INFORMATION SECURITY

FOR ALL UG STUDENTS

SRI GVG VISALAKSHI COLLEGE FOR WOMEN

UDUMALPET

LEVEL I:

B.A Economics/ History/Literature/Economics with Logistics and Freight Management/ Tamil Literature/B.Sc Zoology/Commerce

LEVEL II:

B.Sc Mathematics/Physics/Chemistry/Computer Science/IT/Statistics BCA/BBA(CA)/B.Com(CA)/B.Com(e-Com)

Sri GVG Visalakshi College for Women (Autonomous), Udumalpet - 642128

Re-Accredited by A++ in NAAC

An ISO Certified Institution

In House Edition, First Impression 2015

Revised Edition 2017

Course framed by

- Mrs. S.Kalaisevi, Associate Professor, Department of Mathematics
- Mrs. R.Jayalakshmi, Head & Assistant Professor, Department of B.Com(E.Com)
- Ms. R.Kavithamani, Assistant Professor, Department of Physics
- Mrs. V.Vadivu, Assistant Professor, Department of IT
- Mrs. J.Aishwarya Lakshmi, Assistant Professor, Department of BCA

Revised & Redesigned by

- Mrs. S.Shobana, Head & Assistant Professor, Department of Computer Science
- Mrs. B.Sasikala, Assistant Professor, Department of Computer Science
- Ms. G.Krishnaveni, Assistant Professor, Department of Computer Science
- Mrs. D.Pavithra, Assistant Professor, Department of Computer Science
- Mrs.N.Sathyapriya, Assistant Professor, Department of Computer Science
- Ms.E.Kokilamani, Assistant Professor, Department of Computer Science
- Ms.P.Yasodha, Assistant Professor, Department of Computer Science
- Ms.S.Ponmalar, Assistant Professor, Department of Computer Science
- Mrs.S.Mahalakshmi, Assistant Professor, Department of Computer Science
- Mrs.J.Rajeswari, Assistant Professor, Department of Computer Science
- Ms.R.Subhasree, Assistant Professor, Department of Computer Science
- Mrs.S.Saranya, Assistant Professor, Department of Computer Science
- Mrs.G.Kowsalya, Assistant Professor, Department of Computer Science

Preface

The most information security problems we humans face are not matters of life and death. However, they are vexing, expensive and frequent enough to make information security a contemporary profession and the topic of information security a worthwhile subject to study.

This book is designed to serve as the textbook for a one-semester course devoted to information security. It is focused on helping students to acquire the skills sought in the professional workforce.

We start by introducing the professional environment of information security. After the student is convinced of the merits of the subject, the book introduces the basic model of information security consisting of assets, vulnerabilities, threats and controls. The rest of the course is devoted to characterizing assets, vulnerabilities and threats and responding to them using security controls. The book ends by integrating all these topics within the general umbrella of organizational risk management.

At the end of the course, students should have an awareness of how information security concerns have evolved in our society and how they can use contemporary frameworks to respond to these concerns in a professional environment.

B.A Economics/ History/Literature/Economics with Logistics and Freight Management/ Tamil Literature/B.Sc Zoology

Semester- IV

Part IV - Information Security 415GIS

Level - I

(For the students admitted from the academic year 2015-2016 onwards)

[30 Hours]

Unit I

Introduction- Meaning of Security- Need for Security- Challenges and applications- Security policies and standards.

Unit II

Threats –Types of threats-Attacks–Types of attacks-Applications: Bank Sectors, Mobile Applications, Share Investments, System Softwares.

Unit III

Introduction to Firewalls- Cryptography-Encryption-Decryption- Basics of Mobile information Security – Social Information Security.

Books for reference

1.”Network Security and Management”,Brijendra Singh,PHI Learning Limited,Second Edition.

2.”Firewalls and Network Security”,Whitman,Mattord,Austin,Holden,Cengage Learning India Private Learning

3.”Cryptography and Information security”,V.K.Pachghare, PHI Learning Limited.

B.Sc Mathematics/Physics/Chemistry/Computer Science/I.T/ Commerce/BCA/BBA(CA)/B.Com(CA)/B.Com(e-Com)

Semester - IV

Part IV-Information Security 415GIS

Level – II

(For the students admitted from the academic year 2015-2016 onwards)

[30 Hours]

Unit I

Information Security – Security Concerns - Security Requirements – Security Awareness - Security Challenges - Characteristics – Principles – Applications.

Security Mechanism – Encryption – Digital Signature – Digital Certificates – Public key Infrastructure – Proxy Servers. Information Security polices and Standards.

Unit II

Security Analysis: Security in TCP/IP Networks – LAN Security – Levels of Security – Threats - Types of Threats – Attacks. EDI Security – Hijacking EDI Messages in Transit – Security of EDI System while creating, processing and data retention.

Unit III

Security Issues – Authentication: Protecting Passwords, Viruses, Firewalls - Security for Smart cards – Safe payments – Electronic Banking – Electronic Fund Transfer.

Mobile Information Security – Bluetooth Security – WLAN Security. Social Networking – Measures for Secured Transactions.

Books for Reference

1. “Network Security and Management”,Brijendra Singh,PHI Learning Limited,Second Edition.
2. “Firewalls and Network Security”,Whitman,Mattord,Austin,Holden,Cengage Learning India Private Learning
3. “Cryptography and Information security”,V.K.Pachghare, PHI Learning Limited.

B.A Economics/ History/Literature/Economics with Logistics and Freight Management/ Tamil Literature/B.Sc Zoology/Commerce

Semester- IV

Part IV - Information Security 417GIS

Level - I

(For the students admitted from the academic year 2017-2018 onwards)

Course Objective: 30 Hrs

- To promote the core competency skills and augment citizenship values.
- To create awareness about different communication media and different security measures.
- To understand the concepts such as security policy, host based security, firewall, and packet filtering and intrusion detection.
- It helps to differentiate the threats of information systems from attacks.

Unit I:

Introduction-Meaning of Security- Need for Security- Challenges and applications- Security policies and standards.

Unit II:

Threats -Types of threats-Attacks-Types of attacks-Applications: Bank Sectors, Mobile Applications, Share Investments, and System Softwares.

Unit III:

Introduction to Firewalls- Cryptography-Encryption-Decryption- Basics of Mobile information Security - Social Information Security.

Books for Reference:

1. Brijendra Singh, “Network Security and Management”, PHI Learning Limited, Second Edition.
2. Whitman,Mattord,Austin,Holden ,“Firewalls and Network Security” ,Cengage Learning India Private Learning.
3. V.K.Pachghare, “Cryptography and Information security”, PHI Learning Limited.

B.Sc Mathematics/Physics/Chemistry/Computer Science/IT/Statistics
BCA/BBA(CA)/B.Com(CA)/B.Com(e-Com)
Semester - IV
Part IV-Information Security 417GIS
Level - II

(For the students admitted from the academic year 2017-2018 onwards)

Course Objective: **30 Hrs**

- To promote the core competency skills and augment citizenship values.
- To create awareness about different communication media and different security measures.
- To understand the concepts such as security policy, host based security, firewall, and packet filtering and intrusion detection.
- It helps to differentiate the threats of information systems from attacks.

Unit I:

Information Security - Security Concerns - Security Requirements - Security Awareness - Security Challenges - Characteristics - Principles - Applications.

Security Mechanism - Encryption - Digital Signature - Digital Certificates - Public key Infrastructure - Proxy Servers. Information Security polices and Standards.

Unit II:

Security Analysis: Security in TCP/IP Networks - LAN Security - Levels of Security - Threats - Types of Threats - Attacks.EDI Security - Hijacking EDI Messages in Transit - Security of EDI System while creating, processing and data retention.

Unit III:

Security Issues - Authentication: Protecting Passwords, Viruses, Firewalls - Security for Smart cards - Safe payments - Electronic Banking - Electronic Fund Transfer.

Mobile Information Security - Bluetooth Security - WLAN Security. Social Networking - Measures for Secured Transactions.

Books for Reference:

1. Brijendra Singh, “Network Security and Management”, PHI Learning Limited, Second Edition.
2. Whitman,Mattord,Austin,Holden, “Firewalls and Network Security”, engage Learning India Private Learning
3. V.K.Pachghare, “Cryptography and Information security”, PHI Learning Limited.

LEVEL I

Introduction

Security

Security is defined as the quality or state of being of secure-to be free from danger.

A successful organisation should have multiple layers of security in place:

- **Physical security-**to protect people, physical assets, and the workplace from various threats.
- **Personal security-**to protect individuals who are authorized to access the organisation.
- **Operational security-**focuses on the protection of the details of particular operations.
- **Communications security-**encompasses the protection of organization's communications media, technology and content.
- **Network security-**protection of networking components, connections, and contents.
- **Information security-**protection of information assets.

Uses of security

- Governments, military, financial institutions, hospitals, and private businesses.
- Protecting confidential information is a business requirement.

CIA Triangle

- It is the industry standard for computer security based on three characteristics of information (confidentially, integrity, and availability).
- This model no longer adequately constant changing environment of computer industry.

The expanded C.I.A triangle addresses the complexities of the current information security environment because it consists of list of critical characteristics of information, which are described in the next.

Need for Security

IT Security Requirements describe functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of an IT system.

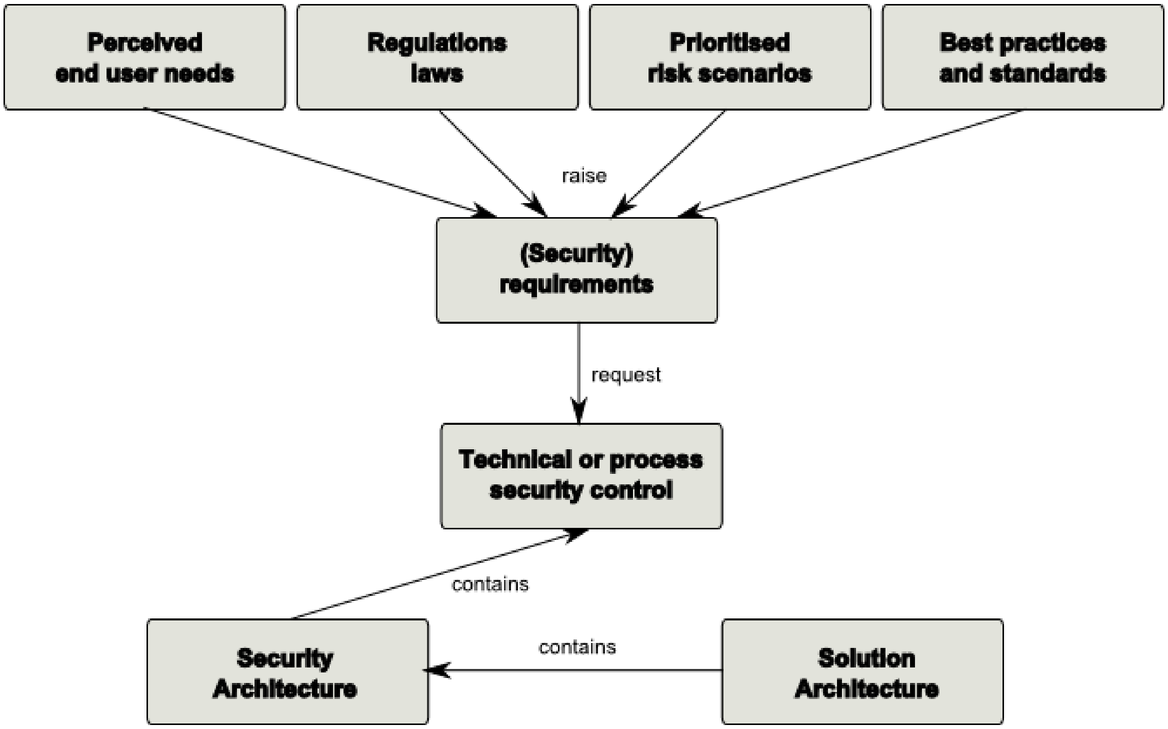
Types

Security requirements can be formulated on different abstraction levels. At the highest abstraction level they basically just reflect security objectives. An example of a security objectives could be "The system must maintain the confidentially of all data that is classified as confidential".

More useful for a SW architect or a system designer are however security requirements that describe more concretely what must be done to assure the security of a system and its data. OSA suggests to distinguish 4 different security requirement types:

- **Secure Functional Requirements**, this is a security related description that is integrated into each functional requirement. Typically this also says what shall not happen. This requirement artifact can for example be derived from misuse cases
- **Functional Security Requirements**, these are security services that needs to be achieved by the system under inspection. Examples could be authentication, authorization, backup, server-clustering, etc. This requirement artifact can be derived from best practices, policies, and regulations.
- **Non-Functional Security Requirements**, these are security related architectural requirements, like "robusteness" or "minimal performance and scalability". This requirement type is typically derived from architectural principals and good practice standards.
- **Secure Development Requirements**, these requirements describe required activities during system development which assure that the outcome is not subject to

vulnerabilities. Examples could be "data classification", "coding guidelines" or "test methodology". These requirements are derived from corresponding best practice frameworks like "CLASP".



Security Challenges

The challenges of information security can be divided into the following areas:

- **Confidentiality and Privacy** - Ensuring that only the intended recipients can read certain information
- **Authentication** - Ensuring that information is actually sent by the stated sender
- **Integrity** - Ensuring that the original information was not altered and that no one tampered with it
- **Availability** - Ensuring that important information can be accessed at all times and places

Security Characteristics

The value of information comes from the characteristics it possesses. When a characteristics of inform are given below.

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

Availability

It enables authorized users (persons or computer system) to access information without interference and receives it in the required format.

Availability does not imply that the information is accessible to any user; rather it means availability to authorized users.

Accuracy

Accuracy of information refers to information which is free from mistakes or errors and has the value the end user expects. (EG: Inaccuracy of your bank account may result in mistakes such as bouncing of a check).

If the information has been intentionally or unintentionally modified, it is no longer accurate.

Authenticity

It refers to quality or state of being genuine or original, rather than reproduction or fabrication. Information is authentic when the contents are original as it was created placed or stored or transmitted.

Attacks to authenticity:

- **E-Mail spoofing:** Sending E-Mail with modified address field.
- **Phishing :** Obtain personal or financial information in a fraudulent manner.

Confidentiality

Information has confidentiality when exposure to unauthorized individuals or systems in prevented. Confidentiality ensures that only those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can vie information confidentiality is breached.

To product the confidentiality of information, the numbers of measures are used:

- ✓ Information classification.
- ✓ Secured documents storage.
- ✓ Application of general security policies.
- ✓ Education of information custodians and end use.

Example:

When confidential information is mistakenly e-mailed to some –one outside the organisation rather to someone inside the organisation.

Attacks to confidentiality:

1. By mistake sending E-mail to unauthorize outside person.
2. Salami theft-employee steals a few pieces of information at a time but in the long run that employee gets the whole thing.

Integrity

Integrity means that data cannot be modified without authorization. Information has Integrity when it is whole, complete, and uncorrupted. The Integrity of information is threatened when it is exposed to corruption, damage, destruction and other disruption of its authentic state.

Utility

The utility of information is the quality or state of having value for some purpose or end. This means that if information is available, but not in a meaningful format to the end user, it is not useful. Thus the value of information depends on its utility.

Possession

The possession of information security is the quality or state of having ownership or control of some object or item. Information is said to be in one's possession if one obtains it independent of format or other characteristic.

EG: Illegal possession of encrypted data never allows someone to read it without proper decryption methods.

Introduction on information security policies and standards

In order to most effectively secure its network environment, an organization must establish a functional and well-designed information security program. Firewalls, network security, and intrusion detections systems can only succeed within the context of a well- planned and fully defined information security program. Uncoordinated security initiative seldom as effective as those that the operate under a complete and effective policy environment. The creation of an information security program begins with the creation or review of the organization‘s information security polices, standards, and practices, followed by the selection or creation of information security architecture and a detailed information security blue print. Without policy, blue prints and planning, the organization will not be able to meet the information security needs of the various communities of interest. The role of planning in the modern organization is hard to overemphasize. All but the smallest organizations undertake at least some planning: strategic planning to manage the allocation of resources, and contingency planning to prepare for the uncertainties of the business environment.

Information security policies and standards

Management must make polices the basis for all information security planning, design and deployment. Polices direct how issues are addressed and how technologies are used. Polices do not specify the proper operation of equipment or software-this information should be placed in the standards, procedures, and practices of users manuals and systems documentation. In addition, policy should never contradict law, because this can create a significant liability for the organization.

Because information security is primarily a management problem,, not a technical one, quality security programs begin and end with policy. Policy obliges personnel to function in a manner that adds to the security of information assets, rather than threatening them. Securities polices are the least expensive control to design and disseminate –they require only the time and effort of the management team-but the most difficult to implement too properly. Even if the management team hires an outside consultant to assist in the development of policy, the costs are minimal compared to those of technical controls. However, shaping policy is difficult because policy must:

- Never conflict with laws
- Stand up in court, if challenged
- Be properly administered through dissemination and documented acceptance

For a policy to be considered effective and legally enforceable, it must meet the following criteria:

- **Dissemination (distribution):** The organization must be able to demonstrate that the relevant policy has been made really available for review by the employee. Common dissemination techniques include hard- copy and electronic distribution.
- **Review (reading):** The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non English reading, and reading –impaired employees.
- **Comprehension (understanding):** The organization must be able to demonstrate that employees understood the requirements and content of the policy. Common techniques include quizzes and other assessments.
- **Compliance (agreement):** The organization must be able to demonstrate that employees agree to employ with the policy, through act or affirmation. Common techniques are include logon banners that require a specific action (mouse click or keystroke) to acknowledge agreement, or requiring employees to sign a document

clearly indicating that they have read, understood, and agreed to comply with the policy.

- **Uniform enforcement:** The organization must be able to demonstrate that the policy has been uniformly enforced.

A policy is a set of guidelines or instructions that an organization's senior management implements to regulate the activities of the members of the organization who make decisions, take actions, and perform other duties. Policies are organizational law in that dictate acceptable and unacceptable behavior within the organization. Like laws, policies define what is right and what is wrong, what the penalties are for violating policy, and what the appeal process is. Standards, though they have the same compliance requirements as policies, are more detailed description of what must be done to comply with policy. The standards may be informal or other part of an organizational culture, as in de facto standards. Or standards may be published, scrutinized, and ratified a group, as formal or de jure standards. Practices, procedures, and guidelines effectively explain how to comply with policy. Fig 1 shows policies as the force that drives standards, which in turn drive practices, procedures, and guidelines.

Policies are put in place to support the organization's mission, vision, and strategic planning. The mission of an organization is a written statement of an organization's purpose. The vision of an organization is a written statement of an organization's long term goals-where will the organization be in five years? In Ten? Strategic planning is the process of moving the organization towards its vision.

The meaning of the term security policy depends on the context in which it is used. Governmental agencies discuss security policy in terms of national security and national policies to deal with foreign states. The security policy can also be a credit card agency's method of processing credit card numbers. In general, a security policy is a set of rules that protect an organization's assets. An information security policy provides rules for the protection of the information assets of the organization.

Management must define three types of security policies, according to The National Institute of standards and technology's special publication 800-14:

- Enterprise information security policies
- Issue-specific security policies
- System- specific security policies

Each of these management security policies is examined in greater detail in the sections that follow:

Enterprise Information Security Policy (EISP)

An enterprise information security policy is also known as a general security policy. IT security policy or information security policy. The EISP is based on and directly supports the mission, vision and direction of the organization and sets the strategic direction, scope, and tone for all security efforts .The EISP is an executed level document, usually drafted by, or in cooperation with, the chief information officer of the organization. The EISP usually need to be modified only where there is a change in the strategic direction of the organization.

The EISP guides the development, implementation, and management of the security program. It specifies the requirements to be met by the information security blue print or frame work. It defines the purpose, scope, constraints, and applicability of the security program in the organization.

It also assigns responsibilities for the various area security, including systems administration, maintenance of the information security policies, and the practices and responsibilities of the users. According to the National Institute of standards and technology's the EISP typically addresses compliance in two areas:

- General compliance to ensure meeting the requirements to establish the program and the responsibilities assigned therein to various organizational components and
- The use of specified penalties and disciplinary action.

