significant that they function in an accurate fashion. The notion of system's reliability is connected to its 'selectivity'. Reliability is a prospect that a matcher system will properly identify the mate when the mate is present in the system repository, while selectivity is the number of incorrect mates determined for a specified search.

Only authorized persons must be permissible to access and it must prevent the others without breakdown in performance correctness or speed.

Did u know? The tradeoff between reliability and selectivity provides the greatest system design challenge as these parameters are interdependent.

6.5.6 Data Storage Requirements in Biometrics System

Earlier computer systems had primary and secondary memory size constraints, that are restricted RAM and disk size. This is less of an concern today as computer technology has advanced in both hardware and software. Even then, the size of biometrics data files is still a factor of interest. Provided the large size of biometrics match templates, even with the current ultra-high speed processors, large data files take longer than small files to process. This is particularly so in biometrics systems that performs full identification. Typically, biometrics file size varies between 9 and 10,000 bytes, mostly falling in the 256-1,000 byte range.

6.5.7 Enrolment Time in Biometrics

We have discussed 'matching and enrolment'; enrolment time is also so much of a concern these days. In the previous days, biometrics system sometimes had enrolment process requiring many repetitions and numerous minutes to completes.

6.5.8 Ata Collection Intrusiveness

Origins of this factor come from the user's apprehension regarding the collection of biometrics data from inside the human body- particularly the retina inside the eyeball. Early biometrics systems enlightened the retina with a red light beam that happened to coincide with increasing public awareness of lasers, sometimes demonstrated as red light beams cutting steel. Although there has been never any harm reported owing to retinal scans by means of the light beams, public fear and user sensitivity still remain. An advance form of such public issue is about intrusions into human body, a space that is measured private.

Self Assessment

Fill in the blanks:

13. .... is the rate at which authentic, enrolled persons are discarded as anonymous persons by a biometrics system.

14. .... ability of the biometrics system decides the speed.

15. .... a prospect that a matcher system will properly identify the mate when the mate is present in the system repository.

Caselet

Bartronics Unveils Biometric Products

BARTRONICS India Ltd (BIL), an automatic identification and data collection (AIDC) solution provider, on Friday launched a multi-layered embedded fused biometric security system (MLEFBS) and a touchless fingerprint system (TFPS) that use multiple biometric features for identification purposes.

According to Mr Sudhir Rao, Managing Director, MLEFBS offers a solution for authentication, authorisation, verification and identification management.

It provides integrated support for smart cards, tokens and biometric (voice, iris, vein, face, hand, fingerprint and signature) identifiers.

On the other hand, TFPS incorporates a contact-less finger print sensor that overcomes the drawbacks of existing fingerprint scanners.

Mr Rao told newspersons that BIL had recently tied up with the Singapore-based emBiosys Pte Ltd for introduction of fused biometric systems in the Indian market.

The company has already received enquiries from various quarters including the Defence, the Home Ministry and airports for installation of the systems that would cost ₹ 4-5 lakh each.

BIL is currently implementing its biometric applications at the Sri Venkateswara temple at Tirumala. The company has a two-year contract with the Tirumala Tirupati Devasthanams Trust Board for providing the services at a rate of ₹ 1.5 crore per year.

With an estimated 40,000 pilgrims visiting the Tirumala shrine every day, this is claimed to be the largest biometric application in the world.

Mr Rao said that the market for AIDC in the country is estimated to be ₹ 60 crore and is growing at a rate of 20 per cent per annum over the past four years.

BIL has a 25 per cent share in this market, while the rest of the market was widely fragmented among many players. About 80 per cent of the top 100 companies in the country are its clients.

Source: http://www.thehindubusinessline.in/2003/12/27/stories/2003122701860200.htm

6.6 Summary

- Biometric devices authenticate users to access control systems through some sort of personal identifier such as a fingerprint, voiceprint, iris scan, retina scan, facial scan, or signature dynamics.
- Originally, access control usually refereed to restricting physical access to a facility, building or room to authorized persons.
- Access control is the process by which users are identified and granted certain privileges to information, systems, or resources.
- The primary objective of access control is to preserve and protect the confidentiality, integrity, and availability of information, systems, and resources.
- Authentication is any process by which you verify that someone is who they claim they are. This usually involves a username and a password, but can include any other method of demonstrating identity, such as a smart card, retina scan, voice recognition, or fingerprints.
- Face recognition technology functions by analyzing particular traits in the face such as — the distance between the eyes, width of the nose, position of cheekbones, jaw line, chin, unique shape, pattern, etc.
- Voice biometrics, accesses the person's voice to verify or recognize the person. It confirms as well as identifies the speaker.
- Signature verification technology is the examination of an individual's written signature, involving the speed, acceleration rate, stroke length and pressure applied during the signature.
- When using biometrics verification systems, it is significant that they function in an accurate fashion.

6.7 Keywords

Access Control: It is the process by which users are identified and granted certain privileges to information, systems, or resources.

Access Control Device: It properly identifies people, and verifies their identity through an authentication process so they can be held accountable for their actions.

Authentication: It is a process by which you verify that someone is who they claim they are.

Authorization: It is finding out if the person, once identified, is permitted to have the resource.

Smart Card: It is a device typically the size and shape of a credit card and contains one or more integrated chips that perform the functions of a computer with a microprocessor, memory, and input/output.

6.8 Review Questions

1. What is access control? What are the implementation challenges?
2. Discuss the objectives of access control.
3. Explain the concept of User Identification and Authentication.

Notes

4. What are the basic authentication means by which an individual may authenticate his identity?
5. What are the various biometrics techniques used for identification? Discuss.
6. Make distinction between face recognition and eye recognition.
7. Explain the factors based on the performance of the biometrics system.
8. Compare and contrast between memory card and smart card.
9. Explicate the concept of biometric authentication systems.
10. Differentiate between the RB-RBAC and RBAC.

Answers: Self Assessment

1. Access control
2. Integrity
3. Confidentiality
4. Authorization
5. Identification
6. Authentication
7. Biometric
8. Face recognition
9. Hand geometry
10. Voice
11. Signature verification
12. Keystroke
13. False rejection rate (FRR)
14. Data-processing
15. Reliability

6.9 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online link

idwarehouse.com.au/

Notes

Unit 7: Network Security

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of networking and network types
- Discuss the concept of computer security and network security
- Explain trusted and untrusted networks
- Understand the concept of unknown attacks

Introduction

In this day and age, networks are everywhere. The Internet has also revolutionized not only the computer world, but the lives of millions in a variety of ways even in the "real world". We tend to take for granted that computers should be connected together. A basic understanding of computer networks is requisite in order to understand the principles of network security.

Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and consistent and continuous monitoring and measurement of its effectiveness (lack) combined together.

Firstly we should understand the concept of networking.

7.1 Networking

A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate. Networking is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

7.1.1 Benefits of Networks

You have undoubtedly heard that "the whole is greater than the sum of its parts". This phrase describes networking very well, and explains why it has become so popular. A network isn't just a bunch of computers with wires running between them. Properly implemented, a network is a system that provides its users with unique capabilities, above and beyond what the individual machines and their software applications can provide.

Here, in no particular order, are some of the specific advantages generally associated with networking:

1. ***Connectivity and Communication:*** Networks connect computers and the users of those computers. Individuals within a building or work group can be connected into Local Area Networks (LANs); LANs in distant locations can be interconnected into larger Wide Area Networks (WANs). Once connected, it is possible for network users to communicate with each other using technologies such as electronic mail. This makes the transmission of business (or non-business) information easier, more efficient and less expensive than it would be without the network.

2. ***Data Sharing:*** One of the most important uses of networking is to allow the sharing of data. Before networking was common, an accounting employee who wanted to prepare a report for her manager would have to produce it on his PC, put it on a floppy disk, and then walk it over to the manager, who would transfer the data to her PC's hard disk. (This sort of "shoe-based network" was sometimes sarcastically called a "sneakernet".)

   True networking allows thousands of employees to share data much more easily and quickly than this. More so, it makes possible applications that rely on the ability of many people to access and share the same data, such as databases, group software development, and much more. Intranets and extranets can be used to distribute corporate information between sites and to business partners.

3. ***Hardware Sharing:*** Networks facilitate the sharing of hardware devices.

Notes

Example: Instead of giving each of 10 employees in a department an expensive color printer (or resorting to the "sneakernet" again), one printer can be placed on the network for everyone to share.

- ***Internet Access:*** The Internet is itself an enormous network, so whenever you access the Internet, you are using a network. The significance of the Internet on modern society is hard to exaggerate, especially for those of us in technical fields.
- ***Internet Access Sharing:*** Small computer networks allow multiple users to share a single Internet connection. Special hardware devices allow the bandwidth of the connection to be easily allocated to various individuals as they need it, and permit an organization to purchase one high-speed connection instead of many slower ones.
- ***Data Security and Management:*** In a business environment, a network allows the administrators to much better manage the company's critical data. Instead of having this data spread over dozens or even hundreds of small computers in a haphazard fashion as their users create it, data can be centralized on shared servers. This makes it easy for everyone to find the data, makes it possible for the administrators to ensure that the data is regularly backed up, and also allows for the implementation of security measures to control who can read or change various pieces of critical information.
- ***Performance Enhancement and Balancing:*** Under some circumstances, a network can be used to enhance the overall performance of some applications by distributing the computation tasks to various computers on the network.
- ***Entertainment:*** Networks facilitate many types of games and entertainment. The Internet itself offers many sources of entertainment, of course. In addition, many multi-player games exist that operate over a local area network. Many home networks are set up for this reason, and gaming across wide area networks (including the Internet) has also become quite popular. Of course, if you are running a business and have easily-amused employees, you might insist that this is really a disadvantage of networking and not an advantage.

Notes Most of the benefits of networking can be divided into two generic categories: connectivity and sharing. Networks allow computers, and hence their users, to be connected together. They also allow for the easy sharing of information and resources, and cooperation between the devices in other ways. Since modern business depends so much on the intelligent flow and management of information, this tells you a lot about why networking is so valuable.

Self Assessment

Fill in the blanks:

1. A .... is simply a collection of computers or other hardware devices that are connected together,
2. .... is the term that describes the processes involved in designing, implementing, upgrading, managing and otherwise working with networks and network technologies.

7.2 Network Types

7.2.1 Local Area Networks (LANs)

Networks that connect computers lying within a small distance (such as a room, or within a building) from each other are called Local Area Networks (LANs). A Local Area Network (LAN) is a group of computers and associated devices that share a common communications line or wireless link and share the resources of a single processor or server within a small geographic area usually within an office building. Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or as many as thousands of users.

Example: An FDDI network

LANs have become commonplace in many organizations for providing telecommunications network capabilities that link end users in offices, departments, and other work groups.

Ethernet is by far the most commonly used LAN technology. A number of corporations use the Token Ring technology. FDDI is sometimes used as a backbone LAN interconnecting Ethernet or Token Ring LANs. Another LAN technology, ARCNET, once the most commonly installed LAN technology, is still used in the industrial automation industry. In some situations, a wireless LAN may be preferable to a wired LAN because it is cheaper to install and maintain.

A suite of application programmes can be kept on the LAN server. Users who need an application frequently can download it once and then run it from their local hard disk. Users can order printing and other services as needed through applications run on the LAN server. A user can share files with others at the LAN server; read and write access is maintained by a LAN administrator. A LAN server may also be used as a Web server if safeguards are taken to secure internal applications and data from outside access.

LAN provides access to more computing power, data, and resources than would be practical if each user needed an individual copy of everything.

LAN provides the benefits of personal computing. One is not forced to do personal work through a central computer that may not be able to respond to the users' requests when many of them share its capacity.

LAN can link multiple workstations to one laser printer, fax machine, or modem. This makes a single piece of equipment available to multiple users and avoids unnecessary equipment purchases.

LAN users can select personal files that they want co-workers to see, such as engineering drawings, department plans, contracts, or drafts of memos. Co-workers can look at these files without delays for printing paper copies.

LAN can be used to transmit and manage electronic mail and messages.

LAN also provides access to shared databases. Figure 7.1 shows a LAN system that is set up for this purpose because it contains a file server for retrieving data requested by the workstations. The file server is linked to a disk that contains shared databases, such as the firm's customer list and telephone directory. When a workstation needs data in a shared database, it sends a request message to the file server, which performs the retrieval from the disk and sends the data to the requesting workstation. This arrangement avoids maintaining redundant copies of data.

Caution In addition to not wasting storage, having the databases in one place avoids problems with inconsistent data.

Local area networks normally use coaxial cables to connect the computers together. Two or more computers connected together can share, besides data, their peripherals such as printers, modems, etc. This cuts down a lot on the hardware equipment cost.

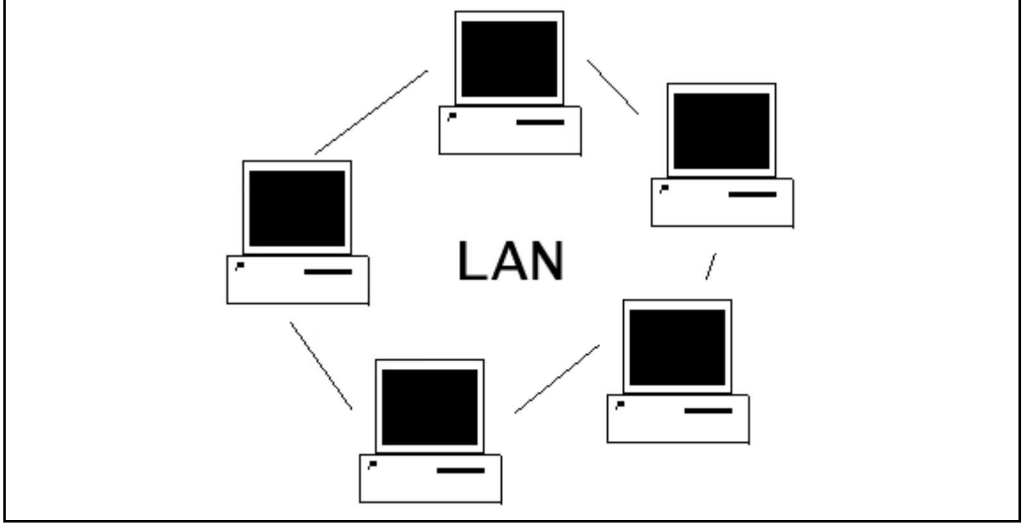
Besides coaxial cables, a plug-in card is also required for each computer. The coaxial cables connect the plug-in cards of the computers to form a network. A special software is also required for the network to operate.

All local area networks transfer data in digital form at a high speed and have a low implementation cost.

Some applications performed by a LAN are as follows:

1. File transfer and access
2. Accessing the internet
3. Providing Management Information System.

Figure 7.1: Local Area Networks



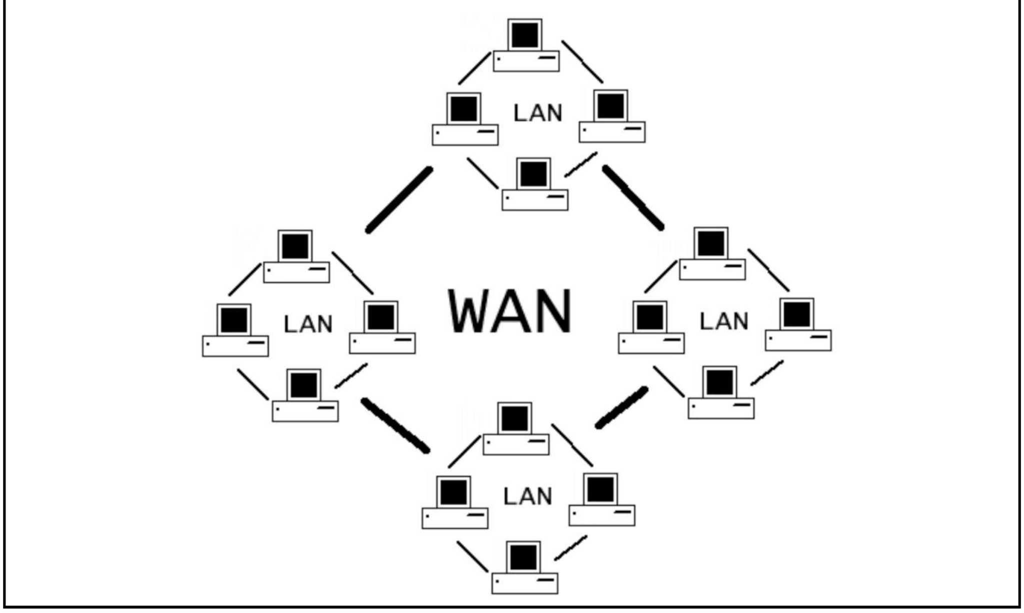
7.2.2 Wide Area Networks (WANs)

A wide area network connects computers which are very remotely placed. It may connect across the countries or continents or the entire globe.

Wide area networks can either be point to point type or broadcast type. In a point to point type network, the source and the destination machines are connected to each other via several intermediate routers. A point to point type network may be separated into two parts — the hosts and the subnet.

The machines between which communication is to be established are called hosts. The hosts are connected to each other by what is known as the subnet. The subnet consists of the transmission lines (coaxial cables, fibre optic cables, etc.) and the intermediate switching elements also called 'routers'.

Figure 7.2: Wide Area Networks



The main function of a router is to receive the transmitted data and then select an appropriate channel to forward it to the destination host or to another router. When a data packet arrives at a router it is stored in the router until the output transmission line is free and is then transmitted or forwarded to destination host.

The broadcast type Wide Area Networks (WANs) use a satellite or ground radio system. All or some routers have antennas through which they can receive the incoming signal from the satellite. When a ground radio system is being used the routers can communicate between each other. It may also be possible that in a network, while some routers receive their outputs through their antennas, others are point to point type.

Did u know? Wide Area Networks are also referred to as Long Haul Networks (LHNs).

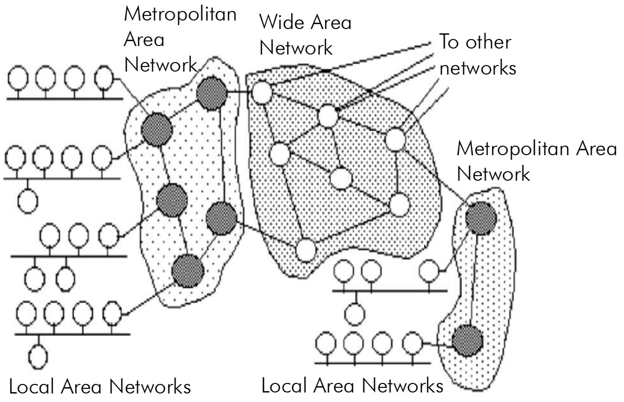
7.2.3 Metropolitan Area Network (MAN)

A Metropolitan Area Network (MAN) is one of a number of types of networks. A MAN is a relatively new class of network; it serves a role similar to an ISP, but for corporate users with large LANs. It is a network that interconnects users with computer resources in a geographical area larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. This is sometimes referred to as a campus network. Large universities also sometimes use the term to describe their networks. A recent trend is the installation of wireless MANs.

Notes

A typical use of MANs to provide shared access to a wide area network is shown in the figure below:

Figure 7.3: The Functioning of MAN



Notes There are three important features which distinguish MANs from LANs or WANs:

1. The network size falls in between LANs and WANs. A MAN typically covers an area of between 5 and 50 km diameter. Many MANs cover an area the size of a city, although in some cases MANs may be as small as a group of buildings.
2. A MAN, like a WAN, is not generally owned by a single organisation. The MAN, its communications links and equipments are generally owned by either a group of users or by a single network provider who sells the service to the users. This level of service provided to each user must be negotiated with the MAN operator, and some performance guarantees are normally specified.
3. A MAN often acts as a high-speed network to allow sharing of regional resources (similar to a large LAN). It is also frequently used to provide a shared connection to other networks using a link to a WAN.

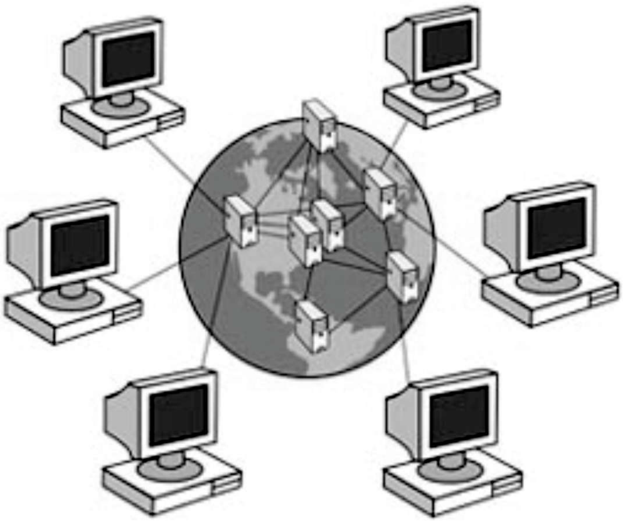
7.2.4 Value Added Network (VAN)

VAN is also an acronym for virtual area network. A value-added network (VAN) is a private network provider that is hired by a company to facilitate Electronic Data Interchange (EDI) or provide other network services. VANs are public networks that add value by transmitting data and by providing access to commercial databases and software. The use of VANs is usually sold by subscription, with users paying for the amount of data they move. VANs are used for a number of reasons. They can be considered as a way of transmitting computerized data, offering a service similar to what the telephone networks do for telephone calls. VANs can send data between computers in different cities or even different countries. They are often used in electronic data interchange (EDI) systems because they reduce the complexity of connecting to the disparate EDI systems of various trading partners.

7.2.5 Internet

The Internet is a worldwide network of computer networks. It is an interconnection of large and small networks around the globe. In other words, it is a global network of networks connecting many millions of computers. Currently, the Internet has more than 30 million users worldwide, and that number is growing rapidly. More than 100 countries are linked into exchanges of data, news and opinions on Web servers.

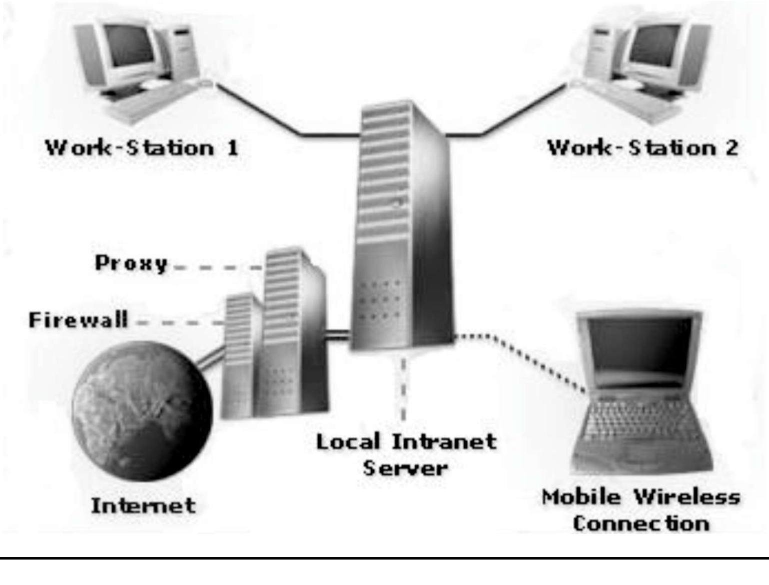
Figure 7.4: The Internet



7.2.6 Intranet

Intranet can be designed as a network connecting an affiliated set of clients using standard Internet protocols, especially TCP/IP and HTTP. Another definition of an intranet would be that an IP-based network of notes behind a firewall, or behind several firewalls connected by secure, possibly virtual, networks. In general, a web is an unstructured client/server network that uses HTTP as its transaction protocol. The World Wide Web comprises all HTTP nodes on the public Internet. An internal web comprises all HTTP nodes on a private network, such as an organization's LAN or WAN. Figure displays the simple model of an organisation's intranet.

Figure 7.5: The Functioning of Intranet



Notes

Task Make distinction between internet and intranet.

7.2.7 Extranet

Extranet can be defined as a 'business-to-business-intranet' that allows limited, controlled, secure access between a company's intranet and designated, authenticated users from remote locations or in other words, an intranet that allows controlled access by authenticated parties. The term intranet and extranet are roughly web-based analogs of LAN (Local Area Network) and WAN (Wide Area Network).

7.2.8 Comparisons

Comparison of different networks on various parameters is shown in the following table:

Parameters	**LAN**	**WAN**
Bandwidth	High	low
Scope	building or campus	city to global
Protocols	diverse	diverse
Security	very high	high
Parameters	**Intranet**	**Extranet**
Bandwidth	high	low
Scope	building or campus	city to global
Protocols	internet	internet
Security	moderate to high	low to moderate

Differences appear with regard to protocol and security. The weaker security of Internet communications relative to leased lines is the reason that terms like controlled and authenticated figure prominently in the definition of extranet.

The relation between intranets, extranets and e-commerce has three parts. First, intranets, extranets and e-commerce have in common the use of Internet protocols to connect business users. Second, intranets are more localized and can therefore move data faster than more distributed extranets. The bandwidth limitations also apply to e-commerce. Third, the amount of control that network managers can exert over users is different for the three technologies.

On an Intranet, administrators can narrowly prescribe access and policy for a fixed group of users.

Example: A company can specify Red Hat Linux as its standard desktop operating system, and Netscape Communicator 5 as its standard browser and mail client. The company can then write intranet workflow applications that leverage the uniform computing environment, over which it exercises strong control.

On a business-to-business extranet, system architects at each of the participating companies must collaborate to ensure a common interface and consistent semantics (data meanings). Since one company cannot reasonably enforce standards on its trading partners, extranet application developers must take into account a wider range of technologies than is the case for intranets.

Example: One company participating in an extranet might be using Microsoft Internet Explorer, another Netscape Navigator 4.5, and another Navigator Gold 3.x.

In order to collaborate via extranet, the applications have to perform adequately on all represented platforms. The same is true for e-commerce, in which the trading partners may be completely unknown to one another. This is the case when we walk into a supermarket: the common interest in communication is based on the need to transact business, and not necessarily on a long-term trust relationship. Thus e-commerce applications often support a level of security and transactional integrity not present in intranet or extranet applications.

Self Assessment

Fill in the blanks:

3. All local area networks transfer data in .... form at a high speed and have a low implementation cost.
4. Wide Area Networks are also referred to as ....
5. .... is a global network of networks connecting many millions of computers.
6. A .... is a private network provider that is hired by a company to facilitate electronic data interchange (EDI) or provide other network services.

7.3 Basic Concepts

Here we will discuss the concept of computer security and network security.

7.3.1 Computer Security

Securing network infrastructure is like securing possible entry points of attacks on a country by deploying appropriate defense. Computer security is more like providing means to protect a single PC against outside intrusion. The former is better and practical to protect the civilians from getting exposed to the attacks.

The preventive measures attempt to secure the access to individual computers – the network itself – thereby protecting the computers and other shared resources such as printers, network-attached storage connected by the network. Attacks could be stopped at their entry points before they spread. As opposed to this, in computer security the measures taken are focused on securing individual computer hosts.

A computer host whose security is compromised is likely to infect other hosts connected to a potentially unsecured network.

Did u know? A computer host's security is vulnerable to users with higher access privileges to those hosts.

7.3.2 Network Security

Attributes of a Secure Network

Network security starts from authenticating any user, most likely a username and a password. Once authenticated, a stateful firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component fails to check potentially harmful contents such as computer worms being transmitted over the network.

An Intrusion Prevention System (IPS) helps detect and prevent such malware. IPS also monitors for suspicious network traffic for contents, volume and anomalies to protect the network from attacks such as denial of service. Communication between two hosts using the network could be encrypted to maintain privacy. Individual events occurring on the network could be tracked for audit purposes and for a later high level analysis.

Honeypots, essentially decoy network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new exploitation techniques. Such analysis could be used to further tighten security of the actual network being protected by the honeypot.

Security Management for Networks

Security Management for networks is different for all kinds of situations. A small home or an office would only require basic security while large businesses will require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming.

Small Homes

1. A basic firewall.
2. For Windows users, basic Anti-virus software like McAfee, Norton AntiVirus or AVG Antivirus.
3. An anti-spyware program such as Windows Defender or Spybot would also be a good idea. There are many other types of antivirus or antispyware programs out there to be considered.
4. When using a wireless connection, use a robust password. Also try and use the strongest security supported by your wireless devices, such as WPA or WPA2.

Medium Businesses

1. A fairly strong firewall.
2. Strong Antivirus software and Internet Security Software.
3. For authentication, use strong passwords and change it on a biweekly/monthly basis.
4. When using a wireless connection, use a robust password.
5. Raise awareness about physical security to employees.
6. Use an optional network analyzer or network monitor.

Large Businesses

1. A strong firewall and proxy to keep unwanted people out.
2. A strong Antivirus software package and Internet Security Software package.
3. For authentication, use strong passwords and change it on a weekly/biweekly basis.

4. When using a wireless connection, use a robust password.
5. Exercise physical security precautions to employees.
6. Prepare a network analyzer or network monitor and use it when needed.
7. Implement physical security management like closed circuit television for entry areas and restricted zones.
8. Security fencing to mark the company's perimeter.
9. Fire extinguishers for fire-sensitive areas like server rooms and security rooms.
10. Security guards can help to maximize security.

School

1. An adjustable firewall and proxy to allow authorized users access from the outside and inside.
2. Strong Antivirus software and Internet Security Software packages.
3. Wireless connections that lead to firewalls.
4. Children's Internet Protection Act compliance.
5. Supervision of network to guarantee updates and changes based on popular site usage.
6. Constant supervision by teachers, librarians, and administrators to guarantee protection against attacks by both internet and sneakernet sources.

Large Government

1. A strong firewall and proxy to keep unwanted people out.
2. Strong Antivirus software and Internet Security Software suites.
3. Strong encryption, usually with a 256 bit key.
4. Whitelist authorized wireless connection, block all else.
5. All network hardware is in secure zones.
6. All host should be on a private network that is invisible from the outside.
7. Put all servers in a DMZ, or a firewall from the outside and from the inside.
8. Security fencing to mark perimeter and set wireless range to this.

Self Assessment

Fill in the blanks:

7. .... is more like providing means to protect a single PC against outside intrusion.
8. A computer host whose security is compromised is likely to infect other hosts connected to a potentially .... network.
9. Communication between two hosts using the network could be encrypted to maintain ....

Notes

7.4 Trusted and Untrusted Networks

7.4.1 Trusted Network

Trusted networks are defined as "the networks within your security boundary, and are typically the networks you are trying to defend."

Computers on the trusted network can clearly access such departmental services as NFS (home and project disks), NIS (distributed account and other information), printers, software packages, etc. Access to this network is restricted to machines supervised by the Lab Staff, so as to protect sensitive data and uphold the accessibility of departmental resources. A current list of machines on the trusted network can be located here.

Caution Users should not effort to attach their individual machines to this network.

7.4.2 Untrusted Network

Mostly, computers on the untrusted network are managed and configured by their possessors. Because this could potentially permit improper access to sensitive or private data, or could cause operational trouble to the production computer network, these machines are cut off on a separate subnet, and are not specified direct access to many core departmental computer services.

Untrusted network is considered as "the networks external your security perimeter. They are untrusted since they are frequently away from your control." Alternatively, untrusted networks are those that may provide services or information that you require to access, but since you are not in control of supervising these networks, they are "untrusted" in the sense that you restrict the communications among them and your network.

Example: An example of this might be a client network you attach to obtain access to some information.

There are also "unknown" networks, which would comprise any network not purposely defined in your firewall's configuration, which would comprise the majority of the networks you see on the Internet.

Self Assessment

Fill in the blanks:

10. .... networks are defined as "the networks within your security boundary, and are typically the networks you are trying to defend."

11. .... network is considered as "the networks external your security perimeter.

12. Untrusted networks are also "................." networks, which would comprise any network not purposely defined in your firewall's configuration, which would comprise the majority of the networks you see on the Internet.

7.5 Unknown Attacks

To avoid highly injurious "superworms" or hackers by means of unknown or unpatched exploits, unusual solutions are required that are intended to avert and react to unknown attacks, instead of known attacks. These methods would like to be automated (as human responses are too slow to avert damage), executable, broadly deployable, and must need no application modifies. Here we will study three technologies that provide imperative levels of protection against unknown attacks: software fault isolation, intrusion detection through program analysis, and fine-grained mandated access controls.

These technologies distribute an imperative property: they do not depend on the accurate operation of the programs; instead, they offer a secondary layer of protection should a program be breached and corrupted. It is possible that these systems may also enclose flaws; but in order for a victorious exploit to take place, both the application and the secondary protection need to be undermined at the same time. As bugs will carry on to be patched, it is much less expected that two overlap bugs will be present and be known concurrently than that a single error will be known.

7.5.1 Software Fault Isolation

The first expertise, Software Fault Isolation (SFI), produced by Wahbe et al. is a method to generate Java-like sandboxes for dynamically-loading random code in a language-neutral manner. Unlike JVM-based systems, it can be functional in spite of source language and compiler. The only semantic restraint is that dynamic code generation is not permitted inside a fault-isolated module.

SFI functions at the assembly level on a code module via a amalgamation of static analysis and dynamic checks to generate the sandbox. The system provides each module its own concealed memory space in which it is isolated as part of the bigger program. The static checks make certain that all statically determinable jumps only appear within the module and to permissible external functions, forming the basic structure of the sandbox.

The dynamic checks are inserted onto every load, store, and dynamic jump (apart from for those that can be deleted through static analysis) to make sure that the program can't flee the sandbox produced by the static analysis and assigned private memory. These checks do not guarantee fine-grained accuracy (like bounds checking) but only a coarse-grained correctness: the module is not permitted to read or write outside its permissible memory ranges or carry out code not enclosed within the module's code base or permitted external functions. Because the module is now limited both statically and dynamically, it is efficiently sandboxed from other modules inside a larger application.

7.5.2 Intrusion Detection by Program Analysis

The second most important technique, host-based intrusion detection by program analysis, was first projected and experienced by Wagner and Dean. This IDS executes a static analysis of the program to generate an abstract, non-deterministic automata model of the function and system calls. While the program is implementing, it matches the system call pattern with a running copy of the automata. If the program ever tries a system call which disobeys the model, the system assumes that a burglar has tainted the program.

Dissimilar to other intrusion detection methods which depend on either sample inputs or rule sets, this technique has a demonstrable zero false positive rate, removing all false alarms. This means the intrusion detection system can begin automatic responses: blocking the system call, shutting down the corrupted program, and alerting the administrator. The zero false positive rate is because of the programmatic nature of the IDS, which encloses a model that displays all possible legal paths via the program, making sure that any detected deviation from the model is not caused by the program's code but by code inserted by a virus or an attacker.

The biggest issue is the very elevated run time needed for the IDS to function. This is because of imprecision in the model of implementation since the IDS only have access to system call information from the running program. There are two solutions: the first is to have the IDS walk the stack to find out the program's call state before permitting a system call, which greatly increases the accuracy. The second has the IDS that is altering the binaries to numerous function calls send information about their incantation to the IDS system.

The other chief drawback is the incapability to manage multi-threaded programs without an overt method to detect the incidence of a thread switch. This is not a difficulty for most UNIX programs, but is a major problem if one would like to apply this method to Windows systems, which rely more heavily on user threads. Yet the same performance-enhancing solution of program annotation can be used to conquer this drawback by transmitting when thread switches happen.

A Code Red-style worm would be able to divide into a system sheltered by such an IDS, but the potential harm would be greatly restricted. It would be simple to deface Web pages by replacing the routines that transport the content to pages that return erroneous content although even though they may act identically at the system call level. As such behavior is not included in the original program, the IDS would discontinue the program before harm could be done.

Task Discuss the drawbacks of Intrusion Detection by Program Analysis technique.

Self Assessment

Fill in the blanks:

13. To avoid highly injurious "superworms" or hackers by means of unknown or unpatched exploits, unusual solutions are required that are intended to avert and react to .... attacks, instead of known attacks.

14. .... is a method to generate Java-like sandboxes for dynamically-loading random code in a language-neutral manner.

15. The .... executes a static analysis of the program to generate an abstract, non-deterministic automata model of the function and system calls.

Caselet

CERT-in to Empanel Network Security Auditors

IN a bid to tackle cyber attacks and make information systems foolproof, Indian Computer Emergency Response Team (CERT-in) has decided to empanel 'security auditors' who would identify vulnerabilities in the network infrastructure of various companies and organisations.

According to sources, the agency has already invited bids from IT security firms and expects to finalise the companies by March-end.

"We had a strong response to the initiative and as many as 35-40 companies have responded. We have set up a technical evaluation committee, which is currently scanning the applications," sources added.

The companies appointed would be responsible for undertaking infrastructure audits and work towards identifying network vulnerabilities or gaps, they said. These firms will

Contd...

audit networks, processes, people and technology that form an integral part of information systems of companies, at a rate that may be prescribed by Cert-in.

"We may fix the man day rate, but there will be enough flexibility.

For instance, much would depend on the size of the network that is to be audited and hence the rates would be a function of the number of man days as well as the size of the network to be assessed," sources said.

The bidding process would comprise two rounds, technical and financial. All the companies that qualify in the technical bid round would be asked to make financial bids.

"The companies which qualify will be expected to match the lowest bid quoted by any player in the financial round," they pointed out.

He said the auditors would identify weaknesses in a network but clarified that the firms would not offer advisory services.

This would ensure that the auditing and consulting functions are not mixed up, sources said.

CERT-in was constituted in January last year to tackle any possible hacking or virus attacks on the information systems including the country's vital networks such as power, railways, aviation and defence. It provides reactive and proactive services to enhance cyber security.

Source: http://www.thehindubusinessline.in/2005/02/07/stories/2005020701351300.htm

7.6 Summary

- A network is simply a collection of computers or other hardware devices that are connected together, either physically or logically, using special hardware and software, to allow them to exchange information and cooperate.
- Networks that connect computers lying within a small distance (such as a room, or within a building) from each other are called Local Area Networks (LANs).
- A wide area network connects computers which are very remotely placed. It may connect across the countries or continents or the entire globe.
- MAN is a network that interconnects users with computer resources in a geographical area larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN).
- Securing network infrastructure is like securing possible entry points of attacks on a country by deploying appropriate defense.
- Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access and consistent and continuous monitoring and measurement of its effectiveness (lack) combined together.
- Trusted networks are defined as "the networks within your security boundary, and are typically the networks you are trying to defend."
- Untrusted network is considered as "the networks external your security perimeter.
- To avoid highly injurious "superworms" or hackers by means of unknown or unpatched exploits, unusual solutions are required that are intended to avert and react to unknown attacks, instead of known attacks.

7.7 Keywords

Computer Security: It is more like providing means to protect a single PC against outside intrusion.

LAN: Networks that connect computers lying within a small distance (such as a room, or within a building) from each other are called Local Area Networks (LANs).

Preventive Measures: It attempt to secure the access to individual computers – the network itself – thereby protecting the computers and other shared resources such as printers, network-attached storage connected by the network.

Securing Network Infrastructure: It is like securing possible entry points of attacks on a country by deploying appropriate defense.

Trusted Networks: Trusted networks are defined as "the networks within your security boundary, and are typically the networks you are trying to defend."

Untrusted network: It is considered as the networks external your security perimeter.

7.8 Review Questions

1. What are the different types of networks? Discuss their comparison.
2. What is computer security? Explain the preventive measures attempted to secure the access to individual computers.
3. Explain the concept of network security.
4. Compare and contrast between computer security and network security.
5. Make distinction between trusted and untrusted network.
6. What are unknown attacks?
7. Explain the technologies that provide imperative levels of protection against unknown attacks.
8. Illustrate the different attributes of a secure network.
9. Explain the technique of Intrusion Detection by Program Analysis.
10. Make distinction between LAN and WAN.

Answers: Self Assessment

1. network
2. Networking
3. digital
4. Long Haul Networks (LHNs).
5. Internet
6. Value-added Network (VAN)
7. Computer security
8. unsecured
9. privacy
10. Trusted
11. Untrusted
12. unknown
13. unknown
14. Software Fault Isolation (SFI)
15. Intrusion detection by program analysis (IDS)

7.9 Further Readings

Notes

Books

Managing Enterprise Information Integrity: Security, Control and Audit Issues, IT Governance Institute.

Risks of Customer Relationship Management: A Security, Control, and Audit Approach, PricewaterHouseCoopers Llp.

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide, 2nd Edition, Deloitte Touche Tohmatsu Research Team, ISACA.

William Stallings, *Computer Security: Principles and Practice*, Prentice Hall, 2008.

Online link

www.interhack.net

Unit 8: Cryptography and Encryption

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the meaning of cryptography and encryption
- Recognize applications of cryptography

- Discuss the concept of digital signature
- Understand cryptographic algorithms

Introduction

Information security is an issue that is receiving a growing attention in today's society and one of the main reasons for this is attributable to the Internet phenomena. During the design of Internet, great importance was given to its functionality rather than other aspects, such as information security, thus making it an inadequate means for certain applications. The unpredictable success of Internet, however, has not been influenced by it's own downfalls and it has by now proved to be a fundamental tool that cannot be discarded in almost all sectors of today's economy. For this reason great effort has been invested in the improvement of the services offered by Internet and one of these is obtained using cryptographic techniques that render Internet not only a useful means of doing business, but at times even indispensable. In fact, through cryptographic techniques, one can obtain: secure communication connections, identity proof, electronic signatures (arguably safer than hand signing a check or credit card receipt) among other benefits.

8.1 Cryptography and Encryption

Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with.

There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography.

When your computer sends the information out, it scrambles it by using some key. This scrambled information would be gibberish to anyone who didn't have the correct key to unscramble it at the other end.

When the information reaches its destination, it gets unscrambled by using the key. This lets the person or website read the information correctly at the other end.

Websites that use an encrypted connection use something called SSL (Secure Sockets Layer) to secure the information going back and forth. This is how websites like Amazon or your bank can ensure your private information like passwords and credit card numbers are safe from prying eyes.

Cryptography can play many different roles in user authentication. Cryptographic authentication systems provide authentication capabilities through the use of cryptographic keys known or possessed only by authorized entities.

Cryptography also supports authentication through its widespread use in other authentication systems.

Example: Password systems often employ cryptography to encrypt stored password files, card/token system often employ cryptography to protect sensitive stored information, and hand-held password generators often employ cryptography to generate random, dynamic passwords.

Cryptography is frequently used in distributed applications to convey identification and authentication information from one system to another over a network. Cryptographic authentication systems authenticate a user based on the knowledge or possession of a cryptographic key. Cryptographic authentication systems can be based on either private key cryptosystems or public key cryptosystems.

Private key cryptosystems use the same key for the functions of both encryption and decryption. Cryptographic authentication systems based upon private key cryptosystems rely upon a shared key between the user attempting access and the authentication system.

Public key cryptosystems separate the functions of encryption and decryption, typically using a separate key to control each function. Cryptographic authentication systems based upon public key cryptosystems rely upon a key known only to the user attempting access.

Today's cryptography is more than encryption and decryption. Authentication is as fundamentally a part of our lives as privacy. We use authentication throughout our everyday lives – when we sign our name to some document for instance – and, as we move to a world where our decisions and agreements are communicated electronically, we need to have electronic techniques for providing authentication.

Cryptography provides mechanisms for such procedures. A digital signature binds a document to the possessor of a particular key, while a digital timestamp binds a document to its creation at a particular time. These cryptographic mechanisms can be used to control access to a shared disk drive, a high security installation, or a pay-per-view TV channel.

The field of cryptography encompasses other uses as well. With just a few basic cryptographic tools, it is possible to build elaborate schemes and protocols that allow us to pay using electronic money, to prove we know certain information without revealing the information itself and to share a secret quantity in such a way that a subset of the shares can reconstruct the secret.

While modern cryptography is growing increasingly diverse, cryptography is fundamentally based on problems that are difficult to solve. A problem may be difficult because its solution requires some secret knowledge, such as decrypting an encrypted message or signing some digital document. The problem may also be hard because it is intrinsically difficult to complete, such as finding a message that produces a given hash value.

Computer encryption is based on the science of cryptography, which has been used throughout history. Before the digital age, the biggest users of cryptography were governments, particularly for military purposes.

Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge. Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended, even those who have access to the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into an intelligible form.

Encryption and decryption generally require the use of some secret information, referred to as a key. For some encryption mechanisms, the same key is used for both encryption and decryption; for other mechanisms, the keys used for encryption and decryption are different.

The existence of coded messages has been verified as far back as the Roman Empire. But most forms of cryptography in use these days rely on computers, simply because a human-based code is too easy for a computer to crack.

Encryption is a process of coding information which could either be a file or mail message in into cipher text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data. Decryption is the reverse process of converting encoded data to its original un-encoded form, plaintext.

A key in cryptography is a long sequence of bits used by encryption/decryption algorithms.

Example: The following represents a hypothetical 40-bit key:

00001010 01101001 10011110 00011100 01010101

A given encryption algorithm takes the original message, and a key, and alters the original message mathematically based on the key's bits to create a new encrypted message. Likewise, a decryption algorithm takes an encrypted message and restores it to its original form using one or more keys.

When a user encodes a file, another user cannot decode and read the file without the decryption key. Adding a digital signature, a form of personal authentication, ensures the integrity of the original message.

To encode plaintext, an encryption key is used to impose an encryption algorithm onto the data. To decode cipher, a user must possess the appropriate decryption key.

A decryption key consists of a random string of numbers, from 40 through 2,000 bits in length. The key imposes a decryption algorithm onto the data. This decryption algorithm reverses the encryption algorithm, returning the data to plaintext. The longer the encryption key is, the more difficult it is to decode. For a 40-bit encryption key, over one trillion possible decryption keys exist.

There are two primary approaches to encryption: symmetric and public-key. Symmetric encryption is the most common type of encryption and uses the same key for encoding and decoding data. Public-key encryption uses two different keys, a public key and a private key. One key encodes the message and the other decodes it. The public key is widely distributed while the private key is secret.

Aside from key length and encryption approach, other factors and variables impact the success of a cryptographic system.

Example: Different cipher modes, in coordination with initialization vectors and salt values, can be used to modify the encryption method.

Cipher modes define the method in which data is encrypted. The stream cipher mode encodes data one bit at a time. The block cipher mode encodes data one block at a time. Although block cipher tends to execute more slowly than stream cipher.

Task Discuss the use of Secure Sockets Layer.

Did u know? **What is session key?**

Symmetric encryption is the most common type of encryption and uses the same key for encoding and decoding data. This key is known as a session key.

Self Assessment

Fill in the blanks:

1. .... cryptosystems use the same key for the functions of both encryption and decryption.

Notes

2. .... is the reverse process of converting encoded data to its original un-encoded form, plaintext.

8.2 Applications of Cryptography

8.2.1 Secrecy in Transmission

Many existing secrecy systems for transmission access a private key system for converting transmitted information since it is the fastest technique that functions with rational guarantee and low overhead.

If the number of conversing parties is minute, key distribution is performed periodically with a courier service and key preservation depends on physical security of the keys over the stage of use and demolition after new keys are disseminated.

If the number of parties is huge, electronic key distribution is generally used. Previously, key distribution was performed with a special key-distribution-key (also called a master-key) preserved by all parties in confidentiality over a longer phase of time than the keys used for a specific transaction. The "session-key" is produced at random either by one of the parties or by a trusted third party and distributed by means of the master-key.

The difficulty with master-key systems is that if the master-key is effectively attacked, the whole system disintegrated. Likewise, if any of the parties under a specified master-key decides to attack the system, they can build or intercept all messages during the whole system. Many compound private-key systems for reducing some of these difficulties have been projected and used for numerous applications.

With the arrival of public-key systems, secrecy can be preserved without a general master-key or a large number of keys. Rather, if Bob wants to interact with Alice, Bob sends Alice a session-key encrypted with Alice's public key. Alice decrypts the session-key and accesses that over the phase of the transaction.

These are instances of cryptographic protocols, techniques for communicating while attaining a specific cryptographic aim. These protocols are accessed initially to deal with key management and system mishandling difficulties. Many other protocols are applied to eradicate other attacks on these systems.

8.2.2 Secrecy in Storage

Secrecy in storage is generally preserved by a one-key system where the user offers the key to the computer at the commencement of a session, and the system then takes concern of encryption and decryption during the stage of normal use.

Example: Many hardware devices are obtainable for personal computers to robotically encrypt all information accumulated on disk. When the computer is turned on, the user must provide a key to the encryption hardware. The information cannot be read significantly without this key, so even if the disk is stolen, the information on it will not be accessible.

Secrecy in storage has its difficulties. If the user does not remember a key, all of the information encrypted with it turns out to be enduringly unusable. The information is only encrypted while in storage, not when in use by the user. This leaves a major hole for the attacker. If the encryption and decryption are executed in software, or if the key is accumulated somewhere in the system, the system may be circumvented by an attacker. Backups of encrypted information are frequently accumulated in plaintext since the encryption method is only functional to certain devices.

8.2.3 Integrity in Transmission

Most of the users of communication systems are not as much worried regarding secrecy as about integrity. In an electronic funds transfer, the sum sent from one account to another is frequently public knowledge. What the bank concerns about is that only proper transfers can happen. If an active tapper could bring in a false transfer, funds would be moved illegally. An inaccuracy in a single bit could factually cause millions of dollars to be incorrectly credited or debited. Cryptographic methods are broadly used to guarantee that intentional or accidental modification of transmitted information does not cause flawed actions to occur.

A classic technique for guaranteeing integrity is to carry out a checksum of the information being transmitted and broadcast the checksum in encrypted form. Once the information and encrypted checksum are obtained, the information is again checksummed and compared to the transmitted checksum after decryption. If the checksums agree, there is a high likelihood that the message is unchanged. Unfortunately, this method is too simple to be of realistic value as it is easily forged. The trouble is that the checksum of the unique message is straight away apparent and a plaintext message with the same checksum can be easily bogus. Scheming strong cryptographic checksums is as a result significant to the guarantee of integrity in systems of this sort.

The key distribution trouble in a one-key system is as before, but an appealing alternative is presented by the use of public keys. If we produce a single public-key for the whole system and throw away the private key that would go with it, we can make the checksum impossible to decrypt. To verify the original message, we simply produce a new checksum, encrypt with the public key, and confirm that the encrypted checksum matches. This is called a one-way function because it is hard to invert.

Definite systems of this sort use high quality cryptographic checksums and complex key distribution and preservation protocols, but there is a tendency towards the use of public keys for key protection.

8.2.4 Integrity in Storage

Integrity beside random noise has been the focus of much study in the fields of error tolerant computing and coding theory, but only lately has the requirement for integrity of stored information beside intentional attack turn out to be a matter for cryptography.

The main mean of assuring integrity of accumulated information has previously been access control. Access control involves systems of locks and keys, guards, and other techniques of a physical or logical nature. The current advent of computer viruses has altered this to a significant degree, and the use of cryptographic checksums for assuring the integrity of stored information is now becoming extensive.

As in the case of integrity in transmission, a cryptographic checksum is formed and compared to expectations, but storage media tends to have dissimilar properties than transmission media. Transmitted information is normally more broadly obtainable over a shorter period of time, used for a comparatively low volume of information, and used at a slower rate than stored information. These parameters cause dissimilar tradeoffs in how cryptosystems are used.

8.2.5 Authentication of Identity

Authenticating the identity of individuals or systems to each other has been a trouble for a very long time. Simple passwords have been used to prove identity. More compound protocols like series of keywords exchanged among sets of parties are frequently shown in the movies or on television. Cryptography is closely associated to the theory and practice of using passwords, and modern systems frequently use strong cryptographic converts in conjunction with physical properties of individuals and shared secrets to offer highly consistent authentication of identity.

Determining good passwords appear into the field called key selection. In real meaning, a password can be considered of as a key to a cryptosystem that permits encryption and decryption of everything that the password permits access to. Actually, password systems have been implemented in just this manner in some commercial products.

The gathering of keys has traditionally been a cause of cryptosystem failure. Even though we know that H(K) is maximized for a key selected with an equal probability of every possible value (i.e. at random), in practice when people select keys, they choose them to make them easy to keep in mind, and so not at random. This is most dramatically established in the poor choice that people make of passwords.

On many systems, passwords are amassed in encrypted form with read access obtainable to all so that programs wishing to confirm passwords needn't be run by privileged users. A side advantage is that the plaintext passwords don't emerge anywhere in the system, so an unintentional leak of information doesn't negotiate system wide protection.

A usual algorithm for converting any string into an encrypted password is intended so that it takes 10 or more msec/transformation to encode a string. By easy calculation, if only capital letters were permitted in a password, it would take .26 seconds to verify all the one letter passwords, 6.76 seconds to confirm all the 2 letter passwords, 4570 seconds for the 4 letter passwords, and by the time we got to 8 letter passwords, it would take about 2*10**9 seconds (24169 days, over 66 years).

For passwords permitting lower case letters, numbers, and special symbols, this goes up significantly. Studies over the years have time after time indicated that key choice by those without knowledge of defense is very poor. In a new study, 21% of the users on a computer system had 1 character passwords, with up to 85% having passwords of 1/2 the maximum allowable length, and 92% having passwords of 4 characters or less. These results are quite typical, and noticeably reveal that 92% of all passwords could be guessed on a usual system in just over an hour.

Notes Numerous suggestions for getting random uniform random numbers comprise the use of low order bits of Geiger counter counts, the use of the time among entries at a keyboard, low order bits of the amount of light in a room as calculated by a light sensitive diode, noisy diode output, the last digit of the first phone number on a specified page of a telephone book, and digits from transcendental numbers like Pi.

8.2.6 Credentialing Systems

A credential is usually a document that introduces one party to another by referencing a normally known trusted party.

Example: When credit is applied for, references are generally requested. The credit of the references is checked and they are contacted to find out the creditworthiness of the applicant. Credit cards are frequently used to credential an individual to achieve further credit cards. A driver's license is a figure of credential, as is a passport.

Notes

Electronic credentials are intended to permit the credence of a claim to be confirmed electronically. Even though no purely electronic credentialing systems are in widespread use at this time, many such systems are being incorporated into the smart-card systems in widespread use in Europe. A smart-card is just a credit-card shaped computer that performs cryptographic functions and accumulates secret information. When used in combination with other devices and systems, it permits a broad variety of cryptographic applications to be performed with relative ease of use to the customer.

8.2.7 Electronic Signatures

Electronic signatures are a means of supplying a lawfully binding transaction between two or more parties. To be as functional as a physical signature, electronic signatures must be at least as hard to fake at least as easy to use, and accepted in a court of law as binding upon all parties to the operation.

The requirement for these electronic signatures is particularly acute in business dealings wherein the parties to a agreement are not in the same physical vicinity.

Example: An global sale of an airplane, signatures are usually required from two bankers, two companies, two insurance agencies, two attorneys, two governments, and frequently several other parties.

The contracts are hundreds of pages long, and signatures must be achieved within a relatively short phase of time on the similar physical document. Faxcimily signatures are not lawfully binding in all jurisdictions, and the sheer length of a document prevents all parties reading the present copy as they meet at the table to affix signatures. Under current law, all parties must meet in one location so as to complete the transaction. In a transatlantic sale, $100,000 in costs can simply be incurred in such a meeting.

An attempt in Europe is at present underway to restore physical signatures with electronic signatures based on the RSA cryptosystem. If this effort succeeds, it will permit many millions of dollars to be saved, and launch the period of digital signatures into full scale motion. It will also make a large savings for those who use the system, and thus act to force others to participate in order to remain competitive.

8.2.8 Electronic Cash

There are patents under force throughout the world today to allow electronic information to replace cash money for financial transactions between individuals. Such a system involves using cryptography to keep the assets of nations in electronic form. Clearly the ability to forge such a system would allow national economies to be destroyed in an instant. The pressure for integrity in such a system is staggering.

8.2.9 Threshold Systems

Thresholding systems are systems intended to permit use only if a minimal number of parties consent to the said use.

Example: In a nuclear arms circumstances, you might want a system in which three out of five members of the joint chiefs of staff have the same opinion. In a banking situation, a safe might only be opened if 4 out of the certified 23 people permitted to open the safe were present. Such systems prevent a single individual acting alone, while permitting many of the parties to a transaction to be missing without the transaction being halted.

Most threshold systems depend on encryption with keys which are distributed in portions. The most ordinary method for partitioning a key into parts is to form the key as the solution to N equations in N unknowns. If N independent equations are recognized, the key can be determined by solving the concurrent equations. If less than N equations are known, the key can be any value as there is still a sovereign variable in the equations. Any number can be selected for N and equations can be held by separate individuals. The same general concept can be used to form arbitrary combinations of key requirements by producing ORs and ANDs of encryptions using different sets of keys for different combinations of key holders. The major troubles with such a system lie in the key distribution difficulty and the large number of keys needed to attain arbitrary key holder combinations.

8.2.10 Systems using Changing Keys

It has been shown us that given sufficient reuse of a key, it can finally be determined. It is therefore common practice to frequently change keys to limit the exposure because of successful attack on any given key. A familiar misconception is that changing a key much more frequently than the average time needed to break the cryptosystem, offers an increased margin of safety.

If we suppose the key is chosen at chance, and that the attacker can ensure a given percentage of the keys before a key change is completed, it is only a matter of time before one of the keys checked by the attacker appears to correspond to one of the casual keys. If the attacker selects keys to attack at random without replacement over the phase of key usage, and begins again at the commencement of each period, it is 50% likely that a at present valid key will be found by the time required to try 50% of the total number of keys, regardless of key changes. So if a PC could try all the DES keys in 10 years, it would be 50% likely that a victorious attack could be launched in 5 years of effort. The real advantage of key changes is that the time over which a broken key is useful is restricted to the time till the next key change. This is known as limiting the exposure from a stolen key.

8.2.11 Hardware to Support Cryptography

Traditionally, cryptography has been executed through the use of cryptographic devices. The use of these devices derives from the complexity in performing cryptographic transforms by hand, the severe nature of errors that effect from the lack of redundancy in many cryptographic systems, and the want to make the breaking of codes computationally complex.

In WWII, the ENIGMA machine was accessed by the Germans to encode messages, and one of the first computers ever built was the BOMB, which was intended to break ENIGMA cryptograms. Modern supercomputers are used mainly by the NSA to attain the computational advantage essential to break many contemporary cryptosystems. The CRAY could be easily used to break most password enciphering systems, RSA systems with keys of length under about 80 (circa 1986) are critically threatened by the CRAY, and even the DES can be attacked by using special purpose computer hardware. Many devices have occurred in the marketplace for the use of cryptography to encrypt transmissions, act as cryptographic keys for verification of identification, protect so called debit cards and smart cards, and executing electronic cash money systems.

Self Assessment

Fill in the blanks:

3. With the arrival of public-key systems, ... can be preserved without a general master-key or a large number of keys.

4. .... involves systems of locks and keys, guards, and other techniques of a physical or logical nature.

5. .... are a means of supplying a lawfully binding transaction between two or more parties.

6. .... systems are systems intended to permit use only if a minimal number of parties consent to said use.

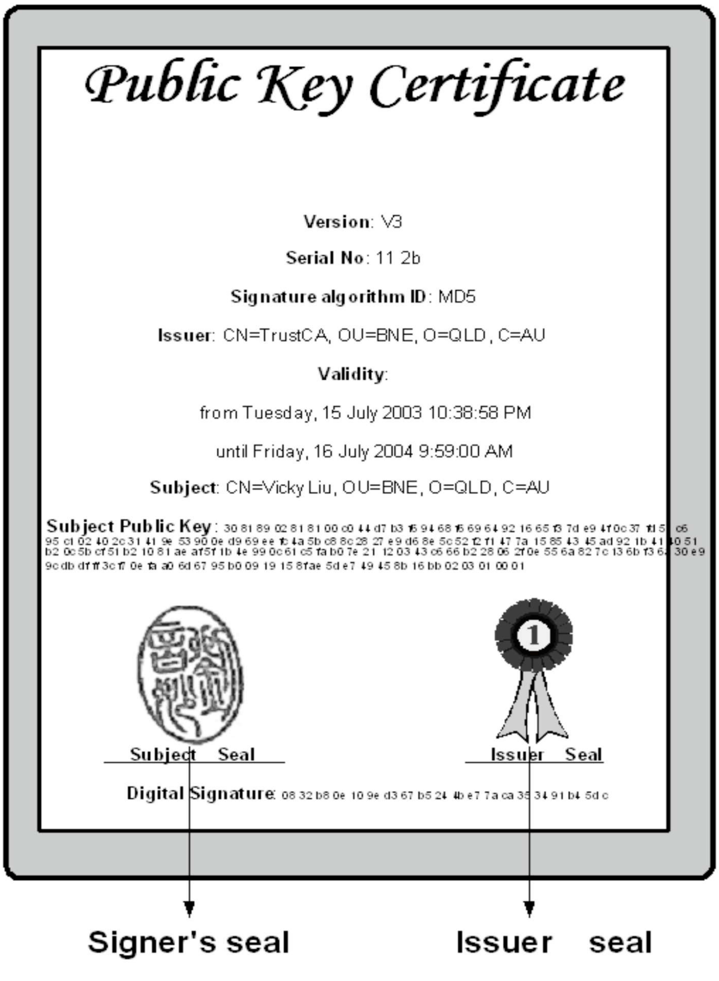
8.3 Digital Certificates

E-commerce has flourished because of the ability to perform secure transactions online using the proper tools. These tools are public key encryption and digital certificates.

The digital equivalent of an ID card used in conjunction with a public key encryption system. Also called a "digital ID," "digital identity certificate," "identity certificate" and "public key certificate," digital certificates are issued by a trusted third party known as a "certification authority" (CA) such as VeriSign (www.verisign.com) and Thawte (www.thawte.com).

Digital certificates are issued by an independent, recognized and mutually trusted third party that guarantees that the website operating is who it claims to be. This third party is known as a Certification Authority (CA). Without digital certificates, the public has little assurance as to the legitimacy of any particular website.

Figure 8.1: Digital Certificate



Public Key Certificate

Version: V3

Serial No: 11 2b

Signature algorithm ID: MD5

Issuer: CN=TrustCA, OU=BNE, O=QLD, C=AU

Validity:

from Tuesday, 15 July 2003 10:38:58 PM

until Friday, 16 July 2004 9:59:00 AM

Subject: CN=Vicky Liu, OU=BNE, O=QLD, C=AU

Subject Public Key: 30 81 89 02 81 81 00 c0 44 d7 b3 f6 94 68 f6 69 64 92 16 65 f3 7d e9 4f 0c 37 fd 5 c6 95 c1 02 40 2c 31 41 9e 53 90 0e d9 69 ee fc 4a 5b c8 8c 28 27 e9 d6 8e 5c 52 f2 f1 47 7a 15 85 43 45 ad 92 1b 41 40 51 b2 0c 5b cf 51 b2 10 81 ae af 5f 1b 4e 99 0c 61 c5 fa b0 7e 21 12 03 43 c6 66 b2 28 06 2f 0e 55 6a 82 7c 13 6b f3 64 30 e9 9c db df ff 3c f7 0e fa a0 6d 67 95 b0 09 19 15 8f ae 5d e7 49 45 8b 16 bb 02 03 01 00 01

Subject Seal

Issuer Seal

Digital Signature: 08 32 b8 0e 10 9e d3 67 b5 24 4b e7 7a ca 35 34 91 b4 5d c

Notes

A digital certificate contains an entity's name, address, serial number, public key, expiration date and digital signature, among other information. When a Web browser like Firefox, Netscape or Internet Explorer makes a secure connection, the digital certificate is automatically turned over for review. The browser checks it for anomalies or problems, and pops up an alert if any are found. When digital certificates are in order, the browser completes secure connections without interruption.

The problem, however, is that anyone can create a website and key pair using a name that doesn't belong to them. This is where digital certificates come in. Digital certificates are trusted ID cards in electronic form that bind a website's public encryption key to their identity for purposes of public trust.

Though rare, there have been cases of phishing scams duplicating a website and 'hijacking' the site's digital certificate to fool customers into giving up personal information. These scams involved redirecting the customer to the real site for authentication, then bringing them back to the duped website.

Other phishing scams use self-signed digital certificates to dispose of the trusted third party or Certificate Authority altogether. The issuer of the digital certificate and the signer are one in the same. A browser will alert in this case, but most users click through anyway, not understanding the difference.

Notes Not all Certificate Authorities are equal. Some CAs are newer and less well known. Two examples of highly trusted CAs are VeriSign and Thawte. If your browser does not recognize a Certificate Authority, it will alert you.

8.3.1 Verifying the Certificate

Digital certificates play an integral role in keeping online commerce safe. If your browser alerts you to a problem with a digital certificate, you are well-advised not to click through. Instead, call the business using a telephone number from your statements or phone book, and inquire as to the problem.

Public key encryption uses SSL (Secure Sockets Layer) to encrypt all data between the customer's computer and the e-commerce website. Information is sent in encrypted form to the site using the site's public key. Upon receiving the information, the site uses its private key to decrypt the information. This is called a key pair. Interlopers that might capture data en route will find it unreadable.

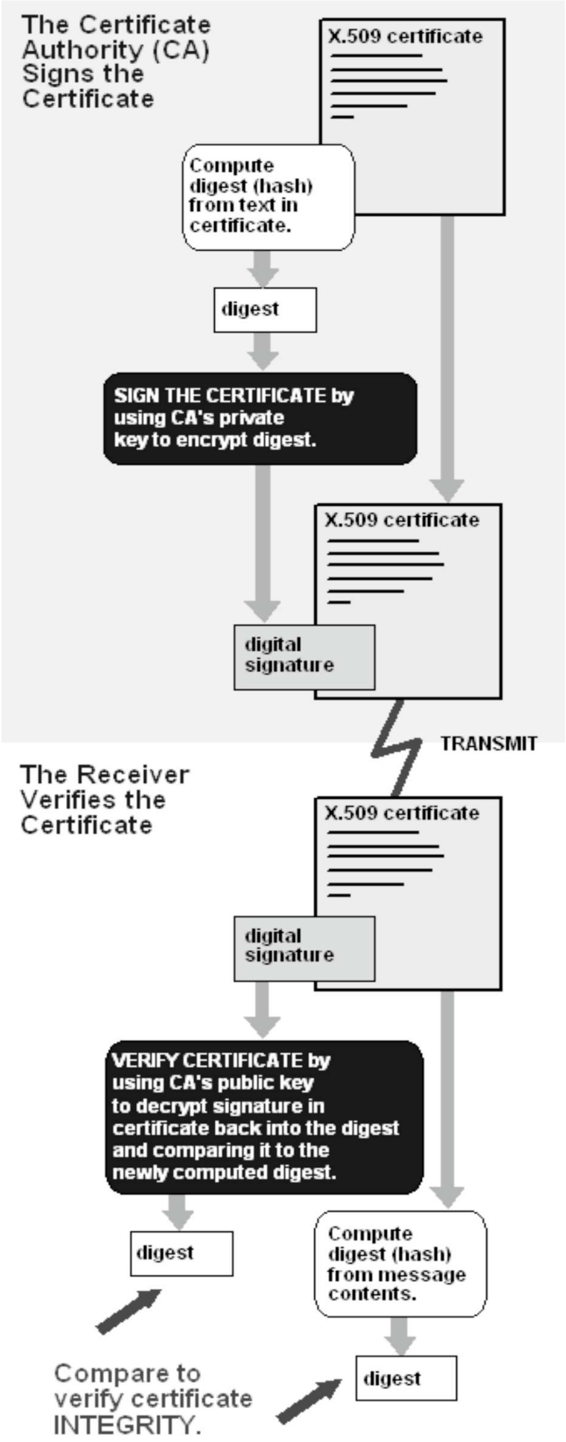
The CA verifies that a public key belongs to a specific company or individual (the "subject"), and the validation process it goes through to determine if the subject is who it claims to be depends on the level of certification and the CA itself.