When the EISP has been developed, the CISO (chief information security officer) begins forming the security team and initiating the necessary changes to the information security program.

EISP Elements:

Although the specifies of EISP‘s vary from organization to organization, most EISP documents should include the following elements:

- An overview of the corporate philosophy on security
- Information on the structure of the information security organization and individuals who fulfill the information security role
- Fully articulated security responsibilities that are shared by the all members of the organization (employees, contractors, consultants, partners and visitors)
- Fully articulated security responsibilities that are unique to each role within the organization.

Issue-Specific Security Policy (ISSP)

As an organization executes various technologies and processes to support routine operations. it must instruct employees on the proper use of those technologies and processes. In general, the issue specific security policy, or ISSP, (1) addresses specific areas of technology as listed below, (2) requires frequents updates,(3) contains the statement on the organization's position on a specific issue. An ISSP can cover the following topics, and others:

- Use of company owned networks and internet
- Use of telecommunications technologies (fax and phone)
- Use of electronic mail
- Specific minimum configurations of computers to defend against worms and viruses
- Prohibition against hacking or testing organization security controls
- Home use of company –owned computer equipments
- Use of personal equipment on company networks
- Use of photo copy equipment

There are a number of approaches to creating and managing ISSPs within an organization
Three of the most common are to create the following types of ISSP documents:

- Independent ISSP documents, each tailored to a specific issue
- A single comprehensive ISSP documents covering all issues
- A modular ISSP document that unifies policy creation and administration, while maintaining each specific issue's requirements.

The independent document typically has a scattershot effect. Each department responsible for a particular application of technology creates a policy governing its use, management, and control. This approach may fail to cover all of the necessary issues, and can need to poor policy distribution, and management, and enforcement.

The single comprehensive ISSP is centrally managed and controlled. With formal procedures for the management of ISSP's in place, the comprehensive policy approach establishes guidelines for issue coverage and clearly identifies processes for the dissemination, enforcement, and review of this guideline. Usually, comprehensive ISSP's are developed by those responsible for managing the information technology resources. Unfortunately, they tend to overly generalize the issues and skip over vulnerabilities.

The optimal balance between the independent and comprehensive ISSP is the modular ISSP. It is also centrally managed and controlled but tailored to the individual technologies issues. The modular approach provides a balance between issue orientation and policy management. The policies created via this approach comprise individual modulus; each created and updated by individual responsible for the issues addressed this individual report to a central policy administration group that incorporates specific issues into an overall comprehensive policy. Even though the details may vary from policy to policy and some sections of a modular policy may be combined, it is essential for management address and completes each section.

Statement of policy:

The policy should begin with a clear statement of purpose. Consider a policy that covers the issue of fair and responsible use of internet. The introductory section of the policy should outline of these topics: what is the scope of the policy? Who is responsible and accountable for policy implementation? What technologies and issues does it address?

Authorized access and usage:

This section of the policy statement addresses who can use the technology governed by the policy, and what it can be used for. Remember that an organization's information systems are the exclusive property of the organization, and users have no general rights of use. Each technology and process is provided for business operations. Use for any other purpose constitutes misuse. This section defines "fair and responsible use" of the covered technology and other organizational assets, and should also address key legal issues, such as protection of personal information and privacy.

Prohibited use:

Unless a particular use of technology is clearly prohibited, the organization cannot penalize its employees for using it in that fashion. The following can be prohibited: personal use, disruptive use or misuse, criminal use, offensive or harassing materials and infringement of copyrighted, licensed, or other intellectual property.

Systems management:

The systems management section of the ISSP policy statement focuses on user's relationship to system management. Specific management rules include regulating the use of e-mail, the storage of materials, authorized monitoring of employees, and the physical and electronic security of e-mail and other electronic components. It is important that all such all responsibilities be designated ti either the systems administrators or the users; otherwise, both parties may infer that the responsibilities belongs to the other party.

Violations of policy:

Once guidelines on use have been outlined and responsibilities have been assigned, the policy must specify the penalties for, and repercussions of, policy violation. Violations should incur appropriate, not draconian, penalties. This section of the policy statement should specify the penalties for each category of violation as well as instructions on how individuals in the organization can report observed or suspected violations. Many people think that powerful individuals in the organization can discriminate, single out, or otherwise retaliate against someone who reports violations. Allowing anonymous submissions is often the only way to convince users to report the unauthorized activities of other, more influential employees.

Policy review and modification:

Because a document is only useful if it is up to date, each policy should contain procedures and a timetable for periodic review. As the organization's needs and technologies change, so must the policies that govern their use. This section should specify a methodology for the review and modification of the policy, to ensure that users do not begin circumventing it as it grows obsolete.

Limitations of Liability:

If an employee is caught conducting illegal activities with organizational equipments, or assets management does not want the organization held liable. The policy should state that the organization will not protect employees who violate a company policy or any law using company technologies, and that the company is not liable for such actions. It is understood that such violations are without the organization's knowledge or authorization.

System - Specific Policy (SysSP):

While issue –specific policies are written documents readily identifiable as policy, system- specific security policies (SysSP) sometimes have a different look. SysSPs often function as standards or procedures to be used when configuring or maintaining systems. For example, a SysSP might describe the configuration and operation of a network firewall. This document could include a statement of managerial intent; guidance to network engineers on the selection, configuration, and operation of firewalls; and an access control list that defines levels of access for each authorized user. SysSP can be separated into two general groups, managerial guidance and technical specifications, or they can be combined into a single policy document.

Threats

In computer security a threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm. A threat can be either "intentional" i.e. hacking: an individual cracker or a criminal organization or "accidental" for e.g. the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado or otherwise a circumstance, capability, action, or event.

Types of Threats

Worms

This malicious program category largely exploits operating system vulnerabilities to spread itself. The class was named for the way the worms crawl from computer to computer, using networks and e-mail. This feature gives many worms a rather high speed in spreading themselves.

Trojans

Programs that carry out unauthorized actions on computers, such as deleting information on drives, making the system hang, stealing confidential information, etc. This class of malicious program is not a virus in the traditional sense of the word. Trojans cannot break into computers on their own and are spread by hackers, who disguise them as regular software. The damage that they incur can exceed that done by traditional virus attacks by several fold.

Sniffer

Sniffer is the programs that secretly search individual packets of data as they pass through the internet, capturing the passwords and contents. It is also called as spoofer. It is a standalone program to intercept and analyze certain data. For example a sniffer can intercept and analyze network traffic and catch certain data, for example passwords. Trojans sometimes use sniffing capabilities to steal passwords and user information from infected computers. There also exist a lot of commercial and free sniffers. They can be used to analyze network traffic for performance, security issues and faults.

Sniffer is a Network analyzing tool. Network analyzing tools are used to monitor the traffic conversations that occur across the network. Often the information obtained from a sniffer can be used to figure out exactly how devices are communicating. But the use of a sniffer is not limited to troubleshooting, it can also be used to help train, design and operate devices on a network.

Spoofing

Spoofing is the process of faking the websites or mails to trick users into passing along critical information like credit card numbers or passwords.

A spoofing attack is user on a network; in order to launch attacks against network hosts, steal data, spread malware etc. Many of the protocols do not provide mechanisms for authenticating the source or destination of a message. They are thus vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. Spoofing attacks which take advantage of protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message.

Malicious Applets

A malicious applet is any applet that attacks the local system of a Web surfer. Malicious applets are written by researchers, crackers, and Net miscreants to annoy and damage Java users. They can even seriously damage a Java user's machine. These are tiny programs, written in the popular java computer language, that misuse your computer resources, modify files on the hard disk, send fake mails or steal passwords. Any applet that performs an action against the will of the user who invoked it should be considered malicious.

Logic bomb

A logic bomb is a piece of programming code buried within another programme, designed to perform some malicious act. It is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting important files of a company or organization, which will lead problems to the organization.

Software that is inherently malicious, such as logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. This technique can be used by a virus or worm to gain momentum and spread before being noticed. Some viruses attack their host systems on specific dates, such as Wednesday the 12th or Independence Day. Viruses that activate on certain dates are often called "Time bombs".

Buffer Overflow

It is a technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer’s memory. This is the type of DoS attack. Data sent to the server at the rate and volume that exceeds the capacity of the system, it will cause errors and damage the system.

Password Crackers

It is the software that can guess passwords. Password attacks can be implemented using several different methods like brute force attacks, Trojan horse programmers. IP spoofing can yield user accounts and passwords. Password attacks usually refer to repeated attempts to identify a user password or account.

Virus

A virus is a form of malicious code and as such is potentially disruptive. It may also be transferred unknowingly from one computer to another. Virus based attack manipulates the legitimate user to by authentication and access control mechanisms in order to execute the malicious code injected by the attacker. Virus attacks are often untargeted and spread among vulnerable systems and users. Virus attacks directly or indirectly decrease the availability of infected systems by consuming excessive amount of processing power or network bandwidth.

Attacks

In computer and computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.

Types of attack:

Classes of attack might include passive monitoring of communications, active network attacks, close-in attacks, exploitation by insiders, and attacks through the service provider. Information systems and networks offer attractive targets and should be resistant to attack from the full range of threat agents, from hackers to nation-states. A system must be able to limit damage and recover rapidly when attacks occur. There are five types of attack:

Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. Passive attacks include traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

Active Attack

In an active attack, the attacker tries to bypass or break into secured systems. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks result in the disclosure or dissemination of data files, DoS, or modification of data.

Distributed Attack

A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a “trusted” component or software that will later be distributed to many other companies and users Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

Insider Attack

An insider attack involves someone from the inside, such as a disgruntled employee, attacking the network Insider attacks can be malicious or no malicious. Malicious insiders intentionally eavesdrop, steal, or damage information; use information in a fraudulent manner; or deny access to other authorized users. No malicious attacks typically result from carelessness, lack of knowledge, or intentional circumvention of security for such reasons as performing a task

Applications

Bank Sectors

With the wide-expansion of mobile telecommunication technology into the business world, mobile banking became the popular and promising banking method in bank industry recently. Mobile banking can provide customers with better quality and more cost-saving services. It refers to provision and availment of banking and financial services with the help of mobile telecommunication devices. The scope of provided services may include facilities to conduct bank and investment market transactions, to administer accounts and to access customized information. Most of the mobile banking researchers agreed that mobile banking consists of three parts: mobile accounting, mobile brokerage and mobile financial information services. For customer service sector including: balance checking, account transactions, payment, etc. conventional banking services. Increasingly, bank customers will expect real-time information and access 24 hours a day, seven days a week, wherever they are in the world. Services such as electronic account management, mobile brokerage and financial information and alerts enable banks and network operators to increase bank's competitive edge and strengthen customer loyalty. A mobile banking system comprises a mobile banking unit and a data processing centre which may be the mainframe computer of the bank responsible for processing banking transactions and data storage. The mobile banking includes one or more banking terminals such as ATMs, deposit machines and multimedia enquiry stations. Mobile banking system has provided a good foundation for providing personalized, customer- oriented, new model of financial services, which incorporates a number of wireless communication channels, integrate the merits of different technologies

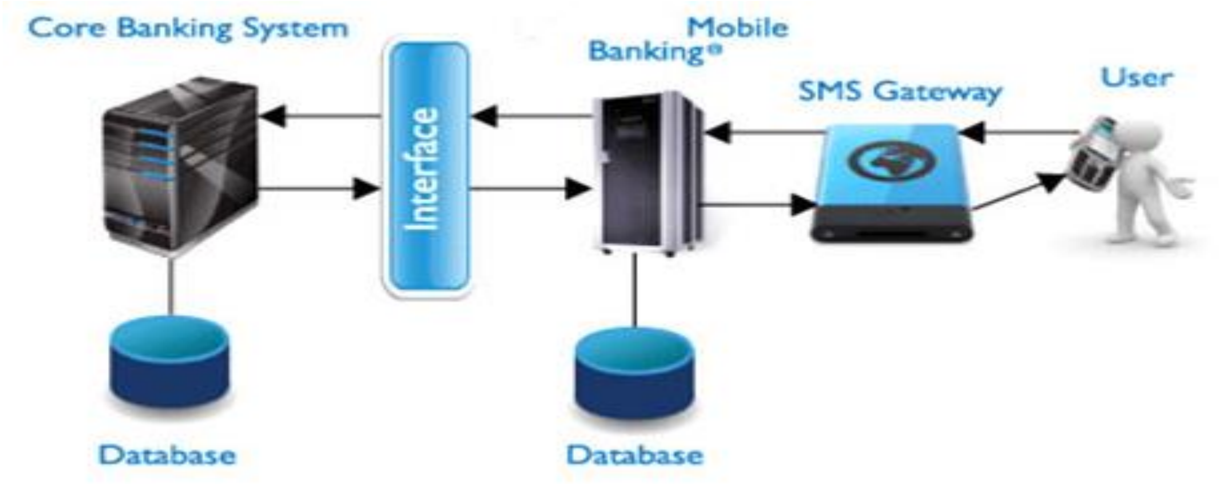


Fig 2.1 Applications

Mobile Applications

Common Issues

1. Mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices. Many devices have the technical capability to support passwords, personal identification numbers (PIN), or pattern screen locks for authentication. Some mobile devices also include a biometric reader to scan a fingerprint for authentication. However, anecdotal information indicates that consumers seldom employ these mechanisms. Additionally, if users do use a password or PIN they often choose passwords or PINs that can be easily determined or bypassed, such as 1234 or 0000. Without passwords or PINs to lock the device, there is increased risk that stolen or lost phones' information could be accessed by unauthorized users who could view sensitive information and misuse mobile devices.

2. Two-factor authentication is not always used when conducting sensitive transactions on mobile devices. According to studies, consumers generally use static passwords instead of two-factor authentication when conducting online sensitive transactions while using mobile devices. Using static passwords for authentication has security drawbacks: passwords can be guessed, forgotten, written down and stolen, or eavesdropped. Two-factor authentication generally provides a higher level of security than traditional passwords and PINs, and this higher level may be important for sensitive transactions. Two-factor refers to an authentication system in which users are required to authenticate using at least two different "factors" something you know, something you have, or something you are before being granted access. Mobile devices can be used as a second factor in some two-factor authentication schemes. The mobile device can generate pass codes, or the codes can be sent via a text message to the phone. Without two-factor

authentication, increased risk exists that unauthorized users could gain access to sensitive information and misuse mobile devices.

3. Wireless transmissions are not always encrypted. Information such as e-mails sent by a mobile device is usually not encrypted while in transit. In addition, manyapplicationsdo not encrypt the data they transmit and receive over the network, making it easy for the data to be intercepted. For example, if an application is transmitting data over an unencrypted WiFi network using http (rather than secure http), the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted.

4. Mobile devices may contain malware. Consumers may download applications that contain malware. Consumers download malware unknowingly because it can be disguised as a game, security patch, utility, or other useful application. It is difficult for users to tell the difference between a legitimate application and one containing malware. For example, an application could be repackaged with malware and a consumer could inadvertently download it onto a mobile device. the data can be easily intercepted. When a wireless transmission is not encrypted, data can be easily intercepted by eavesdroppers, who may gain unauthorized access to sensitive information.

5. Mobile devices often do not use security software. Many mobile devices do not come preinstalled with security software to protect against malicious applications, spyware, and malware-based attacks. Further, users do not always install security software, in part because mobile devices often do not come preloaded with such software. While such software may slow operations and affect battery life on some mobile devices, without it, the risk may be increased that an attacker could successfully distribute malware such as viruses, Trojans, spyware, and spam to lure users into revealing passwords or other confidential information.

6. Operating systems may be out-of-date. Security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner. It can take weeks to months before security updates are provided to consumers' devices. Depending on the nature of the vulnerability, the patching process may be complex and involve many parties. For example, Google develops updates to fix security vulnerabilities in the Android OS, but it is up to device manufacturers to produce a device-specific update incorporating the vulnerability fix, which can take time if there are proprietary modifications to the device's software. Once a manufacturer produces an update, it is up to each carrier to test it and transmit the updates to consumers' devices. However, carriers can be delayed in providing the updates because they need time to test whether they interfere with other aspects of the device or the software installed on it.

In addition, mobile devices that are older than two years may not receive security updates because manufacturers may no longer support these devices. Many manufacturers stop supporting smart phones as soon as 12 to 18 months after their release. Such devices may face increased risk if manufacturers do not develop patches for newly discovered vulnerabilities.

7. Software on mobile devices may be out-of-date. Security patches for third-party applications are not always developed and released in a timely manner. In addition, mobile third-party applications, including web browsers, do not always notify consumers when updates are available. Unlike traditional web browsers, mobile browsers rarely get updates. Using outdated software increases the risk that an attacker may exploit vulnerabilities associated with these devices.

8. Mobile devices often do not limit Internet connections. Many mobile devices do not have firewalls to limit connections. When the device is connected to a wide area network it uses communications ports to connect with other devices and the Internet. A hacker could access the mobile device through a port that is not secured. A firewall secures these ports and allows the user to choose what connections he wants to allow into the mobile device. Without a firewall, the mobile device may be open to intrusion through an unsecured communications port, and an intruder may be able to obtain sensitive information on the device and misuse it.

9. Mobile devices may have unauthorized modifications. The process of modifying a mobile device to remove its limitations so consumers can add features changes how security for the device is managed and could increase security risks. Jailbreaking allows users to gain access to the operating system of a device so as to permit the installation of unauthorized software functions and applications and/or to not be tied to a particular wireless carrier. While some users may jailbreak or root their mobile devices specifically to install security enhancements such as firewalls, others may simply be looking for a less expensive or easier way to install desirable applications. In the latter case, users face increased security risks, because they are bypassing the application vetting process established by the manufacturer and thus have less protection against inadvertently installing malware. Further, jailbroken devices may not receive notifications of security updates from the manufacturer and may require extra effort from the user to maintain up-to-date software.
10. The GAO report went on to state that connecting to an unsecured WiFi network could let an attacker access personal information from a device, putting users at risk for data and identity theft. One type of attack that exploits the WiFi network is known as man-in-the-middle, where an attacker inserts himself in the middle of the communication stream and steals information.9. Communication channels may be poorly secured. Having communication channels, such as Bluetooth communications, "open" or in "discovery" mode (which allows the device to be seen by other Bluetooth-enabled devices so that connections can be made) could allow an attacker to install malware through that connection, or surreptitiously activate a microphone or camera to eavesdrop on the user. In addition, using unsecured public wireless Internet networks or WiFi spots could allow an attacker to connect to the device and view sensitive information.

Share Investments

Securities market is a component of the wider financial market where securities can be bought and sold between subjects of the economy, on the basis of demand and supply. Securities markets encompasses equity markets, bond markets and derivatives where prices can be determined and participants both professional and non professionals can meet.

Securities markets can be split into two levels. Primary markets, where new securities are issued and secondary markets where existing securities can be bought and sold. Secondary markets can further be split into organized exchanges, such stock and over-the-counter where individual parties come together and buy or sell securities directly. For securities a holder knowing that a secondary market exists in which their securities may be sold and converted into cash increases the willingness of people to hold stocks and bonds and thus increases the ability of firms to issue securities.

There are a number of professional participants of a securities market and these include; brokerages, dealers, market, investment managers, speculators as well as those providing the infrastructure, such as houses and securities depositories.

A securities market is used in an economy to attract new capital, transfer real assets in financial assets, determine price which will balance demand and supply and provide a means to invest money both short and long term.

Levels of Securities Market

Primary market

The primary market is that part of the capital markets that deals with the issue of new securities. Companies, governments or public sector institutions can obtain funding through the sale of a new stock or bond issue. This is typically done through a syndicate of securities dealers. The process of selling new issues to investors is called underwriting. In the case of a new stock issue, this sale is a public offering. Dealers earn a commission that is built into the price of the security offering, though it can be found in the prospectus. Primary markets create long term instruments through which corporate entities borrow from capital market.