After the validation process is completed, the CA creates an X.509 certificate that contains CA and subject information, including the subject's public key (details below). The CA signs the certificate by creating a digest (a hash) of all the fields in the certificate and encrypting the hash value with its private key. The encrypted digest is called a "digital signature," and when placed into the X.509 certificate, the certificate is said to be "signed."

The CA keeps its private key very secure, because if ever discovered, false certificates could be created.

The process of verifying the "signed certificate" is done by the recipient's software, which is typically the Web browser. The browser maintains an internal list of popular CAs and their public keys and uses the appropriate public key to decrypt the signature back into the digest. It then recomputes its own digest from the plain text in the certificate and compares the two. If both digests match, the integrity of the certificate is verified (it was not tampered with), and the public key in the certificate is assumed to be the valid public key of the subject.

Figure 8.2: Digital Certificate Verification Process


The Certificate Authority (CA) Signs the Certificate
X.509 certificate
Compute digest (hash) from text in certificate.
digest
SIGN THE CERTIFICATE by using CA's private key to encrypt digest.
X.509 certificate
digital signature
TRANSMIT
The Receiver Verifies the Certificate
X.509 certificate
digital signature
VERIFY CERTIFICATE by using CA's public key to decrypt signature in certificate back into the digest and comparing it to the newly computed digest.
digest
Compute digest (hash) from message contents.
digest
Compare to verify certificate INTEGRITY.

At this point, the subject's identity and the certificate's integrity (no tampering) have been verified. The certificate is typically combined with a signed message or signed executable file, and the public key is used to verify the signatures (see digital signature and code signing). The subject's public key may also be used to provide a secure key exchange in order to have an encrypted two-way communications session.

Self Assessment

Fill in the blanks:

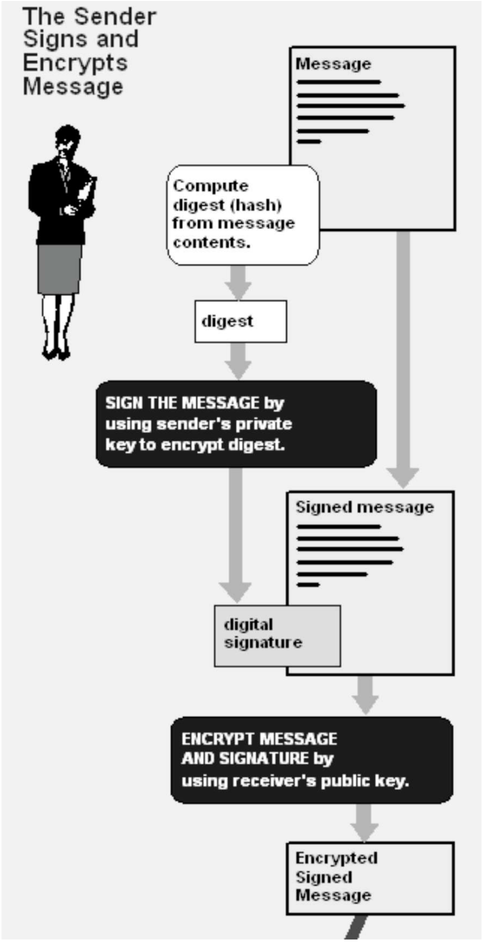
7. Digital certificates are issued by a trusted third party known as a "..........................." .

8. Public key encryption uses ....to encrypt all data between the customer's computer and the e-commerce website. Information is sent in encrypted form to the site using the site's public key.

8.4 Digital Signature

These techniques are designed to provide the digital counterpart to handwritten signatures and can be achieved using cryptography. In substance a digital signature of a message is a number dependant on some secret known only to the signer and on the content of the message being signed. Signatures must be verifiable without requiring access to the signers secret information.

Figure 8.3: Sender is Sending the Message with Digital Signature


The Sender Signs and Encrypts Message
Message
Compute digest (hash) from message contents.
digest
SIGN THE MESSAGE by using sender's private key to encrypt digest.
Signed message
digital signature
ENCRYPT MESSAGE AND SIGNATURE by using receiver's public key.
Encrypted Signed Message

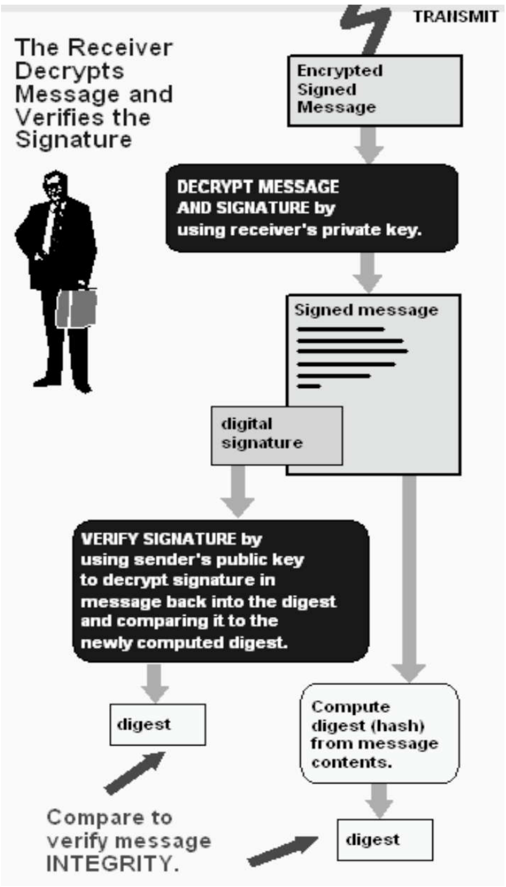
The idea is similar to asymmetric cryptography but it is complimentary. Whereas in public-key encryption schemes, the public key is used to encrypt the message and the private key to decrypt, digital signatures are obtained generating a number using the private key and verified with the public key.

Digital signatures have many applications in information security, including authentication, data integrity and non-repudiation. One of the most significant applications of digital signatures is the certification of public keys in large networks.

Certification is a means for a Trusted Third Party (TTP) to bind the identity of a user to a public key, so that at some later time, other entities can authenticate a public key without assistance from a trusted third party. It now becomes clear how asymmetric cryptography surmounts the key distribution problem. A user, destined to receive an encrypted message, can send his certificate containing his public key issued by a TTL or Certificate Authority. The receiver, who desires to encrypt and send the message, can authenticate that the certificate was issued by the common Certificate Authority (CA) using the CA public key thus acquiring the guaranty that the public key received belongs to the intended recipient (or at least the CA's guaranty).

The first method discovered was the RSA signature scheme (an RSA public key encryption compliment scheme) and is still widely used in Internet together with another digital scheme called Digital Signature Algorithm (DSA) proposed by the National Institute of Standards and Technology (NIST) and is the first digital signature scheme to be recognized by any government (1991).

Figure 8.4: Receiver is receiving the Message with Digital Signature


TRANSMIT
The Receiver Decrypts Message and Verifies the Signature
Encrypted Signed Message
DECRYPT MESSAGE AND SIGNATURE by using receiver's private key.
Signed message
digital signature
VERIFY SIGNATURE by using sender's public key to decrypt signature in message back into the digest and comparing it to the newly computed digest.
digest
Compute digest (hash) from message contents.
digest
Compare to verify message INTEGRITY.

Notes

Self Assessment

Fill in the blanks:

9. .... techniques are designed to provide the digital counterpart to handwritten signatures and can be achieved using cryptography.

10. Certification is a means for a .... to bind the identity of a user to a public key.

8.5 Cryptographic Algorithms

8.5.1 Symmetric (or Shared) Key Cryptography

Symmetric-key cryptography is also known as shared-key, secret-key, single-key, one-key and eventually private-key cryptography.

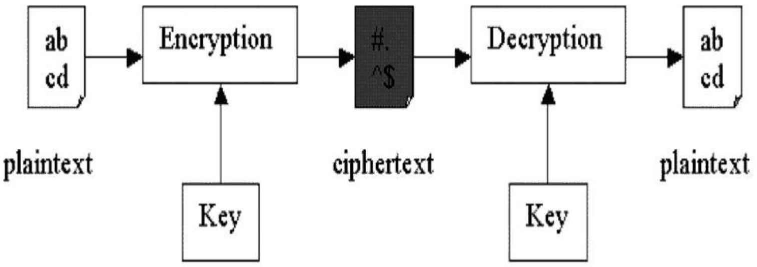
With symmetric key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, symmetric key cryptography is also called symmetric encryption.

With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the shared. The biggest difficulty with this approach, of course, is the distribution of the key.

Symmetric key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Stream ciphers operate on a single bit (byte or computer word) at a time and implement some form of feedback mechanism so that the key is constantly changing.

A block cipher is so-called because the scheme encrypts one block of data at a time using the same key on each block. In general, the same plaintext block will always encrypt to the same ciphertext when using the same key in a block cipher whereas the same plaintext will encrypt to different ciphertext in a stream cipher.

Figure 8.5: Symmetric-key Cryptography



Stream ciphers come in several flavors but two are worth mentioning here. Self-synchronizing stream ciphers calculate each bit in the keystream as a function of the previous n bits in the keystream. It is termed "self-synchronizing" because the decryption process can stay synchronized with the encryption process merely by knowing how far into the n-bit keystream it is.

One problem is error propagation; a garbled bit in transmission will result in n garbled bits at the receiving side. Synchronous stream ciphers generate the keystream in a fashion independent of the message stream but by using the same keystream generation function at sender and receiver. While stream ciphers do not propagate transmission errors, they are, by their nature, periodic so that the keystream will eventually repeat.

Block ciphers can operate in one of several modes; the following four are the most important:

1. Electronic Codebook (ECB) mode is the simplest, most obvious application: the shared key is used to encrypt the plaintext block to form a ciphertext block. Two identical plaintext blocks, then, will always generate the same ciphertext block. Although this is the most common mode of block ciphers, it is susceptible to a variety of brute-force attacks.

2. Cipher Block Chaining (CBC) mode adds a feedback mechanism to the encryption scheme. In CBC, the plaintext is exclusively-ORed (XORed) with the previous ciphertext block prior to encryption. In this mode, two identical blocks of plaintext never encrypt to the same ciphertext.

3. Cipher Feedback (CFB) mode is a block cipher implementation as a self-synchronizing stream cipher. CFB mode allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input. If we were using 1-byte CFB mode.

Example: Each incoming character is placed into a shift register the same size as the block, encrypted, and the block transmitted. At the receiving side, the ciphertext is decrypted and the extra bits in the block (i.e., everything above and beyond the one byte) are discarded.

4. Output Feedback (OFB) mode is a block cipher implementation conceptually similar to a synchronous stream cipher. OFB prevents the same plaintext block from generating the same ciphertext block by using an internal feedback mechanism that is independent of both the plaintext and ciphertext bitstreams.

Task Explain the function of Stream ciphers.

8.5.2 Public Key Cryptography

Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years. Modern PKC was first described publicly by Stanford University professor Martin Hellman and graduate student Whitfield Diffie in 1976. Their paper described a two-key crypto system in which two parties could engage in a secure communication over a non-secure communications channel without having to share a secret key.

Public-key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys — a public key and a private key.

The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can be decrypted only with the corresponding private key.

The two main branches of public key cryptography are:

1. ***Public Key Encryption:*** A message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality.

2. ***Digital Signatures:*** A message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This is used to ensure authenticity.

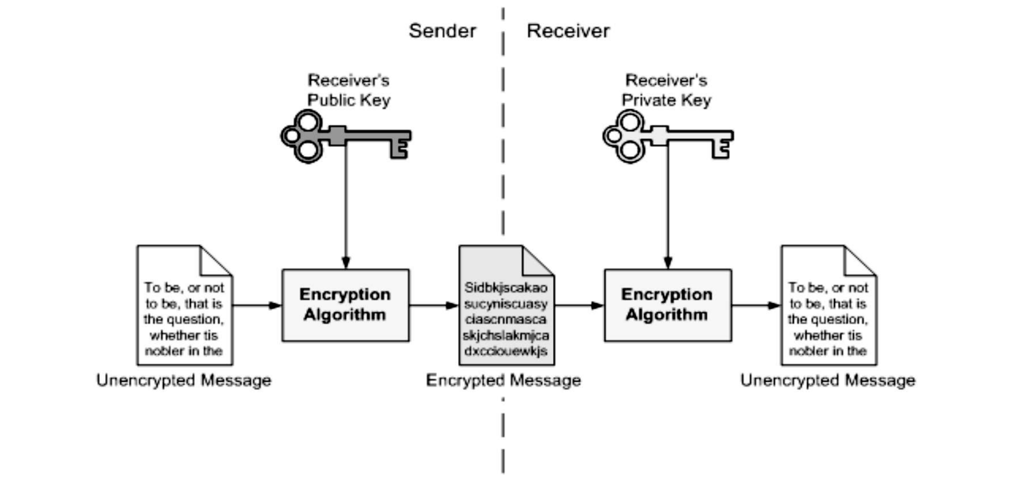
Notes

An analogy for public-key encryption is that of a locked mailbox with a mail slot. The mail slot is exposed and accessible to the public; its location (the street address) is in essence the public key. Anyone knowing the street address can go to the door and drop a written message through the slot; however, only the person who possesses the key can open the mailbox and read the message.

An analogy for digital signatures is the sealing of an envelope with a personal wax seal. The message can be opened by anyone, but the presence of the seal authenticates the sender.

A central problem for public-key cryptography is proving that a public key is authentic, and has not been tampered with or replaced by a malicious third party. The usual approach to this problem is to use a Public-key Infrastructure (PKI), in which one or more third parties, known as certificate authorities, certify ownership of key pairs. Another approach, used by PGP, is the "web of trust" method to ensure authenticity of key pairs.

Figure 8.6: Public-key Cryptography


Sender
Receiver
Receiver's Public Key
Receiver's Private Key
To be, or not to be, that is the question, whether tis nobler in the
Encryption Algorithm
Sidbkjscakao sucyniscuasy ciascnmasca skjchslakmjca dxcciouewkjs
Encryption Algorithm
To be, or not to be, that is the question, whether tis nobler in the
Unencrypted Message
Encrypted Message
Unencrypted Message

Public key techniques are much more computationally intensive than purely symmetric algorithms. The judicious use of these techniques enables a wide variety of applications. In practice, public key cryptography is used in combination with secret-key methods for efficiency reasons.

For encryption, the sender encrypts the message with a secret-key algorithm using a randomly generated key, and that random key is then encrypted with the recipient's public key. For digital signatures, the sender hashes the message (using a cryptographic hash function) and then signs the resulting "hash value". Before verifying the signature, the recipient also computes the hash of the message, and compares this hash value with the signed hash value to check that the message has not been tampered with.

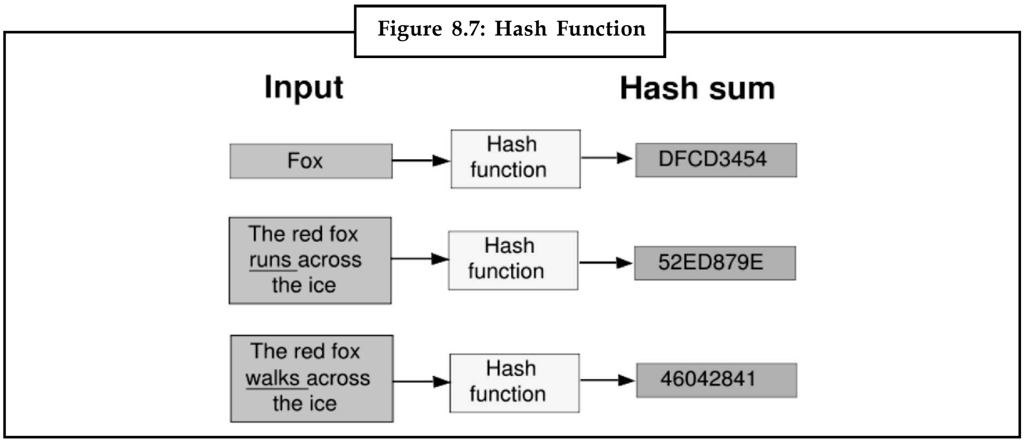
Did u know? The private key is kept secret, while the public key may be widely distributed.

8.5.3 Hashing

Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered.

Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus. Hash functions are also commonly employed by many operating systems to encrypt passwords. Hash functions, then, provide a measure of the integrity of a file.

Figure 8.7: Hash Function



Broadly speaking, a cryptographic hash function should behave as much as possible like a random function while still being deterministic and efficiently computable.

A cryptographic hash function is considered insecure if either of the following is computationally feasible:

1. Finding a (previously unseen) message that matches a given digest.
2. Finding "collisions", wherein two different messages have the same message digest.

An attacker who can do either of these things might, for example, use them to substitute an unauthorized message for an authorized one.

Ideally, it should not even be feasible to find two messages whose digests are substantially similar; nor would one want an attacker to be able to learn anything useful about a message given only its digest. Of course, the attacker learns at least one piece of information, the digest itself, which for instance gives the attacker the ability to recognize the same message should it occur again.

8.5.4 Pretty Good Privacy (PGP)

It is one of today's most widely used public key cryptography programs. Developed by Philip Zimmermann in the early 1990s and long the subject of controversy, PGP is available as a plug-in for many e-mail clients, such as Claris Emailer, Microsoft Outlook/Outlook Express, and Qualcomm Eudora.

PGP can be used to sign or encrypt e-mail messages with the mere click of the mouse. Depending upon the version of PGP, the software uses SHA or MD5 for calculating the message hash; CAST, Triple-DES, or IDEA for encryption; and RSA or DSS/Diffie-Hellman for key exchange and digital signatures.

When PGP is first installed, the user has to create a key-pair. One key, the public key, can be advertised and widely circulated. The private key is protected by use of a passphrase. The passphrase has to be entered every time the user accesses their private key.

Figure 8.8 shows a PGP signed message. This message will not be kept secret from an eavesdropper, but a recipient can be assured that the message has not been altered from what the sender transmitted. In this instance, the sender signs the message using their own private key. The receiver uses the sender's public key to verify the signature; the public key is taken from the receiver's keyring based on the sender's e-mail address.

Notes

Figure 8.8: A PGP signed Message

```
−−BEGIN PGP SIGNED MESSAGE−−
 Hash: SHA1

Hi Carol.

 What was that pithy Groucho Marx quote?

 /kess

 −−BEGIN PGP SIGNATURE−−
 Version: PGP for Personal Privacy 5.0
 Charset: noconv

iQA/AwUBNFUdO5WOcz5SFtuEEQJx/ACaAgR97+vvDU6XWELV/
GANjAAgBtUAnjG3
Sdfw2JgmZIOLNjFe7jP0Y8/M
=jUAU
−−END PGP SIGNATURE−−
```

Caution The signature process does not work unless the sender's public key is on the receiver's keyring.

Figure 8.9: A PGP Encrypted Message

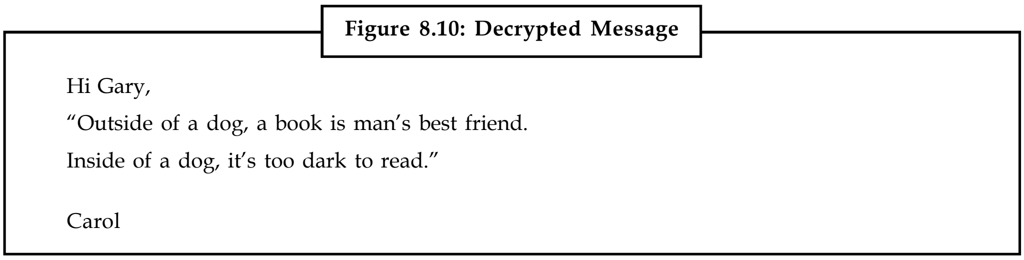
```
−−BEGIN PGP MESSAGE−−
Version: PGP for Personal Privacy 5.0
MessageID: DAdVB3wzpBr3YRunZwYvhK5gBKBXOb/m

qANQR1DBwU4D/TlT68XXuiUQCADfj2o4b4aFYBcWumA7hR1Wvz9rbv2BR6WbEUsy
ZBIEFtjyqCd96qF38sp9IQiJIKlNaZfx2GLRWikPZwchUXxB+AA5+lqsG/ELBvRa
c9XefaYpbbAZ6z6LkOQ+eE0XASe7aEEPfdxvZZT37dVyiyxuBBRYNLN8Bphdr2zv
z/9Ak4/OLnLiJRk05/2UNE5Z0a+3lcvITMmfGajvRhkXqocavPOKiin3hv7+Vx88
uLLem2/fQHZhGcQvkqZVqXx8SmNw5gzuvwjV1WHj9muDGBY0MkjiZIRI7azWnoU9
3KCnmpR60VO4rDRAS5uGl9fioSvze+q8XqxubaNsgdKkoD+tB/4u4c4tznLfw1L2
YBS+dzFDw5desMFSo7JkecAS4NB9jAu9K+f7PTAsesCBNETDd49BTOFFTWWavAfE
gLYcPrcn4s3EriUgvL3OzPR4P1chNu6sa3ZJkTBbriDoA3VpnqG3hxqfNyOlqAka
mJJuQ53Ob9ThaFH8YcE/VqUFdw+bQtrAJ6NpjIxi/x0FfOInhC/bBw7pDLXBFNaX
HdlLQRPQdrmnWskKznOSarxq4GjpRTQo4hpCRJJ5aU7tZO9HPTZXFG6iRIT0wa47
AR5nvkEKoIAjW5HaDKiJriuWLdtN4OXecWvxFsjR32ebz76U8aLpAK87GZEyTzBx
dV+lH0hwyT/y1cZQ/E5USePP4oKWF4uqquPee1OPeFMBo4CvuGyhZXD/18Ft/53Y
WIebvdiCqsOoabK3jEfdGExce63zDI0=
=MpRf
−−END PGP MESSAGE−−
```

Figure 8.9 shows a PGP encrypted message (PGP compresses the file, where practical, prior to encryption because encrypted files lose their randomness and, therefore, cannot be compressed). In this case, public key methods are used to exchange the session key for the actual message encryption using secret-key cryptography. In this case, the receiver's e-mail address is the pointer to the public key in the sender's keying; in fact, the same message can be sent to multiple recipients and the message will not be significantly longer since all that needs to be added is the session key encrypted by each receiver's private key.

Caution When the message is received, the recipient must use their private key to extract the session secret key to successfully decrypt the message.

Figure 8.10: Decrypted Message



Hi Gary,

"Outside of a dog, a book is man's best friend.

Inside of a dog, it's too dark to read."

Carol

It is worth noting that PGP was one of the first so-called "hybrid cryptosystems" that combined aspects of SKC and PKC. When Zimmermann was first designing PGP in the late-1980s, he wanted to use RSA to encrypt the entire message. The PCs of the days, however, suffered significant performance degradation when executing RSA so he hit upon the idea of using SKC to encrypt the message and PKC to encrypt the SKC key.

PGP went into a state of flux in 2002. Zimmermann sold PGP to Network Associates, Inc. (NAI) in 1997 and himself resigned from NAI in early 2001. In March 2002, NAI announced that they were dropping support for the commercial version of PGP having failed to find a buyer for the product willing to pay what NAI wanted. In August 2002, PGP was purchased from NAI by PGP Corp. Meanwhile, there are many freeware versions of PGP available.

8.5.5 Kerberos

Kerberos is a commonly used authentication scheme on the Internet. Developed by MIT's Project Athena, Kerberos is named for the three-headed dog who, according to Greek mythology, guards the entrance of Hades (rather than the exit, for some reason!).

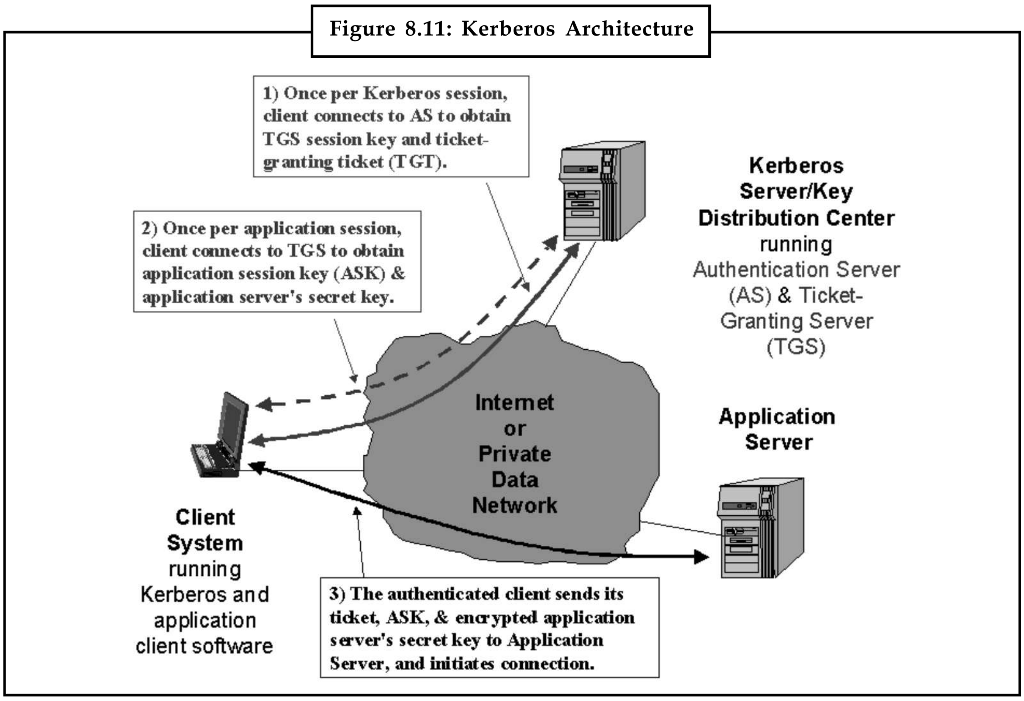
Kerberos employs a client/server architecture and provides user-to-server authentication rather than host-to-host authentication. In this model, security and authentication will be based on secret key technology where every host on the network has its own secret key.

It would clearly be unmanageable if every host had to know the keys of all other hosts so a secure, trusted host somewhere on the network, known as a Key Distribution Center (KDC), knows the keys for all of the hosts (or at least some of the hosts within a portion of the network, called a realm).

In this way, when a new node is brought online, only the KDC and the new node need to be configured with the node's key; keys can be distributed physically or by some other secure means.

Notes

Figure 8.11: Kerberos Architecture


1) Once per Kerberos session, client connects to AS to obtain TGS session key and ticket-granting ticket (TGT).
2) Once per application session, client connects to TGS to obtain application session key (ASK) & application server's secret key.
Kerberos Server/Key Distribution Center running Authentication Server (AS) & Ticket-Granting Server (TGS)
Internet or Private Data Network
Application Server
Client System running Kerberos and application client software
3) The authenticated client sends its ticket, ASK, & encrypted application server's secret key to Application Server, and initiates connection.

The Kerberos Server/KDC has two main functions (Figure 8.11), known as the Authentication Server (AS) and Ticket-Granting Server (TGS). The steps in establishing an authenticated session between an application client and the application server are:

1. The Kerberos client software establishes a connection with the Kerberos server's AS function. The AS first authenticates that the client is who it purports to be. The AS then provides the client with a secret key for this login session (the TGS session key) and a Ticket-granting Ticket (TGT), which gives the client permission to talk to the TGS. The ticket has a finite lifetime so that the authentication process is repeated periodically.

2. The client now communicates with the TGS to obtain the Application Server's key so that it (the client) can establish a connection to the service it wants. The client supplies the TGS with the TGS session key and TGT; the TGS responds with an Application Session Key (ASK) and an encrypted form of the Application Server's secret key; this secret key is never sent on the network in any other form.

3. The client has now authenticated itself and can prove its identity to the Application Server by supplying the Kerberos ticket, application session key, and encrypted Application Server secret key. The Application Server responds with similarly encrypted information to authenticate itself to the client. At this point, the client can initiate the intended service requests (e.g., Telnet, FTP, HTTP, or e-commerce transaction session establishment).

Self Assessment

Fill in the blanks:

11. With .... cryptography, a single key is used for both encryption and decryption.

12. Public-key cryptography, also known as .... cryptography, is a form of cryptography in which a user has a pair of cryptographic keys — a public key and a private key.

13. ...., also called message digests and one-way encryption, are algorithms that, in some sense, use no key.

Notes

14. .... can be used to sign or encrypt e-mail messages with the mere click of the mouse.

15. .... employs a client/server architecture and provides user-to-server authentication rather than host-to-host authentication.

Caselet

SafeScrypt Issues Digital Signature to Mahajan

SAFESCRYPT Ltd, a Satyam Infoway company affiliated with VeriSign Inc, issued the country's first digital signature certificate to the Minister for Communications and IT & Parliamentary Affairs, Mr Pramod Mahajan, at an official ceremony here on Wednesday.

SafeScrypt is the first Indian company to get a certifying authority licence for digital signature from the Controller of Certifying Authorities (CCA). The company received this licence earlier this week.

Speaking at the ceremony, Mr Mahajan said, "This event marks the beginning of a 100-per cent implementation of the IT Act 2000 and will encourage the growth of e-commerce, e-learning and e-governance in India. With this, India now becomes part of a group of around 12 countries that use digital signatures."

The Governor, Reserve Bank of India, Mr Bimal Jalan, who was also present, received the second digital signature.

A digital signature is an encryption and decryption process which uses the public key infrastructure (PKI) technology that allows for proper identification of the author of an electronic message as well as authentication and non-repudiation.

The digital certificate is a computer-generated record containing the identity of the subscriber, the public key and is digitally signed by the CA.

The certificates issued by the CA, in this case SafeScrypt, are legally recognised by the courts and are given the same status as a physical signature.

Mr Ramraj, MD & CEO, Satyam Infoway Ltd, said, "Digital signatures are the key to secure online transactions. As an Internet and networking company in India, catalysing the growth of e-commerce by enabling secure online transactions is a critical point of focus at Sify."

Source: http://www.thehindubusinessline.in/2002/02/07/stories/2002020700890700.htm

8.6 Summary

- There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography.
- Cryptography is frequently used in distributed applications to convey identification and authentication information from one system to another over a network.
- Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge.
- Digital Signature techniques are designed to provide the digital counterpart to handwritten signatures and can be achieved using cryptography.

Notes

- With symmetric key cryptography, a single key is used for both encryption and decryption. The sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver.
- Public-key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys — a public key and a private key.
- Hash algorithms are typically used to provide a digital fingerprint of a file's contents often used to ensure that the file has not been altered by an intruder or virus.
- Kerberos employs a client/server architecture and provides user-to-server authentication rather than host-to-host authentication.

8.7 Keywords

Block Cipher: It is one kind of encryption scheme which encrypts one block of data at a time using the same key on each block.

Cipher Block Chaining: It is one kind of encryption mode which adds a feedback mechanism to the encryption scheme.

Cipher Feedback: It is one kind of encryption mode which allows data to be encrypted in units smaller than the block size, which might be useful in some applications such as encrypting interactive terminal input.

Decryption: It is the reverse process of converting encoded data to its original un-encoded form, plaintext.

Digital Certificate: It is trusted ID card in electronic form that binds a website's public encryption key to their identity for purposes of public trust.

Electronic Codebook: It is one kind of encryption mode where the shared key is used to encrypt the plaintext block to form a ciphertext block.

Encryption: It is a process of coding information which could either be a file or mail message in into cipher text a form unreadable without a decoding key in order to prevent anyone except the intended recipient from reading that data.

Hash Function: It is one-way encryption that uses no key.

Output Feedback: It is one kind of encryption mode which prevents the same plaintext block from generating the same ciphertext block by using an internal feedback mechanism that is independent of both the plaintext and ciphertext bitstreams.

Public-key Cryptography: It is a form of cryptography in which a user has a pair of cryptographic keys—a public key and a private key; the private key is kept secret, while the public key may be widely distributed.

Stream Cipher: It is one kind of encryption scheme where the plaintext block is encrypted to the different ciphertext.

Symmetric Key Cryptography: It is one kind of encryption process where a single key is used for both encryption and decryption.

8.8 Review Questions

1. What is cryptography? Elucidate various applications of cryptography.
2. Illustrate the process of symmetric key cryptography.

3. Enlighten the procedure of asymmetric key cryptography.
4. What is digital certificate? Illustrate the process of verifying the certificate.
5. Explain the concept of sending and receiving messages with digital signature.
6. Make distinction between Symmetric Key Cryptography and public Key Cryptography.
7. What is hashing? Explain the use of hash function.
8. Explain the approaches used to encryption.
9. Symmetric key cryptography schemes are generally categorized as being either stream ciphers or block ciphers. Comment.
10. Write short notes on:

    (a) PGP

    (b) Hash Function

    (c) Kerberos

    (d) Certificate Authority

Answers: Self Assessment

1. Private key
2. Decryption
3. secrecy
4. Access control
5. Electronic signatures
6. Thresholding
7. Certification authority
8. SSL (Secure Sockets Layer)
9. Digital Signatures
10. Trusted Third Party (TTP)
11. Symmetric key
12. Asymmetric
13. Hash functions
14. Pretty Good Privacy (PGP)
15. Kerberos

8.9 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online links

http://all.net/edu/curr/ip/Chap2-4.html

Notes

Unit 9: Firewalls

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of Firewalls
- Discuss demilitarized zone, proxy servers, packet filtering, etc.
- Explain application level and hardware level firewalls

Introduction

A firewall is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

In this unit, you will understand various concepts of firewalls.

9.1 Meaning

Basically, a firewall is a barrier to keep destructive forces away from your property. In fact, that's why its called a firewall.

A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system. If an incoming packet of information is flagged by the filters, it is not allowed through. Let's say that you work at a company with 500 employees. The company will therefore have hundreds of computers that all have network cards connecting them together.

In addition, the company will have one or more connections to the Internet through something like T1 or T3 lines. Without a firewall in place, all of those hundreds of computers are directly accessible to anyone on the Internet. A person who knows what he or she is doing can probe those computers, try to make FTP connections to them, try to make telnet connections to them and so on. If one employee makes a mistake and leaves a security hole, hackers can get to the machine and exploit the hole.

With a firewall in place, the landscape is much different. A company will place a firewall at every connection to the Internet (for example, at every T1 line coming into the company). The firewall can implement security rules.

Example: One of the security rules inside the company might be:

Out of the 500 computers inside this company, only one of them is permitted to receive public FTP traffic. Allow FTP connections only to that one computer and prevent them on all others.

A company can set up rules like this for FTP servers, Web servers, Telnet servers and so on. In addition, the company can control how employees connect to Websites, whether files are allowed to leave the company over the network and so on. A firewall gives a company tremendous control over how people use the network.

Firewalls use one or more of three methods to control traffic flowing in and out of the network:

1. ***Packet filtering:*** Packets (small chunks of data) are analyzed against a set of filters. Packets that make it through the filters are sent to the requesting system and all others are discarded.
2. ***Proxy service:*** Information from the Internet is retrieved by the firewall and then sent to the requesting system and vice versa.
3. ***Stateful inspection:*** A newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information.

Information traveling from inside the firewall to the outside is monitored for specific defining characteristics, then incoming information is compared to these characteristics. There are many creative ways that unscrupulous people use to access or abuse unprotected computers:

1. ***Remote login:*** When someone is able to connect to your computer and control it in some form. This can range from being able to view or access your files to actually running programs on your computer.
2. ***Application backdoors:*** Some programs have special features that allow for remote access. Others contain bugs that provide a backdoor, or hidden access, that provides some level of control of the program.
3. ***SMTP session hijacking:*** SMTP is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send unsolicited junk e-mail (spam) to thousands of users. This is done quite often by redirecting the e-mail through the SMTP server of an unsuspecting host, making the actual sender of the spam difficult to trace.
4. ***Operating system bugs:*** Like applications, some operating systems have backdoors. Others provide remote access with insufficient security controls or have bugs that an experienced hacker can take advantage of.

Notes

5. ***Denial of Service:*** You have probably heard this phrase used in news reports on the attacks on major Websites. This type of attack is nearly impossible to counter. What happens is that the hacker sends a request to the server to connect to it. When the server responds with an acknowledgement and tries to establish a session, it cannot find the system that made the request. By inundating a server with these unanswerable session requests, a hacker causes the server to slow to a crawl or eventually crash.

6. ***E-mail Bombs:*** An e-mail bomb is usually a personal attack. Someone sends you the same e-mail hundreds or thousands of times until your e-mail system cannot accept any more messages.

7. ***Macros:*** To simplify complicated procedures, many applications allow you to create a script of commands that the application can run. This script is known as a macro. Hackers have taken advantage of this to create their own macros that, depending on the application, can destroy your data or crash your computer.

8. ***Viruses:*** Probably the most well-known threat is computer viruses. A virus is a small program that can copy itself to other computers. This way it can spread quickly from one system to the next. Viruses range from harmless messages to erasing all of your data.

9. ***Spam:*** Typically harmless but always annoying, spam is the electronic equivalent of junk mail. Spam can be dangerous though. Quite often it contains links to Websites. Be careful of clicking on these because you may accidentally accept a cookie that provides a backdoor to your computer.

10. ***Redirect Bombs:*** Hackers can use ICMP to change (redirect) the path information takes by sending it to a different router. This is one of the ways that a denial of service attack is set up.

11. ***Source Routing:*** In most cases, the path a packet travels over the Internet (or any other network) is determined by the routers along that path. But the source providing the packet can arbitrarily specify the route that the packet should travel. Hackers sometimes take advantage of this to make information appear to come from a trusted source or even from inside the network! Most firewall products disable source routing by default.

Some of the items in the list above are hard, if not impossible, to filter using a firewall. While some firewalls offer virus protection, it is worth the investment to install anti-virus software on each computer. And, even though it is annoying, some spam is going to get through your firewall as long as you accept e-mail.

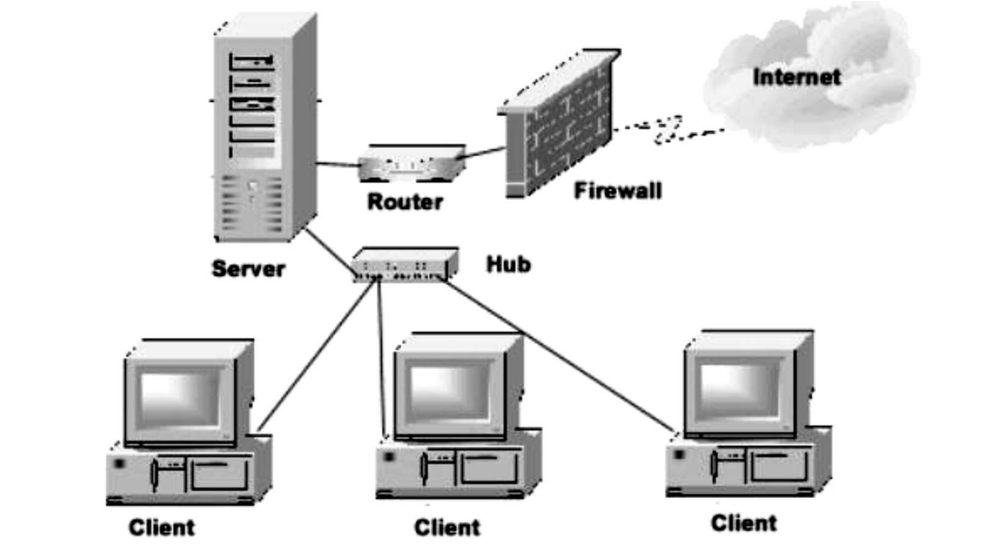
The level of security you establish will determine how many of these threats can be stopped by your firewall. The highest level of security would be to simply block everything. Obviously that defeats the purpose of having an Internet connection. But a common rule of thumb is to block everything, then begins to select what types of traffic you will allow.

You can also restrict traffic that travels through the firewall so that only certain types of information, such as e-mail, can get through. This is a good rule for businesses that have an experienced network administrator that understands what the needs are and knows exactly what traffic to allow through.

For most of us, it is probably better to work with the defaults provided by the firewall developer unless there is a specific reason to change it. One of the best things about a firewall from a security standpoint is that it stops anyone on the outside from logging onto a computer in your private network.

While this is a big deal for businesses, most home networks will probably not be threatened in this manner. Still, putting a firewall in place provides some peace of mind.

Figure 9.1: Firewall



Task Discuss the use of macros.

Did u know? The job of firewall is similar to a physical firewall that keeps a fire from spreading from one area to the next.

Caution If the comparison yields a reasonable match, the information is allowed through. Otherwise it is discarded.

Self Assessment

Fill in the blanks:

1. A .... is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system.
2. Firewalls are frequently used to prevent .... Internet users from accessing private networks connected to the Internet, especially intranets.
3. A .... is a small program that can copy itself to other computers.

9.2 Demilitarized Zone (DMZ)

In computer networking, Demilitarized Zone (DMZ) is a firewall configuration for protecting local area networks (LANs).

In a DMZ configuration, most computers on the LAN run behind a firewall associated to a public network like the Internet. One or more computers also run outside the firewall, in the DMZ. Those computers on the outside intercept traffic and broker, asks for the remaining LAN, adding an additional layer of defense for computers behind the firewall.

Notes

Traditional DMZs permit computers behind the firewall to start requests outbound to the DMZ. Computers in the DMZ in turn respond, forward or reissue needs out to the Internet or other public network, as proxy servers do. Many DMZ implementations, actually, simply utilize a proxy server or servers as the computers inside the DMZ. The LAN firewall, however, averts computers in the DMZ from commencing inbound requests.

DMZ is a generally-touted trait of home broadband routers. Though, in most instances these traits are not true DMZs. Broadband routers frequently implement a DMZ just through additional firewall rules, signifying that incoming requests arrive at the firewall directly.

⚠

Caution In a true DMZ, incoming requests must first pass via a DMZ computer before attaining the firewall.

Self Assessment

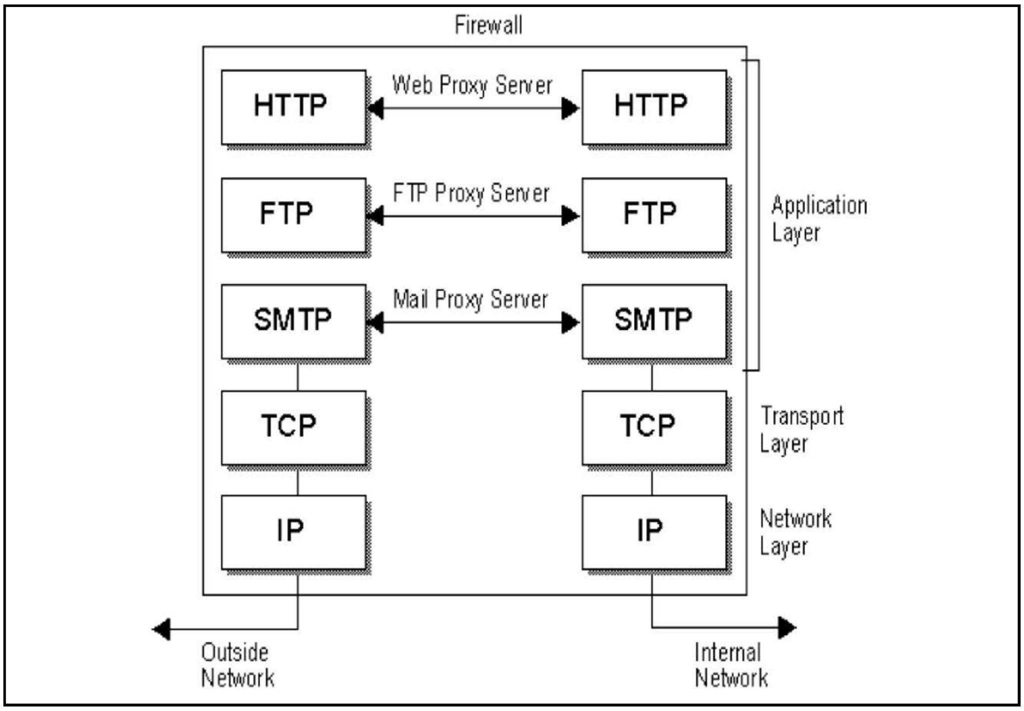
Fill in the blanks:

4. .... is a firewall configuration for protecting local area networks (LANs).

5. Computers in the DMZ in turn respond, forward or reissue needs out to the Internet or other public network, as .... do.

9.3 Proxy Servers

A firewall proxy server is considered an application that appears as an mediator among tow end systems. Firewall proxy servers function at the application layer of the firewall, where both ends of an association are forced to carry out the session through the proxy. They do this by producing and running a process on the firewall that mirrors a service as if it were running on the end host.



Source: http://www.akadia.com/services/firewall_proxy_server.html

A *firewall proxy server* fundamentally turns a two-party session into a four-party session, with the middle procedure emulating the two real hosts. A proxy service must be run for every type of Internet application the firewall will support — a Simple Mail Transport Protocol (SMTP) proxy for e-mail, an HTTP proxy for Web services and so on.

Did u know? Since *firewall proxy server* function at the application layer, proxy servers are also known as *application layer firewalls*.

> *Notes* Proxy servers are approximately always one-way preparations running from the internal network to the external network.

Self Assessment

Fill in the blanks:

6. Firewall proxy servers function at the .... layer of the firewall, where both ends of an association are forced to carry out the session through the proxy.

7. A *firewall proxy server* fundamentally turns a two-party session into a .... session, with the middle procedure emulating the two real hosts.

9.4 Packet Filtering

In a packet filtering firewall, the firewall inspects five packet traits:

1. Source IP address
2. Source port
3. Destination IP address
4. Destination port
5. IP protocol (TCP or UDP)

Depending upon rules configured into the firewall, the packet will either be permitted through, rejected, or dropped. If the firewall discards the packet, it sends a message back to the sender allowing him/her recognize that the packet was discarded. If the packet was dropped, the firewall just does not respond to the packet. The sender must linger for the communication to time out. Dropping packets rather than rejecting them greatly enlarges the time needed to scan the network. Packet filtering firewalls function on Layer 3 of the OSI model, the Network Layer. Routers are a very common form of packet filtering firewall.

An enhanced structure of the packet filtering firewall is a packet filtering firewall with a state oriented examination engine. With this augmentation, the firewall "remembers" conversations among systems and networks. It is then essential to fully scrutinize only the conversation's first packet.

Self Assessment

Fill in the blanks:

8. In packet filtering, depending upon rules configured into the firewall, the .... will either be permitted through, rejected, or dropped.

9. .... firewalls function on Layer 3 of the OSI model, the Network Layer.

9.5 Screening Routers

A screening router is a fundamental part of most firewalls. A screening router can be a commercial router or a host-based router with some sort of packet filtering potential. Usual screening routers have the aptitude to block traffic among networks or specific hosts, on an IP port level. Some firewalls contain nothing more than a screening router between a private network and the Internet.

Many networks are firewalled by means of only a screening router among the private network and the Internet. This type of firewall is dissimilar from a screened host gateway in that typically there is direct communication allowed among multiple hosts on the private network, and multiple hosts on the Internet. The region of risk is equivalent to the number of hosts on the private networks, and the number and type of services to which the screening router allows traffic. For each service provided via peer-to-peer connection the size of the zone of risk increases sharply. Finally it is impossible to quantify. Damage control is hard as well because the network administrator would require to frequently examine every host for traces of a break-in. If there is no usual audit one must hope to stagger on a clue.

Example: A mismatched system accounting record.

In the case of total devastation of the firewall, it tends to be very tough to trace or even to find out. If a commercial router (which does not preserve logging records) is used, and the router's administrative password is negotiated, the whole private network can be laid unlock to attack very easily. Cases are recognized where commercial routers have been configured with erroneous screening rules, or have come up in some pass-through mode due to hardware or operator error. Usually, this configuration is a case of "That which is not specifically prohibited is allowed" as the ingenious consumer can fairly easily piggyback protocols to attain a higher level of access than the manager expects or wants.

Screening routers are not the most protected solution, but they are popular as they authorize fairly free Internet access from any point inside the private network. Many consultants and network service providers display screening routers in a "firewall" configuration.

Notes It is uncertain if the a variety of trade-offs concerned are clear to the customer; therefore the use of a screening router to protect sensitive information or trade secrets would not be suggested since screening routers are very permeable from the within.

Self Assessment

Fill in the blanks:

10. A .... can be a commercial router or a host-based router with some sort of packet filtering potential.

11. Many networks are firewalled by means of only a screening router among the .... network and the Internet.

9.6 Application Level Firewalls

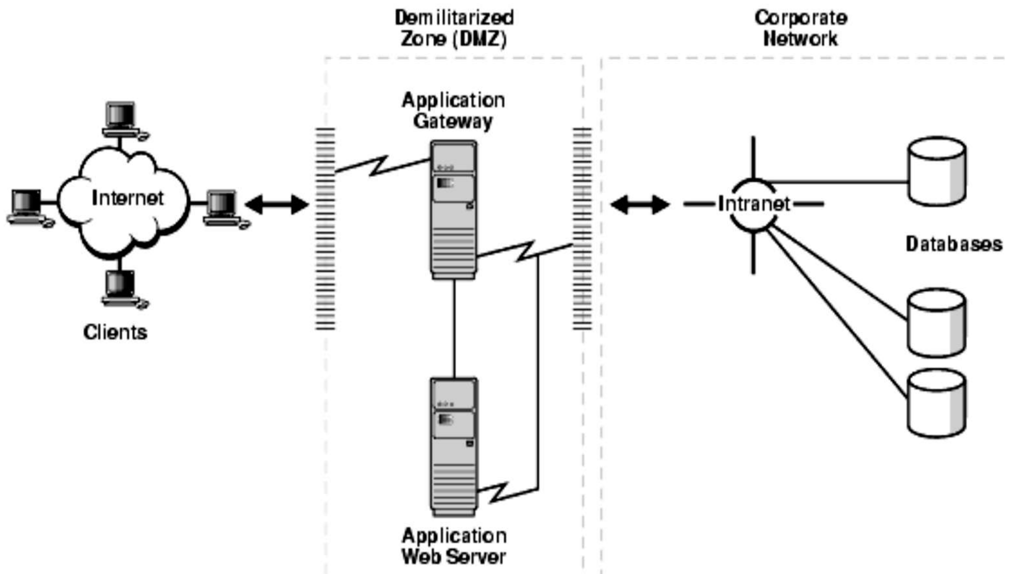
An application gateway is an application program that runs on a firewall system between two networks. It is also known as application proxy or application-level firewalls. When a client program establishes a connection to a destination service, it connects to an application gateway, or proxy. The client then negotiates with the proxy server in order to communicate with the destination service.

In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall.

This creates two connections: one between the client and the proxy server and one between the proxy server and the destination. Once connected, the proxy makes all packet-forwarding decisions. Since all communication is conducted through the proxy server, computers behind the firewall are protected.

While this is considered a highly secure method of firewall protection, application gateways require great memory and processor resources compared to other firewall technologies, such as stateful inspection.

Figure 9.2: Internet Network Access Control with an Application Gateway



Task Discuss the types of connections used in Application Level Firewalls.

Self Assessment

Fill in the blanks:

12. An .... is an application program that runs on a firewall system between two networks.

13. When a client program establishes a connection to a .... service, it connects to an application gateway

9.7 Hardware Level Firewalls

Hardware firewalls are precisely what the name entails; a hardware device that is positioned anywhere in the traffic flow of an organization's network. Once in place, the device obtains and

Notes

examines packets traveling into and out of the network. The device then verifies a list of previously mentioned access rules to observe if it should permit the packet to carry on to its destination, or if the packet should be unnecessary. There are a number of benefits to by means of hardware firewalls. The devices do not rely on general operating systems, for instance Microsoft Windows or Linux, so they are resistant to the seemingly infinite number of bugs, viruses, and other malicious attacks that those operating systems undergo from. Hardware firewalls also carry out much improved (faster) than a software dependent solution, and are much more scalable – additional devices can be added as required with relative simplicity. Performance should be one of the key considerations when choosing a firewall solution because of the fact that all network traffic traveling into and out of the organization's network will pass via the device and it takes time and processing overhead to examine each packet to determine what requires to be done with it. Another benefit is that hardware firewalls only perform firewall associated duties and are not loaded with other tasks. This type of single-purpose functionality permits these hardware devices to execute their designed tasks much more successfully than a multi-function software dependent solution. Counter to the benefits, hardware firewalls also undergo from a number of disadvantages.

Example: If the device goes down, all inbound and outbound network traffic discontinues, which can be operationally intolerable to an organization. Also, due to their proprietary nature, hardware firewalls need specialized knowledge to install, configure, and administer efficiently. Lastly, the financial costs of hardware based solutions are fairly high because of initial acquisition in addition to the previously mentioned specific administrative resources necessary to function them.

Self Assessment

Fill in the blanks:

14. .... firewalls are precisely what the name entails; a hardware device that is positioned anywhere in the traffic flow of an organization's network.

15. .... is one of the key considerations when choosing a firewall solution.

9.8 Summary

- A firewall is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.
- Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets.
- A firewall is simply a program or hardware device that filters the information coming through the Internet connection into your private network or computer system.
- In computer networking, Demilitarized Zone (DMZ) is a firewall configuration for protecting local area networks (LANs).
- Firewall proxy servers function at the application layer of the firewall, where both ends of an association are forced to carry out the session through the proxy.
- A screening router is a fundamental part of most firewalls. A screening router can be a commercial router or a host-based router with some sort of packet filtering potential.
- An application gateway is an application program that runs on a firewall system between two networks. It is also known as application proxy or application-level firewalls.

- Hardware firewalls are precisely what the name entails; a hardware device that is positioned anywhere in the traffic flow of an organization's network.

9.9 Keywords

Application Gateway: It is an application program that runs on a firewall system between two networks.

Firewall: It is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.

Macro: To simplify complicated procedures, many applications allow you to create a script of commands that the application can run; this script is known as a macro.

Stateful Inspection: It is a newer method that doesn't examine the contents of each packet but instead compares certain key parts of the packet to a database of trusted information.

Virus: A virus is a small program that can copy itself to other computers.

9.10 Review Questions

1. How firewalls control the in and out flowing traffic of the network?
2. What is firewall? How can firewall be implemented?
3. Explain the methods that unscrupulous people use to access or abuse unprotected computers.
4. How firewall controls the traffic flowing in and out of the network?
5. What is proxy server? Explain the function of firewall proxy server.
6. Explain the various characteristics of packet filtering firewall.
7. Make distinction between application level gateway and hardware level gateway.
8. Describe different types of firewall.
9. Write short note on application gateway.
10. Explain the concept of Demilitarized Zone (DMZ) configuration.

Answers: Self Assessment

1. firewall
2. unauthorized
3. virus
4. Demilitarized Zone (DMZ)
5. proxy servers
6. application
7. four-party
8. packet
9. Packet filtering
10. screening router
11. private
12. application gateway
13. destination
14. Hardware
15. Performance

Notes

9.11 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

*Risk Management Guide for Information Technology System*s

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online link

http://compnetworking.about.com/cs/networksecurity/g/bldef_dmz.htm

Unit 10: Databases Security

Notes

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of databases security
- Discuss need for database security
- Explain mobile database security
- Understand enterprise database security
- Discuss database security policy

Introduction

As the utilization of Internet technology is mounting for both the Intranet and the Internet, information security is turning out to be exceedingly vital for organizations. The World Wide Web offers a suitable, cheap, easily accessible and instantaneous manner of information distribution. It makes the distribution very simple but, it is evenly significant to make sure that information should only be available to equitable users who have access rights to it.

With many organizations using database dependent dynamic web pages, corporate information security has turn out to be tremendously significant. Previously, strict database access or specialized client software was necessary for viewing the data, but nowadays a simple web browser is enough to view data in a database that is not correctly protected. Therefore, information security is at a susceptible stage. Therefore, the more a computing firm moves from the processor of the client/server to the Internet the more possibilities of security dispersion.

Security database professionals have to depend on network administrators for executing firewalls or other mechanisms to defend local data as the nature of Intranet/Internet information access

Notes

is such; though, the database administrator (DBA) has to carry out many security function. This unit will scrutinize the primary security areas that fall inside the field of the DBA, who then has to create database familiarized solutions.

10.1 Database Security

You must understand that security is a voyage, and not the final target. We cannot suppose a method is completely secure, we may not be alert of fresh/new attacks on that method. Many security vulnerabilities are not even available as attackers want to postponed a fix, and manufacturers do not want the harmful publicity. There is an ongoing and uncertain discussion over whether highlighting security vulnerabilities in the public field encourages or assists avoidance of further attacks.

The safest database you can visualize must be found in a most firmly locked bank, or nuclear-proof bunker, installed on a standalone computer devoid of an Internet or network connections, and under protector for 24×7×365. Though, that is not a probable scenario with which we would like to function. A database server is to continue with services, which frequently enclose security problems, and you should be practical about probable threats. You must suppose failure at some point, and never amass truly sensitive data in a database that illegal users may easily penetrate/ access.

A main point to think here is that most data loss appears due to social exploits and not technical ones. Therefore, personnel procedures may more than encryption algorithms require to be looked into.

You will be able to build up an effective database security, if you understand that securing data is necessary to the market reputation, productivity and business objectives.

Example: As personal information like credit card or bank account numbers are now usually obtainable in many databases; so, there are more opportunities for identity theft.

As per estimation, more than half of all identity theft cases are devoted by employees who have access to large monetary databases. Banks, companies that take credit cards services outwardly must place greater stress on safeguarding and scheming access to this proprietary database information.

10.1.1 Levels of Database Security

Securing the database is a basic principle for any security workers while mounting his or her security plan. The database is a compilation of useful data and can be considered as the most essential constituent of an organization and its economic enlargement. As a result, any security effort must remember that they need to offer the strongest level of control for the database.

As is accurate for any other expertise, the security of database management systems is based on many other systems. These chiefly comprise the operating system, the applications that use the DBMS, services that interrelate with the DBMS, the web server that makes the application obtainable to end users, etc.

Caution Be aware that most prominently, DBMS security is based on us, the-users.

Common Database Security Failures

The common drawbacks that intimidate database security are:

1. ***Weak User Account Settings:*** Many of the database user accounts do not enclose the user settings that may be establish in operating system surroundings.

Example: The user accounts name and passwords, which are generally known, are not disabled or customized to avert access.

The user account settings permit restricted capabilities for security, without password controls on dictionary checks or account controls assisting expiration of user account.

2. ***Insufficient Segregation of Duties:*** No recognized security administrator role is mentioned in the database management of the organization. This effects in database administrators (DBAs) performing both the functions of the manager (for users accounts), in addition to the performance and operations specialist. This may consequence in management inefficiencies.

3. ***Inadequate Audit Trails:*** The auditing potentials of databases since it need keeping track of additional needs, are frequently ignored for improved performance or disk space. Inadequate auditing consequences in abridged accountability. It also decreases the effectiveness of data history analysis. The audit trails records information concerning the actions taken on firm critical of data. They log events directly connected with the data, therefore they are essential for monitoring the access and the actions on a database system.

4. ***Unused DBMS Security Features:*** The security of an individual application is typically sovereign of the security of the DBMS. **Please note** that security dimensions that are built into an application pertain to users of the client software only. The DBMS itself and many other tools or utilities that can attach to the database directly via ODBC or any other protocol, may bypass this application level security totally. So, you must attempt to use security limitations that are reliable.

Example: Try using security mechanism that are defined inside the database.

Fundamentally database security can be broken down into the following levels:

1. Server Security
2. Database Connections
3. Table Access Control
4. Restricting Database Access.

These database security levels are discussed as below:

Server Security: Server security includes limiting access to data accumulated on the server. It is the most significant choice that has to be taken in deliberation and planned suspiciously.

Database Connections: By means of the ODBC will have to be followed by inspecting that every connection corresponds to a particular user who has access to data.

Database contact should be restricted to machines that have to converse to it while assuring standard safeguards are in position.

Also, if a company accesses a Web application to use its database — with such scripts in Active Server Page, or ASP.NET technology — and the scripts crash, it can possibly disclose its source code when it generates an error report.

In this case, limiting database access to the accurate users is necessary. If through appropriate security gauges the database access is already restricted to the true users, any script crashes will not disclose database connection information to the erroneous users.

This takes place more than a few times — the database connection name and password for all the world to view. It is recommended to change the password for the database connection on a regular basis, which adds just one more layer of security to the procedure.

Table Access Control: The access control table is the most general type of securing a database. A suitable use of the table access control includes a close association among the administrator and the base developer.

Restricting Database Access: There are situations when access to a specific database should be restricted to some assured users. The NCSA httpd server has incorporated user authentication traits that can be simply adapted to function with an online database.

What to Protect

The server authentication scheme is proposed to handle access to file system objects. Access can be approved to some people or sites or certain sites can be declined access.

Here, we consider a CGI script we want to control access to since it comprises the database interface routines. Access control can be recognized in the directory where the CGI script appears and only selected users or sites will be able to interact with our database.

If all of our interface functions are contained in a single executable then protecting certain interface **functions** from illegal access is a little difficult. You can perform this by creating a symbolic link to the CGI executable in a secluded directory and calling the secluded version whenever a prohibited procedure is preferred.

The Access Control File

In the directory where the secluded script appears, generate a file known as .htaccess. In the file, put the following:

```
AuthUserFile /home/beowulf/public_html/.htpasswd

AuthGroupFile /dev/null

AuthName Test

AuthType Basic


<Limit GET>

require user pumpkin

</Limit>
```

Select a suitable name and directory for AuthUserFile, which will be generated shortly. It should not be in the secluded directory, as it will enclose all the usernames and passwords for access to that directory. The AuthGroupFile can be accessed to set up access for particular groups, which are defined in a "group file".

The AuthName above is the name of the form that will emerge on the dialog box asking for a password.

The Password File

NCSA httpd occurs with a program known as htpasswd. To generate the password file and add a user to it, execute htpasswd /home/beowulf/public_html/.htpasswd pumpkin substituting the path for the password file to the path suitable for your system. The file will be generated and the username "pumpkin" added to it. You will be prompted twice for "pumpkin's" password.

There is totally no connection among users in this file and users on your local host. Users with local accounts can use the similar (or different) names in your local password file, with same (or different) passwords. Outside users can have usernames in this file without having an account on your system. This technique only controls access to the files in the preferred directory.

Any user trying to use a file in the secluded directory will be encouraged for a password by their client browser, which will pass it back to your server for confirmation. If they are in the password file, access will be permitted.

Did u know? Database security is of dominant significance for an organization, but many organizations do not take this truth into deliberation, till an ultimate problem appears.

Task What is audit trail?

Self Assessment

Fill in the blanks:

1. With many organizations using database dependent dynamic web pages, ... information security has turn out to be tremendously significant.

2. Many security .... are not even available as attackers want to postponed a fix, and manufacturers do not want the harmful publicity.

3. The .... is a compilation of useful data and can be considered as the most essential constituent of an organization and its economic enlargement.

4. The .... records information concerning the actions taken on firm critical of data.

10.2 Need for Database Security

The general factor in nowadays global economy where most of the business is prepared electronically by means of B2B [Business to Business] or by means of B2C [business to consumer] or other more conventional methods' is electronic transfer and storage of data. This very electronic data is the organization major information assets. A negotiation of this data could bang the business out or holdup in the processing this data could direct to customer approval concerns and loss of market share.

Regardless of how we look into this challenge, it is greatest significant from the viewpoint of the guardian of that electronic data to have it in a protected form that is readily available to the applications that are certified to access and influence it. In the interest of best practice in addition to keep this electronic data protected in the databases, here is a tool that adds value and highlights concerns before they could be demoralized. We are conversing about Secure Audit.

Compliance with Regulation

In the United States, the Gramm-Leach-Bliley Act needs companies to inform consumers of their privacy policies and to offer opt-out provisions for customers who do not want their personal information distributed away from the company. Additionally, the Gramm-Leach-Bliley Act protects non-public financial data. Data amassed on a computer that has even a remote possibility of enclosing information like social security numbers, credit card and financial account numbers, account balances, and investment portfolio information must be confined. The use and revelation of patient medical information initially was confined by a patchwork of U.S. state laws, leaving gaps in the security of patients' privacy and confidentiality. The United States Congress also documented the requirement for national patient record privacy standards in 1996 when it endorsed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), caring all medical records and other independently identifiable health information used or disclosed by an enclosed entity in any form, whether electronically, on paper, or orally. In addition to the legal consequences of a security breach, independent research firm, Computer Economics has validated that malicious attacks effect in actual financial costs, decreases in revenue, and an unbelievable force on productivity.

In the last numerous years, there has been a considerable growth in cyber crimes. These days more and more hacker are objecting enterprise applications and database servers. Most large organizations have already installed antivirus software, firewalls and even Intrusion Detection Systems (IDSs) to protect their networks and host operating systems, but fail to provide proper concentration to enterprise database servers, on the supposition that they are secluded by firewalls and other defenses at the network perimeter. Yet these databases are the main reason enterprises invest in IT in the first place, and the data they enclose are frequently the enterprise's most valuable assets. Certainly, an enterprise without database security is like a bank with locks on the doors and armed protectors by every entrance, but no vault.

Database servers are attacked by hackers because:

1. If we gaze closely we will see why the hackers adore hacking the database server.
2. Most of the database servers are configures with default usernames and passwords, etc. user Scott password Tiger or user system password manager.
3. Most of the database servers are using default setting which was set by manufacturers, etc., by default public have opportunity to implement.
4. Database servers are not patched correctly.

Task Describe Why hackers attack database servers.

Self Assessment

Fill in the blanks:

5. The general factor in today's .... economy where most of the business is prepared electronically by means of B2B [Business to Business] or by means of B2C [business to consumer]
6. An .... without database security is like a bank with locks on the doors and armed protectors by every entrance, but no vault.

10.3 Mobile Databases Security

A mobile database is said to be a database that can be associated to by a mobile computing device over a mobile network .The client and server contain wireless connections. A cache is sustained to hold recurrent data and transactions so that they are not lost because of connection failure. A database is a structured manner to organize information. This could be a list of contacts, price information or distance travelled. The utilization of laptops, mobiles and PDAs is growing and possible to augment in the future with progressively more applications locating in the mobile systems. While those similar analysts can't tell us precisely which applications will be the most well-liked, it is obvious that a large percentage will need the use of a database of some class. Many applications like databases would need the ability to download information from an information storehouse and function on this information even when out of range or detached.