Features of primary markets are:

- This is the market for new long term equity capital. The primary market is the market where the securities are sold for the first time. Therefore, it is also called the new issue market (NIM).
- In a primary issue, the securities are issued by the company directly to investors.
- The company receives the money and issues new security certificates to the investors.
- Primary issues are used by companies for the purpose of setting up new business or for expanding or modernizing the existing business.
- The primary market performs the crucial function of facilitating capital formation in the economy.
- The new issue market does not include certain other sources of new long term external finance, such as loans from financial institutions. Borrowers in the new issue market may be raising capital for converting private capital into public capital; this is known as "going public."

Secondary market

The secondary market, also known as the aftermarket, is the financial market where previously issued securities and financial instruments such as stock, bonds, options, and futures are bought and sold. The term "secondary market" is also used to refer to the market for any used goods or assets, or an alternative use for an existing product or asset where the customer base is the second market for example, corn has been traditionally used primarily for food production and feedstock, but a "second" or "third" market has developed for use in ethanol production. Stock exchange and over the counter markets.

With primary issuances of securities or financial instruments, or the primary market, investors purchase these securities directly from issuers such as corporations issuing shares in an IPO or private placement, or directly from the federal government in the case of treasuries. After the initial issuance, investors can purchase from other investors in the secondary market.

The secondary market for a variety of assets can vary from loans to stocks, from fragmented to centralized, and from illiquid to very liquid. The major stock exchanges are the most visible example of liquid secondary markets - in this case, for stocks of publicly traded companies. Exchanges such as the New York Stock Exchange, Nasdaq and the American Stock Exchange provide a centralized, liquid secondary market for the investors who own stocks that trade on those exchanges. Most bonds and structured products trade “over the counter,” or by phoning the bond desk of one’s broker-dealer. Loans sometimes trade online using a Loan Exchange.

System Software

System software is computer software designed to provide services to other software. Examples of system software include operating systems, computational science software, game engines, industrial automation, and software applications. In contrast to system software, software that allows users to do things like create text documents, play games, listen to music, or web browsers to surf the web are called application software.

System software is a type of computer program that is designed to run a computer’s hardware and application programs. The computer system is a layered model; the system software is the interface between the hardware and user applications.

The line where the distinction should be drawn isn't always clear. All operating systems bundle application software. Such software is not considered system software when it can be uninstalled without affecting the functioning of other software. Exceptions could be e.g. web browsers such as Internet Explorer where Microsoft argued in court that it was system software that could not be uninstalled. Later examples are Chrome OS and Firefox OS where the browser functions as the only user interface and the only way to run programs and other web browser cannot be installed in their place, and then they can well be argued to be part of the operating system and then system software.

Another borderline example is cloud based software. This software provides services to a software client usually a web browser or a JavaScript application running in the web browser, not to the user directly, and is therefore systems software. It is also developed using system programming methodologies and systems programming languages. Yet from the perspective of functionality there is little difference between a word processing application and word processing web application.

Operating System

The operating system prominent examples being Microsoft Windows, Mac OS X and Linux, allows the parts of a computer to work together by performing tasks like transferring data between memory and disks or rendering output onto a display device. It provides a platform (hardware abstraction layer) to run high-level system software and application software.

A kernel is the core part of the operating system that defines an API for applications programs (including some system software) and an interface to device drivers.

Device drivers, including also computer BIOS and device firmware, provide basic functionality to operate and control the hardware connected to or built into the computer.

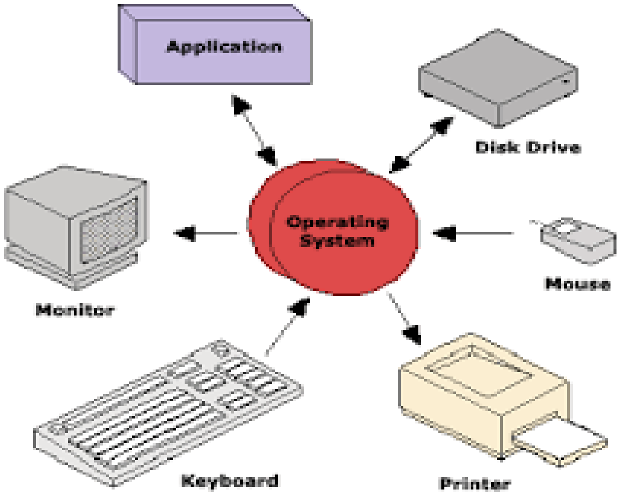


Fig 2.2 System Software

A user interface "allows users to interact with a computer." Either a command-line interface (CLI) or, since the 1980s a graphical user interface (GUI). Since this is the part of the operating system the user directly interacts with, it may be considered an application and therefore not a system software.

Utility Software

Some organizations use the term systems programmer to describe a job function which would be more accurately termed systems administrator. Software tools these employees use are then called system software. This so-called Utility software helps to analyze, configure, optimize and maintain the computer, such as virus protection. In some publications, the term system software also includes software development tools like a compiler, linker or debugger.

Other examples of system software

- The BIOS (basic input/output system) gets the computer system started after you turn it on and manages the data flow between the operating system and attached devices such as the hard disk, video adapter, keyboard, mouse, and printer.
- The boot program loads the operating system into the computer's main memory or random access memory (RAM).
- An assembler takes basic computer instructions and converts them into a pattern of bits that the computer's can use to perform its basic operations.
- A device driver controls a particular type of device that is attached to your computer, such as a keyboard or a mouse. The driver program converts the more general input/output instructions of the operating system to messages that the device type can understand.
- According to some definitions, system software also includes system utilities, such as the disk defragmenter and System Restore, and development tools such as compilers and debuggers.

Firewalls

A firewall is a system designed to prevent unauthorized access to or from a private network. 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.

Need of Firewalls

Without a firewall, user computer is operating with an "open door" policy. Bank account information, passwords, credit card numbers, virtually any sensitive information on their computer becomes available to hackers. Hackers can get in, take what they want, and even leave one of their own "back doors" in place for ongoing access to computer whenever they like.

Firewalls have a wide range of capabilities. Types of firewalls include:

- Packet filtering firewalls
- Stateful inspection firewalls
- Proxy firewalls
- Guards
- Personal firewalls

Packet filter

Packet filtering is “controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination. Packet filtering is one technique, among many, for implementing security firewalls. ”i Packet filtering is both a tool and a technique that is a basic building block of network security. It is a tool in that it is an instrument that aids in accomplishing a task. It is a technique because it is a method of accomplishing a task.

In the context of a TCP/IP network, a packet filter watches each individual IP datagram, decodes the header information of in-bound and out-bound traffic and then either blocks the datagram from passing or allows the datagram to pass based upon the contents of the source address, destination address, source port, destination port and/or connection status. This is based upon certain criteria defined to the packet filtering tool. The leading IP routers, including Cisco, Bay, and Lucent, can be configured to filter IP datagrams. Many operating systems can be configured for packet filtering. Packet filtering can be added to *nix operating systems. Support for packet filtering via ipchains is included by default in the Linux kernel. Windows NT and

Windows 2000 support packet filtering. Virtually all commercial firewalls support packet filtering. Some commercial firewalls also have the capability of filtering packets based upon the state of previous packets (stateful inspection).

Purpose of Packet Filter

Packet filtering generally is inexpensive to implement. However it must be understood that a packet filtering device does not provide the same level of security as an application or proxy firewall. All except the most trivial of IP networks is composed of IP subnets and contain routers. Each router is a potential filtering point. Because the cost of the router has already been absorbed, additional cost for packet filtering is not required. Packet filtering is appropriate where there are modest security requirements. The internal (private) networks of many organizations are not highly segmented. Highly sophisticated firewalls are not necessary for isolating one part of the organization from another. However it is prudent to provide some sort of protection of the production network from a lab or experimental network. A packet filtering device is a very appropriate measure for providing isolation of one subnet from another.

Functionality

All packet filters function in the same general fashion. Operating at the network layer and transport layer of the TCP/IP protocol stack, every packet is examined as it enters the protocol stack. The network and transport headers are examined closely for the following information:

- **protocol (IP header, network layer)** – In the IP header, byte 9 (remember the byte count begins with zero) identifies the protocol of the packet. Most filter devices have the capability to differentiate between TCP, UPD, and ICMP.(TCP-Transmission Control Protocol,UDP-User Datagram Protocol,Internet Control Message Control)
- **source address (IP header, network layer)** – The source address is the 32-bit IP address of the host which created the packet.
- **Destination address (IP header, network layer**) – The destination address is the 32-bit IP address of the host the packet is destined for
- **Source port (TCP or UDP header, transport layer)** – Each end of a TCP or UDP network connection is bound to a port. TCP ports are separate and distinct from UDP ports. Ports numbered below 1024 are reserved – they have a specifically defined use. Ports numbered above 1024 (inclusive) are known as ephemeral ports. They can be used however a vendor chooses. For a list of "well known" ports, refer to RFP1700. The source port is a pseudo-randomly assigned ephemeral port number. Thus it is often not very useful to filter on the source port.
- **Destination port (TCP or UDP header, transport layer)** – The destination port number indicates a port that the packet is sent to. Each service on the destination host listens to a port. Some well-known ports that might be filtered are 20/TCP and 21/TCP - ftp connection/data, 23/TCP - telnet, 80/TCP - http, and 53/TCP - DNS zone transfers.
- **Connection status (TCP header, transport layer)** – The connection status tells whether the packet is the first packet of the network session. The ACK bit in the TCP header is set to "false" or 0 if this is the first packet in the session. It is simple to disallow a host from establishing a connection by rejecting or discarding any packets which have the ACK bit set to "false" or 0.

The filtering device compares the values of these fields to rules that have been defined, and based upon the values and the rules the packet is either passed or discarded. Many filters also allow additional criteria from the link layer to be defined, such as the network interface where the filtering is to occur.

Types of Packet Filtering

Packet filtering firewall allows only those packets to pass, which are allowed as per their firewall policy. Each packet passing through is inspected and then the firewall decides to pass it or not. The packet filtering can be divided into two parts:

1. Stateless packet filtering.
2. Stateful packet filtering.

The data travels through the internet in the form of packets. Each packet has a header which provides the information about the packet, its source and destination etc. The packet filtering firewalls inpects these packets to allow or deny them. The information may or may not be remembered by the firewall.

Stateless Packet Filtering

If the information about the passing packets is not remembered by the firewall, then this type of filtering is called stateless packet filtering. This type of firewalls are not smart enough and can be fooled very easily by the hackers. These are especially dangerous for UDP type of data packets. The reason is that, the allow/deny decisions are taken on packet by packet basis and these are not related to the previous allowed/denied packets.

Stateful Packet Filtering

If the firewall remembers the information about the previously passed packets, then that type of filtering is stateful packet filtering. These can be termed as smart firewalls. This type of filtering is also known as Dynamic packet filtering.

Stateful Inspection Firewall

Stateful Inspection Firewall is a firewall that keeps track of the state of network connections traveling across it.

Functionality

Firewall protection uses stateful inspection to track current connections. Stateful inspection tracks source and destination IP addresses, ports, applications, and other connection information. Before the client inspects the firewall rules, it makes the traffic flow decisions that are based on the connection information.

For example, if a firewall rule allows a computer to connect to a Web server, the firewall logs the connection information. When the server replies, the firewall discovers that a response from the Web server to the computer is expected. It permits the Web server traffic to flow to the initiating computer without inspecting the rule base. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection eliminates the need to create new rules. For the traffic that is initiated in one direction, they do not have to create the rules that permit the traffic in both directions. The client traffic that is initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443). The client computers initiate this outbound traffic; they create a rule that permits the outbound traffic for these protocols. Stateful inspection automatically permits the return traffic that responds to the outbound traffic. Because the firewall is stateful in nature, they only need to create the rules that initiate a connection, not the characteristics of a particular packet. All packets that belong to an allowed connection are implicitly allowed as being an integral part of that same connection.Stateful inspection supports all rules that direct TCP traffic.

Stateful inspection does not support the rules that filter ICMP traffic. For ICMP traffic, they must create the rules that permit the traffic in both directions. For example, for the clients to use the ping command and receive replies, they must create a rule that permits ICMP traffic in both directions.

The state table that maintains the connection information may be periodically cleared. For example, it is cleared when a Firewall policy update is processed or if Symantec Endpoint Protection services are restarted.

Proxy Firewalls

A Proxy is a central machine on the network that allows other machines in that network to use a shared Internet connection. Proxy servers are intermediate servers which accept requests from clients and forward them to other proxy servers, a source server, or service the request from their own cache. The proxy is also called 'server' or 'gateway'. Proxy allows users on a network to browse the Web, send files over FTP, and work with E-mail and other Internet services.

A Firewall Proxy provides Internet access to other computers on the network but is mostly deployed to provide safety or security. It controls the information going in and out the network. Firewalls are often used to keep the network safe and free of intruders and viruses. Firewall proxy servers filter, cache, log, and control requests coming from a client. A firewall proxy is one that is used for restricting connections from a proxy to the outside world or to the source server inside of the LAN. This is different from a conventional firewall, in that a conventional firewall restricts connections coming from the outside world.

Functionality

Simply put, proxy are gateway applications used to route Internet and web access from within a firewall. Proxy servers work by opening a socket on the server and allowing the connection to pass through. There is often only one computer in a company with direct Internet connection. Other computers have access to the Internet using that computer as gateway.A proxy basically does the following:

1. Receives a request from a client inside the firewall
2. Sends this request to the remote server outside of the firewall
3. Reads the response
4. Sends it back to the client

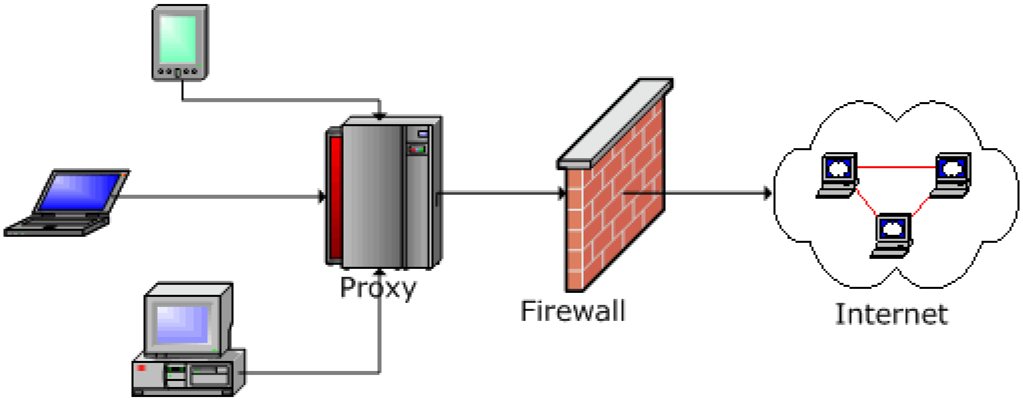


Fig3.1ProxyFirewalls

Usually, the same proxy is used by all of the clients on the network. This enables the proxy to efficiently cache documents that are requested by several clients.

SOCKS4 or SOCKS5 Proxy

In a SOCKS network, all network application data flows through SOCKS, enabling SOCKS to collect, audit, screen, filter and control the network data, and create a network application data warehouse.

It is recommended to use SOCKS5 proxy with PostCast Server. SOCKS4 performed three functions: connection request, proxy server setup and application data relay. SOCKS5 brings authentication to the table. With authentication, SOCKS5 adds two messages. SOCKS5 makes configuring clients easier and includes support for UDP and TCP applications such as SNMP and audio/video applications such as RealAudio. It supports communications among networks with different IP addressing schemes, and supports authentication and encryption.

Tunneling Proxy

Tunneling allows users to perform various Internet tasks despite the restrictions imposed by firewalls. This is made possible by sending data through HTTP (port 80). Additionally, Tunneling protocol is very secure, making it indispensable for both average and business communications. SSL (Secure Sockets Layer) tunneling protocol allows a web proxy server to act as a tunnel for SSL enhanced protocols. The client makes an HTTP Request to the proxy and asks for an SSL tunnel. A Tunneling Proxy operates on port 443.

Guard

In information security, a guard is a device or system for allowing computers on otherwise separate networks to communicate, subject to configured constraints. In many respects a guard is like a firewall and guards may have similar functionality to a gateway.

Whereas a firewall is designed to limit traffic to certain services, a guard aims to control the information exchange that the network communication is supporting at the business level. Further, unlike a firewall a guard provides assurance that it is effective in providing this control even under attack and failure conditions.

A guard will typically sit between a protected network and an external network, and ensure the protected network is safe from threats posed by the external network and from leaks of sensitive information to the external network.

A guard is usually dual-homed, though guards can connect more than two networks, and acts as a full application layer proxy, engaging in separate communications on each interface. A guard will pass only the business information carried by the protocols from one network to another, and then only if the information passes configured checks which provide the required protection.

Guards were initially designed to control the release of information from classified systems, protecting the confidentiality of the sensitive information handled by the protected system. Since then their scope has been extended to cover controls over the import of data, in order to protect the integrity of information and availability of services in the protected network. Guards generally provide the following functionality:

- Source and destination address authentication
- Source and destination address white listing
- Security label checks against source and destination clearances
- Data format whitelisting
- Data format consistency and validity checking
- Scanning data for known malware
- Validation of digital signatures
- Inspection of encrypted content
- Checking text against a blacklist of phrases
- Removal of redundant data
- Generation of logs recording security relevant events
- Self-test mechanisms

Personal firewall

A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. Typically it works as an application layer firewall.

A personal firewall differs from a conventional firewall in terms of scale. A personal firewall will usually protect only the computer on which it is installed, as compared to a conventional firewall which is normally installed on a designated interface between two or more networks, such as a router or proxy server. Hence, personal firewalls allow a security policy to be defined for individual computers, whereas a conventional firewall controls the policy between the networks that it connects.

The per-computer scope of personal firewalls is useful to protect machines that are moved across different networks. For example, a laptop computer may be used on a trusted intranet at a workplace where minimal protection is needed as a conventional firewall is already in place, and services that require open ports such as file and printer sharing are useful. The same laptop could be used at public Wi-Fi hotspots, where strict security is required to protect from malicious activity. Most personal firewalls will prompt the user when a new network is connected for the first time to decide the level of trust, and can set individual security policies for each network.

Unlike network firewalls, many personal firewalls are able to control network traffic allowed to programs on the firewalled computer. When an application attempts an outbound connection, the firewall may block it if blacklisted, or ask the user whether to blacklist it if it is not yet known. This protects against malware implemented as an executable program. Personal firewalls may also provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted.

Common personal firewall features:

- Block or alert the user about all unauthorized inbound or outbound connection attemptsAllows the user to control which programs can and cannot access the local network and/or Internet and provide the user with information about an application that makes a connection attempt
- Hide the computer from port scans by not responding to unsolicited network traffic
- Monitor applications that are listening for incoming connections
- Monitor and regulate all incoming and outgoing Internet users
- Prevent unwanted network traffic from locally installed applications
- Provide information about the destination server with which an application is attempting to communicate

Cryptography

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1) **Confidentiality** (the information cannot be understood by anyone for whom it was unintended)

2) **Integrity** (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) **Non-repudiation** (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

4) **Authentication** (the sender and receiver can confirm each other's identity and the origin/destination of the information)

Procedures and protocols that meet some or all of the above criteria are known as cryptosystems. Cryptosystems are often thought to refer only to mathematical procedures and computer programs; however, they also include the regulation of human behavior, such as choosing hard-to-guess passwords, logging off unused systems, and not discussing sensitive procedures with outsiders.

The word is derived from the Greek *kryptos*, meaning hidden. The origin of cryptography is usually dated from about 2000 BC, with the Egyptian practice of hieroglyphics. These consisted of complex pictograms, the full meaning of which was only known to an elite few. The first known use of a modern cipher was by Julius Caesar (100 BC to 44 BC), who did not trust his messengers when communicating with his governors and officers. For this reason, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet.

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

Because governments do not wish certain entities in and out of their countries to have access to ways to receive and send hidden information that may be a threat to national interests, cryptography has been subject to various restrictions in many countries, ranging from limitations of the usage and export of software to the public dissemination of mathematical concepts that could be used to develop cryptosystems. However, the Internet has allowed the spread of powerful programs and, more importantly, the underlying techniques of cryptography, so that today many of the most advanced cryptosystems and ideas are now in the public domain.