Example: An example of this is a mobile workforce. Here user would need to access and modernize information from files in the home directories on a server or customer proceedings from a database. This sort of access and work load produced by such users is dissimilar from the traditional workloads observed in client–server systems of today.

With the arrival of mobile databases, now users can load up their smart phones or PDAs with mobile databases to substitute mission-critical data distantly without distressing regarding time or distance. Mobile databases allow employees to enter data on the fly. Information can be harmonized with a server database later on.

With the growth in popularity of smartphones has come an increasing requirement to secure them. As their introduction mobile phones have becoming risingly smaller, more strong with rising storage potential and have remained costly items. With the rise of their popularity so has the requirement to protect the devices from theft in addition to traditional threats that effect computers like malware and the requirement to back and protect the data on the devices.

Database security is also an expertise within the broader discipline of _computer security. For many businesses applications are going mobile that signifies using enterprise data in mobile context, therefore using a mobile DBMS. With these new enhancements the business data of an enterprise can be made obtainable to an even larger number of users and a broader range of applications than before. To function on business data anytime and anywhere is the major objective pursued by developing mobility assistance in database context. The confidentiality of mission-critical data must be assured, although most mobile devices do not offer a secure surroundings for storage of such data. Security needs that apply to a central company database should apply identically and in a proper manner to the parts of the database replicated on mobile devices in the field. A mobile database security infrastructure is required to fulfill this goal. When producing such an infrastructure, we can benefit from the consequences of traditional database security work. But we also require to adapt the current techniques and approaches to the mobile context, and we require to produce new ones that attack some issues particular to use of database systems in mobile environment.

The need of databases in contemporary businesses and governmental institutions is enormous and still mounting. Many mission-critical applications and business processes depend on databases. These databases enclose data of different amount of significance and discretion, and are used by a broad variety of users. Integrity violations for a database can have severe impact on business processes; revelation of confidential data in some cases has the similar effect. Traditional database security offers techniques and approaches to manage such problems with respect to database servers in a non-mobile context.

For many businesses applications are using mobile by means of enterprise data in a mobile context, therefore using a mobile DBMS.

To function on business data anytime and anywhere is the main goal pursued by rising mobility support in database circumstance. The confidentiality of mission- vital data must be assured, although most mobile devices do not offer secure surroundings for storage of such data. Security needs that apply to a central company database should apply likewise and in an suitable manner to the parts of the database simulated on mobile devices in the field. A mobile database security infrastructure is required to fulfill this goal.

> *Notes* When producing such an infrastructure we can benefit from the results of customary database security work. But we also require to adapt the obtainable techniques and approaches to the mobile context, and we require to develop new ones that attack certain concerns particular to use of database systems in a mobile surroundings.

Did u know? With the new enhancements the business data of an enterprise can be made obtainable to an even larger number of users and a broader range of applications than before.

Mobile work by means of mobile devices and wireless links figures out a row of problems regarding security concerns such as availability, integrity and responsibility. These needs appear for network components in addition to database systems. Mobile work involving mobile database access makes ever-present computing, anywhere and anytime probable. The mobility needs appropriate hardware and software. Mobile devices such as handhelds connected through wireless networks aid mobile users, particularly in connection with position penetrating tools. New hazards and challenges for security and privacy appear in this environment. The objective is the defense of mobile users and their data. Security measures must consider the distribution of data and their heterogeneous treatment concerning security models. Limited mobile resources build insecure communication essential to imitate used data and augment the risk of limiting or dismissing security measures.

10.3.1 Mobile Conditions

Mobile work is context-sensitive work with contexts illustrating environmental traits and the relationships among them. In Lubinski, 1998, the particular problems of database systems in such a mobile environment are illustrated in more detail manner. Now, we sum up the main mobile circumstances causing different threats. Applications and needed data are location reliant, but their access must be location see-through. Determined tasks are valid on particular whereabouts. The mobile infrastructure limits the obtainable volume and type of data and the data transfer. Context information figures out further which people and objects in the environment stay. Assisting mobile work includes offering access to interesting data at the suitable location, time and device, i.e. where and when the data are used depending on user aims, preferences, knowledge and skills. For this point we need different information about the current infrastructure, obtainable mobile resources, connectivity, costs and period of connections, and bandwidths. Mobile work is characterized by uncommon and momentary short connections to the fixed network (low connectivity) and by different access types. The mobile user accesses data that are also used by other users or itself on dissimilar locations and devices, correspondingly. The mobile context involves mobile work and communication attending meta data to support users. This meta-information is included in following parts of the mobile context:

1. Human factors, their tasks, roles, other persons.
2. Location (and altering location in time), hard and software (mobile site and network traits, equipment and tools).
3. Information, application traits (such as type, size). These mobile traits, and particularly their dynamics, and limits like frequent disconnections create a mobile work with database systems difficult. This is the reason for a variety of difficulties in protecting mobile work and for needing a new perspective to renowned security measures, or stipulate new ones.

Wireless network is turning out to be a usually used communication platform. It offers a cheaper manner to get associated and in some cases this is the only method to reach people. Though, it has a number of simple and hard problems and they must be solved before Mobile database system can be constructed.

The rising trend is to make all service offering disciplines, like web, E-commerce, workflow systems, etc., fully mobile in order that any service can be offered from any position. Customer can look for the information space from any position at anytime and do their shopping, make flight reservation, open bank account, and so on. This is what the wireless technology forcing us to.

Self Assessment

Fill in the blanks:

7. Database security is an expertise within the broader discipline of .... security.
8. To function on business data anytime and anywhere is the major objective pursued by developing .... assistance in database context.
9. Traditional database security offers techniques and approaches to manage problems with respect to database servers in a .... context.

10.4 Enterprise Database Security

For many system administrators, the expressions “open systems” and “security” can appear impossibly conflicting. Preserving security for a centralized database system is hard enough, and when faced with a network of networked databases, preserving a level of access and update security is a formidable confront. Security is frequently an afterthought, and the database industry is overwhelmed with sub-standard security, particularly for enterprise databases that are cobbled-together as an effect of external factors such as business acquisitions.

There are many troubles with security for enterprise databases, far more than the IT industry would be concerned to acknowledge. These security disclosures stem from the following architectural concerns:

1. ***Multiple entry points:*** Unlike a customary centralized database, web-based databases have several entry points. These entry points comprise web servers, VPN access, app server access and access to databases through web portal protocols. When dealing with accurately hundreds of entry points, special care requires to be taken to insure that damaging viruses are not introduced into the system.
2. ***Weakest link problem:*** The current publicity regarding security holes in enterprise security underscores the weakest link problem. When dealing with such a broad variety of entry points and platforms, the overall system security is only as protected as the weakest link in the federation.

Notes

Caution No matter how much care is taken to assure security at the database level, troubles can still be introduced from a diversity of other sources.

Example: Once a hack get root access to a web server, it is frequently easy to gain access to the database server, particularly when remote shell ability is enabled.

3. ***Web-based databases:*** Database that are configured to permit external communications from other web portals face an outstanding data security challenge. Hacker can continually try to hack into web portals, finally locating a weakness in the Net Services architecture.

Self Assessment

Fill in the blanks:

10. .... entry points comprise web servers, VPN access, app server access and access to databases through web portal protocols.
11. The current publicity regarding security holes in enterprise security underscores the ....
12. No matter how much care is taken to assure .... at the database level, troubles can still be introduced from a diversity of other sources.

10.5 Database Security Policy

With all the government and industry policies affecting almost every business, sooner or later, the time will come when you're fundamentally forced to put some information security policies in position. You may already have the fundamental policies for passwords and data backups. But there's more. So, if your association is just now putting together its safety policies or you've realized it may be time to inform a few things, there are numerous database security-related issues you'll require to wrap.

To be precise, in order to find out exactly which security policies are required, you need to perform an information risk assessment. Though, I understand that reality frequently dictates otherwise. That said, I can think of little, if any, situations that wouldn't need the following database connected security policies at the very least:

1. ***Acceptable usage*** – What can/cannot be finished on database servers like web browsing and installing/disabling malware and personal firewall protection in addition to installation of MSDE, SQL Server Express 2005, and other database software on non-server systems.
2. ***Authentication controls*** – for databases in addition to related applications and operating systems including password requirements, multi-factor usage, etc.
3. ***Business associates*** – dealing with external contractors, auditors, hosting providers, etc. counting contract provisions and service level agreements where applicable.
4. ***Business continuity*** – disaster recovery and/or business continuity plan requirements to help keep your databases up and accessible.
5. ***Change management*** – documenting the who, why, when, how, and any related backout procedures, etc.
6. ***Data backup*** – what, when, and methods used.
7. ***Data retention and destruction*** – what, why, methods used and timelines.

8. ***Encryption*** – including both data at rest such as encrypting specific rows, and data in transit such as TLS between the database server and Web application. Data backups would also be incorporated.
9. ***Information classification*** – labeling needs for public, internal, confidential, etc.
10. ***Physical security*** – building, data center, and server security.
11. ***Removal of property*** – servers, drives, tapes, and other property.
12. ***Security testing and audits*** – what, how, when, and who will perform testing along with what tools will be used.
13. ***Separation of duties*** – the roles/responsibilities of users, DBAs, security auditors and others involved with database management.
14. ***System maintenance*** – patching, system purging/cleanups and malware updates.
15. ***System monitoring and incident response*** – the who, why, when and how of real-time monitoring and audit logging, as well as specific requirements for maintaining a formal incident response plan.
16. ***User authorization*** – adding/removing users and conceding admin rights for whom, why, when and for how long.

There are a number of significant points I would like to make connected to database-centric security policies. Firstly, if management hasn't affirmed their support (i.e. they're going to squeeze and impose the policies), you might additionally decline this exercise on the whole. So get them on board first. Second, range your policies at the highest level probable so you can maximize the number of departments and systems included. Maximize the number of rules you can really be in fulfillment with. Alternatively, if you can support it, don't produce all of the above policies for your databases and have another set for wireless networks, storage systems and so on. Similarly, appreciate your organization's regulatory needs at least to the point where one set of policies addresses PCI, GLBA, HIPAA, SOX, etc. This will be best served if you have compliance or IT governance committee that oversees and executes security policies. You don't want your own set of policies to handle if you can assist it.

Lastly, confirm you document your policies in a method that'll make comprehension and administration as simple as possible. The following policy elements are necessary for keeping policies simple and convenient long-term.

1. ***Introduction*** – a short overview of the topic such as encryption.
2. ***Purpose*** – briefly outlines the high-level goal(s) and approach of the policy.
3. ***Scope*** – States which employees, departments and database systems are covered.
4. ***Roles and responsibilities*** – outlines who's concerned and what they're expected to do to support the policy.
5. ***Policy statement*** – your actual policy statement/statements. You should have one policy statement per subject. Alternatively, create a separate template for each of the policies listed above that you prefer to use.
6. ***Exceptions*** – underscores the people, departments, databases, etc. that are not covered by the policy.
7. ***Procedures*** – detailed steps on how the policy is being executed and enforced in your environment. You may want to reference this information and place it in a separate document.

Notes

8. ***Compliance*** – outlines measures on how compliance with this policy will be calculated including any metrics involved.
9. ***Sanctions*** – outlines what appears when the policy is violated. This may include X happens on the first offense, Y happens on the second offense, and Z happens on the third offense.
10. ***Review and evaluation*** – states when the policy must be reviewed for accuracy, applicability, and compliance purposes (i.e. SOX, HIPAA, GLBA, PCI, etc.).
11. ***References*** – Points to rigid code sections and information security standards (ISO/IEC 17799, ITIL, COBIT, etc.).
12. ***Related documents*** – refers to other policies, guidelines, standards, and related documents.
13. ***Revisions*** – section for documenting ongoing alterations made to this policy document.
14. ***Notes*** – highlights notes, tips, etc. that can help with future policy management and enforcement.

Notes If you do all of this to construct out your policies in the right method, it'll save you a lot of time over the long drag and make your auditors pleased to boot.

Self Assessment

Fill in the blanks:

13. To be precise, in order to find out exactly which security policies are required, you need to perform an information .... assessment.
14. .... include detailed steps on how the policy is being executed and enforced in your environment.
15. .... points to rigid code sections and information security standards (ISO/IEC 17799, ITIL, COBIT, etc.).

Caselet

Symantec Corp Launches Database Security Products

Trying to keep ahead of security threats that could affect consumers, Symantec Corp has introduced the Symantec Database Security and the Raw Disk Virus Scan. Most of the development work has been carried out from its Pune development centre.

Talking to presspersons, Mr Mark Bregaman, Chief Technology Officer, Symantec Corp, said it had developed a new tool that would help identify root kits in the users' systems that usually escape its antivirus tools. The new product, called "Raw Disk Virus Scan," goes below the file level to read raw blocks of data, enabling it to "see" rootkits that otherwise would be difficult to spot. It is a technology that has been developed bringing together storage management technologies from the erstwhile Veritas and security technology from Symantec.

He said that most of the development work was handled by the Pune development team. The company was now shipping products to the customers. On the Symantec database security, he said that it was always 'trying to keep the bad boys out.' But this software would sit on the system and continuously monitor what was being sent out or received.

Contd...

This would be recorded and could help organisations keep track of whatever data packet was sent out. He said that this would help in auditing, fraud and extrusion detection. This concept has again been conceived in the Pune development centre, with much of the work done here.

R&D

Mr Mark said that there was always a notion that Symantec was not doing much in the innovation space other than buying out or partnering others for its various products, as most of its growth has been through acquisition. "But we are spending close to 15 per cent of our annual revenue for research and development and last year it was approximately $750 million."

Mr Mark said that globally it was more concerned by the changes in technology which required better security measures, the disappearing boundary lines of the companies and consumerisation of IT.

Challenges

"In India, the challenges are the changing technology areas, fostering innovation and ensuring that the momentum does not fall," the newly appointed CTO, Mr Basant Rajan said.

Security Products

Mr Rajan said that it was keeping track of the one billion Internet users who would be accessing the net for various purposes. He said the devices that would be used to access would be different and Symantec was already on the path to develop security products for these new users.

As CTO, Mr Rajan would be instrumental in steering the Symantec Research Labs and Advanced Concept Group projects in the country. He would be working with Government agencies in security and compliance domains. Currently there was two advanced concept groups based out of the US and was looking at Government related and defence segments. Europe was also another location where they have set up a research consortium and Asia Pacific was the next location they were looking at, he said. In Singapore, it is the security wireless access that was of main concern, while for India it was drawing up its plans, he added.

Source: http://www.thehindubusinessline.in/2007/06/06/stories/2007060601260400.htm

10.6 Summary

- As the utilization of Internet technology is mounting for both the Intranet and the Internet, information security is turning out to be exceedingly vital for organizations.
- The safest database you can visualize must be found in a most firmly locked bank, or nuclear-proof bunker, installed on a standalone computer devoid of an Internet or network connections, and under protector for 24×7×365.
- A database server is to continue with services, which frequently enclose security problems, and you should be practical about probable threats.
- Securing the database is a basic principle for any security workers while mounting his or her security plan.
- The database is a compilation of useful data and can be considered as the most essential constituent of an organization and its economic enlargement.

- The general factor in nowadays global economy where most of the business is prepared electronically by means of B2B [Business to Business] or by means of B2C [business to consumer] or other more conventional methods' is electronic transfer and storage of data.
- Database security is also an expertise within the broader discipline of computer security. For many businesses applications are going mobile that signifies using enterprise data in mobile context, therefore using a mobile DBMS.
- Security is frequently an afterthought, and the database industry is overwhelmed with sub-standard security, particularly for enterprise databases that are cobbled-together as an effect of external factors such as business acquisitions.
- To be precise, in order to find out exactly which security policies are required, you need to perform an information risk assessment.

10.7 Keywords

Database: The database is a compilation of useful data and can be considered as the most essential constituent of an organization and its economic enlargement.

Web-based Databases: Database that are configured to permit external communications from other web portals face an outstanding data security challenge.

10.8 Review Questions

1. Explain the concept of database security with examples.
2. Illustrate the basic principle used for any security workers.
3. What are the common failures that intimidate database security? Illustrate.
4. Explain the security traits for an unused DBMS.
5. Explain why database servers are attacked by hackers.
6. Describe the need for database security.
7. Explain the concept of securing mobile databases.
8. Illustrate the issues related with Enterprise Database Security.
9. To be precise, in order to find out exactly which security policies are required, you need to perform an information risk assessment. Comment.
10. Describe the various policy elements necessary for keeping policies simple and convenient long term.

Answers: Self Assessment

1. corporate
2. vulnerabilities
3. database
4. audit trails
5. global
6. enterprise
7. computer
8. mobility
9. non-mobile
10. Multiple
11. weakest link problem.
12. security

13. risk

14. Procedures

15. References

10.9 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online link

www.howstuffworks.com/firewall.htm

Notes

Unit 11: Security Models & Frameworks and Methodologies for Information System Security

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of security models and frameworks
- Discuss the models ISO 27001, COBIT, and SSE-CMM
- Understand methodologies of information system security such as IAM, IEM and SIPES

Introduction

A model is an theoretical, conceptual build that represents processes, variables, and associations without offering particular guidance on or practice for execution. A framework is a defined sustains structure in which another software project can be controlled and developed. In this unit you will understand the concept of security models and frameworks. A methodology is a body of practices, procedures, and regulations accessed by those who work in a discipline or connect in an inquiry. You will understand various methodologies for information system security such as IAM, IEM, and SIPES.

11.1 Introduction to Security Models

Information Security Models overpass the gap among security policy declarations (which clarify which clients should have access to data) and the operating system execution (which permits an administrator to organize access control). The models assist map theoretical goals onto mathematical associations that strengthen whichever execution is eventually selected.

Example: Windows, Unix, MacOS, etc.

The mainly fitting description of a model from appears to be for an "abstract" or "theoretical" model, which is defined as "a hypothetical build that symbolizes physical, biological or social processes, with a set of variables and a set of rational and quantitative associations between them.". For the purposes of this classification, a model is a high-level build displaying processes, variables, and relationships. Models are conceptual and abstract in nature and generally do not go into precise detail on how to be executed.

Moreover, a high-quality model will be self-governing of technology, offering a general reference frame.

The following technique has been identified to be theoretical and conceptual in nature, offering common direction toward attaining an objective without going into particular implementation details. It is categorized as a model.

Notes It is of huge importance here to note that there is, actually, only one technique classified as a model inside the situation of this document. Whereas numerous methods were measured as candidates for models – like IA-CMM, SSE-CMM, ISM3, ISO/IEC 17799:2005, and COBIT– they all failed the description test for the similar reason: they all comprise widespread practice statements that explain how to put into practice the method.

Only one technique did not include practice statements, and as such deserves to unconnected. This technique fulfils the definition of a model by being theoretical conceptual, and technology-independent. As such, this model could be functional to other areas exterior of information security (like physical security) with little or no alteration of its core tenets.

The McCumber Cube ("Information Systems Security: A Comprehensive Model")

Its purpose is to offer an information-centric model that captures the association among the disciplines of interactions and computer security, without the restrictions of organizational or technical modifications.

As designated in the Stated purpose above, the McCumber Cube is an information-centric model that has been practical to computer security. It concentrates on three proportions of information: Information States, Critical Information traits, and Security Measures. Inside every dimension are three aspects, which, when attached, effect in a three-dimensional cube where every dimension is on an axis of the cube.

Dissimilar the frameworks portrayed below, the McCumber Cube does not go into particulars on execution, like with widespread practice statements. Rather, discusses instances of how the model can be accessed within an organization after first offering a foundational conversation of computer security (or information security, or information guarantee, based on your preferred term today) and introducing the model in its entirety.

This model is very functional for accepting a highly compound topic (computer security) in a very concise, albeit conceptual, manner. Moreover, the concentration on information permits the model to be applied to other topics beyond security with relative simplicity.

Notes

The disadvantage to the model is that it does not offer detailed execution details. Therefore, in order to make utilization of the model, one must first appreciate it and interpret that understanding into an attainable purpose or task. As such, selling this notion to senior management may do well or fail, based on their ability to clutch the overall picture presented.

As a high-level model, the McCumber Cube is a very expensive tool for assessing an organization to help concentrates resources. It would be very functional united with a compatible framework and method as discussed in the below sections.

Self Assessment

Fill in the blanks:

1. The .... assist map theoretical goals onto mathematical associations that strengthen whichever execution is eventually selected.
2. Models are conceptual and .... in nature and generally do not go into precise detail on how to be executed.
3. As a .... model, the McCumber Cube is a very expensive tool for assessing an organization to help concentrates resources.

11.2 Terminology

Performance Reference Mode (PRM): Framework for performance dimension offering common output dimensions during the federal government. It permits agencies to better handle the business of government at a strategic level by offering a means for using an agency's EA to dimension the success of information systems investments and their influence on strategic outcomes.

Preproduction Model: Version of INFOSEC equipment utilizing standard parts and suitable for complete evaluation of form, design, and performance. Preproduction models are frequently known as beta models.

Production Model : INFOSEC equipment in its concluding mechanical and electrical form.

Role-based Access Control (RBAC): A model for handling access to resources where allowed actions on resources are recognized with roles instead of individual subject identities.

Technical Reference Model (TRM): A component-driven, technological framework that classifies the standards and technologies to assist and enable the delivery of service components and capabilities.

IA Infrastructure: The fundamental security framework that lies away from an enterprise's defined border, but assists its IA and IA-enabled products, its security position and its risk management plan.

Risk Management Framework: A structured approach used to manage and control risk for an enterprise.

Information Security: The defense of information and information systems from unofficial access, use, revelation, disruption, alteration, or destruction so as to provide confidentiality, integrity, and accessibility.

Information Security Policy: Collective of directives, policies, rules, and practices that stipulate how an organization organizes, protects, and distributes information.

Information Systems Security (INFOSEC): Security of information systems beside unauthorized access to or amendment of information, whether in storage, processing, or transit, and against the denial of service to authorized users, counting those measures important to detect, document, and answer such threats.

Self Assessment

Fill in the blanks:

4. Preproduction models are frequently known as .... models.

5. Production Model is .... equipment in its concluding mechanical and electrical form.

11.3 Frameworks

Having called a model as a basic, high-level build, it turns out to be clear that another expression must be defined to address that class of technique that goes away from the theoretical space and begins to dabble in execution guidance. The word "framework" appears to fit that bill.

In software development, a framework is a defined preserved structure in which another software project can be controlled and developed. This definition seems to be promising as it hints that a framework offers more detail and construction than a model.

While a model is abstract and intangible, a framework is connected to comprehensible work. Moreover, frameworks set suppositions and practices that are intended to directly impact executions. In distinction, models offer the general direction for attaining a goal or outcome, but without obtaining into the muck and mire of practice and measures.

A framework is a basic construct that defines suppositions, concepts, values, and practices, and that involves guidance for executing itself.

The following methods have been identified to offer general guidance toward attaining an outcome without going into particular detail on a single concentrated task. Each of these techniques has been categorized as a framework.

The Security Framework

1. The Security Framework is a harmonized system of security tools.

2. It is similar to the Enterprise management framework.

3. It extends end to end of the customer enterprise architecture.

4. Security data centrally monitored 24x7 in a Security Operations Center.

5. In this data is analyzed by means of correlation tools.

Security Framework Considerations

1. Mapped to the customer's architecture to offer end to end security.

2. Uses obtainable commercial and open source tools.

3. Leverages obtainable security infrastructure to.

4. Rapidly construct out the security framework.

Notes

Benefits of a Security Framework

1. It offers Enterprise security that is:
   (a) Consistent
   (b) Constant
   (c) Covers everything.
2. Traits of good Enterprise Security are:
   (a) Reliable
   (b) Robust
   (c) Repeatable.
3. An effectual Security Framework is:
   (a) Monitored
   (b) Managed
   (c) Maintained.

11.3.1 Introduction to ISO 27001

The ISO 27001 standard was available in October 2005, fundamentally substituting the old BS7799-2 standard. It is the requirement for ISMS, an Information Security Management System. BS7799 itself was a extended standing standard, first available in the nineties as a code of practice. As this developed, a second portion occurred to cover up management systems. It is this beside which documentation is decided. Today in surplus of a thousand certificates are in position, across the world.

Its purpose is to identify "the needs for establishing, implementing, operating, monitoring, reviewing, preserving and improving documented ISMS inside the context of the organization's on the whole business risks.

ISO 27001 improved the content of BS7799-2 and coordinated it with other standards. A system has been developed by a variety of certification bodies for exchange from BS7799 certification to ISO27001 certification.

The purpose of the standard itself is to "offer a model for establishing, implementing, operating, monitoring, reviewing, sustaining, and improving an Information Security Management System". Concerning its adoption, this should be a tactical decision. Moreover, "The design and execution of an organization's ISMS is influenced by their needs and aims, security needs, the process employed and the size and organization of the organization".

The standard defines its 'process technique' as "The application of a system of procedures within an organization, jointly with the identification and communications of these processes, and their management". It employs the PDCA, Plan-Do-Check-Act model to organize the processes, and reflects the values set out in the OECG guidelines.

11.3.2 COBIT

The COBIT Framework offers a tool for the business procedure owner that influence the discharge of business process tasks. COBIT is an IT-centric framework intended to offer users, businesses, and auditors with a standard technique for designing, executing, and testing IT controls. This framework has been generally produced and adopted by the Big N audit houses as a solution to most IT audit, compliance, and control "problems."

The framework offers maturity models, critical success factors, main goal indicators, and performance indicators, all for use in organizing Information and associated Technology. Additionally, COBIT defines control aims and audit guidelines to hold up its implementation. These practice statements go into adequate detail to teach an IT or audit practitioner in how to best execute the framework.

At the core of COBIT is a repeated procedure that circles about "Information" and "IT Resources." The four stages (or domains, as COBIT calls them) of the cycle are "Planning & Organization," "Acquisition & Implementation," "Delivery & Support," and "Monitoring." The cycle begins with "Information" that has ties to COBIT and "IT Resources," and then directs to P&O, which leads to A&I, which leads to D&S, which leads to Monitoring. Each of the four domains defines detailed, particular practices for execution.

COBIT is best defined by this process-flow statement "The control of IT Processes which convince Business Requirements is enabled by Control Statements allowing for Control Practices."

At its finest, COBIT is a very methodical framework for defining, implementing, and reviewing IT controls. For audit organizations, either internal or external, those are hoping to get their hands around the often times demanding task of assuring that effective controls are in position on key systems ("monetarily significant" in the SOX vocabulary), then COBIT is precisely what the doctor ordered.

Unfortunately, COBIT can be a very confusing framework for information security practitioners.

For beginners, COBIT is *not* an information safety framework. It is an IT controls framework, of which infosec displays one (1) practice out of 34. Moreover, to execute COBIT inside an organization means dedicating an extraordinarily significant amount of resources to the task. In this day and age of decreasing functional budgets and increasing threats and narrow burden, it is not sensible to suppose that an organization can readily execute all of COBIT.

Furthermore, there is no understandable security advantage for an organization to execute COBIT. Information security, being a holistic difficulty that must be addressed at all levels of an organization, is not IT specific.

As such, any on the whole framework executed to improve the information security posture of an organization requires to speak to those different levels, and not be bound painfully to one focus (IT). If one were to listen to the leadership of public accounting firms, one might think that COBIT was the best solution for solving security difficulties.

What one would want to bear in mind, however, is that COBIT was produced by the Big N audit firms, for the Big N audit firms. Deployment of COBIT across an organization offers the added advantage to the audit firms of being able to decrease total hours spent on an yearly audit, therefore reducing the investment in personnel necessary, optimizing the productivity of the engagement. Whether or not the association being audited will see any price savings from executing COBIT is debatable. And, in the end, the association will not have addressed information security, but as an alternative addressed the audit ability of its IT resources.

COBIT (Control Objectives for Information and Related Technology) is an global open standard that defines needs for the control and safety of sensitive data and offers a reference framework. COBIT, which offers a reference framework, was produced in the 1990s by the IT Governance Institute.

COBIT includes an executive summary, management guidelines, framework, control objectives, execution toolset and audit guidelines. Extensive support is offered, counting a list of critical success factors for dimensioning security program effectiveness and benchmark for auditing reasons. COBIT has been revised numerous times since inception and upgrades are available at regular intervals.

The reason of COBIT is to offer management and business process owners with an information technology (IT) governance model that assists in delivering value from IT and understanding and organizing the risks connected with IT. COBIT helps bridge the gaps between business requirements, control requirements and technical issues. It is a control model to meet the needs of IT governance and ensure the reliability of information and information systems.

COBIT is used internationally by those who have the most important responsibilities for business processes and technology, those who depend on technology for applicable and dependable information, and those offering quality, reliability and organization of information technology.

Did u know? **Full form of COBIT**

Control Objectives for Information and related Technology.

Task Discuss the functions of COBIT framework.

11.3.3 SSE-CMM

"The SSE-CMM is defined as a process reference model. It is concentrated upon the needs for executing security in a system or series of connected systems that are the Information. The SSE-CMM is a common framework for executing security engineering within an organization; if possible in conjunction with other manufacturing CMMs. SSE-CMM builds on the work of Deming much as other CMMs have completed, concentrated on process description and enhancement as concentrating on process definition and enhancement as a core value.

Taking this procedure development approach, SSE-CMM views at the occurrence of security defects, or incidents, and ask for identifying the flaw in the associated process so as to remediate the flaw, therefore removing the overall fault. In order to attain improvements in processes, those processes must be expected, with predictable results. Moreover, controls must be defined and unstated neighboring those processes.

Caution Efforts should be made to enhance the overall usefulness of processes.

SSE-CMM is a very tough, well-tested structure for incorporation into an engineering-oriented organization. If your organization performs engineering, like through product development, then use of SSE-CMM, mainly in amalgamation within other CMMs, would be very valuable.

Though, specified the engineering focus, SSE-CMM is not a superior match for service organizations that are not prepared around an engineering function. While SSE-CMM surely has key lessons to instruct in terms of administrating information security holistically, those lessons will be hard to execute outside of an engineering context.

The CMM approach in common is very sound, yet very overseas to American business culture. It is believed to be starting with a statistical analysis of procedures, and then using those statistics to isolated defects within those processes, toward the end-goal of gaining improved insight into processes and to foster an surroundings of continuous quality improvement with respect to processes.

Even if an engineering organization has begin on a non-CMM path (like Six Sigma), the SSE-CMM could offer value to the organization.

Example: Non-CMM path is Six Sigma.

Caution For those organizations that are previously leveraging a CMM approach, then the addition of SSE-CMM to the blend should be relatively uncomplicated and could yield traceable consequences in a short time era.

Self Assessment

Fill in the blanks:

6. A .... is a defined preserved structure in which another software project can be controlled and developed.

7. The purpose of .... is to identify "the needs for establishing, implementing, operating, monitoring, reviewing, preserving and improving documented ISMS inside the context of the organization's on the whole business risks.

8. The .... Framework offers a tool for the business procedure owner that influence the discharge of business process tasks.

9. .... is defined as a process reference model which is concentrated upon the needs for executing security in a system or series of connected systems that are the Information.

10. The SSE-CMM is a common framework for executing .... engineering within an organization.

11.4 Methodologies for Information System Security

By defining a high-level and mid-level construct, it is then reasonable to search for a low-level build that can be used to describe those techniques that go into particular details for executing within a concentrated area. In software engineering and project management, a methodology is a codified set of suggested implementations, sometimes escorted by training materials, formal educational programs, worksheets, and diagramming devices.

A methodology is a targeted build that defines particular practices, procedures, and rules for accomplishment or execution of a particular task or function.

The following seven methods have been located to supply specific direction toward implementation or execution of a specific task. Each method is classified as a methodology.

11.4.1 INFOSEC Assessment Methodology (IAM)

Its purpose is to offer a method that "can be used as a consistent baseline for the investigation of the INFOSEC position of automated information systems." IAM is concentrated on offering a high-level assessment of "a specified, operational system for the reason of identifying possible vulnerabilities.

Notes

IAM is subdivided into three phases: Pre-Assessment, On-Site Activities, and Post-Assessment. The Pre-Assessment phase is proposed to build up a general perceptive of customer needs, classify target systems, and institute the "rules of engagement" for the assessment. Pre-Assessment concludes with a written measurement plan.

The On-Site Activities segment displays the primary thrust of IAM in that it takes the effects of the Pre-Assessment Phase, validates those effects, and performs additional data assembly and validation.

The consequence of this phase is a statement of initial analysis. In conclusion, the Post-Assessment phase concludes the IAM by pulling jointly all the details from the preceding two phases, mixing them into a final analysis and report.

IAM training is usually broken into four modules. The first module offers a background for and summary of IAM. The succeeding three modules each concentrate on a phase, beginning with Pre-Assessment, moving on to On-Site Activities, and closing with Post-Assessment.

This methodology is usually high-level and no technical. In contrast, IAM is approximately comparable to the presentation of a full SAS 70 Type II assessment. The testing starts with paper based definitions, and then moves into a stage of basic corroboration of those definitions, without doing major technological testing.

As it addresses Level 1 of the "Vulnerability Discovery Triad," IAM does not contrast directly to IEM, but is as an alternative the first step of the on the whole process, leading up to IEM in Level 2. IAM may best be compared to OCTAVESM below in that it is a non-technical evaluation of vulnerabilities and, by expansion, risk.

11.4.2 INFOSEC Evaluation Methodology (IEM)

Its purpose is to provide a technique for technically assessing susceptibility in systems and to legalize the actual INFOSEC posture of those systems.

The IEM is a escort methodology to IAM, fitting under the on the whole umbrella of the IA-CMM framework, but target Level 2 of the "Vulnerability Discovery Triad." As such, IEM functions hand-in-glove with IAM, comparing the overall process format approximately exactly. The key differentiation between IAM and IEM is that the IEM performs actual hands-on assessment of systems in order to authenticate the actual existence of vulnerabilities, as opposed to the IAM's consequence of document probable vulnerabilities in those systems.

Alike to the IAM, the IEM is separated into three stages: Pre-Evaluation, On-Site, and Post-Evaluation. The Pre-Evaluation phase starts with taking the IAM Pre-Assessment report as input and then coordinating the regulations of engagement for carry out technical assessment of the systems under objective. This phase terminates with a Technical Evaluation Plan.

The On-Site phase of the IEM then displays the bulk of the hands-on technical work, performing diverse discoveries, scans, and evaluations. All findings are physically validated to make sure accuracy.

Lastly, the Post-Evaluation phase concludes the methodology in a way similar to the IAM by pulling together all data produced, putting it into a final report that details findings, suggestions, and a security roadmap.

Did u know? The IEM closes with purchaser follow-up and support.

Notes It is appealing to note that the IEM can be conducted either following, or in combination with, the IAM. In difference to the IAM, the IEM will execute actual testing of systems, validating findings physically to make sure accuracy of reporting. The deliverable from the IEM is more important and complete than the IAM report, offering analysis, matrices, and reporting of findings.

11.4.3 Security Incident Policy Enforcement System (SIPES)

Its purpose is to offer a methodology for defining and executing a Security Incident Policy Enforcement Systems. This methodology is planned for completeness. Though, because of its status as an "Incomplete" work that has not confirmed progress over the past two years, it is supposed that work has not sustained and that this methodology is, actually, obsolete. The listing is offered here for completeness.

The Security Incident Policy Enforcement System (SIPES) draft displays a relatively abstract method to addressing the difficulty of incident response management. The paper begins by deconflicting the description of failure inside IT systems and then proceeds to build its "state-full" methodology. The fundamental approach is to converse security state and those points where states modify. By means of that dynamic basis, they then move into the argument for incident policy enforcement, with numerous sidebars into what each of these terms means.

Task Illustrate the function of SIPES.

Self Assessment

Fill in the blanks:

11. A .... is a targeted build that defines particular practices, procedures, and rules for accomplishment or execution of a particular task or function.
12. .... is concentrated on offering a high-level assessment of "a specified, operational system for the reason of identifying possible vulnerabilities.
13. The purpose of .... is to provide a technique for technically assessing susceptibility in systems and to legalize the actual INFOSEC posture of those systems.
14. The .... draft displays a relatively abstract method to addressing the difficulty of incident response management.
15. In IAM , the .... phase is proposed to build up a general perceptive of customer needs, classify target systems, and institute the "rules of engagement" for the assessment.

11.5 Summary

- A model is an theoretical, conceptual build that represents processes, variables, and associations without offering particular guidance on or practice for execution.
- The purpose of *McCumber Cube* is to offer an information-centric model that captures the association among the disciplines of interactions and computer security, without the restrictions of organizational or technical modifications.

Notes

- A framework is a defined sustains structure in which another software project can be controlled and developed.
- The purpose of ISO 27001 is to identify "the needs for establishing, implementing, operating, monitoring, reviewing, preserving and improving documented ISMS inside the context of the organization's on the whole business risks.
- The COBIT Framework offers a tool for the business procedure owner that influence the discharge of business process tasks.
- SSE-CMM is defined as a process reference model which is concentrated upon the needs for executing security in a system or series of connected systems that are the Information.
- A methodology is a targeted build that defines particular practices, procedures, and rules for accomplishment or execution of a particular task or function.
- IAM is concentrated on offering a high-level assessment of a specified, operational system for the reason of identifying possible vulnerabilities.
- The purpose of IEM is to provide a technique for technically assessing susceptibility in systems and to legalize the actual INFOSEC posture of those systems.
- The Security Incident Policy Enforcement System (SIPES) draft displays a relatively abstract method to addressing the difficulty of incident response management.

11.6 Keywords

COBIT: The COBIT Framework offers a tool for the business procedure owner that influence the discharge of business process tasks.

Framework: A framework is a defined sustains structure in which another software project can be controlled and developed.

IAM: IAM is concentrated on offering a high-level assessment of "a specified, operational system for the reason of identifying possible vulnerabilities.

IEM: The purpose of IEM is to provide a technique for technically assessing susceptibility in systems and to legalize the actual INFOSEC posture of those systems.

ISO 27001: The purpose of ISO 27001 is to identify "the needs for establishing, implementing, operating, monitoring, reviewing, preserving and improving documented ISMS inside the context of the organization's on the whole business risks.

Methodology: A methodology is a targeted build that defines particular practices, procedures, and rules for accomplishment or execution of a particular task or function.

Model: A model is an theoretical, conceptual build that represents processes, variables, and associations without offering particular guidance on or practice for execution.

SIPES: The Security Incident Policy Enforcement System (SIPES) draft displays a relatively abstract method to addressing the difficulty of incident response management.

SSE-CMM: SSE-CMM is defined as a process reference model which is concentrated upon the needs for executing security in a system or series of connected systems that are the Information.

11.7 Review Questions

1. What is a model? Explain the concept of security models.
2. Illustrate the process of a Comprehensive Model of information system security.

3. Depict the advantages and disadvantages of security models.
4. What is a framework? Illustrate the concept of security framework.
5. Elucidate the benefits and considerations of a security framework.
6. Discuss the purpose of ISO 27001 and illustrate the use of it.
7. Illustrate the perception of COBIT framework and explain the four stages included in COBIT.
8. Enlighten how SSE-CMM is used as a common framework for executing security engineering within an organization.
9. Make distinction between INFOSEC Assessment Methodology (IAM) and INFOSEC Evaluation Methodology (IEM)
10. The Security Incident Policy Enforcement System (SIPES) draft displays a relatively abstract method to addressing the difficulty of incident response management. Comment.

Answers: Self Assessment

1. models
2. abstract
3. high-level
4. beta
5. INFOSEC
6. framework
7. framework
8. COBIT
9. SSE-CMM
10. security
11. methodology
12. IAM
13. IEM
14. Security Incident Policy Enforcement System (SIPES)
15. pre-Assessment

11.8 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online link

citeseerx.ist.psu.edu

Notes

Unit 12: Security Metrics and Privacy

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of security metrics
- Discuss basics of security metrics

- Understand security matrix and security metrics classification
- Explain the concept of privacy
- Understand business issue in privacy
- Discuss privacy vs security
- Identify related terms for privacy
- Understand information privacy principles

Introduction

A metric refers to a system of dimension that depends on quantifiable procedures. Useful metrics point to the degree to which protection goals, like data confidentiality, are being met, and they drive measures taken to recover an organization's overall security program. Privacy can be illustrated as exercising control over what access others have to private magnitude of us, like information privacy. In this unit, you will understand various concepts of security metrics and privacy.

12.1 Introduction to Security Metrics

Good metrics are those that are elegant, i.e. specific, quantifiable, attainable, repeatable, and time reliant. Dimensions offer single-point-in-time views of specific, discrete factors, while metrics are resultant by comparing to a prearranged baseline two or more dimensions taken over time.

Dimensions are produced by counting; metrics are produced from analysis.

Alternatively, dimensions are objective raw data and metrics are either objective or subjective human explanations of those data. The method of dimension that is employed should be reproducible, and should attain the similar result when performed independently by dissimilar competent evaluators. Also, the consequence should be repeatable, so that a second evaluation by the original team of evaluators generates the same result. A method of dimension used to find out the unit of a quantity could be a measuring instrument, a reference material, or a measuring system. The dimension of an information system for security includes the application of a method of dimension to one or more parts of the system that have an measurable security property so as to obtain a considered value of dimensions should be timely and applicable to the organization.

Self Assessment

Fill in the blanks:

1. A .... refers to a system of dimension that depends on quantifiable procedures.
2. .... offer single-point-in-time views of specific, discrete factors, while metrics are resultant by comparing to a prearranged baseline two or more dimensions taken over time.

12.2 Basics

12.2.1 Background

The phrase "security metrics" is used frequently today, but with a series of meanings and explanations. "Metrics are tools intended to facilitate decision making and recover performance and accountability during collection, analysis, and reporting of pertinent performance-associated

Notes

data. The point of measuring performance is to observe the status of considered activities and facilitate enhancement in those activities by applying counteractive actions, based on observed dimensions. While a case can be made for using different terms for more comprehensive and aggregated items, like 'metrics' and 'measures,' this document accesses these terms interchangeably."

"Measurements offer single-point-in-time views of particular, discrete factors, whereas metrics are derived by comparing to a fixed baseline two or more dimensions taken over time. Measurements are generated by counting; metrics are produced from analysis. Alternatively, measurements are objective raw data and metrics are either objective or biased human explanation of those data."

For information system security, the procedures are related with aspects of the system that supply to its security. That is, security metrics engage the application of a method of dimension to one or more entities of a system that possess an quantifiable security property to attain a measured value.

Metric Lifecycle

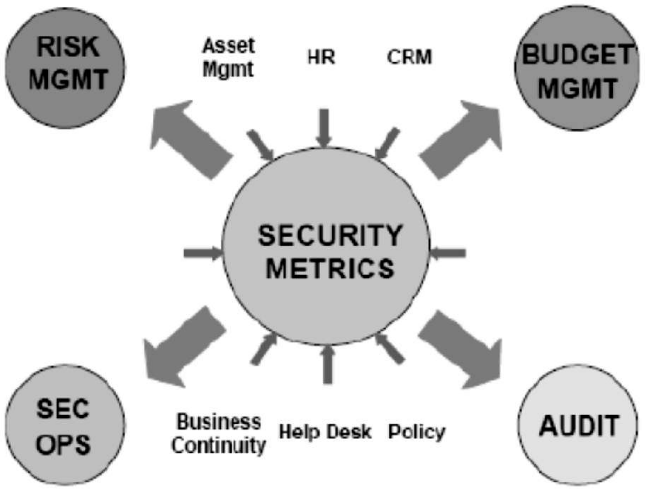
The business logic connected with a metric follows a straightforward dealing out sample:

- ***Create:*** Obtain primary input data from one or more authoritative providers, including commercial products or homegrown customer applications.
- ***Calculate:*** Apply a series of analytic operations (called actions) on the primary data to derive a result and store the result in the metric results database in the form of one or more rows in a table.
- ***Communicate:*** Communicate the metric results in any of the following formats: default visualization, e-mail notification, e-mail alert based upon detection of some policy violation.

12.2.2 Security Metrics Management: More than Measurement

A metric generates results that are accumulated in a specified metric database which is usable through standard SQL and JDBC interfaces to sustain the following functions.

Figure 12.1: Security Metrics Management: More than Measurement



- *Risk Management:* Metrics that calculate threat probability, vulnerability, Counter measure coverage and asset value capitulate consequences that can be used to model risk.
- *Budget Management:* Metrics that determine level of effort, impact, and obtainable can be transformed into dollar values for the reason of establishing budgets as well as computing return on investment.
- *Audit & Compliance Assessment (Internal or External):* Metrics that compute policy compliance for individual in addition to groups of definitions capitulate results that can enhance reports generated by compliance tools.
- *Security Operations:* Metrics that collect data over time can be used to recognize trends that suggest particular actions to be taken by data center functions staff.

12.2.3 Issues/Aspects of Security Measurement

Approaching into some significant aspects of security measurement are illustrated below. The idea is not to give a list of general drawbacks rather the objective is to emphasize those factors that are supposed to be related to a research attempt in security metrics.

1. *Correctness and Effectiveness:* Correctness signifies assurance that the security-enforcing techniques have been rightly executed (i.e., they do accurately what they are proposed to do, like performing some calculation). Effectiveness signifies assurance that the security-enforcing techniques of the system meet the declared security objectives (i.e., they do not do anything other than what is proposed for them to do, while fulfilling expectations for resiliency).
2. *Leading versus Lagging Indicators:* Leading and covering indicators reproduce security circumstances that exist correspondingly before or after a shift in security. A covering security metric with a short latency phase or lag time is favored over one with a long latency phase. Many security metrics can be observed as lagging marker.
3. *Organizational Security Objectives:* Organizations subsist for different reasons, hold different assets, have dissimilar exposure to the public, face dissimilar threats, and have dissimilar tolerances to risk. Due to these and other differences, their security purposes can vary considerably. Security metrics are usually used to resolve how well an organization is fulfilling its security objectives.
4. *Qualitative and Quantitative Properties:* Qualitative assignments can be accessed to symbolize quantitative procedures of security properties (e.g., low means no vulnerabilities instituted; medium, between one and five found; and high, more than five found). Quantitative valuations of numerous security properties may also be weighted and shared to derive a compound value.
5. *Measurements of the Large Versus the Small:* Security measurements have confirmed to be much more victorious when the target of evaluation is small and simple instead of large and complex. As the number of components in a system enlarges, the number of probable interactions grows with the square of the number of components.

Did u know? Greater difficulty and functionality usually relate inversely to security and need more scrutiny to evaluate.

Task Make distinction between qualitative and Quantitative properties.

Notes

12.2.4 The Value of Security Metrics

Metrics can be an effectual tool for security executives to discern the efficiency of various components of their protection programs, the security of a particular system, product or process, and the aptitude of staff or departments inside an organization to address security concerns for which they are accountable. Metrics can also help recognize the level of risk in not taking a given action, and in that way supply guidance in prioritizing counteractive actions. Additionally, they may be used to raise the level of security alertness inside the organization. In conclusion with knowledge gained via metrics, security managers can better answer tough questions from their executives and others, like:

1. Are we more secure these days than we were before?
2. How do we contrast to others in this regard?
3. Are we protected enough?

Self Assessment

Fill in the blanks:

3. .... signifies assurance that the security-enforcing techniques have been rightly executed.
4. A covering security metric with a short latency phase or lag time is favored over one with a .... latency phase.

12.3 Security Matrix

Security matrix is used to concentrate measures where they are required, and to be aware of what measures are being (purposely) abandoned. Security matrix includes the following:

1. Drawing a threat/risk landscape. What regions are mainly at risk?
2. Define upcoming measures, baselines, or project particular security
3. Relating security topics.
4. Dept & diversity of defence
5. List/audit existing measures
6. Follow variations in focus over time
7. Divide "Computer Equipment" as per your needs, e.g. : OS, DBs, Middleware, Applications

12.4 Security Metrics Classification

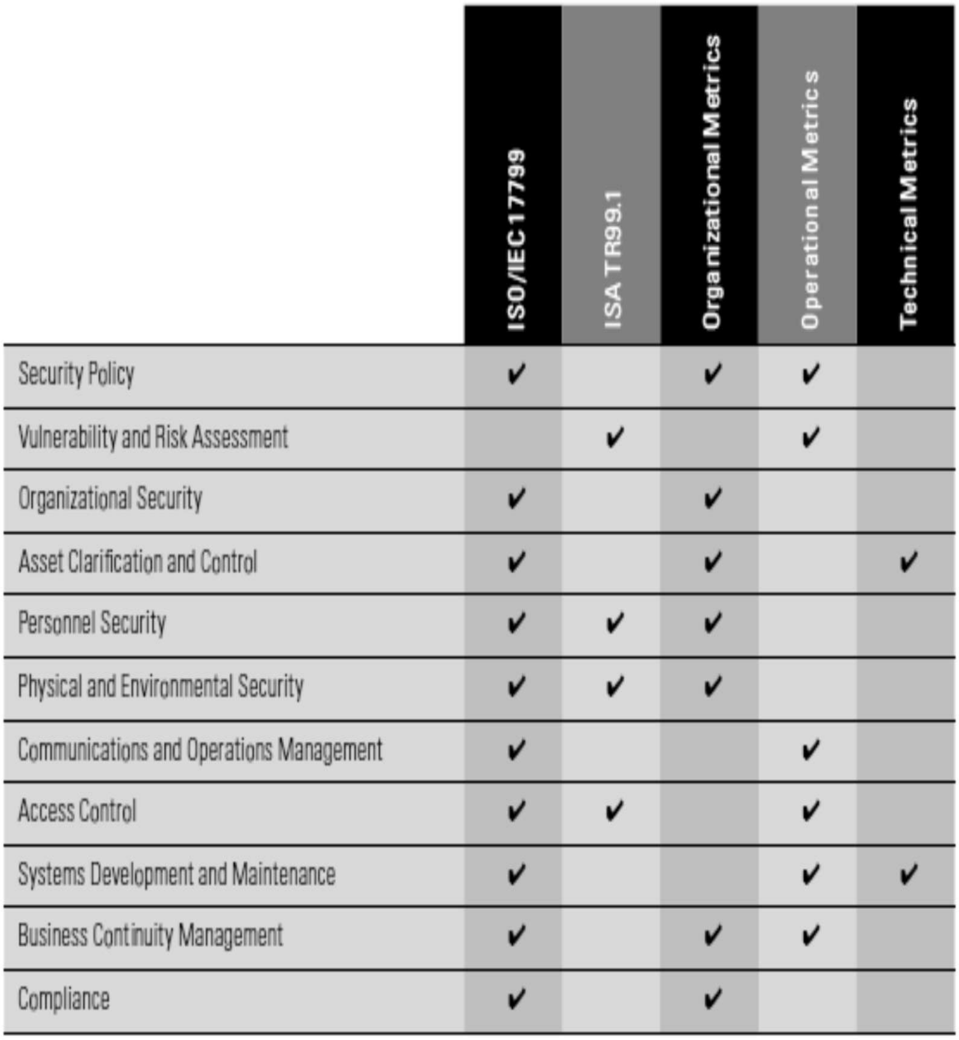
The security metrics is divided into the three types:

1. Organizational
2. Operational
3. Technical

Then add two additional categories to capture security controls selected in ISO/IEC 17799 and ANSI/ISA-TR99.00.01-2004. The taxonomists advise that the following calculable aspects of an information security movement or system can be mapped to procedures in one or more of the five high-level categories, as illustrated in Figure 12.2.

Notes

Figure 12.2: Mapping of Measurable Security Elements to Metrics Categories



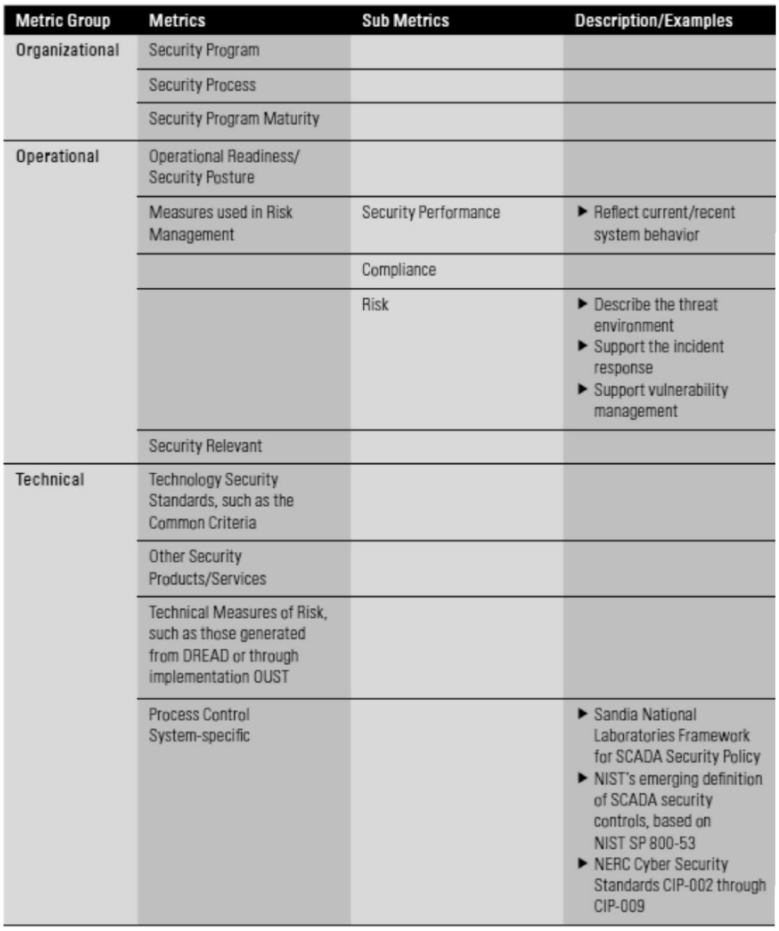
	ISO/IEC17799	ISA TR99.1	Organizational Metrics	Operational Metrics	Technical Metrics
Security Policy	✓		✓	✓	
Vulnerability and Risk Assessment		✓		✓	
Organizational Security	✓		✓		
Asset Clarification and Control	✓		✓		✓
Personnel Security	✓	✓	✓		
Physical and Environmental Security	✓	✓	✓		
Communications and Operations Management	✓			✓	
Access Control	✓	✓		✓	
Systems Development and Maintenance	✓			✓	✓
Business Continuity Management	✓		✓	✓	
Compliance	✓		✓		

At the time of recommending its categorization, it has been defined as a more inclusive hierarchy of metrics categories and subcategories, nor had it occupied its proposed classification. The researchers had, though, recognized an extensive list of possible sources for such metrics, and categorized these inside the first three categories of their taxonomy; they had also surveyed and evaluated the potential usefulness of the metrics in each source for dimensioning security attributes of process control systems.

In performing this survey, the researchers in fact implied a more absolute classification of applicable security metrics than is designated by their formally projected classification. Table 12.1 illustrates that implied categorization of security metrics.

Notes

Table 12.1: Classification of Security Metrics for Process Control Systems



Metric Group	Metrics	Sub Metrics	Description/Examples
Organizational	Security Program		
	Security Process		
	Security Program Maturity		
Operational	Operational Readiness/ Security Posture		
	Measures used in Risk Management	Security Performance	▶ Reflect current/recent system behavior
		Compliance	
		Risk	▶ Describe the threat environment ▶ Support the incident response ▶ Support vulnerability management
	Security Relevant		
Technical	Technology Security Standards, such as the Common Criteria		
	Other Security Products/Services		
	Technical Measures of Risk, such as those generated from DREAD or through implementation OUST		
	Process Control System-specific		▶ Sandia National Laboratories Framework for SCADA Security Policy ▶ NIST's emerging definition of SCADA security controls, based on NIST SP 800-53 ▶ NERC Cyber Security Standards CIP-002 through CIP-009

Self Assessment

Fill in the blanks

5. .... is used to concentrate measures where they are required, and to be aware of what measures are being (purposely) abandoned.

6. Security metrics is categorized into organizational, ... l, and technical groups.

12.5 Privacy

Privacy can be explained as exercising power over what access others have to private extent of us, like information privacy. The IPPs intend to protect information privacy, not privacy in common. Privacy defense is about complementing two challenging interests.

The right to privacy is something that is valued by all and the Act enshrines this right in law. Staff need to maximise the level of control that individuals have over their personal information, however the operation of government requires that some personal information be collected, handled and stored.

The IPPs are not intended to prevent the legitimate use of personal information to offer government services. It does not mean that staff can no longer gather, handle or amass personal information. Though, it does need that staff gaze at how and why the personal information is composed, handled and accumulated.

Self Assessment

Fill in the blanks:

7. The IPPs intend to protect .... privacy, not privacy in common.

8. The right to .... is something that is valued by all and the Act enshrines this right in law.

12.6 Business Issue

Why is privacy of apprehension to e-commerce? We consider this issue stems from a new technical surroundings for consumers and businesses, the resultant data flow with considerable advantages to businesses and consumers, consumer issues in this new environment, and regulatory efforts to govern this surroundings. It is significant to understand each one of these, and to appreciate the tradeoffs. Privacy as a business concern or issue is tremendously sensitive to changes in the surrounding context. Changes in people's expectations (like when they become accustomed to data transfer in commercial settings) or in authoritarian governance (such as new laws, governmental rules, or even case law in the US) can noticeably alter business issues and potentials.

Below is an indication of the research and business issues. This will comprise the consumers' issues, technical issues, and regulatory efforts to ameliorate privacy issues. In this assessment, our attempt is not to forecast what will occur or should occur, but to display issues to guide further investigate and business activity.

Obviously, there are many business chances in the changing technical surroundings. The use of digital systems permits data capture at a much larger rate and extent than previously; e-commerce sites could potentially gather an enormous amount of data about personal inclinations, shopping patterns, patterns of information hunt and use, and the like regarding consumers, especially if combined across sites. Not only is it simpler than ever to gather the data, it is also much simpler to investigate these data. New computational methods permit data mining for trading patterns and other personal trends. These data can be accessed to personalize a customer's e-commerce experience, enhance an organization's customer support, or perk up a customer's specific e-site experience. The data are expensive for reuse,

Example: In discovering potential sales to existing customers.

Additionally, the data are also important to aggregators (who may look for other personal trends and patterns) or for other types of resale. Certainly, reuse and resale are concurrently both potential opportunities and tribulations. "Paradoxically, the same practices that offer value to organizations and their customers also elevate privacy concerns."

From the perspective of consumers, many e-commerce sites have done stupid things with their customers' data. Consumers' estimations in this have been established by media stories of particularly egregious privacy malfunctions and public relations nightmares. Generally speaking, consumers are simply confirmed in their opinions by the media. As declared, few consumers trust companies to keep their data private. In one survey, 92% of respondents indicated that even when companies guaranteed to keep personal data private, they would not in fact do so. Culnan

Notes

and Armstrong make the argument that consumers have two types of privacy concerns. Firstly, they are worried over unauthorized access to personal data due to security breaches (see below) or the lack of internal controls. Secondly, consumers are alarmed regarding the risk of secondary use – the reclaim of their personal data for unrelated reasons without their consent. This involves sharing with third parties who were not element of the business in which the consumer connected his or her personal data. It also involves the aggregation of a consumers' transaction data and other individual data to generate a profile. Smith, Milberg, and Burke raise two additional issues based on Delphi studies, common concerns regarding personal data being collected and issues over one's inability to accurate any errors.

Apart from the research literature describing a common anxiety (and its extent), there is some research literature providing more aspect. A unrelenting finding, over several decades, is that it is productive to consider US consumers not as a common block but as consisting of 3 groups privacy fundamentalists, the pragmatic majority, and the marginally concerned. These groupings have been dependable across studies (e.g., [Ackerman, Cranor, and Reagle 1999], [Spiekermann, Grossklags, and Berendt 2001]). (Spiekermann et al. separated the pragmatics into those who were measured with revealing their identity and those who were more concerned regarding making their individual profiles obtainable.) In Ackerman et al., these groups were 17%, 56%, and 27% of the sample correspondingly. Spiekermann et al. observed a larger group of isolation fundamentalists and fewer marginally associated in Germany. The groups vary significantly in their privacy favorites and attitudes. The marginally concerned group is typically indifferent to privacy concerns; privacy fundamentalists, alternatively, are quite uncompromising regarding their privacy. The majority of the US population, though, is concerned regarding its privacy, but is willing to operate personal data for some advantage (e.g., customer service). However, consumers still want sufficient measures to guard their information from inappropriate sale, unintentional leakage or loss, and deliberate attack. In [Ackerman, Cranor, and Reagle 1999], the issues of pragmatists were frequently significantly reduced by the occurrence of privacy protection measures such as privacy laws or privacy policies on Web sites Another interesting finding, also pretty persistent, is that there is a large gap among most people's declared preferences and their genuine behavior. While this is frequently the case in social studies, it is of particular attention here. It is not yet recognized, however, whether this gap is enduring, in that it is unlikely to modify, or is the indication of people's aggravation with existing technologies.

Self Assessment

Fill in the blanks:

9. Privacy as a .... concern or issue is tremendously sensitive to changes in the surrounding context.

10. .... in people's expectations or in authoritarian governance can noticeably alter business issues and potentials.

12.7 Privacy vs Security

Certain perplexity occurs in the industry concerning security and privacy. Some people associate security for privacy, whereas others consider privacy is something that will only fascinate "those with something to hide". Security is a essential tool to construct privacy, but a communication or transaction surroundings can be very secure, yet completely unprivate. Privacy is a fundamental human right and is documented as a requirement by the European Union (Privacy Directive) and the OECD (Principles of Fair Information Practice). Lastly, privacy is just good business, and will be necessary for M-Commerce to increase extensive adoption by consumers about the world.

Security and privacy are intimately related technologies, though, there are significant differences that require to be understood so as to design new systems that address both. Privacy is regarding informational self-determination—the capability to decide what information regarding you goes where. Security provides the capability to be confident that those decisions are appreciated.

Example: We converse about GSM voice privacy—can somebody listen to my call? There is a privacy objective, which is to permit me to say no, and a security technology, encryption, that permits me to implement it.

In this example, the aims of security and privacy are the similar. But there are other times when they may be orthogonal, and there are also times when they are in argument.

There is a security objective of authenticating a handset. In some cases this may be completed by RF fingerprinting, which is not a privacy concern-we securely authenticate that the handset is the one that is associated to an account, therefore ensuring that the correct person is billed. Here, security and privacy are orthogonal.

Example: Caller presentation is an example of a position where security and privacy can argument. I may want privacy, in not allowing anyone else see my number; while the caller may would like the security of thinking they recognize who is calling. In this circumstances, in most countries, a balance has been struck in favour of informational self-determination, permitting the caller to select if caller information is obtainable.

In the area of location information, permitting disclosure of location information out on an continuous basis generates a number of privacy concerns, but infrequently, when calling for emergency services, it is functional to reveal. It is significant to design these system so that the phone's owner is in control and pleased, and to ensure that the security procedures in place sustain the owner's conclusion effectively.

SSL is often confused with privacy. SSL offers "privacy" against eavesdroppers, but this is better called confidentiality. The well-publicized break-ins at CDNow and other retailers using SSL show that privacy requires more than SSL. (The same issues apply to WTLS, although WTLS also creates a problem with the decryption at the WTLS gateway, and a question of is that trustworthy?) It requires minimizing the amount of information that is transmitted and stored.

So, in managing payments, one can achieve strong security by transferring around the electronic equivalents of cheques, which are cleared, online. The cheque is signed, the bank is inquired if there is sufficient money, and everything flows easily. Excellent privacy with the similar security can be obtained by means of modern e-cash systems. E-cash with online verification permits the money to be spent without enlightening the account number. Since the account number is never given to the merchant, privacy is strongly conserved, even when there is a security lapse. Private Credentials can facilitate a totally secure AND private environment for mobile payment and signatures.

Caution Whether it is for payment, signature or location-dependent services, Privacy protection technologies must be an essential part of future mobile infrastructure in order for new mobile services to be adopted by customers.

Self Assessment

Fill in the blanks

11. .... provides the capability to be confident that those decisions are appreciated.

12. SSL offers "privacy" against eavesdroppers, but this is better called ....

Notes

12.8 Related Terms

Access Control: It is the avoidance of unauthorized access of information assets. It is the policy rules and deployment technique which control use to information systems, and physical access to premises.

Access: The ability or the resources necessary to read, write, modify, or converse data/information or else use any system resource.

Authentication: The work of verifying the identity of an individual, originator, terminal, or workstation, to find out that entity's right to use specific categories of information and a measure intended to defend against fraudulent transmission by verifying the authority of a transmission, message, station, or originator.

Authorization: Consent from an individual, or his or her personal representative providing the Department of Human Services (Department) authorization to attain, release or use information concerning the individual from third parties for particular purposes or to disclose information to a third party precise by the individual.

Business Associate: An individual or thing performing any movement or function on behalf of the Department concerning the use or disclosure of secluded health information (PHI) and is not a member of the Department's workforce.

Client: An individual who requests or obtains services from the Department.

Client Services: The condition of assistance, care, treatment, training or assistance to a client by DHS.

Confidentiality: The extent to which sensitive data, about both individuals and organizations, must be secluded. Information is not made obtainable or disclosed to unauthorized individuals, entities, or procedures.

Confidential Information: Any client information that DHS may have in its records or files on any DHS client that must be protected.

Cookies: Cookies register information regarding a visit to a Web site for upcoming use by the server. A server may obtain information of cookies of other sites also, which create concern in view of breach of privacy.

Decrypting: It is the process of overturning the encryption of a file or message to improve the original data so as to use or read it.

Encryption: The process by which data is provisionally rearranged into an unreadable or incomprehensible form for confidentiality, transmission, or other security reasons.

File Server: A computer system that offers a way of sharing and working on files accumulated on the system among users with use to these files over a network.

Individual: The person who is the subject of information composed, used, or revealed by the Department.

Individually Identifying Information: Any single item or collection of information or data that indicates or discloses the identity of an individual, either specifically (such as the individual's name or social security number), or from which the individual's identity can sensibly be ascertained.

Information: Personal information connecting to an individual, a participant, or a Department client.

Information Owner/User: An (human) entity that makes use of computer systems and networks.

Information Security: Management and technology programs to defend the organization from improper risks to the organization's information possessions.

Information Systems: The computer systems and information sources accessed by an organization to sustain its day-to-day operations.

Integrity: The property that data or information have not been tainted or damaged in an unauthorized manner.

Licensee: A human being or entity that applies for or obtains a license, certificate, registration, or similar authority from the Department to carry out or conduct a service, activity, or function.

Malicious Software: Software, for instance, a virus, intended to damage or disrupt a system.

Password: Confidential authentication information included a string of characters.

Physical Safeguards: Physical measures, policies and procedures to defend a covered entity's electronic information systems and connected buildings and equipment, from natural and environmental hazards and unauthorized intrusion.