The Purpose of Cryptography

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts argue that cryptography appeared spontaneously sometime after writing was invented, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

- *Authentication:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message.

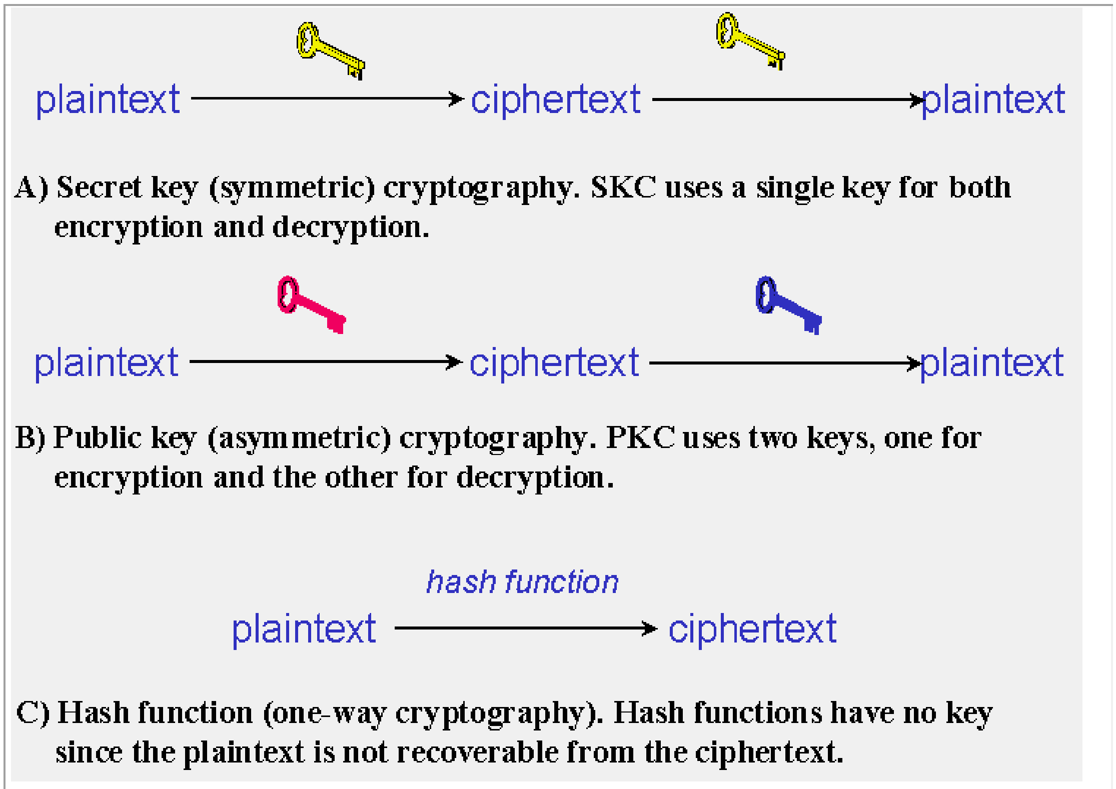
Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *ciphertext*, which will in turn (usually) be decrypted into usable plaintext.

In many of the descriptions below, two communicating parties will be referred to as Alice and Bob; this is the common nomenclature in the crypto field and literature to make it easier to identify the communicating parties. If there is a third or fourth party to the communication, they will be referred to as Carol and Dave. Mallory is a malicious party, Eve is an eavesdropper, and Trent is a trusted third party.

Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

FIGURE 1: Three types of cryptography: secret-key, public key, and hash function.

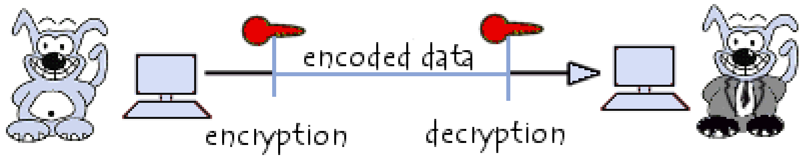
Secret Key Cryptography

In cryptography, a private or secret key is an encryption/decryption key known only to the party or parties that exchange secret messages. In traditional secret key cryptography, a key would be shared by the communicators so that each could encrypt and decrypt messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. A more recent alternative is to use a combination of public and private keys. In this system, a public key is used together with a private key. See public key infrastructure (PKI) for more information.

The basic principle

Encryption and decryption using a secret key

To secretly communicate with Bob, Aliice encrypts her messages before sending them. There are many techniques (cryptographic algorithms) that she can use. All these algorithms have in common that they can transform a message using a **key** into something that resembles random noise. This is called **encrypting the message**. Only the persons who know the key can transform the random noise back into the original message, or in other words, **decrypt the message**. This means that those persons must keep this key a secret, hence the name **secret key Cryptography**.



How to get the key to the recipient

A fundamental problem with secret key encryption is that somehow the secret key has to be delivered to the recipient of the message in a secure way. Once that key has been securely delivered, other keys can be delivered by simply encrypting them with that first key. One way to solve this problem is to have Alice and Bob meet in person so they can agree on a key. They must make sure that Eve is not listening in on them, otherwise Eve also learns the key. This applies especially if Alice and Bob agree on a key via telephone or e-mail. Of course Bob must also be able to distinguish Alice and Eve if they meet for the first time (for Alice it shouldn't be a problem to tell Bob from Eve).

If Alice and Bob can not meet in private to agree on the key, it is very difficult for them to use secret key cryptography. If they simply agree on a key by e-mail for example, Eve could be listening in on their e-mail conversation and thus also learn what the key is. If Alice and Bob had a secure channel that Eve could not tap, they could use that channel to agree on a secret key. However, then they could also use the secure channel to simply transmit their messages.

This problem is solved by using public key cryptography, which is discussed in the next chapter.

How secret key cryptography works

Secret key cryptography transforms (scrambles) a message into something resembling random noise. The precise transformation is determined by the key. Mathematically seen, a cryptographic algorithm is a function that maps a message onto a ciphertext (an encrypted message). By using keys, it is possible to encrypt many different messages using one particular cryptographic algorithm in different ways. And keeping the key a secret is much easier than keeping a complete algorithm a secret.

Some cryptographic algorithms operate on single characters of the message. These are called stream ciphers. Others operate on entire blocks, and therefore are called block ciphers. Stream ciphers are easier to implement in hardware than block ciphers, and they are also generally faster. Block ciphers tend to be harder to crack.

Secret key cryptography also in:

- DES Encryption Algorithm
- Encrypting using XOR and a password
- Popular cryptographic algorithms are DES, 3-DES, IDEA, Blowfish and recently also the Advanced Encryption Standard (AES).

An example of a secret key cryptographic system

A very simple technique to encrypt messages is to replace every letter of the message with one that is a certain number of positions further in the alphabet. The key then is the number of positions. For example, the message "This is an example" can be encrypted using the key "1 position" into the encrypted message "Uijt jt bo fybnqmf". Taking the letter that is 1 position previous in the alphabet results in the original message again.

This system is of course not very secure. There are only twenty-six possible keys. Eve can simply try out all the keys to see which one results in a readable message. Furthermore, it is a well-known fact that certain letters occur more often in messages than others. The letter "e" is the most frequently used letter in the English language, for example. Using this fact Eve can simply count which letter occurs the most often in the encrypted message and replace that one with the letter "e". She then knows how many positions she has to rotate to get from "e" to the encrypted version of "e" and thus she immediately knows the key.

One-time pads

In principle, all cryptographic systems can be broken. At the very least, Eve can try out all different keys until she finds one that successfully decrypts the message. Eve might also be able to break one of the mathematical principles behind the cryptographic algorithm that Alice and Bob use. For example, some cryptographic systems assume that it is very difficult to divide a number into its prime factors. Eve might find a quick way to do this. This then enables Eve to read Alice and Bob's messages or to recover their keys.

There is one cryptographic algorithm that cannot be broken. This algorithm is called the one-time pad (OTP). According to this algorithm, Alice generates a very large sequence of random numbers. The numbers in the sequence serve as the key. The sequence is called the "pad". Alice communicates the sequence to Bob in a secure way, so that Eve cannot obtain a copy of the key.

Every character in the message that Alice wants to send to Bob is encrypted with a different number in the sequence. In practice this means that the first character of the message will be encrypted with the first number in the sequence, the second character with the second number, and so on. When Bob receives the encrypted message, he takes out his copy of the sequence and simply decrypts the first character with the first number in the sequence, the second character with the second number, and so on.

Because every character of the message is encrypted with a different key, there is nothing Eve can do to guess the key. Even if she knew that the first words of the message were "Dear Bob", she could not use this information to recover the key of other words in the message. Every number is chosen randomly, so Eve has no way to know which number is the right one, even if Eve knew how to decrypt all other characters.

It is absolutely essential that every number in the sequence is chosen randomly and is only used once. If Eve can recover some of the numbers in the sequence and use those to predict other numbers, she can eventually reconstruct the entire sequence and thereby decrypt the message. For this reason it is not a good idea to use a random number generator implemented in software. Those generators are unable to generate really random numbers. They use a mathematical function that generates a set of numbers that appears to be random. But if user know the mathematical function and the number that it last generated, they can immediately compute the next "random" number.

To achieve this unbreakability, Alice and Bob must have very large sequences that contain only really random numbers. This makes an OTP very difficult to manage. It is said to have been used for the "hotline" between Washington and Moscow during the Cold War. In a case like that, it is practical to send couriers carrying suitcases chained to their arms to securely transmit the pad.

Applications of secret key cryptography

Secret key encryption is most often used to encrypt data to be stored on a particular location. If the encrypted data has to be transmitted, there always is the problem of how to get the secret key to the recipient in a safe way. Usually the key is encrypted using public key encryption so it can be transmitted safely.

Hiding spoilers

Even though it is not secure, the simple alphabet shifting system is still in use on the Internet. It is used to hide "spoilers" (revealing plot twists in movies or books) and potentially offensive messages from unsuspecting readers. Such messages are encrypted using the key "13 positions". Anyone can thus decrypt the message by simply taking the letter that is 13 positions previous in the alphabet. However, this requires some active step by the reader, and so he should then not be surprised or upset if the decrypted message reveals something about the plot of a movie he wanted to see. This system is commonly known as "ROT-13".

Encrypting the contents of hard disks

Using secret key encryption Alice can encrypt her entire hard disk so the data on it is safe if the disk (or laptop containing it) is ever stolen. Disk encryption programs exist that can encrypt and decrypt data as it is being written and read to and from the hard disk. This way Alice does not notice that her data is stored encrypted, except for the fact that disk access might be a bit slower. Once she turns off her computer, it is not possible anymore for Eve to read the data.

Protecting pay TV transmissions

Secret key encryption and smart cards are used for example in pay TV applications. Sometimes this is referred to as "conditional access" television. Television programs (usually premium movies, football or soccer matches and adult content) are encrypted using a secret key. To make it difficult for Eve to obtain this key, the secret key is changed every few minutes or sometimes even every few seconds. This way, even if Eve can successfully use a brute force attack to guess the key, she only has a very small portion of the television program. Alice has a set-top box and a smart card that allows her to decrypt the television programs. The set-top box passes the decrypted television program on to the television. Originally these boxes were designed to be placed on top of the television set, hence the name.

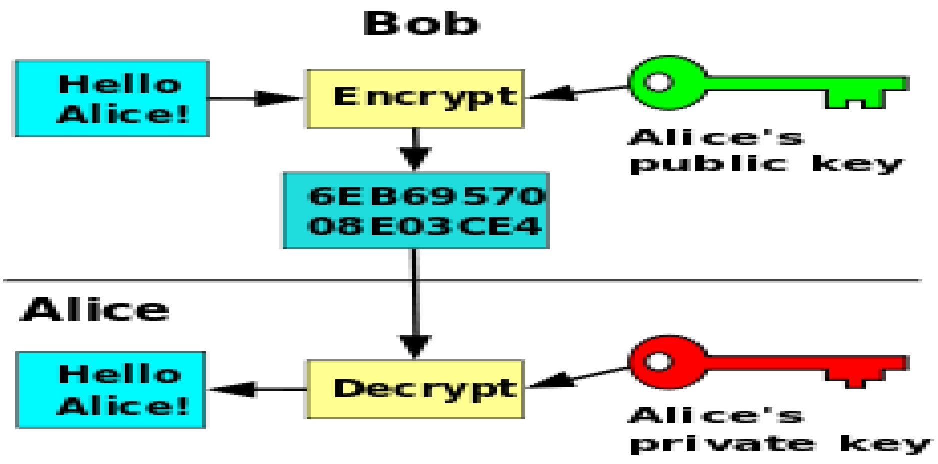
Special messages, called Entitlement Control Messages (ECMs), are sent along with the program. These messages contain the secret keys. Of course the ECMs themselves are also encrypted, this time using a key stored on the smart card. Alice's set-top box receives the ECMs and passes them on to the smart card. The smart card decrypts the ECMs and extracts the secret keys contained therein. This allows the set-top box to decrypt the television program.

The keys needed to decrypt the ECMs can be programmed on the smart card in advance. By regularly changing these keys, Alice is forced to purchase a new smart card every month or so. If Eve manages to make a copy of the smart card, or to extract the keys from it, she will only be able to watch the programs for the rest of that particular month.

Another option is to regularly send out so-called Entitlement Management Messages (EMMs) that contain the keys needed to decrypt the ECMs. The EMMs themselves are then encrypted with keys stored on the smart card. The service provider then every month simply sends out a new EMM. This provides much greater flexibility, and Alice does not have to go to the store every month. Every smart card can now have a different key. The service provider sends out different EMMs for all the smart cards in the system. Every EMM thus is readable only by one smart card. If the service provider thinks a particular smart card has been copied illegally, he simply does not send out a new EMM for that particular smart card.

Public-key Cryptography

Asymmetric cryptography or public-key cryptography is cryptography in which a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Initially, a network user receives a public and private key pair from a certificate authority. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. They use this key to encrypt the message, and they send it to the recipient. When the recipient gets the message, they decrypt it with their private key, which no one else should have access to.



Witfield Diffie & Martin Hellman, researchers at Stanford University, first publicly proposed asymmetric encryption in their 1977 paper, New Directions In Cryptography. (The concept had been independently and covertly proposed by James Ellis several years before when he was working for the British Government Communications Headquarters.) An asymmetric algorithm, as outlined in the Diffie-Hellman paper, is a *trap door* or *one-way* function. Such a function is easy to perform in one direction, but difficult or impossible to reverse. For example, it is easy to compute the product of two given numbers, but it is computationally much harder to find the two factors given only their product. Given both the product and one of the factors, it is easy to compute the second factor, which demonstrates the fact that the hard direction of the computation can be made easy when access to some secret key is given. The function used, the algorithm, is known universally. This knowledge does not enable the decryption of the message. The only added information that is necessary and sufficient for decryption is the recipient's secret key.

In cases where the same algorithm is used to encrypt and decrypt, such as in RSA, a message can be securely signed by a specific sender: if the sender encrypts the message using their *private* key, then the message can be decrypted only using that sender's p*ublic* key, authenticating the sender.

There are three types of cryptography algorithms: secret key, public key, and hash functions. Unlike secret key and public key algorithms, hash functions, also called message digests or one-way encryption, have no key. Instead, a fixed-length hash value is computed based on the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered.

The primary application of hash functions in cryptography is message integrity. The hash value provides a digital fingerprint of a message's contents, which ensures that the message has not been altered by an intruder, virus, or by other means. Hash algorithms are effective because of the extremely low probability that two different plaintext messages will yield the same hash value.

There are several well-known hash functions in use today:

- Hashed Message Authentication Code (HMAC): Combines authentication via a shared secret with hashing.
- Message Digest 2 (MD2): Byte-oriented, produces a 128-bit hash value from an arbitrary-length message, designed for smart cards.
- MD4: Similar to MD2, designed specifically for fast processing in software.
- MD5: Similar to MD4 but slower because the data is manipulated more. Developed after potential weaknesses were reported in MD4.

- Secure Hash Algorithm (SHA): Modeled after MD4 and proposed by NIST for the Secure Hash Standard (SHS), produces a 160-bit hash value.

Basis of Mobile Information Security

Introduction

The “Data stored on the device is worth more than the device”might well apply to desktops and laptops as well. But it’s much more probable that their mobile device might be used by someone or lost, compared to their laptop or desktop. This fact changes the entire scenario. With the advent of mobile phones and smart phones, the game has enormously changed in the last few years with respect to the ease with which tasks are accomplished. This article focuses on various security-related aspects which are involved with increased use of mobiles. Before jumping into the security concerns, here is a small introduction about how the mobile technology has slowly taken over the world.

The first hand-held mobile device was demonstrated by two Motorola employees in 1973. After 10 years, i.e. in 1983, the first mobile was commercially made available. From 1990 to the early 2000s, mobile phones spread rapidly; people used it mainly for communication. In the last 10 years, with the rapid increase in internet usage, mobiles started accommodating the features of personal computers and finally took a new shape with the introduction of “smart phones.” Today mobiles have penetrated into each and every corner of this world, serving a variety of tasks including mobile applications, GPS navigation, storage, entertainment, etc. In this article we will mainly focus on mobile applications and their security concerns.

Mobile Applications

Mobile phone applications extend the functionality of mobile phones. Everything is readily available and the tasks which were previously accomplished in a desktop world are now available on mobile just with a single click. People now use mobile applications to assist them in several day-to-day activities and enterprises are in a mad rush to develop the mobile apps to reach out to the users in a better way.

What is a mobile app anyway?

A mobile app is a software application developed to run on mobiles. Each mobile operating system has a corresponding distribution platform from where these mobile apps can be downloaded. For example, Android apps can be downloaded from Google Play and iPhone apps can be downloaded from the Apple App Store. So an individual or a company can develop a mobile application and upload it to the distribution platform and advertise it so that users can download and use it. The general demand and the ease of development of these mobile apps have resulted in their enormous growth. So these days we have a mobile app for everything – fox example, mobile banking, online shopping, ticket purchases, games etc. The real question is how secure are the mobile apps that deal with sensitive information. So let’s have a look at general mobile security-related issues which are common to all the platforms.

Mobile Security

Mobile security is increasingly playing a crucial role as more sensitive and personal information is now stored in the mobile phones. Security is considered as a crucial and central aspect during the unveiling of any Smartphone. Moreover, with the corporate world embracing the mobiles in a big way, the focus is very much on the security of these devices. Attacks that have been seen on PCs are now slowly making their way onto the mobiles. At a higher level, mobile-related attacks can be classified into these categories:

- Attacks based on OS–Exploiting the loopholes present at OS level. So the concerned vendor has to release a patch to fix the issue.

- Attacks based on mobile apps–Exploiting the security holes present in mobile application, which are a result of poor coding/development.
- Attacks based on communication networks–Attacks on GSM, Wi-Fi, Bluetooth, etc.

Malware-related attacks–Malware attacks on mobiles have been rising continuously. A successful attack can steal the photos on their mobile, hijack the camera click, hack the emails, and delete the files on the mobile.Let’s now move on and talk a little bit more about the current issues related to mobile security. The following is a list of the main issues in the field of mobile security. Please note that this is not the complete list and it is not in any particular order. Let’s have brief look into the security issues which revolve around the mobile devices currently.

Physical security

Physical security is one of the biggest challenges to the designers of mobile phones and their applications. Mobile phones are lost, stolen, and borrowed (many times by others to make a call or view the photos). When a mobile device is lost, the real concern is not about the cost of the mobile but the amount of sensitive data that is present on that mobile. Imagine that the personal phone which is provided by their employer for enterprise activities falls into the hands of the wrong person, who tweaks the data present in it. Imagine a situation where their neighbor asks their mobile for a quick call and then downloads a malware onto that phone (by the way, it just takes a few seconds to do that). These issues are rather less when they are dealing with a desktop, because it would be unusual if they lose their desktop computer. So the bottom line is that mobile applications and systems are to be designed assuming that untrusted parties will be granted access to the phone.