Privacy: An individual's or organization's right to establish whether, when and to whom personal or organizational information is released.

Privacy Rights: The particular actions that an individual can take or demand to be taken with regard to the uses and revelation of their information.

Protected Information: Any participant or customer information that the Department may have in its records or files that must be safeguarded pursuant to Department policy. This involves but is not restricted to "individually identifying information".

Server: A server is a computer system, or a set of procedures on a computer system offering services to clients across a network.

User: A person or entity with certified access.

Vulnerability: Vulnerability is the survival of a weakness, design, or execution error that can lead to an unexpected, undesirable event negotiating the security of the system, network, application, or protocol concerned.

Worm: A computer program, which replicates itself and is self-propagating. Worms, as conflicting to viruses, are meant to generate in network surroundings.

Self Assessment

Fill in the blanks

13. .... is a human being or entity that applies for or obtains a license, certificate, registration, or similar authority from the Department to carry out or conduct a service, activity, or function.

14. .... is a computer system that offers a way of sharing and working on files accumulated on the system among users with use to these files over a network.

12.9 Information Privacy Principles (IPPs)

There are ten Information Privacy Principles (IPPs) which cover the entire life cycle of information from compilation and handling to storage and removal. The IPPs direct how this Department should manage personal information. We will require to be maximize our practices in line with the IPPs and beside our particular work context to determining whether existing practice requirements to change. This procedure may need the balancing of privacy with challenging interest and governmental needs.

The Northern Territory IPPs have their genesis in the privacy rules produced by the Organization for Economic Cooperation (OECD).

Did u know? Australia accepted the OECD Guidelines in 1984 and underpin the *National Privacy Principles* managed by the Federal Privacy Commissioner.

12.9.1 IPP 1: Collection

Gather only personal information that is essential for the performance of an agency's purposes or activities. The personal information must be composed lawfully, moderately and not intrusively. If possible, information should be composed from the person concerned. This principle includes the following:

1. An agency must not gather personal information unless the information is essential for one or more of its functions or activities.
2. An agency must gather personal information only by legalized and fair means and not in an irrationally intrusive manner.
3. At or before the time (or, if that is not feasible, as soon as workable after) an agency gathers personal information regarding an individual from the individual, the agency must take sensible steps to make certain that the individual is conscious of all of the following:

   (a) the identity of the organisation and how to contact it

   (b) the fact that the individual is able to have access to the information

   (c) the purpose for which the information is collected

   (d) the persons or bodies, or classes of persons or bodies, to which the agency usually discloses information of the same kind

   (e) any law that requires the particular information to be collected

   (f) the main consequences (if any) for the individual if all, or part ,of the information is not provided.

   If it is sensible and practicable to do so, an agency must gather personal information regarding an individual only from the individual.
4. If an agency gathers personal information about an person from another person, it must take rational steps to make certain that the individual is or has been made attentive of the matters listed above that the person must be made aware of, except for to the extent that making the individual aware of the matters would front a serious threat to the life or health of the person or another person.

Notes This principle is an imperative principle. If an agency fulfils the needs of this principle it will be simpler to fulfill the other nine IPPs.

12.9.2 IPP 2: Use and Disclosure

Use and reveal personal information simply for the main purpose for which it was composed or a related reason the person would sensible expect. Use for some particular secondary purposes without approval is permitted. Or else, ask for consent.

To resolve how personal information can next be used and who it can be revealed to requires an understanding of the chief purpose that the information is composed for. If the needs of *IPP 1: Collection* have been fulfilled, the main purpose should be apparent and should have been conversed to the person at the time of compilation.

This principle positions limits on the use of personal information for secondary reasons. Simply, use for an unconnected secondary purpose or one that the person could not expect should only happen with the person's approval or if a strong public interest needs it. This principle includes the following:

1. An agency must not utilize or reveal personal information about an individual for a reason (the secondary reason) other than the main purpose for collecting it, unless one or more of the following apply:

   (a) If the information is receptive information - the secondary reason is directly connected to the primary reason; and the individual would reasonably anticipate the organization to use or reveal the information for the secondary purpose.

   (b) If the information is not receptive information, the secondary reason is related to the main purpose and the individual would reasonably anticipate the organization to use or reveal the information for the secondary reason.

   (c) The individual approval to the use or revelation of the information.

   (d) An agency sensibly believes that the use or revelation is necessary to lessen or prevent a serious and imminent threat to the individual's or another individual's life, health or safety; or a serious danger to public health or public safety.

   (e) An agency has motive to suspect that unlawful activity has been, is being or may be occupied in and uses or reveals the information as a necessary part of its investigation of the matter or in reporting its issues to relevant persons or authorities.

   (f) The use or revelation is needed or authorized by law.

   (g) An agency sensibly believes that the use or disclosure is sensibly necessary for one or more of the following by or on behalf of a law enforcement agency:

      (i) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law.

      (ii) enforcing a law relating to the confiscation of proceeds of crime.

      (iii) protecting public revenue.

      (iv) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct.

      (v) preparing for or conducting events before a court or tribunal or implementing the orders of a court or tribunal.

   (h) The Australian Security Intelligence Organisation (ASIO) has demanded the agency to reveal the information, the disclosure is made to an officer or employee of ASIO.

   (i) Authorised by the Director-General of ASIO to obtain the information and an officer or employee of ASIO authorized by the Director-General of ASIO to do so has proficient in writing that the information is necessary in connection with the performance of the functions of ASIO.

(j) The Australian Secret Intelligence Service (ASIS) has demanded the organization to disclose the information, the revelation is made to an officer or employee of ASIS.

(k) Authorized by the Director-General of ASIS to obtain the information and an officer or employee of ASIS authorized by the Director-General of ASIS to do so has proficient in writing that the information is essential in connection with the performance of the functions of ASIS.

> *Notes* It is not proposed to deter agencies from lawfully assisting with law enforcement agencies in the concert of their functions. This does not prevail any existing legal obligations not to reveal personal information and does not need an agency to reveal personal information. An agency is always entitled not to reveal personal information in the absence of a legal obligation to reveal it.

2. An agency is also accountable to the needs of IPP 9 if it transfers personal information to a person outside the Territory.
3. If an agency uses or revelations personal information to a law enforcement agency, the agency must make a printed note of the use or revelation.

12.9.3 IPP 3: Data Quality

Ensure that your personal information is:

1. Accurate
2. Complete
3. Up to date
4. Principle

An agency must take sensible steps to make sure that the personal information it collects uses or discloses is accurate, absolute and up to date.

12.9.4 IPP 4: Data Security

Take sensible steps to defend personal information from misuse, loss, unauthorized access, alteration or revelation. This principle includes the following:

1. An agency must take sensible steps to defend the personal information it holds from mistreatment and loss and from unauthorized access, alteration or revelation.
2. An agency must take sensible steps to destroy or enduringly de-identify personal information if it is no longer required for any reason.

12.9.5 IPP 5: Openness

Document evidently articulated polices on organization of personal information and offer the policies to anyone who asks. This principle includes the following:

1. All agencies should expand clear privacy policies and offer the policies to anyone who asks.

2. This illustrates that there is an awareness of privacy concerns and a commitment to information privacy.
3. It will also donate generally to enlarged public confidence and trust. Privacy rules should depend on the IPPs.
4. The privacy policies should be largely displayed and easily available. Including being downloadable if on a website.
5. If an agency is gathering personal information all through their website/channel, the agency should include a link to its privacy rules at each point personal information is composed.
6. The privacy policy should begin with a positive declaration of commitment, be clearly written and use easily understood, just language.
7. Agency contact details should also be offered so that people have somewhere to express further queries connecting to information solitude, and an agency should have a system in place for managing such queries.
8. An agency must make obtainable to the public a document in which it evidently expresses its policies for the management of personal information that it holds.
9. On the demand of an individual, an agency must take sensible steps to inform the individual of the sort of personal information it holds, why it holds the information and how it gathers, holds, uses and reveals the information.

12.9.6 IPP 6: Access and Correction

Individuals have a right to search for access to their personal information and make alterations.

Access and correction is typically managed under the provisions of the *Information Act.* It is significant to discriminate freedom of information from information privacy. The differences between them are:

1. Freedom of information is typically concerned with convincing openness, privacy with compelling discretion.
2. Under freedom of information, anybody can hunt for documents, while privacy deals with the person who is the matter of the information.
3. Freedom of information deals typically with access, while privacy goes broader to also include the collection, use, quality, security and allotment of the information.

This principle includes the following:

1. If an individual demands an agency having personal information regarding the individual for access to the personal information, the agency must offer the individual with access to the information except to the degree that:
   (a) offering access would pose a severe threat to the life or health of the person or another person;
   (b) offering access would prejudice procedures for the defense of the health or safety of the public;
   (c) offering access would irrationally interfere with the privacy of another individual;
   (d) the request for access is dizzy or vexatious;

(e) the information links to existing or anticipated legal proceedings among the agency and the individual, and the information would not be accessible by the procedure of discovery or subpoena in those proceedings;

(f) offering access would reveal the intentions of the agency in association to negotiations with the individual in such a way that would prejudice the negotiations;

(g) offering access would be illegal denying access is required or authorized by law;

(h) offering access would be likely to prejudice an examination of possible unlawful activity;

(i) offering access would be likely to injustice one or more of the following by or on behalf of a law enforcement agency;

(j) preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a agreed law;

(k) implementing a law relating to the confiscation of proceeds of crime;

(l) defensing public revenue;

(m) preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;

(n) preparing for or performing proceedings in a court or tribunal or executing the orders of a court or tribunal;

(o) offering access would injustice the security or defence of the Commonwealth or a State or Territory of the Commonwealth; or the maintenance of law and order in the Territory.

2. Though, where offering the individual with access to the information would disclose evaluative information produced within an agency in association with a commercially sensitive decision making process, the agency may provide the individual an explanation for the commercially sensitive decision instead of access to the decision.

3. If an agency holds personal information about an individual and the individual establishes that the information is not precise, complete or up to date, the agency must take rational steps to correct the information so that it is accurate, complete and up to date.

4. The agency must take rational steps to comply with a request to accurate personal information so that it is accurate, complete and up to date, if:

   (a) an individual and an agency conflict about whether personal information regarding the individual held by the agency is accurate, complete or up to date, and

   (b) the individual demands the organization to associate with the information a declaration to the effect that, in the individual's opinion, the information is imprecise, incomplete or out of date.

5. An agency must offer reasons for refusing to provide access to, or correct, personal information.

6. If an agency charges a charge for offering access to personal information, the fee is not to be extreme.

7. If an individual demands an agency for access to, or to correct, personal information apprehended by the agency, the agency must inside a reasonable time:

   (a) offer access or reasons for refusing access

(b) make the improvement or provide reasons for refusing to make it, or

(c) offer reasons for the delay in responding to the request.

Task Differentiate freedom of information from information privacy.

12.9.7 IPP 7: Identifiers

It restricts the adoption and sharing of unique identifiers. It is intended to maximize cross-matching of data across agencies.

A unique identifier is typically a number allocated to an individual in order to identify the person for the reasons of an agency' operations.

Example: A tax file number, drivers licence number, data collection identifier.

This principle restricts the sharing of unique identifiers between agencies. It offers a safeguard against the creation of a single identifier that could be used to cross-match data across agencies.

This principle includes the following:

1. An agency must not assign unique identifiers to individuals, unless it is necessary to enable the agency to perform its functions efficiently.

2. An agency must not adopt a unique identifier of an individual that has been assigned by another agency unless:

   (a) it is essential to enable the agency to perform its functions efficiently;

   (b) it has obtained the permission of the individual to do so, or

   (c) it is an outsourcing agency accepting the unique identifier created by a contract service provider in the concert of its obligations to the outsourcing agency under a service contract.

3. An agency must not utilize or reveal a unique identifier allocated to an individual by another agency unless:

   (a) the use or revelation is essential for the agency to fulfil its obligations to that other agency;

   (b) it has received the consent of the individual to the use or disclosure, or

   (c) the agency reveals personal information about an individual for a reason (the secondary purpose) other than the primary purpose for collecting it, if:

      (i) an agency reasonably considers that the use or revels is essential to lessen or prevent a serious and looming threat to the individual's or another individual's life, health or safety; or a serious danger to public health or public safety;

      (ii) an agency has cause to suspect that unlawful activity has been, is being or may be occupied in and uses or discloses the information as a necessary part of its investigation of the matter or in reporting its issues to relevant persons or authorities;

      (iii) the use or disclosure is required or authorised by law;

(iv) an agency reasonably considers that the use or disclosure is reasonably essential for one or more of the following by or on behalf of a law enforcement agency:

- preventing, detecting, investigating, prosecuting or punishing an offence or a breach of a prescribed law;
- enforcing a law relating to the confiscation of proceeds of crime;
- protecting public revenue;
- preventing, detecting, investigating or remedying seriously improper conduct or prescribed conduct;
- preparing for or performing proceedings before a court or tribunal or implementing the orders of a court or tribunal.

(v) the Australian Security Intelligence Organisation (ASIO) has demanded the agency to reveal the information, the revelation is made to an officer or employee of ASIO authorized by the Director-General of ASIO to obtain the information and an officer or employee of ASIO authorized by the Director-General of ASIO to do so has certified in writing that the information is required in connection with the presentation of the functions of ASIO.

(vi) the Australian Secret Intelligence Service (ASIS) has requested the organization to disclose the information, the revelation is made to an officer or employee of ASIS authorised by the Director-General of ASIS to obtain the information and an officer or employee of ASIS authorised by the Director-General of ASIS to do so has certified in writing that the information is necessary in connection with the performance of the functions of ASIS.

4. An agency must not need an individual to provide a unique identifier so as to obtain a service unless its provision is required or authorized by law, or is in connection with the purpose for which the unique identifier was assigned or for a directly connected purpose.

12.9.8 IPP 8: Anonymity

This is a very important principle as government agencies move into the electronic background where, more and more, we leave electronic traces of where we have been, what we have obtained, who we have had contact with and what our favorites are.

This principle includes the following:

1. If an agency considers carefully regarding the anonymity principle, it gathers less personal information and that makes complying with the IPPs that much simpler.
2. An agency must give individual entering transactions with the organization the option of not identifying himself or herself, unless it is required by law or it is not practicable that the individual is not identified.

Caution Agencies must provide individuals the option of not recognizing themselves when entering dealings, if that is legal and feasible.

12.9.9 IPP 9: Transporter Data Flows

Personal information can be conveyed to other places only if the recipient guards privacy under standards that are alike to the Northern Territory IPPs.

This opinion is intended to make sure that steps are taken to defend the privacy of personal information if it is sent to a third party exterior the Northern Territory, either throughway or overseas. It recognizes that in a worldwide information economy, it is significant to consider the manners in which personal information may be conveyed. For instance, personal information may be gathered in a jurisdiction that has information privacy in place, but then be transmitted for processing offshore and arrive in a authority that has no privacy security in place.

This principle includes the following:

1. An agency must not transport personal information regarding an individual to a person (other than the individual) outside the Territory unless:
   - (a) the transfer is necessary or authorised under a law of the Territory or the Commonwealth;
   - (b) the agency reasonably considers that the person receiving the information is subject to a law, or a contract or other lawfully binding arrangement, that requires the person to comply with principles for managing the information that are substantially similar to the Northern Territory IPPs;
   - (c) the individual approval to the transfer;
   - (d) the transfer is essential for the performance of a contract among the agency and the individual or for the execution of pre-contractual measures taken in response to the individual's request;
   - (e) the transfer is essential for the performance or completion of a contract among the agency and a third party, the performance or achievement of which benefits the person all of the following apply:
     - (i) the transfer is for the advantage of the individual;
     - (ii) it is unfeasible to obtain the consent of the individual to the transfer;
     - (iii) it is probable that the individual would sanction to the transfer;
     - (iv) the agency has taken rational steps to ensure that the information will not be held, used or revelation by the person to whom it is transported in a manner that is conflicting with the Northern Territory IPPs.

12.9.10 IPP 10: Sensitive Information

Here, Compilation of sensitive information is firmly limited. The IPPs permit for a higher level of defense for sensitive information. This means information or opinion regarding an individual:

1. political choices
2. religious or philosophical beliefs
3. sexual preferences or practices
4. membership of professional associations, trade unions or political groups
5. racial or ethnic origin
6. criminal record.

This principle includes the following:

1. An agency must not gather sensitive information regarding an individual unless:
   - (a) the individual approval to the collection;

Notes

(b) the organization is necessary by law to gather the information;

(c) the individual is physically or lawfully unable of giving consent to the compilation; or physically not capable to converse his or her consent to the collection and gathering the information is essential to prevent or lessen a serious and looming threat to the life or health of the individual or another individual;

(d) gathering the information is necessary to establish, exercise or defend a legal or equitable claim. Though, an agency may collect sensitive information regarding an individual if:

(i) the compilation is essential for research, or the compilation or examination of statistics, relevant to government funded targeted welfare or instructive services; or is of information connecting to an individual's racial or ethnic origin and is for the reason of offering government funded targeted welfare or educational services

(e) there is no other sensibly practicable alternative to gathering the information for that reason, and

(f) it is unfeasible for the association to seek the individual's approval to the collection.

Self Assessment

Fill in the blanks

15. Access and correction is typically managed under the provisions of the ....

16. A unique .... is typically a number allocated to an individual in order to identify the person for the reasons of an agency' operations.

12.10 Summary

- Good metrics are those that are elegant, i.e. specific, quantifiable, attainable, repeatable, and time reliant.
- Metrics are tools intended to facilitate decision making and recover performance and accountability during collection, analysis, and reporting of pertinent performance-associated data.
- Metrics can be an effectual tool for security executives to discern the efficiency of various components of their protection programs, the security of a particular system, product or process, and the aptitude of staff or departments inside an organization to address security concerns for which they are accountable.
- Metrics can also help recognize the level of risk in not taking a given action, and in that way supply guidance in prioritizing counteractive actions.
- Security matrix is used to concentrate measures where they are required, and to be aware of what measures are being (purposely) abandoned.
- Privacy can be explained as exercising power over what access others have to private extent of us, like information privacy.
- Privacy as a business concern or issue is tremendously sensitive to changes in the surrounding context. Changes in people's expectations or in authoritarian governance can noticeably alter business issues and potentials.

- Privacy is regarding informational self-determination—the capability to decide what information regarding you goes where and Security provides the capability to be confident that those decisions are appreciated.
- There are ten Information Privacy Principles (IPPs) which cover the entire life cycle of information from compilation and handling to storage and removal.

12.11 Keywords

Metric: A metric refers to a system of dimension that depends on quantifiable procedures.

Privacy: An individual's or organization's right to establish whether, when and to whom personal or organizational information is released.

Security matrix: It is used to concentrate measures where they are required, and to be aware of what measures are being (purposely) abandoned.

12.12 Review Questions

1. Explain the process of security metrics and also discuss metrics lifecycle.
2. Describe the concept of security metrics management.
3. Explain the various issues or aspects of security measurement.
4. Explain various categories of security metrics for process control systems.
5. What is security matrix? Enlighten its uses.
6. How do you consider privacy as business issue? Illustrate with examples.
7. Explain the concept of differentiation between privacy and security.
8. What are Information Privacy Principles? Explain each of them in detail.
9. Individuals have a right to search for access to their personal information and make alterations. Comment.
10. Describe the rules and regulations used for compilation of sensitive information.

Answers: Self Assessment

1. metric
2. Dimensions
3. Correctness
4. long
5. Security matrix
6. Operational
7. information
8. privacy
9. business
10. Changes
11. Security
12. confidentiality
13. Licensee
14. File Server
15. Information Act
16. identifier

Notes

12.13 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by PricewaterHouseCoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online links

www.ijecbs.com

www.letu.edu

Notes

Unit 13: Privacy Technological Impacts

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand implications of RFID
- Discuss use with biometrics
- Discuss smart card applications

Introduction

In this unit, you will understand privacy impacts on various technologies such as RFID, biometrics and smart card. Biometric devices authenticate users to access control systems through some sort of personal identifier such as a fingerprint, voiceprint, iris scan, retina scan, facial scan, or signature dynamics. Smart Cards are plastic cards that have integrated circuits or storage receptacles embedded in them.

13.1 RFID Security

RFID chips are everywhere – companies and labs use them as access keys, Prius owners use them to start their cars, and retail giants like Wal-Mart have deployed them as inventory tracking devices. Drug manufacturers like Pfizer rely on chips to track pharmaceuticals.

The tags are also about to get a lot more personal. Next-gen US passports and credit cards will contain RFIDs, and the medical industry is exploring the use of implantable chips to manage patients.

RFID technology dates back to World War II, when the British put radio transponders in Allied aircraft to help early radar system crews detect good guys from bad guys. The first chips were developed in research labs in the 1960s, and by the next decade the US government was using tags to electronically authorize trucks coming into Los Alamos National Laboratory and other secure facilities.

Notes

Commercialized chips became widely available in the '80s, and RFID tags were being used to track difficult-to-manage property like farm animals and railroad cars. But over the last few years, the market for RFIDs has exploded, driven by advances in computer databases and declining chip prices. Now dozens of companies, from Motorola to Philips to Texas Instruments, manufacture the chips.

The tags work by broadcasting a few bits of information to specialized electronic readers. Most commercial RFID chips are passive emitters, which mean they have no on-board battery. They send a signal only when a reader powers them with a squirt of electrons.

Once juiced, these chips broadcast their signal indiscriminately within a certain range, usually a few inches to a few feet. Active emitter chips with internal power can send signals hundreds of feet; these are used in the automatic toll-paying devices (with names like FasTrak and E-ZPass) that sit on car dashboards, pinging tollgates as autos whiz through.

For protection, RFID signals can be encrypted.

Example: The chips that will go into US passports will likely be coded to make it difficult for unauthorized readers to retrieve their on-board information (which will include a person's name, age, nationality, and photo).

But most commercial RFID tags don't include security, which is expensive: A typical passive RFID chip costs about a quarter, whereas one with encryption capabilities runs about $5. It's just not cost-effective for your average office building to invest in secure chips.

This leaves most RFIDs vulnerable to cloning or – if the chip has a writable memory area, as many do – data tampering.

Example: Chips that track product shipments or expensive equipment, for example, often contain pricing and item information. These writable areas can be locked, but often they aren't, because the companies using RFIDs don't know how the chips work or because the data fields need to be updated frequently. Either way, these chips are open to hacking.

Did u know? **Full form of RFID**

Radio Frequency Identification

Task Illustrate the functioning of RFID chips.

13.1.1 Privacy Aspects

Impending risks to privacy are usually significant issues for individuals and organizations. Main traits and functionalities of RFID technologies have the potential to provide advantages (*such as* convenience, expediting processes) in addition to foster misperceptions and to impact privacy. RFID systems that gather data associated to identifiable individuals raise particular privacy issues that should be regarded as a priority challenge to the acceptance of the technology in a huge number of regions. In many cases, the potential attack of privacy via the use of RFID is based on both the technology accessed and the context. Invisibility of the data compilation may be the primary trait of RFID that raises concerns. It is also a risk multiplier for the possible privacy challenges connected with the use of the technology. RFID might disclose to third parties information regarding objects carried by individuals without their information. It might permit inferences allowing links to more information on the individual and more accurate profiling.

Example: Inferences completed from numerous tags carried by an individual or from sensitive data, like biometrics in an unsecured RFID passport, or from tagged medicines.

Such a scenario would need the occurrence of readers in the tags' environment in addition to the capacity for the third party to convert the objects' tag information into meaningful data. Likewise, tracking in real time or after the fact may be the major functionality of RFID that raises issues. Particularly, due to the invisibility of the technology, tracking of individuals could take place without their knowledge, if they are provided with hidden tags or tags that are not sufficiently secured. In other cases, tracking people could also be the purpose of the RFID application (e.g. tracking children in an amusement park). Another apprehension is that interoperable ("open loop") RFID technologies make possible and as a result multiply the collection and processing of personal information. Invasive RFID taking benefit of interoperability and ever-present Internet connectivity is often described as a predictable future, although there are currently few instances of open loop systems. In cases where RFID systems collect data which is connected with an identified or identifiable individual, the OECD Privacy Guidelines offer a useful framework. When an RFID system processes personal data, transparency of the function of the processing and consent of individuals are necessary. Beyond fundamental data protection information, privacy observe may usefully comprise additional information like:

1. The existence of the tags,
2. Their content, use and control,
3. The presence of readers,
4. The reading activity,
5. The ability to disable tags, and
6. Where to obtain assistance.

Innovative means of informing individuals competently could be discovered. Continued stakeholder dialogue among stakeholders, across sectors and in each of the particular application areas, would help elucidate or reach a consensus on what information to offer to individuals, the best means to converse it to attain efficient transparency, in addition to the cases where consent should be or not be needed. Naturally, security safeguards are necessary for the defense of privacy in RFID systems.

The broad variety of technical configurations and use scenarios make privacy impact assessments a good practice for identifying and accepting privacy risks and best approaches to mitigate them in a specified system. As for protection, since RFID systems are often components of broader information systems, it cannot be predictable that all privacy challenges can be solved at the RFID level. A holistic method to privacy management may be tinted as a good practice. Such an approach would regard all the components of the information systems implicated, besides the core RFID components in addition to the whole life cycle of the tag when it remains useful beyond the reach of the data controller. The option of the RFID technology to be used in a system influences the defense of privacy just as it impacts the security of the system. Privacy by design or embedding privacy in the design of the technology and of the systems can considerably help the protection of privacy and promote trust in RFID systems. Strategies to offer incentives to industry and business for scheming and using RFID technologies that comprise sufficient privacy protections could be pursued. Yet, as for security, privacy protection should not solely depend on technical dimensions but instead on a mix of technical and non-technical safeguards. Some parties do not connect tag data with individuals yet supply them with consumer goods tagged with functional RFID tags that they or third parties could later read. It could be recommended that such parties take accountability for either deactivating the tag or offering information to individuals regarding the presence of the tags, the privacy risks associated to them and the means to avert or mitigate such risks. Lastly, and more usually, RFID is not well understood by individuals. Mounting the level of awareness and understanding about RFID, its possibilities and limits in addition to benefits and risks, can contribute to falling this perception concern. It may also assist individuals make suitable options and support efforts by organizations to organize privacy pleasant systems.

Notes Efforts to increase RFID privacy enhancing technologies are continuing and could be encouraged. Methods like data minimization and anonymisation can be applied to RFID.

Self Assessment

Fill in the blanks:

1. RFID chips are everywhere such as companies and labs and are used as ....
2. The RFID .... work by broadcasting a few bits of information to specialized electronic readers.
3. The potential .... of privacy via the use of RFID is based on both the technology accessed and the context.
4. RFID might disclose to .... parties information regarding objects carried by individuals without their information.
5. The option of the RFID technology to be used in a system influences the defense of privacy just as it impacts the .... of the system.

13.2 Use with Biometrics

Biometric devices authenticate users to access control systems through some sort of personal identifier such as a fingerprint, voiceprint, iris scan, retina scan, facial scan, or signature dynamics. The nice thing about using biometrics is that end-users do not lose or misplace their personal identifier. It's hard to leave your fingers at home. However, biometrics have not caught on as fast as originally anticipated due to the false positives and false negatives that are common when using biometric technologies.

Biometric authentication systems employ unique physical characteristics (or attributes) of an individual person in order to authenticate the person's identity. Physical attributes employed in biometric authentication systems include fingerprints, hand geometry, hand -written signatures, retina patterns and voice patterns. Biometric authentication systems based upon these physical attributes have been developed for computer login applications.

Biometric authentication systems generally operate in the following manner:

1. Prior to any authentication attempts, a user is "enrolled" by creating a reference profile (or template) based on the desired physical attribute. The reference profile is usually based on the combination of several measurements. The resulting template is associated with the identity of the user and stored for later use.

2. When attempting to authenticate themselves, the user enters his login name or, alternatively, the user may provide a card/token containing identification information. The user's physical attribute is then measured.
3. The previously stored reference profile of the physical attribute is then compared with the measured profile of the attribute taken from the user. The result of the comparison is then used to either accept or reject the user.
4. Biometric systems can provide an increased level of security for IT systems, but the technology is still less matures than memory or smart cards. Imperfections in biometric authentication devices arise from technical difficulties in measuring and profiling physical attributes as well as from the somewhat variable nature of physical attributes.

Example: A person's speech pattern may change under stressful conditions or when suffering from a sore throat or cold.

Caution Many physical attributes change depending on various conditions.

Did u know? Biometric systems are typically used in conjunction with other authentication means in environments requiring high security.

Self Assessment

Fill in the blanks:

6. .... devices authenticate users to access control systems through some sort of personal identifier such as a fingerprint, voiceprint, iris scan, retina scan, facial scan, or signature dynamics.
7. Biometric authentication systems employ unique physical characteristics (or attributes) of an individual person in order to authenticate the person's ....
8. .... attributes employed in biometric authentication systems include fingerprints, hand geometry, hand -written signatures, retina patterns and voice patterns.
9. The .... profile is usually based on the combination of several measurements.
10. .... in biometric authentication devices arise from technical difficulties in measuring and profiling physical attributes as well as from the somewhat variable nature of physical attributes.

13.3 Smart Card Applications

A smart card is a device typically the size and shape of a credit card and contains one or more integrated chips that perform the functions of a computer with a microprocessor, memory, and input/output. Smart cards may be used to provide increased functionality as well as an increased level of security over memory cards when used for identification and authentication.

Smart Cards are plastic cards that have integrated circuits or storage receptacles embedded in them. Smart cards with integrated circuits that can execute transactions and are often referred to as "active" smart cards.

Cards with memory receptacles that simply store information (such as your bank ATM card) are referred to as "passive." Whether or not a memory card is a type of smart card depends on who you ask and what marketing material you are reading. Used to authenticate users to domains, systems, and networks, smart cards offer two-factor authentication — something a user has, and something a user knows. The card is what the user has, and the personal identification number is what the person knows.

A smart card can process, as well as store, data through its microprocessor; therefore, the smart card itself (as opposed to the reader/writer device), can control access to the information stored on the card. This can be especially useful for applications such as user authentication in which security of the information must be maintained. The smart card can actually perform the password or PIN comparisons inside the card.

As an authentication method, the smart card is something the user possesses. With recent advances, a password or PIN (something a user knows) can be added for additional security and a fingerprint or photo (something the user is) for even further security. As contrasted with memory cards, an important and useful feature of a smart card is that it can be manufactured to ensure the security of its own memory, thus reducing the risk of lost or stolen cards.

The smart card can replace conventional password security with something better, a PIN, which is verified by the card versus the computer system, which may not have as sophisticated a means for user identification and authentication.

The card can be programmed to limit the number of login attempts as well as ask biographic questions, or make a biometric check to ensure that only the smart card's owner can use it. In addition, non-repeating challenges can be used to foil a scenario in which an attacker tries to login using a password or PIN he observed from a previous login. In addition, the complexity of smart card manufacturing makes forgery of the card's contents virtually impossible.

Use of smart devices means the added expense of the card itself, as well as the special reader devices. Careful decisions as to what systems warrant the use of a smart card must be made. The cost of manufacturing smart cards is higher than that of memory cards but the disparity will get less and less as more and more manufacturers switch to this technology. On the other hand, it should be remembered that smart cards, as opposed to memory only cards, can effectively communicate with relatively 'dumb', inexpensive reader devices.

Notes The proper management and administration of smart cards will be a more difficult task than with typical password administration. It is extremely important that responsibilities and procedures for smart card administration be carefully implemented.

Smart card issuance can be easily achieved in a distributed fashion, which is well suited to a large organizational environment.

Caution Just as with password systems, care should be taken to implement consistent procedures across all involved systems.

Task Explain the process of smart card as an authentication method.

Self Assessment

Fill in the blanks:

11. A .... a device typically the size and shape of a credit card and contains one or more integrated chips that perform the functions of a computer with a microprocessor, memory, and input/output.
12. Smart Cards are .... cards that have integrated circuits or storage receptacles embedded in them.
13. Cards with memory receptacles that simply store information (such as your bank ATM card) are referred to as ".......................”
14. Use of smart devices means the added expense of the card itself, as well as the .... reader devices.
15. The .... of smart card manufacturing makes forgery of the card’s contents virtually impossible.

Caselet

Concern Over ICAO Move for ‘Biometric’ Passports

The International Civil Aviation Organisation’s (ICAO) biometrics-approach to securing travel documents has invited the wrath of civil liberties and human rights activists around the world who fear this would lead to the creation of a global surveillance infrastructure.

An open letter to the ICAO signed by leading activist organisations led by Privacy International and the American Civil Liberties Union expressed concern about ICAO plans requiring passports and other travel documents to contain biometrics and remotely readable “contact-less integrated circuits.”

Respecting the privacy of individuals was essential to an open society, including travel privacy. Border and aviation security necessarily involved scrutinising travellers and the use of personal information, but in light of the fundamental human rights involved, must be approached with the utmost thought and care. But the biometrics-based approach to securing travel documents unfortunately did not reflect such care.

The letter goes on to add: “We are increasingly concerned that the biometric travel document initiative is part and parcel of a larger surveillance infrastructure monitoring the movement of individuals globally that includes Passenger-Name Record transfers, Advance Passenger Information (API) systems, and the creation of an intergovernmental network of interoperable electronic data systems to facilitate access to each country’s law enforcement and intelligence information.

“We are concerned that the ICAO is setting a surveillance standard for the rest of the world to follow. In this sense, the ICAO is setting domestic policy, implementing profiling and ID cards where previously none may have existed, or enhancing ID documentation through the use of biometrics, and increasing the data pouring into national databases, or creating them when none previously existed.