No such thing as “logging” into mobile

In the desktop world, each user supplies a username and password and logs into the system where he gets access to his environment. Each user has a different environment and thus the privileges and data that each user has are separated. This ensures that one account doesn’t have access to the data of other account. But this concept is not valid in a mobile world because there is nothing like logging into a mobile for each user. So sharing and accessing of data between applications is a big concern.

Secure storage of data on the phone

In addition to the sensitive files present on their mobile (photos, contacts, documents, etc.), mobile applications also store sensitive information like authentication tokens, password-related files etc. It’s very important that these files are protected. One way is by storing them securely on the mobile so that they are not accessible or usable. For instance, password files must be stored in encrypted fashion so that even after accessing those files they are of not much use.

Mobile browsing environment

In a mobile browser, it is not possible to see the entire URL; sometimes the URL can’t be seen at all. This paves the way for hackers to unleash phishing-related attacks. So the display space on a mobile device increases the possibility of phishing attacks many fold. The fact that people are more inclined to follow links on mobile blindly adds to this problem. So in this mobile browsing environment, it’s impossible to expect a normal user to verify every link before following it.

Isolating the applications

The range of mobile applications that we install today is diverse: social applications to connect to family and friends, enterprise applications to manage their work, banking applications to transfer funds, gaming applications for entertainment, and many more. So it’s very important that a social networking app does not gain access to their corporate app or that a gaming app does not gain access to the banking app. In short, application isolation is crucial. This would depend on the factors like OS permissions in different platforms and how these permissions are granted. Exploiting the existing mechanisms to gain unauthorized access is one area where hackers are actively updating.

Update Process

Operating systems require patches/updates to resolve any security issues that are discovered. OS's like Windows look continuously for updates and install them. But when it comes to mobile OS the patching process is not as simple as that. When a bug is reported in a particular OS, the OS vendor comes with a patch. He then publishes this information to all the carriers (like AT&T, Sprint, and Airtel etc.). Now these carriers will not be proactive in installing these updates because there is every chance that during patching processes other applications might break down. Hence if these carriers find such cases with the patching, they hold it on for some time without applying the patch/update immediately.

Proper Authentication

The authentication process is very important in mobile phones because, as explained earlier, it is just a matter of seconds before someone asks their phone and does something malicious and they have no idea about it. In the cases where a company offers extranet access to its corporate network through mobiles, there should be a means of multifactor authentication because if that mobile falls into the hands of the wrong guys, it would expose the internal network of the company. Multifactor authentication needs to be implemented and improved in order to solve many issues.

Poor coding of mobile apps

Poor coding or development practices of the developers could lead to severe consequences. For example: hard coding of sensitive data like passwords, transmission of information in unencrypted channel, weak server side controls, improper session handling, etc. Many of the vulnerabilities that apply to the web will apply to mobile applications as well.

Bluetooth and other attacks

Bluetooth and other drivers pose a security threat to the overall security posture of the mobiles. We have seen in the past about the vulnerabilities reported on Bluetooth and other third-party drivers. Since these have system access, by exploiting a critical vulnerability an attacker might even get access to everything on a mobile. So even if the underlying operating system has excellent built-in mechanisms that do not easily grant system access, these vulnerable third-party drivers would be a setback at any time.

Malware Attacks

Many surveys point out that malware attacks on mobile phones is on the rise. If they are someone who browses through tech news every now and then, they must have seen some news about android phones getting infected by malware in a big way. Malware is something which harms the system in which in resides. With a new computing environment, a new class of threats in new forms arise. It is very important that these issues are addressed proactively leveraging on our experiences of the 1990s. Reports have also been published which forecast the situation to be worse in the coming year and some say that 2013 will be the" year of mobile malware"!

Jail breaking the phones

Many users jailbreak the phone in order to run applications for free or to run applications which are not authorized by the vendor. Jailbreaking a phone removes the restrictions imposed on a device by its vendor. Hence jailbroken devices are more susceptible to computer viruses and malware. Downloading the apps from an unauthorized third-party store will only put their mobile at risks.

New features like NFC pose a serious threat

NFC (Neat Field Communication) is a technology that allows user to beam the content to nearby devices and lets user use their mobile as a wallet to purchase items. It has been demonstrated in Black hat conferences that by brushing a tag with an embedded NFC chip over an android phone, it is possible to take over the control of the phone. So with increase in technology, they will need to address more complex attack scenarios. In future, many more advanced technologies like these are expected to come and they bring a whole lot of new issues to address.

User awareness

User awareness is major factor in controlling many of the attacks and, when it comes to mobiles, it's even more important. There are many things from the user end which he should be careful about: having a passcode for the device and looking out for the permissions granted to application (a gaming application may not need access to dialling), not following the links sent by unknown persons. As the time progresses, the industry has more challenges to face and answer. For instance new ideas pose a security threat like BYOD (Bring their Own Device) where employees bring their personal mobile devices to their work place. Since there are huge number of devices out there, each having its own security issues, it's a huge task for any organization to guarantee the corporate equivalent of privacy on these devices. These are some of the basic issues that are involved in current mobile security. If anyone of they has more points to make, I sincerely ask that user comment and share with the community.

Social Information Security

Alternatively referred to as a **virtual community** or **profile site,** a **social network** is a website that brings people together to talk, share ideas and interests, or make new friends. This type of collaboration and sharing of data is often referred to as **social media**. Unlike traditional media that is often created by no more than 10 people, social media sites contain content that has been created by hundreds or even millions of different people. Below is a small list of some of the biggest social networks used today.

Examples of social networks

- **Bebo** (http://www.bebo.com/) - A popular social networking site where users can share photo's, stories, their journal, and more with friends and family privately or publicly on the Internet.
- **Classmates** (http://www.classmates.com/) - One of the largest and most used websites that brings together and allows people who graduated from high school and allows user to keep in touch with them and any future reunions.
- **Facebook** (http://www.facebook.com/) - The most popular social networking websites on the Internet. Facebook is a popular destination for users to setup their own personal web pages, connect with friends, share pictures, share movies, talk about what they're doing, etc.
- **Friendster** (http://www.friendster.com/) - A popular social network that brings together friends, family, and allows user to meet new people who share similar interests to user from all over the world.
- **Google+** (http://plus.google.com/) - The latest social networking service from Google.
- **LinkedIn** (http://www.linkedin.com/) - One of the best if not the best locations to connect with current and past co-workers and potentially future employers.
- **MySpace** (http://www.myspace.com/) - One of the most popular social networks and one of the most viewed website on the Internet. See the MySpace definition for further information about this service.

- **Orkut** (http://www.orkut.com/) - A popular service from Google that provides user a location to socialize with their friends and family, and meet new acquaintances from all around the world.
- **Path** (http://path.com/) - A mobile only social network that allows user to keep in contact with their closest friends and family.
- **Pinterest** (http://www.pinterest.com/) - An upcoming and popular picture and sharing service that allows anyone to easily share pictures, create collections, and more.
- **StumbleUpon** (http://www.stumbleupon.com/) - Another very popular community of Internet users who vote for web pages they like and dislike and allows users to create their own personal page of interesting sites they come across. See theStumbleUpon definition for additional information about this service.
- **Twitter** (http://www.twitter.com/) - Another fantastic service that allows users to post 140 character long posts from their phones and on the Internet. A fantastic way to get the pulse of what's going on around the world.
- **Yik Yak** - Smartphone social network that connects users who are in close to each other.
- **YouTube** (http://www.youtube.com/) - A great network of users posting video blogs or Vlog's and other fun and interesting videos.

Security implications

Social networking sites rely on connections and communication, so they encourage user to provide a certain amount of personal information. When deciding how much information to reveal, people may not exercise the same amount of caution as they would when meeting someone in person because

- the Internet provides a sense of anonymity
- the lack of physical interaction provides a false sense of security
- they tailor the information for their friends to read, forgetting that others may see it
- they want to offer insights to impress potential friends or associates

While the majority of people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available. The more information malicious people have about user, the easier it is for them to take advantage of user. Predators may form relationships online and then convince unsuspecting individuals to meet them in person. That could lead to a dangerous situation. The personal information can also be used to conduct a social engineering attack. (See Avoiding Social Engineering and Phishing Attacks for more information.) Using information that they provide about their location, hobbies, interests, and friends, a malicious person could impersonate a trusted friend or convince user that they have the authority to access other personal or financial data.

Additionally, because of the popularity of these sites, attackers may use them to distribute malicious code. Sites that offer applications developed by third parties are particularly susceptible. Attackers may be able to create customized applications that appear to be innocent while infecting their computer or sharing their information without their knowledge.

Protect Personally

Limit the amount of personal information they post - Do not post information that would make user vulnerable, such as their address or information about their schedule or routine. If their connections post information about user, make sure the combined information is not more than user would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about their connections**.**

- **Remember that the Internet is a public resource** - Only post information they are comfortable with anyone seeing. This includes information and photos in their profile and in blogs and other forums. Also, once they post information online, they can't retract it.

Even if they remove the information from a site, saved or cached versions may still exist on other people's machines.

- **Be wary of strangers** - The Internet makes it easy for people to misrepresent their identities and motives. (See Using Instant Messaging and Chat Rooms Safely.) Consider limiting the people who are allowed to contact they on these sites. If they interact with people they do not know, be cautious about the amount of information user reveal or agreeing to meet them in person.
- **Be skeptical** - Don't believe everything they read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.
- **Evaluate user settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see their profile, but they can customize their settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that user wouldn't want the public to see. Sites may change their options periodically, so review their security and privacy settings regularly to make sure that their choices are still appropriate.
- **Be wary of third-party applications** - Third-party applications may provide entertainment or functionality, but use caution when deciding which applications to enable. Avoid applications that seem suspicious, and modify their settings to limit the amount of information the applications can access.
- **Use strong passwords** - Protect their account with passwords that cannot easily be guessed. (See Choosing and Protecting Passwords.) If their password is compromised, someone else may be able to access their account and pretend to be user.
- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. (See Reducing Spam.) Also, try to locate the policy for handling referrals to make sure that they do not unintentionally sign their friends up for spam. Some sites will continue to send email messages to anyone they refer until they join.
- **Keep software, particularly user web browser, up to date** - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. (See Understanding Patches.) Many operating systems offer automatic updates. If this option is available, they should enable it.
- **Use and maintain anti-virus software** - Anti-virus software helps protect their computer against known viruses, so they may be able to detect and remove the virus before it can do any damage. (See Understanding Anti-Virus Software.) Because attackers are continually writing new viruses, it is important to keep their definitions up to date.

LEVEL II

Security

Security is defined as the quality or state of being of secure-to be free from danger.

A successful organisation should have multiple layers of security in place:

- **Physical security-**to protect people, physical assets, and the workplace from various threats.
- **Personal security-**to protect individuals who are authorized to access the organisation.
- **Operational security-**focuses on the protection of the details of particular operations.
- **Communications security-**encompasses the protection of organization's communications media, technology and content.
- **Network security-**protection of networking components, connections, and contents.
- **Information security-**protection of information assets.

What it has been used?

- Governments, military, financial institutions, hospitals, and private businesses.
- Protecting confidential information is a business requirement.

CIA Triangle

- It is the industry standard for computer security based on three characteristics of information (confidentially, integrity, and availability).
- This model no longer adequately constant changing environment of computer industry.

The expanded C.I.A triangle addresses the complexities of the current information security environment because it consists of list of critical characteristics of information, which are described in the next.

Security Requirements

Definition:

IT Security Requirements describe functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of an IT system.

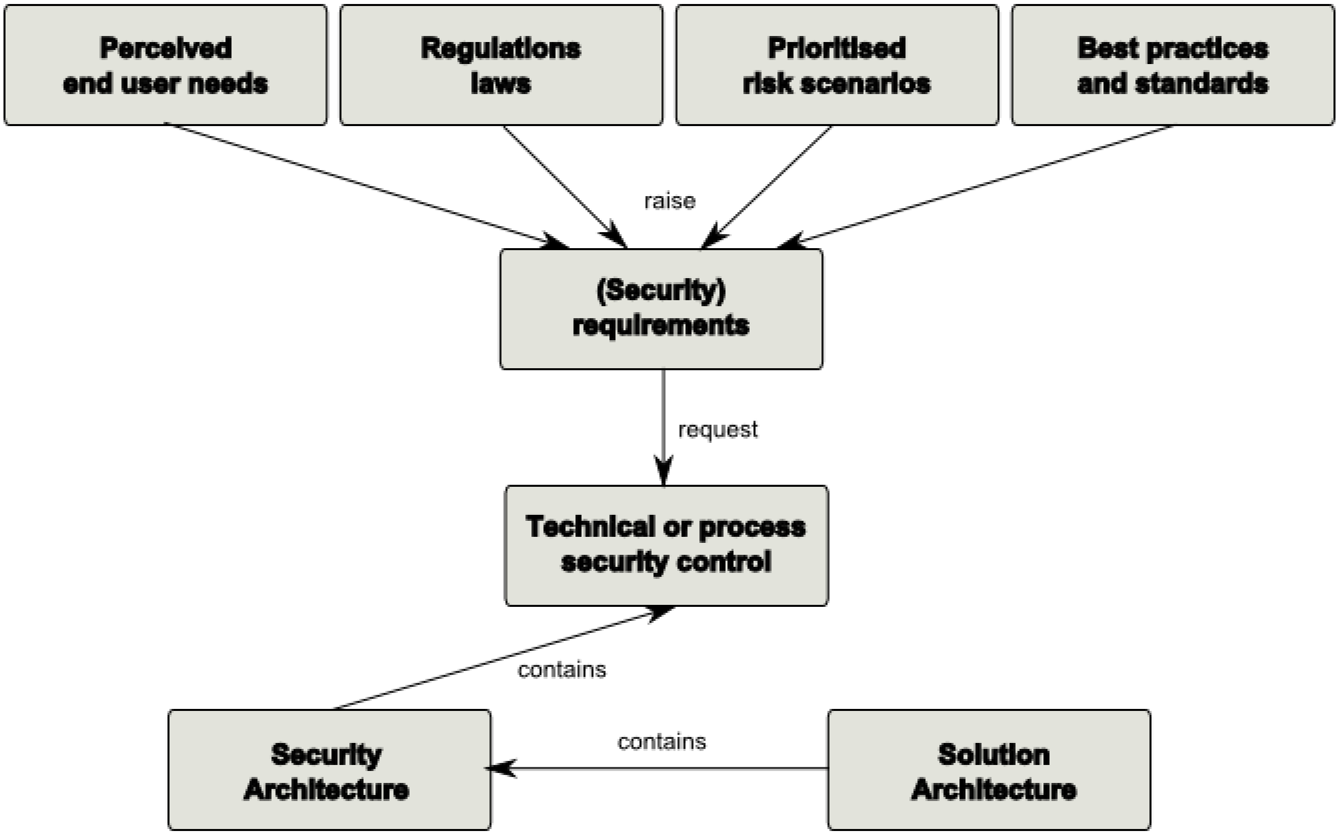
Type of security requirements:

Security requirements can be formulated on different abstraction levels. At the highest abstraction level they basically just reflect security objectives. An example of a security objectives could be "The system must maintain the confidentially of all data that is classified as confidential".

More useful for a SW architect or a system designer are however security requirements that describe more concretely what must be done to assure the security of a system and its data. OSA suggests to distinguish 4 different security requirement types:

- **Secure Functional Requirements**, this is a security related description that is integrated into each functional requirement. Typically this also says what shall not happen. This requirement artifact can for example be derived from misuse cases
- **Functional Security Requirements**, these are security services that needs to be achieved by the system under inspection. Examples could be authentication, authorization, backup, server-clustering, etc. This requirement artifact can be derived from best practices, policies, and regulations.
- **Non-Functional Security Requirements**, these are security related architectural requirements, like "robusteness" or "minimal performance and scalability". This requirement type is typically derived from architectural principals and good practice standards.

- **Secure Development Requirements**, these requirements describe required activities during system development which assure that the outcome is not subject to vulnerabilities. Examples could be "data classification", "coding guidelines" or "test methodology". These requirements are derived from corresponding best practice frameworks like "CLASP".



Security awareness

It is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially informational, assets of that organization. Many organizations require formal security awareness training for all workers when they join the organization and periodically thereafter, usually annually.

Security awareness training includes:

- The nature of sensitive material and physical assets they may come in contact with, such as trade secrets, privacy concerns and government classified information
- Employee and contractor responsibilities in handling sensitive information, including review of employee nondisclosure agreements
- Requirements for proper handling of sensitive material in physical form, including marking, transmission, storage and destruction
- Proper methods for protecting sensitive information on computer systems, including password policy and use of two-factor authentication
- Other computer security concerns, including malware, phishing, social engineering, etc.
- Workplace security, including building access, wearing of security badges, reporting of incidents, forbidden articles, etc.
- Consequences of failure to properly protect information, including potential loss of employment, economic consequences to the firm, damage to individuals whose private records are divulged, and possible civil and criminal penalties

Being security aware means you understand that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within a company's computer systems and throughout its organization. Therefore, it would be prudent to support the assets of the institution (information, physical, and personal) by trying to stop that from happening.

Security Challenges

The challenges of information security can be divided into the following areas:

- **Confidentiality and Privacy** - Ensuring that only the intended recipients can read certain information
- **Authentication** - Ensuring that information is actually sent by the stated sender
- **Integrity** - Ensuring that the original information was not altered and that no one tampered with it
- **Availability** - Ensuring that important information can be accessed at all times and places

Security Characteristics

The value of information comes from the characteristics it possesses. When a characteristics of inform are given below.

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

Availability

It enables authorized users (persons or computer system) to access information without interference and receives it in the required format. Availability does not imply that the information is accessible to any user; rather,it means availability to authorized users.

Accuracy

Accuracy of information refers to information which is free from mistakes or errors and has the value the end user expects. (EG: Inaccuracy of your bank account may result in mistakes such as bouncing of a check). If the information has been intentionally or unintentionally modified, it is no longer accurate.

Authenticity

It refers to quality or state of being genuine or original, rather than reproduction or fabrication. Information is authentic when the contents are original as it was created placed or stored or transmitted.

Attacks to authenticity:

- **E-Mail spoofing:** Sending E-Mail with modified address field.
- **Phishing:** Obtain personal or financial information in a fraudulent manner.

Confidentiality

Information has confidentiality when exposure to unauthorized individuals or systems in prevented. Confidentiality ensures that only those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can vie information confidentiality is breached.

To product the confidentiality of information, the numbers of measures are used:

- Information classification.
- Secured documents storage.
- Application of general security policies.
- Education of information custodians and end use.

Example:

When confidential information is mistakenly e-mailed to some –one outside the organisation rather to someone inside the organisation.

Attacks to confidentiality:

1. By mistake sending E-mail to unauthorize outside person.
2. Salami theft-employee steals a few pieces of information at a time but in the long run that employee gets the whole thing.

Integrity

Integrity means that data cannot be modified without authorization. Information has Integrity when it is whole, complete, and uncorrupted. The Integrity of information is threatened when it is exposed to corruption, damage, destruction and other disruption of its authentic state.

Utility

The utility of information is the quality or state of having value for some purpose or end. This means that if information is available, but not in a meaningful format to the end user, it is not useful. Thus the value of information depends on its utility.

Possession

The possession of information security is the quality or state of having ownership or control of some object or item. Information is said to be in one's possession if one obtains it independent of format or other characteristic.

EG: Illegal possession of encrypted data never allows someone to read it without proper decryption methods.

Security Principles

Integrity

In information security, data integrity means maintaining and assuring the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically provide message integrity in addition to data confidentiality.

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system essentially forcing it to shut down.

Authenticity

In computing and information security, it is necessary to ensure that the data, transactions, communications or documents (electronic or physical) are genuine. It is also important for authenticity to validate that both parties involved are who they claim to be. Some information security systems incorporate authentication features such as "digital signatures", which give evidence that the message data is genuine and was sent by someone possessing the proper signing key.

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.

It is important to note that while technology such as cryptographic systems can assist in non-repudiation efforts, the concept is at its core a legal concept transcending the realm of technology. It is not, for instance, sufficient to show that the message matches a digital signature signed with the sender's private key, and thus only the sender could have sent the message and nobody else could have altered it in transit. The alleged sender could in return demonstrate that the digital signature algorithm is vulnerable or flawed, or allege or prove that his signing key has been compromised. The fault for these violations may or may not lie with the sender himself, and such assertions may or may not relieve the sender of liability, but the assertion would invalidate the claim that the signature necessarily proves authenticity and integrity and thus prevents repudiation.

Electronic commerce uses technology such as digital signatures and public key encryption to establish authenticity and non-repudiation.

Security Mechanism

There are many security procedures in use at the present time. The most important ones are as follows:

1.Encryption
2.Digital signatures
3.Key Management
4.sealing

Encryption

Encryption is the scrambling of data or messages to prevent them being understood by unauthorized person or organizations. It can be used to prevent undetectable alteration of messages and to check the identity of the creator. It is widely acknowledged that the most effective protection available is encryption-many of the threats discussed in danger threatening EDI messages in transit can be countered by its use.

Encryption may be used for:

- User authentication –verification by the receiver that the sender is the genuine article and not somebody else
- Message authentication-verification that messages have not been lost or tampered with
- Confidentiality-encrypted data cannot normally be understood by anyone other than the sender or the receiver
- Error detection –checking that the contents of a message have not accidentally changed and
- Proof or origin-proving to a third party that the message came from the stated sender

In simple term encryption normally works in the following way:

- A message in its original form (plaintext) is encrypted into an unintelligible from (ciphertext) by a set of procedures known as an encryption algorithm and a variable, called a key ;and
- The ciphertext is transformed(decrypted) back into plaintext using the encryption algorithm and a key.

There are two types of encryption-private key system and public key system. In private key systems the same key is used for encryption and decryption. Private key systems are also known as ‘symmetric’ systems because the same key is used on both sides of the process. Obviously the transmission of the agreed key from the sender to the recipient needs to be secure and this is discussed in key management. The most well known symmetric system is probably the data encryption standard(DES).

In public key system there is a public key, which may be known to many people and a secret key, which is unique and known only to the sender. Because a different key is used on each side of the process, public key systems are also known as 'asymmetric system'. The distribution of keys for public key system is generally much easier because it is not normally necessary to keep the public key secret. The private key, on the other hand ,must remain secret or else security is compromised. The best known public key system is RSA, named after its authors, Rivest, Shamirand Adelman.

Digital signatures

Digital signature use asymmetric encryption to provide assurance of authentication of the origin of message and, sometimes, the integrity of its contents. They can also prevent repudiation as they can be used to prove, that providing the private key has not been disclosed ,the signature is that of the sender.

Very briefly ,a typical digital signature works like this:

- A signature in the form of a code is generated by applying an algorithm, such as RSA ,and the sender's private key to some or all of the message contents; and
- The recipient verifies the signature by using the sender's public key

Key management

Key management is the procedures for generating, storing, exchanging, archiving and deleting keys and the success of any security mechanism using encryption is heavily depending on its adequacy.

The requirements vary depending upon whether symmetric or asymmetric encryption is being used and whether the keys are encrypting keys or data encrypting keys.

In symmetric encryption system the overriding requirement is to keep the key secret amongst the parties who are transferring enciphered data .In a symmetric encryption system, the overriding need is for the decrypting party to be sure that the public key they receive really is the public key of the encryptor. If they use a false key, they may act on messages from a bogus sender.

Generation

Keys should be securely generated-it should not be possible for any unauthorised person to find out how keys are generated as this may enable them to determine what the keys are. Ideally, the initiation and controlling of the generation should be under dual control, i.e no one person should be able to generate the keys.

Distribution

The subsequent security depends on whether the keys are being distributed manually or electronically and whether the keys are public or private.

Manual distribution and receipt

Manually distributed keys should be split into two parts and sent separately in secure envelopes (special, sealed envelopes, which show if they have been opened) to two separate individuals. Regardless of whether a key is public or private, the recipient still has to be assured that it is genuine-this may be certified using an individual's written signature.

Electronic distribution

Private keys which are distributed electronically, should be encrypted. Data encrypting keys should be sent in ciphertext utilizing key encrypting keys.

Certification authorities

Third parties, trusted by senders and receivers, called certification authorities, can be used to certify the authenticity of public keys.

X.509 certification

Part of the X.500 recommendations,X.509, sets out how directories can be used to certify the public key of a sender. When the message is received, the recipient requests the sender public key .The certification authority sends the public key of the sender to the recipient.

Archiving

Where encryption has been used for authentication it is particularly important that various keys are securely archived.

Sealing

Message can be 'sealed' to show that the contents have not been accidentally or intentionally changed. This is normally done using a checksum which is appended to the message or sent separately. A checksum is the result of a calculation which uses data from the message. To check that the message has not been altered, the checksum is recalculated. If the data used in the calculation haven changed that the result is different, indicating that the seal has been broken. Most seals use encryption to increase the security of the checksum.

Digital Signature

When the asymmetric process is reversed- the private key encrypts a (usually short) message, and the public key decrypts it- the fact that the message was sent by the organization that owns the private key is difficult to refute. The non repudiation is the foundation of digital signatures. Digital signatures are encrypted messages that can be independently verified by a central facility (registry) as authentic, but can also be used to prove certain characteristics of messages or file with which they are associated. They are often used in internet software updates. A pop-up window shows that the downloaded files come from the purported agency and thus can be trusted. A digital certificate is similar to digital structures and asserts that a public key is associated with a particular identity (for example, which a particular public key really belongs to Alex). A certificate authority (CA) is an agency that manages the issuance of certificates and serves as the electronic notary public to verify their origin and integrity.

Public key infrastructure

A public key infrastructure (PKI) is the entire set of hardware, software cryptosystems necessary to implement public key encryption PKI systems are based on public key cryptosystems and include digital certificate authorities common implementations of PKI include:

- Systems to issue digital certificates to users and servers
- Encryption enrollment
- Key –issuing systems
- Tools for managing the key issuance
- Verification and return of certificates
- Key revocation services
- Other services associated with PKI that vendors bundle into their products.

The uses of cryptographic tools are made more manageable when using PKI. PKI can increase the capabilities of an organization in protecting its information assets by providing the following services:

- **Authentication:** Digital certificates in a PKI system permit individuals, organization, and web servers to authenticate the identity of each of the parties in an internet transaction.
- **Integrity:** Digital certificates asset that the content signed by the certificate has not been altered while in transit.
- **Confidentiality:** PKI keeps information confidential by ensuring that it is not intercepted during transmission over the internet.

- **Authorization:** Digital certificates issued in a PKI environment can replace user IDs and passwords, enhance security, and reduce some of the overhead for authorization processes and controlling access privileges for specific transaction.
- **Non repudiation:** Digital certificates can validate action, snaking it less likely that customers or partners can later repudiate a digitally signed transaction, such as an online purchase.

Proxy Servers

- A proxy server is a computer server which acts in the place of individual users when connecting to Web sites. The proxy server receives requests from individual workstations and PCs and then sends this request to the Internet. It then delivers the resultant information to the requesting PC on the network.
- When used in conjunction with a firewall, a proxy server's identify (and its connected PCs) is completely masked or hidden from other users. This is the manner in which secure sites operate.

Introduction on information security policies and standards

In order to most effectively secure its network environment, an organization must establish a functional and well-designed information security program. Firewalls, network security, and intrusion detections systems can only succeed within the context of a well- planned and fully defined information security program. Uncoordinated security initiative seldom as effective as those that the operate under a complete and effective policy environment. The creation of an information security program begins with the creation or review of the organization‘s information security polices, standards, and practices, followed by the selection or creation of information security architecture and a detailed information security blue print. Without policy, blue prints and planning, the organization will not be able to meet the information security needs of the various communities of interest. The role of planning in the modern organization is hard to overemphasize. All but the smallest organizations undertake at least some planning: strategic planning to manage the allocation of resources, and contingency planning to prepare for the uncertainties of the business environment.

Information security policies and standards

Management must make polices the basis for all information security planning, design and deployment. Polices direct how issues are addressed and how technologies are used. Polices do not specify the proper operation of equipment or software-this information should be placed in the standards, procedures, and practices of users manuals and systems documentation. In addition, policy should never contradict law, because this can create a significant liability for the organization.

Because information security is primarily a management problem,, not a technical one, quality security programs begin and end with policy. Policy obliges personnel to function in a manner that adds to the security of information assets, rather than threatening them. Securities polices are the least expensive control to design and disseminate –they require only the time and effort of the management team-but the most difficult to implement too properly. Even if the management team hires an outside consultant to assist in the development of policy, the costs are minimal compared to those of technical controls. However, shaping policy is difficult because policy must:

- Never conflict with laws
- Stand up in court, if challenged
- Be properly administered through dissemination and documented acceptance

For a policy to be considered effective and legally enforceable, it must meet the following criteria:

- **Dissemination (distribution):** The organization must be able to demonstrate that the relevant policy has been made really available for review by the employee. Common dissemination techniques include hard- copy and electronic distribution.
- **Review (reading):** The organization must be able to demonstrate that it disseminated the document in an intelligible form, including versions for illiterate, non English reading, and reading –impaired employees.
- **Comprehension (understanding):** The organization must be able to demonstrate that employees understood the requirements and content of the policy. Common techniques include quizzes and other assessments.
- **Compliance (agreement):** The organization must be able to demonstrate that employees agree to employ with the policy, through act or affirmation. Common techniques are include logon banners that require a specific action (mouse click or keystroke) to acknowledge agreement, or requiring employees to sign a document clearly indicating that they have read, understood, and agreed to comply with the policy.
- **Uniform enforcement:** The organization must be able to demonstrate that the policy has been uniformly enforced.

A policy is a set of guidelines or instructions that an organization's senior management implements to regulate the activities of the members of the organization who make decisions, take actions, and perform other duties. Policies are organizational law in that dictate acceptable and unacceptable behavior within the organization. Like laws, policies define what is right and what is wrong, what the penalties are for violating policy, and what the appeal process is. Standards, though they have the same compliance requirements as policies, are more detailed description of what must be done to comply with policy. The standards may be informal or other part of an organizational culture, as in de facto standards. Or standards may be published, scrutinized, and ratified a group, as formal or de jure standards. Practices, procedures, and guidelines effectively explain how to comply with policy. Fig 1 shows policies as the force that drives standards, which in turn drive practices, procedures, and guidelines.

Policies are put in place to support the organization's mission, vision, and strategic planning. The mission of an organization is a written statement of an organization's purpose. The vision of an organization is a written statement of an organization's long term goals-where will the organization be in five years? In Ten? Strategic planning is the process of moving the organization towards its vision.

The meaning of the term security policy depends on the context in which it is used. Governmental agencies discuss security policy in terms of national security and national policies to deal with foreign states. The security policy can also be a credit card agency's method of processing credit card numbers. In general, a security policy is a set of rules that protect an organization's assets. An information security policy provides rules for the protection of the information assets of the organization.

Management must define three types of security policies, according to The National Institute of standards and technology's special publication 800-14:

- Enterprise information security policies
- Issue-specific security policies
- System- specific security policies

Each of these management security policies is examined in greater detail in the sections that follow.

Enterprise Information Security Policy (EISP)

An enterprise information security policy is also known as a general security policy. IT security policy or information security policy. The EISP is based on and directly supports the mission, vision and direction of the organization and sets the strategic direction, scope, and tone for all security efforts .The EISP is an executed level document, usually drafted by, or in cooperation with, the chief information officer of the organization. The EISP usually need to be modified only where there is a change in the strategic direction of the organization.

The EISP guides the development, implementation, and management of the security program. It specifies the requirements to be met by the information security blue print or frame work. It defines the purpose, scope, constraints, and applicability of the security program in the organization.

It also assigns responsibilities for the various area security, including systems administration, maintenance of the information security policies, and the practices and responsibilities of the users. According to the National Institute of standards and technology's the EISP typically addresses compliance in two areas:

- General compliance to ensure meeting the requirements to establish the program and the responsibilities assigned therein to various organizational components and
- The use of specified penalties and disciplinary action.

When the EISP has been developed, the CISO (chief information security officer) begins forming the security team and initiating the necessary changes to the information security program.

EISP ELEMENTS:

Although the specifies of EISP‘s vary from organization to organization, most EISP documents should include the following elements:

- An overview of the corporate philosophy on security
- Information on the structure of the information security organization and individuals who fulfill the information security role
- Fully articulated security responsibilities that are shared by the all members of the organization (employees, contractors, consultants, partners and visitors)
- Fully articulated security responsibilities that are unique to each role within the organization.

Issue-Specific Security Policy (ISSP)

As an organization executes various technologies and processes to support routine operations. it must instruct employees on the proper use of those technologies and processes. In general, the issue specific security policy, or ISSP, (1) addresses specific areas of technology as listed below, (2) requires frequents updates,(3) contains the statement on the organization's position on a specific issue. An ISSP can cover the following topics, and others:

- Use of company owned networks and internet
- Use of telecommunications technologies (fax and phone)
- Use of electronic mail
- Specific minimum configurations of computers to defend against worms and viruses
- Prohibition against hacking or testing organization security controls
- Home use of company –owned computer equipments
- Use of personal equipment on company networks
- Use of photo copy equipment

There are a number of approaches to creating and managing ISSPs within an organization Three of the most common are to create the following types of ISSP documents:

- Independent ISSP documents, each tailored to a specific issue
- A single comprehensive ISSP documents covering all issues
- A modular ISSP document that unifies policy creation and administration, while maintaining each specific issue's requirements.

The independent document typically has a scattershot effect. Each department responsible for a particular application of technology creates a policy governing its use, management, and control. This approach may fail to cover all of the necessary issues, and can need to poor policy distribution, and management, and enforcement.

The single comprehensive ISSP is centrally managed and controlled. With formal procedures for the management of ISSP's in place, the comprehensive policy approach establishes guidelines for issue coverage and clearly identifies processes for the dissemination, enforcement, and review of this guideline. Usually, comprehensive ISSP's are developed by those responsible for managing the information technology resources. Unfortunately, they tend to overly generalize the issues and skip over vulnerabilities.

The optimal balance between the independent and comprehensive ISSP is the modular ISSP. It is also centrally managed and controlled but tailored to the individual technologies issues. The modular approach provides a balance between issue orientation and policy management. The policies created via this approach comprise individual modulus; each created and updated by individual responsible for the issues addressed this individual report to a central policy administration group that incorporates specific issues into an overall comprehensive policy. Even though the details may vary from policy to policy and some sections of a modular policy may be combined, it is essential for management address and completes each section.

Statement of policy:

The policy should begin with a clear statement of purpose. Consider a policy that covers the issue of fair and responsible use of internet. The introductory section of the policy should outline of these topics: what is the scope of the policy? Who is responsible and accountable for policy implementation? What technologies and issues does it address?

Authorized access and usage:

This section of the policy statement addresses who can use the technology governed by the policy, and what it can be used for. Remember that an organization's information systems are the exclusive property of the organization, and users have no general rights of use. Each technology and process is provided for business operations. Use for any other purpose constitutes misuse. This section defines "fair and responsible use" of the covered technology and other organizational assets, and should also address key legal issues, such as protection of personal information and privacy.

Prohibited use:

Unless a particular use of technology is clearly prohibited, the organization cannot penalize its employees for using it in that fashion. The following can be prohibited: personal use, disruptive use or misuse, criminal use, offensive or harassing materials and infringement of copyrighted, licensed, or other intellectual property.

Systems management:

The systems management section of the ISSP policy statement focuses on user's relationship to system management. Specific management rules include regulating the use of e-mail, the storage of materials, authorized monitoring of employees, and the physical and electronic security of e-mail and other electronic components. It is important that all such all responsibilities be designated ti either the systems administrators or the users; otherwise, both parties may infer that the responsibilities belongs to the other party.

Violations of policy:

Once guidelines on use have been outlined and responsibilities have been assigned, the policy must specify the penalties for, and repercussions of, policy violation. Violations should incur appropriate, not draconian, penalties. This section of the policy statement should specify the penalties for each category of violation as well as instructions on how individuals in the organization can report observed or suspected violations. Many people think that powerful individuals in the organization can discriminate, single out, or otherwise retaliate against someone who reports violations. Allowing anonymous submissions is often the only way to convince users to report the unauthorized activities of other, more influential employees.

Policy review and modification:

Because a document is only useful if it is up to date, each policy should contain procedures and a timetable for periodic review. As the organization's needs and technologies change, so must the policies that govern their use. This section should specify a methodology for the review and modification of the policy, to ensure that users do not begin circumventing it as it grows obsolete.

Limitations of Liability:

If an employee is caught conducting illegal activities with organizational equipments, or assets management does not want the organization held liable. The policy should state that the organization will not protect employees who violate a company policy or any law using company technologies, and that the company is not liable for such actions. It is understood that such violations are without the organization's knowledge or authorization.

System –Specific Policy (SysSP):

While issue –specific policies are written documents readily identifiable as policy, system- specific security policies (SysSP) sometimes have a different look. SysSPs often function as standards or procedures to be used when configuring or maintaining systems. For example, a SysSP might describe the configuration and operation of a network firewall. This document could include a statement of managerial intent; guidance to network engineers on the selection, configuration, and operation of firewalls; and an access control list that defines levels of access for each authorized user. SysSP can be separated into two general groups, managerial guidance and technical specifications, or they can be combined into a single policy document.

Security in TCP/IP Networks

Allowing access to your hosts for only the users that you intended is the goal of security in a TCP/IP network. A, discussed previously, once a user is logged into a system, the security within that system is all that prevents the user from accessing information that user should not be able to access. Thus, first level of security in a network is to make sure that all the security on the various hosts themselves is carefully policed. Unfortunately, security in UNIX hosts is based on userid and password. Thus, userids and passwords need to be very difficult to guess. The most effective method used to create a truly secure system is to have userids that are not personal names or initials but computer - generated in some reasonable random style and to passwords that are likewise computer- generated. Users will not like having userids and passwords that are not easy to remember. But, if someone trespassed into your system, that person will able to work out userids if it appears that some form of a person's name is being used as userid. If you find using computer – generated userids too difficult, you should at least force people to change their passwords regularly. Further, you should regularly use password scanning software to make sure people aren't using simple, easy-to-guess passwords like their name or car type.

A second level of security is to ensure that only users whom you want are even accessing your network. If your network is completely disconnected from the outside world, you only need to concentrate on the security of your individual hosts. But if you are part of the internet community and have linked up to the outside world, you need to consider measure to isolate your network from the rest of the internet. One method is to place a ”wall” between your network and the outside networks. This mechanism is often called a firewall because a “fire” in the outside network will not be allowed to enter your work. Routers can be programmed to analyze the network address of a user attempting to access your network and exclude those addresses of users whom you do not want to access your system.

Another issue is security: The **rlogin** command is sometimes used in place of the **telnet** command because system administrators can set up user validation so that no password is needed for a user to log in on another host. The **telnet** command always requires a password to be entered. Unfortunately, this approach while convenient for users, opens a security hole on the remote system when you use it. With access to the outside world via the internet a reality for many networks, you should not have any passwordless userids. If you need to provide a guest password for a short period of time, you should create a special account for this purpose and then only assign a password when you want to provide access to that guest. By the way, userids on most UNIX systems can be set up not to allow login on that userid at all. These userids are normally present in the system for allowing ownership of system files.

Another issues of security involves permitting the use of anonymous file transfers. You can set up your system so that a file can be transferred between you system and another system without the user having a userid registered on your system. This is accomplished by setting up the FTP user with a special home directory for that user. Then a user can log in using the user anonymous and any password will be accepted for that user. Once logged in, the anonymous user will have access to those files that are in the home directory of the anonymous user. With careful attention to the permissions on other directories, only this one directory can be made available to outside users.

LAN Security

Security for microcomputer LANs has increased in importance and more vendors are supplying LAN security systems. As end-users become more aware of the value of the vast amounts of data being accumulated and the need to protect that data, more users adopt such systems.

Newspapers carry stories almost every week about some computer network being penetrated, either for financial gain or as a prank. Most of these break-ins involve large corporate networks and wide area networks. As local area networks proliferate and tap into national and international data communication systems, these local networks will also become targets.