“While we understand the desire of the ICAO to increase confidence in travel documents, reduce fraud, combat terrorism, and protect aviation security, the implementation of biometrics will have disproportionate effects on privacy and civil liberties.”

Contd...

Because they are not carefully crafted, the ICAO standards risk ignoring these international warnings, resulting in the creation of centralised national databases of personal biometric information.

Central databases become privacy risks through the disclosure of personal information, through the challenges of securing such large data stores, and through the use of biometric data for other purposes.

Additionally, the centralised storage of biometric data increases the risk of the use of biometric data as a key to interconnecting databases.

Source: http://www.thehindubusinessline.in/2004/05/03/stories/2004050301310200.htm

13.4 Summary

- RFID chips are everywhere – companies and labs use them as access keys.
- The tags work by broadcasting a few bits of information to specialized electronic readers.
- Most commercial RFID chips are passive emitters, which mean they have no on-board battery. They send a signal only when a reader powers them with a squirt of electrons.
- Main traits and functionalities of RFID technologies have the potential to provide advantages (*such as* convenience, expediting processes) in addition to foster misperceptions and to impact privacy.
- RFID might disclose to third parties information regarding objects carried by individuals without their information.
- Biometric devices authenticate users to access control systems through some sort of personal identifier such as a fingerprint, voiceprint, iris scan, retina scan, facial scan, or signature dynamics.
- Biometric authentication systems employ unique physical characteristics (or attributes) of an individual person in order to authenticate the person's identity.
- A smart card is a device typically the size and shape of a credit card and contains one or more integrated chips that perform the functions of a computer with a microprocessor, memory, and input/output.
- Use of smart devices means the added expense of the card itself, as well as the special reader devices.

13.5 Keywords

Biometric: Biometric devices authenticate users to access control systems through some sort of personal identifier such as a fingerprint, voiceprint, iris scan, retina scan, facial scan, or signature dynamics.

RFID: RFID (radio frequency identification) is a technology that includes the utilization of electromagnetic or electrostatic combination in the radio frequency (RF) part of the electromagnetic spectrum to exclusively recognize an object, animal, or person.

Smart card: A smart card is a device typically the size and shape of a credit card and contains one or more integrated chips that perform the functions of a computer with a microprocessor, memory, and input/output.

13.6 Review Questions

1. What are RFID tags? Explain the working of RFID tags.
2. "Most RFIDs are vulnerable to cloning". Explain.
3. Illustrate the privacy impact of RFID.
4. What are biometric devices? Illustrate the working of biometrics devices.
5. Elucidate the steps used in Biometric authentication systems.
6. Enlighten how the biometrics devices assist in preserving privacy.
7. What is a smart card? Illustrate the concept.
8. Illustrate the various applications of smart card.
9. Describe how smart card applications support in maintaining privacy.
10. Prior to any authentication attempts, a user is "enrolled" by creating a reference profile (or template) based on the desired physical attribute. Comment.

Answers: Self Assessment

1. access keys
2. tags
3. attack
4. third
5. security
6. Biometric
7. identity
8. Physical
9. reference
10. Imperfections
11. smart card is
12. plastic
13. passive
14. special
15. complexity

13.7 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by Pricewaterhousecoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online link

www.aimglobal.org

Notes

Unit 14: Web Services and Privacy

CONTENTS

Objectives

After studying this unit, you will be able to:

- Understand the concept of privacy on internet
- Discuss web services
- Explain privacy aspects of SOA

Introduction

The term "Web Services" can be puzzling. It is, unluckily, frequently used in many dissimilar manners. Compounding this perplexity is term "services" that has a dissimilar meaning than the term "Web Services." Privacy is a position wherein an entity can work on his/her information in isolation, resulting in a choosy revelation of one's uniqueness and information.

In this unit, you will understand internet privacy, web services and various privacy aspects of SOA.

14.1 Privacy on Internet

Internet privacy is a main issue of today. Privacy over the Internet has increased some ethical issues, which is required to be dealt with. While catering to the privacy requirements of the Internet users, we require executing certain ethics.

Privacy can signify ambiguity in case a person would like to remain anonymous. Privacy can also be associated to the security aspect of an individual or information. The definitions of privacy can fluctuate across individuals and cultures. The assault of privacy can be averted by the concern of privacy laws.

With Internet, hosting a massive information base, a new notion has evolved - information privacy. The information on the Internet has security requirements. Unauthorized access to information is unwanted. Data privacy points to the association among technology and the legal rights that come with it. Whenever any information concerning a person or a person's data is stored, privacy requirements arise. Internet privacy is the control one has over what information regarding oneself, the person would like to reveal. Internet privacy deals with managing the access to information on the Internet.

Using the Internet frequently includes the use of social networking sites, e-mail amenities and the browse of a variety of other websites. Internet privacy occurs on the scene when it comes to website users offering out their individual details on the Internet. For sure websites, which help online shopping, the users are made to input their credit card numbers. In case of e-mailing sites, there are concerns about whether third parties should be permitted to store or read e-mails without informed consent. Whether or not, the third parties should be permitted to track the visitors on a website, is another major privacy concern. The other significant Internet privacy issue is whether the sites that congregate personally express information from the users should accumulate or share it.

Internet privacy can be measured as a division of computer privacy. Computer privacy comprises the data privacy connecting to the escaping of the improper revelation of the personally identifiable information composed and stored by websites. The effective sharing of data while defensing the private information is the real confront.

One school of thought refutes the survival of Internet privacy while the other supports the requirement of the Internet privacy. Complete secrecy is not the intention of Internet privacy. It somewhat intends to attain a controlled revelation of one's personal information. Internet is a network of networks and when a person accesses the Internet, he/she attaches to it and is identified by an address. In technological terms this address is called an IP address. For security reasons, a website may desire to track these addresses of its users. Websites may gather the non-personally particular information of their users. Such information is the one, which in no method can be used to exclusively identify a person. The revelation of these forms of information is satisfactory. It is in fact the means by which websites track the users' Internet actions.

Is it morally right to permit users to make use of the Internet with a fake or an anonymous identity? While it caters to the privacy requirement of some users, it may endanger the Internet procedure for the others. Many users grumble of being stalked by the unidentified users.

The autonomy of expression gifted by social networking has resulted in some Internet users broadcasting wrong or undesired information under bogus names. They are free to converse and opine about any and all topics in forums, chat rooms, interacts and blogs. Furthermore, such expressions do not need the users to reveal their identities. This raises concerns in research ethics pertaining to the privacy of research matters and informed consent. This is an unnecessary advantage of the Internet privacy whereby the border among the private and the public spaces is made blurred. While offering open platforms for discussions, the Internet is ironically becoming a stage where forged people can influence false opinions and foster fallacies.

Does Internet privacy entail that all the information placed on to the Internet remains private and confidential? Does Internet privacy ascertain the privacy of every Internet user? There are people who fear using online banking and shopping websites since they doubt the unauthorized revelation of their personal information. Some cover themselves while using the Internet. Mailing lists and forum posts are a component of the search results on the topics conversed in them. Is it ethically accurate to expose people's views in these manners? Some people fear the truth that they have a visibility over the Internet for such purposes.

The trade-off would be to describe the demarcating line between what's public and what's private. Internet privacy is certainly significant in case of the exposure of personally identifiable information but it needs to be surrounded in cases where solitude puts the Internet ethics on stake.

Notes Internet privacy is a urgent matter due to the growing number of peeping toms on the Internet. There are a number of advertisers, a number of stalkers and hackers on the Internet coming up to infringe our privacy over the Internet and getting unwanted access to our protected, unnamed information. Experts in this field say that Internet Privacy is a non-existent entity but here is an insight into the planet of Internet privacy.

Did u know? Some users favor stricter forms of privacy like anonymity to the Internet.

14.1.1 Violation of Internet Privacy

Initially the bulky community of hackers that survive over the Internet can hack into your accounts and get unwanted access to your private information that can not just damage your privacy but can be a reason of social in addition to financial worry. The advertisers lurking at the back of the virtual walls can track your Internet activity to send you modified commercial offers as well. Many employers can also get use to your Internet activity while you are using your computers at the place of work. In case you are accessing an Internet café, the proprietor of the café can keep a label of your Internet access also. Your Internet service provider can get whole and thorough information regarding your internet activities though this is normally not a danger because of the existing legal structure that prohibits them from violating the privacy of their users.

14.1.2 How can the Websites Violate my Privacy?

The websites can mark you with a simple technical element known as 'cookie'. Once a website labels you with a cookie which gets saved with them and assists them to keep in mind you the next time you visit the same site. Even though most of the websites accessing these cookies are harmless, the difficulty begins when websites permit advertisers to have an access to this information that will disclose you entire Internet activity and assist the advertisers to goal you according to your interests.

14.1.3 Are there any Organizations that Support Generate Awareness and Recommend Ways to Promote Internet Privacy?

Yes, there survive numerous organizations that strongly believe in preserving Internet privacy. Some of the famous organizations between these are American Civil Liberties Union, Electronic Frontier foundation and Electronic Privacy Information Center.

14.1.4 Safeguarding Internet Privacy

Well providing you are on the Internet you cannot end the broadcast of information for sure. Though one thing that you can surely do is - evade browsing websites that are not dependable or seem fishy. Especially if you would like to safeguard your privacy in terms of financial and communal matters do not danger it by shopping on untrustworthy websites or signing up apprehensive membership forms that needs you to fill up your social safekeeping numbers, credit card details and other significant information. You can also modify your privacy settings in Internet options setting of your computer. You can utilize anti-spyware programs to remove spyware items and tracking cookies that intimidate your Internet safety. Therefore if you cannot discontinue sending out your information whereas you are browsing you can surely prefer the websites that you can trust your information with.

In an age where we show off about the advantages of technology and the manner the world is getting closer and closer, there is no alternative but to bear the little limitations of this technology.

Self Assessment

Fill in the blanks:

1. .... points to the association among technology and the legal rights that come with it.
2. Internet privacy can be measured as a division of .... privacy.
3. The websites can mark you with a simple technical element known as '........................'.
4. You can utilize .... programs to remove spyware items and tracking cookies that intimidate your Internet safety.

14.2 Web Services

The term "Web Services" can be puzzling. It is, unluckily, frequently used in many dissimilar manners. Compounding this perplexity is term "services" that has a dissimilar meaning than the term "Web Services." The term Web Services points to the technologies that permit for making connections. *Services* are what you attach together using Web Services. A service is the endpoint of a connection. Also, a service has some sort of original computer system that assists the connection provided. The combination of services i.e. internal and external to an organization – generate a service-oriented architecture.

A classic Web transaction includes three components: users, services and databases. This obviously defines a privacy model with three dissimilar types of privacy: user privacy, service privacy, and data privacy.

Example: Examples of web transaction includes voting, tax payment, online shopping, hotel reservation.

14.2.1 User Privacy

Users of a Web service comprise persons (e.g., citizens and case officers), applications, and other Web services. In many cases, users conversing with a Web service are needed to offer a major amount of personal sensitive information (example, their social security number, credit card number, health information, and address). Users of Web services, though, may expect or need dissimilar levels of privacy as per their observation of the information sensitivity.

Notes

Example: A user may have tighter privacy needs concerning medical records than employment history.

The user's awareness of privacy also is based on the information receiver (i.e., who receives the information) and the information usage (i.e., the reasons for which the information is used) .

The set of privacy favorites appropriate to a user's information is known as user privacy profile. A user privacy profile is usually defined by the user but can also be consistently set for a group of individuals. Privacy profiles are dynamic: users can create, view, update, or delete their privacy profiles. To offer support for resolving lawful disputes over privacy violation, the underlying Web service architecture must outline all of these operations. We also define a user's privacy credentials as a signature that is obviously appended to any request that the client submits to the Web service. They find out the privacy scope for the equivalent user. A privacy scope for a specified user defines the information that a Web service can reveal that to user.

Example: A case officer using a government Web service may have solitude credentials conceding a privacy scope that involves information regarding citizens' employment, housing, etc. Privacy credentials may be allocated to users on an individual or group basis.

14.2.2 Service Privacy

A Web service usually has its own *privacy policy* that mentions a set of regulations applicable to all users. Service privacy usually mentions three types of policy: usage policy, storage policy, and disclosure policy. The usage policy specifies the reasons for which the information composed can be used.

Example: Think of a government Web service Medicaid that offers healthcare coverage for low-income citizens. Medicaid may affirm that the information composed from citizens will not be used for reasons other than those directly associated to providing health services to citizens.

The storage policy mentions whether and until when the information gathered can be amassed by the service.

Example: Medicaid may specify that the information it gathers from citizens will remain accumulated in the underlying databases one year after they go away the welfare program.

The disclosure policy mentions if and to whom the information gathered from a specified user can be exposed. This information may associate to individual persons or to groups of individuals.

Example: The privacy policy of the Web service Medicaid may mention that external users cannot use statistical information that disposes general traits of the recipients (e.g., average income, racial background distribution, etc.).

Task Discuss various types of service policy.

14.2.3 Data Privacy

A data object may be used by several Web services.

Example: Think of the US National Database for New Hires (NDNH) that encloses information concerning over 200 millions hired employees.

A record in this database can be used (by means of a government Web service) by an IRS officer to ensure the accuracy of an employee's tax form. It may also be used (by means of another government Web service) by an officer at a child carry agency to check whether a parent is acquiescent with his child hold obligations. This displays that different Web services may require dissimilar information from the same data object. Therefore, data objects must be able to expose dissimilar views to dissimilar Web services. For every data object, we define a data privacy profile that specifies the access views that it exposes to the dissimilar Web services.

Moreover, data objects with comparable *data* privacy profiles form a privacy cluster. A major inspiration of data clustering is that legal rules and self-defined policies enforcing privacy are usually applicable to great segments of populations (e.g., residents of a state). A privacy cluster has one solitary international privacy profile. Overlapping privacy clusters may survive.

Example: The manager of a government database that encloses information regarding citizens may partition the database into two clusters *C*1 and *C*2. The information in *C*1 is usable to local, state, and federal Web services, and information in *C*2 is usable only to local and state Web services.

Task Make distinction between service privacy and data privacy.

Self Assessment

Fill in the blanks:

5. The term .... points to the technologies that permit for making connections.

6. The set of privacy favorites appropriate to a user's information is known as ....

7. The .... policy specifies the reasons for which the information composed can be used.

8. The .... policy mentions whether and until when the information gathered can be amassed by the service.

9. A major inspiration of .... is that legal rules and self-defined policies enforcing privacy are usually applicable to great segments of populations

10. Data objects with comparable .... privacy profiles form a *privacy cluster.*

14.3 Privacy Aspects of SOA

Service-oriented Architecture (SOA) is a method of designing software to offer services to applications, or to other services, via published and discoverable interfaces. Each service offers a discrete chunk of business functionality by a loosely coupled (frequently asynchronous), message-dependent communication model.

Much of the software industry concentrates so far has been on the underlying method for executing Web services and their communications. Inadequate attention has been provided to the techniques and tools needed for architecting enterprise-scale software solutions by means of Web services. The design of a high-quality software solution, such as any other complex structure,

Notes

needs early architectural decisions assisted by well-understood design methods, structural patterns, and styles. These patterns address general service concerns like scalability, reliability, and security.

Business stakeholders are based on the IT organization to offer solutions to their business needs. For both financial and market-driven purposes, stakeholders want to shorten the investment in time and money it takes to give IT solutions. They also wish to grow the value they derive from IT solutions by maximizing the needs coverage each software project offers. As so many of those projects today include Web services, it is very imperative that we have better tools and methods for the rapid and successful execution of those business requirements by means of SOA. We consider modeling to be especially imperative due to its capability to separate concerns and present a unified view of those issues. Security in service executions is a major concern since many applications function across organizational boundaries. The reason of this is to offer a set of primitive modeling elements that permit the business stakeholders to mention the intent of security inside the requirements procedure.

Did u know? System architects who take benefit of SOA can include one or more services into their applications as constituents.

14.3.1 Architectural versus Implementation Models

As IT professionals goes to deliver applications by means of Web services, they frequently find themselves in the place of coming up to speed on an architectural model (SOA) and an execution model (Web services) at the same time. As one might expect under the situations, the distinctions among the model and the execution sometimes get lost. This assumes the utilization of a Model Driven Architecture method that carefully averts commingling the platform-independent model of an application's architecture and behavior with the methods and platforms used to execute that modeled behavior. System architects employ either domain-particular languages or profiles for Unified Modeling Language (UML) to model the issues of the service domain. The principles that need architects to keep platform and language issues out of this model also need them to keep implementation-particular security issues out.

Example: A model that involves abstract ideas of services and messages should not also involve details of how messages can access public-key encryption and certificates to execute service authentication and message signatures, since doing so violates a very basic principle (the need to separate concerns) by producing the details of a specific technical execution into the platform-independent model.

Alternatively it is not possible to treat security as an afterthought. Security executions are complex; they can have serious influences on performance, and they can position additional needs on the IT infrastructure assisting the services. It is thus in everyone's best interests to model security issues as carefully as any other issues.

By dividing issues, the IT organization can proficiently engage the business stakeholders in understanding and illustrating the business requirement to maximize needs coverage. We intend to display how to mention security intents in these high-level models while isolating behavioral concerns from execution and platform-specific ones, consistent with the rules of MDA.

14.3.2 Revisiting Security Concerns

The team that produced the RosettaNet family of B2B standards formed concerns that were similar to the ones we just conversed, and made a beginning toward addressing them. The notion was to present a simplified set of options to the business architects — the main stakeholders from whom the RosettaNet team gathered data and processing requirements. These business architects were not versed in the technical details of the security issues, but they were able to contrast data that required to be passed in a secure way from data that could be sent without security measures.

Though, one problem with this method was that a simplified terminology was imperative. As soon as the terms became complicated, the business stakeholder would request every obtainable type of security, just to be secure, and that effected in sub-optimal designs. It was this behavior on the portion of stakeholders that led the architecture group to set out easy guidelines on the specification of such constraints in addition to descriptions that the client could understand. Doing so gave stakeholders the insight they required to make informed cost/benefit trade-off decisions.

Example: The RosettaNet team used examples to help the business user understand when the cost of encrypting data was far greater than the value of the data being protected.

14.3.3 Generalization of Security Issues

There are many texts on common software security concerns, and many more on specific security executions and technologies. Though, we would like to be able to address the underlying intent that drives security-linked technical executions. Particularly, we would like to be able to mention a set of descriptive primitive intents that are simple to understand, and that can be accessed to identify specific technical executions.

Let us take a general instance: withdrawing cash from an ATM machine. Initially, when I walk up to an ATM machine, I am asked to offer two things: my ATM card (which performs as formal identification) and a personal identification number (PIN), which is a “shared secret” familiar to me and my bank, but to no one else. The ATM can now take the identification information and PIN and ask my bank if the person standing in front of it can be presumed, with an acceptable level of confidence, to be the account holder. If the issuing bank verifies the supplied details, it sends back to the ATM a set of security credentials that offer additional information on the account holder. Depending on this account-particular information, the ATM then shows the list of actions I am authorized, as the account holder, to perform — actions that might involve “withdrawal”, “deposit,” and so on.

Notes Note that this set of choices really represents the intersection of two sets:

1. The set of all operations this particular ATM is capable of performing.
2. The set of all operations the issuing bank verifies that I am eligible to perform.

The credentials sent by the bank usually include a restriction on the amount of cash I can withdraw in any single transaction-a limit that the ATM itself can enforce. The ATM system architect must also offer an audit trail by logging all the information flowing to and from the ATM.

How is this communication among bank and ATM completed? How can the bank trust the information it obtains from the ATM and vice versa? Technical details like these, linked to security protocols, data encryption and so on, are both significant and interesting — but these are mainly the kind of details that are outside the level of any high-level behavioral model.

Notes

The ATM instance explains three categories of security concerns or domains:

1. Who are you? (Identification, Authentication)
2. What can you do? (Authorization)
3. What can you, and others, see? (Privacy)

A fourth domain is less obvious, but it is intertwined with the other three domains:

4. What happened? (Audit)

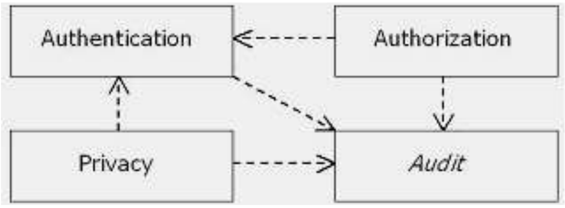
The audit domain frequently appears to be an afterthought in the development of many IT applications. Alternatively, in some business areas, like core security, and in applications like EDI (Electronic Data Interchange), where regulatory issues require important audit capabilities, the audit function is an explicit and significant security concern. Our method considers auditing as an implicit intent; thus, the primitives we introduce all imply an audit trail of their detailed behavior.

So, for example, when we label that party A needs that before it can collaborate with party B, it must authenticate party B, this shows that authentication request and response with the date/ time in addition to other execution details must all be audited. Figure 14.1 Illustrates the Dependencies among these domains.

Example: It is not possible to execute authorization without authentication. Alternatively both authorization and authentication rely on auditing, not for execution but to ensure that any exceptions are captured for analysis and non-repudiation.

Caution Privacy depends on both authentication and auditing.

Figure 14.1: Dependencies between Security Domains



This continues to address the primitive intents that are general in these domains and then describes how such primitives, once introduced into a model, can drive executions in any specified technology.

This domain is mainly related with the identification of one or more parties to a communication or collaboration. We can in fact divide this into two distinct issues: the static notion of identification and the dynamic notion of authentication.

In the ATM instance, the ATM card is the static, bank-issued identification, while the card/PIN pair permits the ATM to authenticate me dynamically as the account holder. It is far more significant to model the ideas of authentication than identification; usually, identification becomes much more entwined in the technical details of its execution than does authentication.

So, for example, we can define very simply that in a specific collaboration between a set of parties there is a need for authentication among those parties. This can be performed explicitly or implicitly; for example, another idea, that of trust, can be used to illustrate trust zones.

Parties within the similar trust zone can consider they do not need to authenticate each other, while for all sensitive communication across trust boundaries, authentication is needed.

Where the trust zone is a useful concept, it does not fulfill all requirements. Trust zones are frequently hierarchical, and some interaction with external parties can be completed without requiring to authenticate the incoming party. A business might see itself as a single trust zone in the sense that no one apart from employees can use network resources inside the firewall. Though, a single-zone picture like this will be misleading if, as generally happens, there is also a trust zone separating the ERP (Enterprise Resource Planning) and CRM (Customer Relationship Management) applications, as each of these executes and maintains its own application-level security. The business might also view itself as a member of an external trust zone via its membership of a trading extranet. In this concern, we suggest that trust and authentication are explicit, yet overlapping, intents that can be accessed to a collaboration model.

This domain is initially accountable for making sure that, once we understand who you are, we can limit your choices to only those functions you are authorized to execute. This needs the potential to perform authentication, since we must know who you are before we can judge what you are efficient to do. The business stakeholder would like to recognize those functions that require to be made protected, in the sense that we know who might execute them and we know (via audit) when they were executed. There are obviously functions that do not need authorization, either as we want them to be usable to everyone, or since, for performance reasons, we have recognized a trust zone inside which services can securely assume the requester's right to use them.

This trust zone thought becomes imperative when we think of performance as another, sometimes competing, issue, and since there is a cost related with implementing security, and sometimes that price is pretty high. Consider a function to return the number of marvelous orders for a customer — a very simple query from a database. If we query for authentication, authorization, and privacy we are forced to accept imperative costs:

1. We have to ask the requester to offer credentials.
2. We have to verify those credentials, probably with a remote service.
3. We have to encrypt the returned information.

If we understand that the requester and provider are both services of the similar application, we can recognize them as a single trust zone, dispense with the overhead, and reap the advantage in increased performance. From an architectural standpoint it is also significant to recognize all the communication that occurs on within trust zones. This kind of communication should be minimized and handled as much as possible as it displays the most likely point of failure in the overall security execution.

In views of execution, there are two main approaches to authorization that are appealing to note here:

1. ***Authorization of Individual Parties:*** Every party can be allocated an explicit set of access rights to functions (even though to optimize the process, we might agree to consider the absence of an explicit access right as either and implicit approval or disapproval of that access right).
2. ***Authorization through Roles:*** Numerous roles can be generated for each application, and access rights allocated as described above to those roles rather than to individual parties. When every party is authenticated, the credentials supplied for the party involve the party's role, which then identifies whether the party is authorized to access a specific function.

Notes The significant point to observe here is that we always wish to *exclude* details like these from our high-level behavioral models. Our intent at the high-level modeling stage is just to note, for instance, that a specified function needs authorization before it can be executed, without detailing how that authorization will be completed.

The issue of the privacy domain is to make sure that you view only the information that is you are authorized to view, and that other parties do not see information they are not ordered to see. Businesses both consume and produce large amounts of data, which is accumulated, manipulated and passed around to assist the running of the business. We have to make sure that information that is sensitive in nature is guarded and that we offer a method to know who is requesting or offering information and services.

Caution We require to know not just which service was the requester or provider, but which authenticated end user was a party to the transaction via that service.

There are two different intents related with the privacy domain:

1. The objective to sign a message or document (potentially by means of multiple signatures) recognizing the end user(s) or service(s) that formed the message or document. This intent, which depends on a number of common standards for digital signatures, is accessed in B2B commerce, government commerce, and even more broadly in corporate e-mail conversations. A document may have a number of signatures.

Example: A supply requisition may be signed by the originator, their manager (approver) and ultimately the purchasing department when the order is positioned; all of these signatures goes with the document.

2. The objective to make sure the privacy of a message, either by sending it over a protected medium or by encrypting or else securing the content. This goal is probably the region with the most variability in the options for execution.

Example: In considering message converting services we can take into account that the message itself is encrypted by the sender and then sent over a protected channel, that the message is sent as plain text over a secure transport like HTTPS or TLS (both of which actually offer encryption as a part of the service, but outside of the sender's control) or even that the message includes an identifier for a document sent by some other protected means.

Another issue that is frequently cited is that of data integrity – the requirement to make sure that the contents of a message or document cannot be modified en route among the numerous parties to the transaction. A message or document that has data integrity is considered to be tamperproof. The anticipation is that if a message is observed as private it should be tamperproof also; though, it should also be possible to signify that a message is just tamperproof without needing a privacy solution.

Finally, the implementer's role is to offer a solution that fulfills the requirements of data privacy in common with guidelines laid down by the business.

Example: It would not be adequate for an e-commerce Website to use a courier to broadcast each customer's credit card number to the bank for verification, while couriers might be an excellent option for delivering secret government documents.

Another area of issue is the idea of non-repudiation of origin and content, a term you will locate in many EDI documents. Non-repudiation is a grand title for the idea that at some point in the coming days one of the parties to a transaction might deny having accomplished the transaction. On the other hand, one of the parties to a transaction might recognize that the transaction occurred but dispute a particular detail of that transaction.

Example: Having purchased 100,000 shares of a stock that consequently lost value, party A might effort to declare that the transaction was for only 100 shares.

In many industries and geographies there are governmental regulations that need the keeping of records for lengthy periods to adjudicate such disputes.

In this view the auditing issue we introduced earlier should offer the required capabilities to accumulate messages. While auditing alone does not essentially suffice for the purposes of non-repudiation, auditing of the message exchange (proof of content) along with validation (proof of origin) usually does offer the necessary level of proof.

Self Assessment

Fill in the blanks:

11. .... is a method of designing software to offer services to applications, or to other services, via published and discoverable interfaces.

12. System architects employ either domain-particular languages or profiles for .... to model the issues of the service domain.

13. Business stakeholders are based on the IT organization to offer .... to their business needs.

14. The .... domain frequently appears to be an afterthought in the development of many IT applications.

15. A message or document that has data integrity is considered to be ....

16. .... is a grand title for the idea that at some point in the coming days one of the parties to a transaction might deny having accomplished the transaction.

Caselet

Cloud Computing for Banking

Computing through the cloud offers new ways of doing business. Choosing a private, public, or a hybrid of private, public and community clouds should create new business models to conduct business in a highly competitive finance industry. Internet-based cloud IT solutions provide not only enormous cost reduction in infrastructure and operating expenditure, but also enable flexibility, agility and ability to scale up or down as per the needs of a business and its affordability.

Banking Sector

Emerging cloud services for banks aim at enhancing productivity by facilitating real time collaboration, being omnipresent and providing virtualisation. Cloud-based services help in knowing the customers' preference by social networking interfaces and focussing on better customer relations, human relations and finance management, helping the banks

Contd...

to retain customers and attract new consumers. Front-end bank offices connected to cloud-based back-end computing and analytics save substantial cost on licensing, energy and space.

Cloud based e-invoicing provides dynamic invoices, making payments when exchange rates are most favourable, and enabling the banks to network constantly with postal and telecommunications companies. It improves access to social network profiles to help reach out to new consumers in new markets.

Security Concerns

The banking industry is not so enthusiastic to embrace cloud computing in spite of its vast potential, because of the industry's concern on security, privacy, confidentiality, data integrity, and authentication requirements, along with location of data, availability, and recoverability.

Moreover, the industry has unique and dynamic regulatory, legal and compliance issues to address before switching to cloud services. Bankers apprehend that computing in "the cloud" is risky, as it involves outsourcing the data of its customers to third-party cloud service operators.

In order to take advantage of the emerging powerful Internet-based business solutions, what is needed is an IT technology architecture that combines the merits of the public cloud with the security and data-privacy of the private cloud.

The appropriate business strategy seems to be to outsource relatively less sensitive data to the public cloud infrastructure service with cryptography and simple password access, along with dedicated servers with firewalls and intrusion detection devices and other updated safety features for housing ultra-secure critical data centres that demand strong authentication for access.

Strategic Policy

There should be a clear strategic policy for cloud computing and management, prioritising data that can be entrusted to the cloud operator, with clearly defined service level agreements (SLA) with milestones and a set time-frame, backed by a comprehensive governance structure.

While choosing the cloud service provider, it is important to look into the firm's financial stability, ability to improve functionality and service levels and integrate data across different technology platforms and cloud services.

The policy-based key management, with industry-standard encryption, is emerging as the cryptography model for better control on data in the cloud as the common encryption key management techniques are susceptible to vulnerability.

Cloud security services are emerging to address data security, privacy and compliance risks, as well as prevention of data theft, ensuring disaster management, and detecting compliance violations with robust server security for virtualised data centres.

Source: http://www.thehindubusinessline.com/features/mentor/article2484918.ece

14.4 Summary

- Privacy over the Internet has increased some ethical issues, which is required to be dealt with.
- Privacy can signify ambiguity in case a person would like to remain anonymous. Privacy can also be associated to the security aspect of an individual or information.

- Internet privacy is a urgent matter due to the growing number of peeping toms on the Internet.
- The term Web Services points to the technologies that permit for making connections. Services are what you attach together using Web Services
- Users of a Web service comprise persons (e.g., citizens and case officers), applications, and other Web services.
- A Web service usually has its own privacy policy that mentions a set of regulations applicable to *all* users.
- Data objects with comparable data privacy profiles form a privacy cluster.
- A major inspiration of data clustering is that legal rules and self-defined policies enforcing privacy are usually applicable to great segments of populations (e.g., residents of a state).
- Service-oriented architecture (SOA) is a method of designing software to offer services to applications, or to other services, via published and discoverable interfaces
- Much of the software industry concentrates so far has been on the underlying method for executing Web services and their communications.

14.5 Keywords

Data Privacy Profile: A data privacy profile specifies that the access views that it exposes to the dissimilar Web services.

Privacy: Privacy is a position wherein an entity can work on his/her information in isolation, resulting in a choosy revelation of one's uniqueness and information.

Service-oriented Architecture (SOA): It is a method of designing software to offer services to applications, or to other services, via published and discoverable interfaces.

Web Services: The term Web Services points to the technologies that permit for making connections.

14.6 Review Questions

1. Describe the significance of internet privacy.
2. How privacy of internet is violated?
3. How do websites affect in violating privacy?
4. Elucidate the issue of safeguarding internet privacy.
5. What are web services? Discuss its function in privacy.
6. Portray a privacy model with three different types.
7. Make distinction between user privacy and service privacy.
8. What is Service-oriented architecture (SOA)? How it is used in designing software?
9. How do you differentiate Architectural from Implementation Models?
10. Illustrate the security issues related with Service-oriented architecture (SOA).
11. What are the approaches used authorization? Discuss.

Notes

Answers: Self Assessment

1. Data privacy
2. computer
3. cookie
4. anti-spyware
5. web services
6. user privacy profile
7. usage
8. storage
9. data clustering
10. data
11. Service-oriented architecture (SOA)
12. Unified Modeling Language (UML)
13. solutions
14. audit
15. tamperproof
16. Non-repudiation

14.7 Further Readings

Books

An Introduction to Computer Security: The NIST Handbook

Managing Enterprise Information Integrity: Security, Control and Audit Issues, By IT Governance Institute

Principles of Information Security by Michael E. Whitman and Herbert Mattord;

Risk Management Guide for Information Technology Systems

Risks of Customer Relationship Management: A Security, Control, and Audit Approach by Pricewaterhousecoopers Llp

Security, Audit & Control Features PeopleSoft: A Technical and Risk Management Reference Guide; 2nd Edition, by Deloitte Touche Tohmatsu Research Team; ISACA

Online link

citeseerx.ist.psu.edu/

LOVELY PROFESSIONAL UNIVERSITY
Jalandhar-Delhi G.T. Road (NH-1)
Phagwara, Punjab (India)-144411
For Enquiry: +91-1824-300360
Fax.: +91-1824-506111
Email: odl@lpu.co.in