Companies that do sensitive wok, such as those with defence contracts are often heavily involved in data security. Other companies may be aware only of the threat, but not of their own vulnerability. Most analysts agree that businesses and institutions, such as schools will have to suffer a loss through theft or vandalism before they actually establish measures to protect their data.

A computing network like any other valuable shared resources, is subject to branches of security. Such breaches can be accidental or international and their effects on network operations can range from harmless to irritating to devastating.

Security is a critical issue to those planning, managing or using a LAN. It is also a very complex issue. Security is a component of overall network reliability. However, reliability depends largely upon the dependability of network hardware, software and technology. In contrast, the security of a network depends almost exclusively upon the behaviour of that network’s authorised users, managers and their guests.

Security is best addressed as part of an overall network strategy. Security concerns must be balanced by other factors that affect the network and its users. Users and managers must therefore discover and implement methods that improve network security without infringing upon users, work patterns or implying that all users are suspected violators of security.

Users have other concerns that network security methods must address as well. Users must be reassured that they can collaborate on projects and share information without being spied upon by managers or other users. Well-implemented password protection schemes can provide much of this reassurance. Managers must also demonstrate to users that procedures for tracking users work patterns on the network are used to improve security and not merely to keep a closer eye on users or their activities.

Security methods must be selected with care and implemented with the full cooperation and knowledge of authorised users if security is to be assured (see Figure 8.1). A first steps towards these goals is a definition of network security.

1. Security cannot exist without a management policy.
2. LAN users should be positively identifiable before they have access to network resources.

Prevention : passwords, passkeys authorization measures.

3. Data, hardware and software should be protected from unauthorized and/or accidental, modification, destruction, theft or disclosure Prevention : locks
4. Data should be reconstructible.

Prevention : frequent, regular backup of files.

5. Equipment must be protected from fire, dirt and natural disasters.

Prevention : smoke detectors, sprinklers, airconditioning.

Levels of Security

There is no such thing as 100% security.with enough skill and thought time to complete the job,a perpetrator can defeat any security measure.

Of the two security elements of skill and time,the most dependable protection is time.If you can make certain that a break in will be a time consuming projects for a thief,you have gone a long way in protecting yoyr data.Therefore,all serious security systems are layered with not but several security measures.For a local area network the following strategies should be considered.

1.Physical security
2.Access control
3.Personal identification
4.Encryption
5.The diskless PC
6.Protection against cable radiation
7.Call-back security

1.Physical security:

Data security can take many forms.The simplest is physical security,which may be a lock on the computer or a guard at the door.with physical security,a would be thief must attack and defeat your security measures before becoming a threat to the data.

An alarm system works in partnership with your physical security measure.Locking devices are designed to increase the time needed for penetration.Alarm put an effective limit on the amount of time available.Professional criminals do not run when they hear an alarm or when they think they have tripped a silent alarm.Most know precisely how muchtime they have before the police arrive,then the criminals will abandon the effort.

2.Access control:

The purpose of access controls is to ensure that only authorised users have access to the system and its individual resources and that access to and modification of particular portion of data is limited to authorised individuals and programmes.

3**. Personal identification:**

A local area network presents some additional security problems because of its dispersed nature and because many people have access to the network.Remote access through modems and telephone lines is used widely on LANs,which makes dispersion essentially infinite.Dispersion thwarts one of the best types of personal identification security systems.

On most networks the first line of security is personal identification.You physically recognise people who are authorised to be in your office,sitting at a PC.with remote access this kind of identification is impossible.Companies must rely on passwords and classified access schemes to protect their data.

Several techniques can be used to restrict access to authorised users.All these techniques are based on some kind of identification:personal,such as ID badge:key word such as a log in name and password:or key number.

Passwords

Passwords security adds no cost to the network and is potentially a useful security measure. After logging onto the network, the user must type a password. Theoretically, if users must give a password, unaudited. But often the password system is misused and ineffective.

4.Encryption

Earlier, we referred to one of the major security risks on LANs,which uses a multi-access medium-the risk of eavesdropping. Eavesdropping can be accomplished by programming the NIU to accept packets other than those addressed to it or by physically tapping into the medium. One counter measure that measure that properly used, is very effective is to encrypt the data in each packet (i.e. sent the data in code).

Encryption is the process of changing intelligible data into un intelligible data: decryption reverses the process. For most local area networks, data encryption is used only when the security threat is substantial.

Ensuring that data is secure in a network environment is more difficult than ensuring the security of physical documents.Typically,data in a network in a common storage facility, and anyone authorised to use the central storage has the potential to access classified fiels.The best solution to this potential problem is to store the data in an encrypted form.Then,any unauthorised person accessing the file would not be able to read its contents.

Encryption techniques cover a broag range,from simple encryption that guards against accidental disclosure to sophisticated methods which protect against all but the highly trained criminal with an in-depth knowledge of cryptanalysis and considerable deciphering equipment.

Most encryption schemes are based on mathematical operations that are “computationally infeasible”. That is they are based on prime numbers which are so large that even the computational power of a mainframe computer cannot break the code within a apractical time period.

Two primary types of encryption exist:link and end-to-end.Link encryption is used to make data unreadable while it is on a point –to-point link,such as between two PCs.

End-to-end encryption protects data anywhere on the systems.This type of encryption corresponds to layer 4 in the OSI model.Because layer 4 is end-to-end, encryption here can provide protection to any number of communication links or intermediate networks.

Types of Threats

A publication of the National Bureau of standards identified some of the threats that have stimulated the upsurge of interest in security:

1. Organised and intentional attempts to obtain economic or market information from competitive organisations in the private sector.
2. Organised and intentional attempts to obtain economic information from government agencies.
3. Inadvertent acquisition of economic or market information.
4. Inadvertent acquisition of information about individuals.
5. International fraud through illegal access to computer data banks with emphasis, in decreasing order of importance, on acquisition of founding data, economic data, law enforcement data and data about individuals.

6. Government intrusion on the rights of individuals.
7. Invasion of individual rights by the intelligence community.

These are examples of specific threats an organization or an individual (or an organisation on behalf of its employees) may feel the need to counter. The nature of the threat that concerns an organisation will vary greatly from set of circumstances to another. Fortunately, we can approach the problem from a different angle by looking at the generic types of threats that might be encountered.

Table 8.1 lists the types of threats that might be faced in the context of network security. The threats can be divided into the categories of passive threats and active threats (see Figure 8.2).

Passive Threats

The monitoring and/or recording of data while the data are being transmitted over a communications facility.

Release of Message Contents

The attacker can read packet headers to determine the location and identity of communicating hosts. The attacker can also observe the length and frequency of messages.

Active Threats

The unauthorised use of a device attached to a communication facility to alter transmitting data or control signals or to generate spurious data or control signals

Message-Stream Modification

The attacker can selectively modify, delete, delay, reorder The attacker can selectively and duplicate real messages.

Denial of Message Service

The attacker can destroy or delay most or all messages.

Masquerade

The attacker can pose as a real host or switch and communicate with another host or switch to acquire data or services.

1. **Passive Threats**

These are in the nature of eavesdropping or monitoring of the transmissions of an organisation. The goal of the attacker is to obtain information that is being transmitted. Two types of threats are involved here: release of message contents and traffic analysis.

The threat of message contents is clearly understood by most managers. A telephone conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent the attacker from learning the contents of these **transmissions.**

The second passive threat, traffic analysis is more subtle and often less applicable. Suppose that we had a way of masking the contents of messages or other information. Traffic so that an attacker, even if he or she captured the message, would be unable to extract the information from the message. The common technique for doing this is encryption, discussed at length subsequently. If we had such protection in place, it might still be possible for an attacker to observe the pattern of these messages. The attacker can determine the location and identity of communicating hosts and can also observe the frequency and length of the communication that is taking place.

Passive threats are very difficult to detect since they do not involve any alteration of the data. However, it is feasible to prevent these attacks from being successful. Thus the emphasis in dealing with passive threats is on prevention and not detection.

2. **Active Threats**

The second major category of threat is active threats. These involve some modification of the data stream or the creation of a false stream. We can subdivide these threats into three categories; message-stream modification, denial of message service and masquerade.

Message-stream modification simply means that some portion of a legitimate message is altered, Or that messages are delayed, replayed or recorded, in order to produce an unauthorised effect. For example, a message meaning " Allow J.N. Saxena to read confidential file accounts" is modified to mean "Allow F.C. Bansal to read confidential accounts".

The **denial of service** prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g. the security audit service). Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so a to degrade performance.

A **masquerade** takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other two forms of active attack. Such an attack can take place , for example, by capturing and replaying an authentication sequence.

Active threats present the opposite characteristics of passive threats. Whereas passive attacks are difficult to detect, measures are available to prevent their success. On the other hand, It is quite difficult to absolutely prevent active attacks, Since this would require physical protection of all communication facilities and paths at all times. Instead, the goal with respect to active attacks is to detect these attacks and to recover from any disruption or delays caused by the attack. Because the detection has a deterrent effect, this may also contribute to prevention.

EDI

Electronic data interchange (**EDI**) is an electronic communication method that provides standards for exchanging data via any electronic means. By adhering to the same standard, two different companies, even in two different countries, can electronically exchange documents (such as purchase orders, invoices, shipping notices, and many others).

In 1996, the National Institute of Standards and Technology defined electronic data interchange as "the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments. EDI implies a sequence of messages between two parties, either of whom may serve as originator or recipient. The formatted data representing the documents may be transmitted from originator to recipient via telecommunications or physically transported on electronic storage media." It distinguishes mere electronic communication or data exchange, specifying that "in EDI, the usual processing of received messages is by computer only. Human intervention in the processing of a received message is typically intended only for error conditions, for quality review, and for special situations. For example, the transmission of binary or textual data is not EDI as defined here unless the data are treated as one or more data elements of an EDI message and are not normally intended for human interpretation as part of online data processing

EDI was one of the earliest uses of Information technology for supply chain management. It involves the electronic exchange of business transaction documents over the internet and other networks between supply chain trading partners. Data representing a variety of business traction documents such as purchase orders, invoices, request for quotations etc., are automatically exchanged between computers using standard document message formats. EDI software is used to convert a company's own document formats into standardized EDI formats as specified by various industry and international protocols. Thus, it is an example of almost complete automation of an e-commerce supply chain process. EDI over the Internet uses the secure virtual private networks.

Formatted transaction data are transmitted over network links directly between computers without paper documents or human intervention. Besides direct network links between the computers of trading partners, third party services are widely used. Value added network companies like Global Exchange Services and Computer Associates offer a variety of EDI services for relatively high fees but many EDI service providers now offer secure, low cost EDI services over the Internet.

EDI is still a popular data transmission format among major trading partners, primarily to automate repetitive transactions. It automatically tracks inventory changes, triggers orders, invoices and other document related to transactions. It schemes and confirms the delivery and payment. By digitally integrating the supply chain, EDI saves time and increases the accuracy. In addition by using Internet technologies lower cost Internet based EDI services are now available to smaller businesses.

EDI Components

An EDI system consists of all of the components necessary to exchange EDI transactions with trading partners who are EDI capable. The major components are EDI translation software, user or system interfaces, hardware, maps, EDI guides, a communication network and EDI experienced personnel. A company that wants to be EDI capable will have to either buy the components or outsource all of the EDI system components to a third party.

EDI transactions are very compact and difficult to read and manipulate. EDI translation software provides the ability to translate EDI data into a file format that can be interfaced with a company's in-house systems or translated into forms that can be used by users.

EDI translation software supports the development and maintenance of maps. Maps are required to manipulate each transaction type. Every transaction type with every partner will be formatted differently. The map translates the EDI transaction into a useable file-format. EDI guides are provided by EDI trading partners to communicate how each transaction type will be formatted. The EDI guides must be followed exactly in order to be EDI compliant with a particular EDI partner. The EDI guides are used to develop maps.

Hardware is required to run EDI translation software. The computer hardware must be sufficiently powerful and reliable to support exchange of EDI transactions 24 X 7 in compliance with trading partners' transmission schedules. A communication network is necessary to send and receive EDI transactions. A company can elect to either communicate EDI transactions using a direct AS/2 connection to a trading partner if the trading supports such a connection, or communicate with trading partners using a VAN. A VAN is a third party network provider that is a communications intermediary with other trading partners. And perhaps most importantly, expertise is required to implement each of the EDI system components and maintain each of the specific maps for all of a company's EDI trading partners.

Three important components of EDI system are as follows:

Application Service

It enables the means of integrating existing or new applications into the EDI systems.

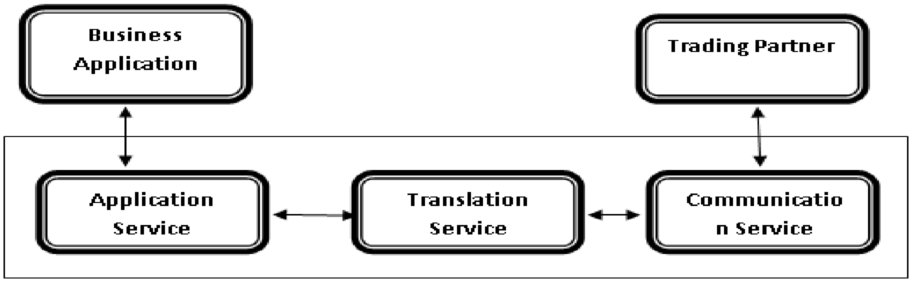


Fig – 2.1 EDI Components

Translation Service

It converts the data from internal format standards to an external format. Similarly, it translates the data from external format to an internal format standard.

Communication Service

It transfers the documents onto a network through the agreed communication protocol.

Process of EDI

EDI process comprises of the following:

Translation of business data: The EDI enabling software translates the outbound film form the business application into an EDI format.

Transmission and reception of data: The EDI document is transmitted between the trading partners based on message standard agreed between them.

Re-transmission of data: Once the EDI document is received, the recipient organisation using its own EDI enabling software retranslates the inbound document back into a format which can be used by its own business application.

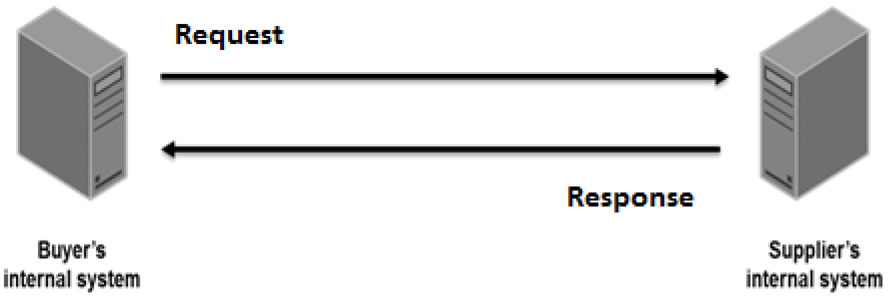


Fig – 2.2 EDI Process

Benefits of EDI

EDI technology allows a company to take advantage of the benefits of sorting and manipulating data electronically without the cost of manual entry.

Computer-to-computer

EDI replaces postal mail, fax and email. While email is also an electronic approach, the documents exchanged via email must still be handled by people rather than computers. Having people involved slows down the processing of the documents and also introduces errors. Instead, EDI documents can flow straight through to the appropriate application on the receiver’s computer (e.g., the Order Management System) and processing can begin immediately. A typical manual process looks like this, with lots of paper and people involvement.

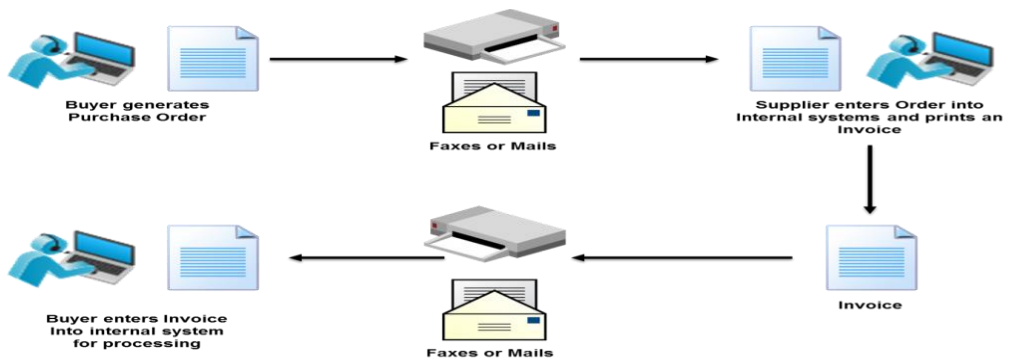

Buyer generates Purchase Order
Faxes or Mails
Supplier enters Order into Internal systems and prints an Invoice
Invoice
Faxes or Mails
Buyer enters Invoice Into internal system for processing

Fig – 2.3 computer to computer

Business documents

These are any of the documents that are typically exchanged between businesses. The most common documents exchanged via EDI are purchase orders, invoices and advance ship notices. But there are many, many others such as bill of lading, customs documents, inventory documents, shipping status documents and payment documents.

Standard format

EDI documents must be processed by computers rather than humans, a standard format must be used so that the computer will be able to read and understand the documents. A standard format describes what each piece of information is and in what format (e.g., integer, decimal, mm/dd/yy). Without a standard format, each company would send documents using its company-specific format and, much as an English-speaking person probably doesn't understand Japanese, the receiver's computer system doesn't understand the company-specific format of the sender's format.

There are several EDI standards in use today, including ANSI, EDIFACT, TRADACOMS and ebXML. And for each standard there are many different versions available. When two businesses decide to exchange EDI documents, they must agree on the specific EDI standard and version.

Businesses typically use an EDI translator – either as in-house software or via an EDI service provider – to translate the EDI format so the data can be used by their internal applications and thus enable straight through processing of documents.

Business partners

The exchange of EDI documents is typically between two different companies, referred to as business partners or trading partners. For example, Company A may buy goods from Company B. Company A sends orders to Company B. Company A and Company B are business partners.

Low Cost

EDI eliminates postage costs and other expenses which are involved in manual entries. There will be a quick flow of information worldwide at any time.

Speed

EDI also saves time over paper processing since the transfer of information from computer to computer is faster. EDI offers the ability to send and receive information at any time, improving the ability to communicate quickly and efficiently. Data automatically interchange with standardized formats. EDI eliminates the need to re-enter or rekey documents on the destination. Hence it greatly reduces the cycle times.

Accuracy

EDI format automatically changes back into the receiver's original format. Errors are reduced because data is not being re-keyed or re-entered.

Simplicity

EDI messages adhere to a set of rules and regulations governing the flow of electronic data, known as "protocols". The use of standardized data formats allows computer to exchange various business documents without a need of customizing the hardware and software system.

Security

EDI can be accessed only by authorized users. Data cannot be easily changed by unauthorized users. It is not subject to viruses. It helps in ensuring accuracy and security, by proper encryption methods; digital signatures or bio-metrics and the translation of software.

Competitive advantage

EDI can be used to form alliances between companies that provide advantages over competitors in several ways, including the ability to offer the lowest market prices and best customer services. Such alliances can also lead to newer or more innovative services.

EDI Security

Today, in paper driven systems there are many checks to ensure that the expected clerical errors are detected and corrected. The scrutiny of the pieces of paper by experienced clerical staff, for example, often identifies errors made by trading partners. In an EDI system, it is necessary to replace these procedures with new procedures that are at least as effective. The replacement not only involves the trading partners but also the other parties in the EDI system.

Whilst security procedures will be in place for each party to the EDI system, it is necessary to ensure that these procedures when taken together will provide security to the whole. Each of the parties contributing to the whole system will have different priorities-security is more important to some organizations than to others. Absolute security is impossibility, mistakes will happen, machines do break down, software does contain bugs. Management therefore need to determine how acceptable commercial security can be achieved in a cost-effective way.

Hijacking EDI Messages in Transit

It must be ensured that a message received is indeed from the organization stated. Otherwise, a competitor could use EDI to obtain sensitive information.

Compromised message integrity An authentic message may be hijacked and critical data altered before arrives at its destination. Messages may be duplicated either accidentally or intentionally. The duplicate message may appear genuine to the recipient because it is an exact copy of a genuine message.

Message repudiation It is important that the counterparty to a message cannot, at a later date, deny knowledge of the message or its contents.

Disclosure of confidential data When a message should be kept secret, how is it ensured that the data is not disclosed during transit?

Delayed messages Delays in delivering messages could have significant adverse effects.

Misrouted messages Misrouted messages may be altered in some way and or never reach the intended recipient.

Temporary or permanent EDI service loss Once an organization has taken full advantage of EDI it is unlikely to have capacity to resort to manual procedures to overcome these problems.

Security of EDI System while Creating, Processing and Data Retention

The security of messages cannot be considered in isolation – the systems and processes which result in transmission of messages and the handling of messages after they are received are as important as the transmission process itself. Some of these processes are:

Secure creation of outward messages, Secure processing of incoming messages and data retention.

Secure Creation of Outward Messages

Where manual input is used to the EDI system, there is very real danger of an incorrect data entry caused by a typing error. If automated input is used, the originating system may have a bug which results in the generation of incorrect input to the EDI system. Bugs within, or incorrect implementation of EDI translation software could result in the transmission of messages which do not comply with message standards.

While it is up the organisation to ensure that a message is from the organisation stated, message senders must prevent unauthorised persons from originating messages from their own systems. There is also a danger that a hacker could log into some organisations systems & generate a seemingly authentic message. There is an obvious need of control the message creation process, this can be achieved by making sure that existing system development and maintenance controls are applied strictly to EDI developments. Checks should be made to ensure that all messages which should be sent are actually sent. In addition, very tight procedural controls should be applied to the log-on Ids and staff's access and authorisation.

Secure Processing of Incoming Messages

Once an EDI message reaches the recipient it is still only part-way through its journey. Authenticity of the sender must be verified and the integrity of the message established. If necessary the receipt of the message should be acknowledged. The message must be translated into formats which can be used by the recipients own application systems. The authenticity and integrity of the message is dealt with under security mechanisms and procedures.

Message translation This is the translation of messages into formats that can be understood by the receiving computer applications.

Rejected messages The translation software should reject any messages that it is unable to process. These rejections should be promptly followed up and in most cases the sender should be asked to send a correct message.

Processing messages The controls over the processing of incoming messages can be handled manually, or through a combination of manual and automated control.

Monitoring controls To make sure that the controls work, a check should be made that no messages are lost between message receipt and the destination application.

Error detection and correction Many translation packages incorporate error detection and editing facilities which allow on-screen correction of errors. All changes and explanations for them should be logged.

Acting on messages It is necessary first of all to ensure that the messages are commercially acceptable and correct.

Data Retention

The primary purposes of data retention are

- Fulfil statutory and regulatory requirements
- Provide evidence of transactions
- Provide sources of information for recording organizational activity, accounting records for example; and
- Provide source of information for planning and marketing activities

Organizations should assess their own requirements for retaining data and develop a data-retention policy which is reflected in operating procedures. Care should be taken to avoid retaining too much data. Where low volumes of data are generated it can be easier to retain everything than to go through the process of identifying what is specifically required. The level of security over retained data will depend upon the intended use. The data retained should be protected against alteration, destruction and disclosure.

Security Management

In order to create cost-effective response to the varied technical and human threats to EDI Security, organisations should publish a security policy which makes clear to all management and staff the organisation’s attitude to security. Deriving from this policy, more detailed security requirements and procedures for specific EDI implementations can be created so that the obligations undertaken by the organisation under the EDI contracts can be demonstrably fulfilled. These requirements can be used in the selection of the security facilities and the implementation of security procedures. The policy definition should go hand in hand with an analysis of the risks, possibly using a formal risk analysis methodology.

Risk analysis Over the past few years a number of risk analysis methodologies have been developed. These seek to measure the cost of a loss and multiply it by an estimate of the frequency of the loss in a given period producing a rank list of the risks. The analysis can be applied to EDI messages and the procedures surrounding their creation and receipt – the risk ranking will vary according to the message type and the area of business.

Managing the risks the use of risk analysis will identify the risk an organisation is exposed to in using EDI and establish the priority in which these risks require to be minimized.

The first step should be to reduce your exposure to risks which cannot be controlled internally. The organisation’s internal risks also require being limited.

For example: making sure that the translation software is functioning properly, the physical and logical access controls are adequate, the clerical procedures are keeping pace with the computer systems and back-ups are adequate and tested.

Never get security out of perspective – security is a mainstream business requirement and has to complement the functions of EDI systems. Only cost – effective security can achieve the aim of secure inter-company European and global, electronic trading.

Confidentiality

Confidentiality requires that all communications between parties are restricted to the parties involved in the transaction. This confidentiality is an essential component in user privacy, as well as in protection of proprietary information and as a deterrent to theft of information services. Confidentiality is concerned with the unauthorized viewing of confidential or proprietary data that one or both of the trading partners does not want known by others. Confidentiality is provided by encryption.

Encryption is the scrambling of data so that it indecipherable to anyone except the intended recipient. Encryption prevents snoopers, hackers, and other prying eyes from viewing data that is transmitted over telecommunications channels. There are two basic encryption schemes, private-key and public-key encryption. Encryption, in general, is cumbersome and expensive.

Private-key encryption requires that both sending and receiving parties have the same private-encryption keys. The sender encrypts the data using his key. The receiver then decrypts the message using his identical key. There are several disadvantages to private-key encryption. In order to remain secure, the keys must be changed periodically and the users must be in synch as to the actual keys being used.

Public-key encryption is gaining wide spread acceptance as the preferred encryption technology. With public-key encryption, a message recipient generates a matched set of keys, one public key and one private key. The recipient broadcasts the public key to all senders or to a public location where the key can be easily retrieved. Any sender who needs to send the receiver an encrypted message uses the recipient's public key to encrypt the message. The private key, which is held in private by the recipient, is the only key that can decipher messages encrypted with the matched public key. This schema requires that the private key cannot be generated from the public key.

Public key technology is the direction encryption technology is currently headed. With the advent of X.500, databases will be built to store public keys and enhance the technology significantly.

Authentication

Both parties should feel comfortable that they are communicating with the party with whom they think they are doing business. A normal means of providing authentication is through the use of passwords.

The latest technology to provide authentication is through the use of digital certificates that function much like ID cards. The digital certificate has multiple functions, including browser authentication.

Data Integrity

Data sent as part of a transaction should not be modifiable in transit. Similarly, it should not be possible to modify data in storage. Data integrity is a guarantee that what was sent by the sender is actually what is received by the receiver. This is necessary if there is a need to ensure that the data has not been changed either inadvertently or maliciously. However, authentication schemes do not hide data from prying eyes.

Providing data integrity is generally cumbersome and not used unless one of the trading partners requires it. The normal mechanism for acquiring data integrity is for the sender to run an algorithm against the data that is being transmitted and to transmit the result of the algorithm separately from the transmission. Upon receipt of the transmission, the receiver runs the identical algorithm and then compares the results. If the results are identical, then data has not been modified.

Non-repudiation

Neither party should be able to deny having participated in a transaction after the fact. The current technology ensures this through the use of digital signatures.

Electronic signatures are the computerized version of the signature function. Signatures are needed in some business applications for authorization purposes. For example, a contracting officer may have a specified spending limit, say $25,000. If that contracting officer decides to place an order for $30,000, the seller may not have the authority to fill the order because the signature of the contracting officer's supervisor is needed on all orders over $25,000. The authorization limits normally will have been agreed upon through a trading partner agreement.

A digital signature algorithm can be used to generate digital signatures. The digital signature itself is used to detect unauthorized modification to data and to authenticate the identity of the signature. The digital signature is also useful to the recipient as a non-repudiation device whereby the recipient can prove to a third party that the signature was in fact generated by the signatory. Thus the signatory cannot repudiate the signature at a later date.

Security Management

In order to create cost-effective response to the varied technical and human threats to EDI Security, organisations should publish a security policy which makes clear to all management and staff the organisation's attitude to security. Deriving from this policy, more detailed security requirements and procedures for specific EDI implementations can be created so that the obligations undertaken by the organisation under the EDI contracts can be demonstrably fulfilled. These requirements can be used in the selection of the security facilities and the implementation of security procedures. The policy definition should go hand in hand with an analysis of the risks, possibly using a formal risk analysis methodology.

Risk analysis Over the past few years a number of risk analysis methodologies have been developed. These seek to measure the cost of a loss and multiply it by an estimate of the frequency of the loss in a given period producing a rank list of the risks. The analysis can be applied to EDI messages and the procedures surrounding their creation and receipt – the risk ranking will vary according to the message type and the area of business.

Managing the risks the use of risk analysis will identify the risk an organisation is exposed to in using EDI and establish the priority in which these risks require to be minimized.

The first step should be to reduce your exposure to risks which cannot be controlled internally. The organisation's internal risks also require being limited.

For example: making sure that the translation software is functioning properly, the physical and logical access controls are adequate, the clerical procedures are keeping pace with the computer systems and back-ups are adequate and tested.

Never get security out of perspective – security is a mainstream business requirement and has to complement the functions of EDI systems. Only cost – effective security can achieve the aim of secure inter-company European and global, electronic trading.

Security Issues

Information Assurance Services works closely with IT Services. IT Services are able to monitor computer and network usage in order to protect University assets and services. Maintaining computer security involves implementing suitable preventative measures, detecting potential vulnerabilities, detecting possible threats, detecting compromised systems and handling incidents.

The term misuse covers various activities including:

- **Hacking** unauthorized access to or use of data, systems, server or networks, including any attempt to probe, scan or test the vulnerability of a system, server or network or to breach security or authentication measures without express authorization of the owner of the system, server or network. Members of the University should not run computer programs that are associated with hacking without prior authorisation. Obtaining and using such programs is not typical of normal usage and may therefore otherwise be regarded as misuse.
- Use of University owned computer equipment, including the network, for illegal activities including copying Copyright material without permission. The vast majority of files shared on **P2P (peer-to-peer)** networks violate copyright law because they were posted without permission of the artist or label.
- Sending **abusive e-mails** or posting offensive Web pages.
- Creation or transmission of any offensive or indecent images.
- Giving unauthorised access to University computing resources e.g. allowing an account to be used by someone not authorised to use it.
- Deliberately creating or **spreading computer viruses** or worms.
- Unauthorised running of applications that involve committing the University to sharing its computing resources, e.g. network bandwidth, in an uncontrolled and unlimited way.

The most common types of **violations** include:

- **Breach of Confidentiality -** Theft of private or confidential information, such as credit-card numbers, trade secrets, patents, secret formulas, manufacturing procedures, medical information, financial information, etc.
- **Breach of Integrity -** Unauthorized **modification** of data, which may have serious indirect consequences. For example a popular game or other program's source code could be modified to open up security holes on users systems before being released to the public.
- **Breach of Availability -** Unauthorized **destruction** of data, often just for the "fun" of causing havoc and for bragging rites. Vandalism of web sites is a common form of this violation.
- **Theft of Service -** Unauthorized use of resources, such as theft of CPU cycles, installation of daemons running an unauthorized file server, or tapping into the target's telephone or networking services.
- **Denial of Service, DOS -** Preventing legitimate users from using the system, often by overloading and overwhelming the system with an excess of requests for service.
- One common attack is **masquerading,** in which the attacker pretends to be a trusted third party. A variation of this is the **man-in-the-middle,** in which the attacker masquerades as both ends of the conversation to two targets.
- A **replay attack** involves repeating a valid transmission. Sometimes this can be the entire attack, (such as repeating a request for a money transfer), or other times the content of the original message is replaced with malicious content.

Security Basics

Vulnerabilities of various Computer systems

People who fall in love with the Net do so for different reasons. Many love the ability to quickly and cheaply keep up with friends and loved ones via e-mail, while others love the vast oceans of information or the rush of playing Internet games.

However, it's likely that most Internet users share one thing in common as they surf: the last thing on their minds is computer security.

While that's understandable, it's also a big mistake. It is important to remember that surfing the Net comes with certain inherent risks. When user log onto the Net, they step into the public arena, even if they're surfing from a bedroom computer while lounging around in their skivvies!

Here are as many bad guys in cyberspace as there are in everyday life, and those shady characters are constantly prowling the Internet in search of new victims to scam.
However, the media often exaggerate these dangers. It is extremely unlikely (though not impossible) that anyone reading this article will fall prey to an Internet crime, and in truth the risks are not much greater than those associated with many fun activities.

The potential of breaking a bone keep user from enjoying their favorite ski slope or bike trail.Of course not. Instead, the smart person uses the necessary caution that will allow for a safe and enjoyable experience.

That ethos also applies to those who want to surf the Web safely. There are countless ways that thieves and mischief makers can wreak havoc with their sense of security, but there are just as many ways to keep intruders at bay via safe-surfing techniques or security software.

Latest Security

For a basic overview of Internet and computer security issues, stop by Security Focus . This site bills itself as the "largest and most comprehensive database of security knowledge and resources freely available to the public."

Here, they'll find pages devoted to the latest security news, information about the vulnerabilities of various systems, reviews of security tools and software, a library of online security information and more. User can also sign up for the BugTraq e-mail updates that keep user abreast of the latest vulnerabilities.

Admittedly, this site is not exactly light reading. But it offers comprehensive coverage of security issues.

Online security risks exist only when a computer is actually connected to the Internet. Anyone who connects to the Net via a phone modem is potentially at risk when they are logged on, but the danger of a new attack upon security disappears as soon as they log off.

It's a different story for those with broadband connections. In essence, a broadband link gives user continuous access to the Net 24 hours a day. Those considering the speed and quality advantages of broadband and mobile broadband should also weigh this additional, very small risk in their decision process.

Building Firewalls

Unleashing viruses and stealing e-mail content are two major threats to their computer's security. But they are hardly the only threats. Information that is stored on their computer is potentially vulnerable to attack. That's why users might consider building their own firewall to keep intruders out. Think of a firewall as a heavy steel, dead-bolted front door that protects all the valuables behind it.

Whenever user log onto the Net, and type in a Web address, user are requesting a page that comes to user via an IP address. Basically, the IP address is a numerical translation of the address that they've just typed in - for example www.allaboutcookies.org is translated into a series of numbers that allows a computer to search for the information they've requested and to send it back to user.

Pretty neat, but there's also a potential downside. In order to receive the information, user too must have an IP address, and it is this address that makes user vulnerable to hackers looking to do naughty things to their computer.

Those with dial-up connections receive a new IP address each time they log on, making them less vulnerable to attack than broadband users, who have a constant, static address. But the risks are real for both groups.

Once hackers get into their IP address, they do their damage by accessing applications through a virtual channel called a port number. Firewall software prevents incoming requests from accessing these ports.

Those looking for more sophisticated protection can purchase software from companies such as Symantec or McAfee . Less comprehensive protection can be obtained via a free download at Zone Labs' Zone Alarm.

Authentication

Authentication is the process to determine who they claim to be. Authentication is accomplished using something the user knows (e.g. password), something the user has (e.g. security token) or something of the user (e.g. biometric).

The authentication process is based on a measure of risk. High risk systems, applications and information require different forms of authentication that more accurately confirm the user's digital identity as being who they claim to be than would a low risk application, where the confirmation of the digital identity is not as important from a risk perspective. This is commonly referred to as "stronger authentication".

Authentication processes are dependant upon identity verification and registration processes. For example, when Jane Doe is hired at an enterprise, she provides the enterprise with information and tokens of who she is (e.g. name, address, driver's license, birth certificate, a SSN number, a passport, etc.). The enterprise may choose to immediately accept this information or, it may instead chose to run background checks on Jane to see if she is who she claims to be and determine if she has any criminal record. When the checks come back favorably, the enterprise will accept her identity and enter her into their systems. The identity registration process will usually involve issuing Jane with enterprise authentication mechanisms such as id and password, security token, digital certificate and/or registering some of her biometrics.

The authentication process is totally dependent on the identity validation and registration process used for Jane. If Jane presents false tokens, which are accepted by the enterprise, then the person acting as Jane will be positively authenticated every time, even though she is not the real Jane Doe. Authentication security therefore is only as good as the weakest link in the chain.

General Authentication

Password Authentication

Password authentication is the most common method of authentication. It is also the least secure. Password authentication requires the identity to input a user id and a password in order to login. Password length, type of characters used and password duration are password management are now critical concern in enterprises. The ability to easily crack passwords has resulted in high levels of identity theft. As a result, the high risk of passwords means most enterprises now deploy a layered security strategy. A user enters in their id and password for initial login to gain access to only low risk information and applications with other forms of authentication required for higher risk information and applications.

Single Sign On Authentication

Single Sign On (SSO), Reduced Sign On (RSO), or Enterprise Single Sign On (ESSO) is the ability to reduce the number of id's and passwords a user has to remember. In most enterprises, a strong business case can be made to implement single sign on by reducing the number of password related help desk calls. SSO is also the architecture to require stronger forms of authentication for higher risk information and applications. Thus a user may login using their id and password to gain general low risk access to an enterprise. The SSO software enables them to not have to use multiple id's and passwords. However, when the user tries to access more sensitive information and applications, the single sign on software will require the identity to input stronger authentication such as a security token, a digital certificate and/or a biometric.

Lightweight Directory Access Protocol (LDAP) Authentication

Most enterprises use Lightweight Directory Access Protocol (LDAP) directories to handle the centralized authentication. LDAP directories, such as Active Directory, Sun One Directory, Novel e-Directory and other vendors, provide a low cost way of doing fast identity look-ups and authentication as compared to traditional databases. Today it is also common to use virtual LDAP directories to quickly integrate the identity and authentication information contained in one or more databases and/or other LDAP directories. The use of these directories is a critical piece of identity infrastructure that leads to integrating access control.

Access Control Authentication

Access control is the process of granting an identity the ability to physically or electronically access a facility or enterprise. By using LDAP directories and single sign on, many enterprises now integrate their building access control security cards, employee time keeping and other access control accessories into their LDAP identity management system. This reduces the number of identity database silos, since most access control systems use their own identity databases. It also reduces the number of access control accessory systems.

Network Authentication

Network authentication is the process of granting an identity the ability authenticate to a network as well as their authorization. Almost all network authentication systems are now LDAP based. This includes Microsoft 2000, Linux, Solaris, AIX and HPUX. Many mainframe authentication systems such as RACF are now LDAP enabled.

Biometric Authentication

Biometric authentication s is the process of taking a "piece of user", digitizing it and then using this to authenticate against an identity directory or database. Typical types of biometric authentications include finger scans, digital finger prints, hand scans, retina scans, digital signature scans and others. The use of DNA biometrics is increasingly used in identity verification (the initial identity registration step prior to authentication). Biometrics are commonly used as part of an array of authentication methods used in enterprises.

Strong Authentication

Strong authentication means higher trust of an authentication. For instance, the successful login using a id and password will be given a low level of trust by the enterprise since the id and password are easily obtained by social engineering or password cracking. Stronger authentication methods include digital certificates, security tokens and biometrics. Often, many enterprises use combinations of these including passwords, to place a higher degree of trust for higher risk applications or information access.

Transaction Authentication

Transaction authentication is the process of using other authentication determinants to verify an identity. Often used by financial institutions for higher risk customers or transactions, the transaction software looks at the IP address the user is coming in on, the identity's computer hardware they're using, the time of day, the geo-location the identity is coming from, etc. If the identity successfully logs on using a id and password BUT the other components are not usual, the transaction authentication software may stop a process, flag in real time an administrator and/or ask the user more questions to have more confidence the identity is who they claim to be.

Federated Authentication

Federated authentication is the ability to trust an incoming electronic identity to the enterprise from a trusted partner or website. Protocols enabling this include SAML, Liberty Alliance, Web Services Federation and Shibboleth. When combined with enterprise single sign on systems, the user experience is improved since they no longer have to remember another id and password. Further, enterprise identity authentication standards can be automatically enforced on external identities using the enterprise systems. Identity authentication federation also works in reverse for enterprise employees who access there 401k, benefits, etc, to outside supplier websites. By using federated authentication, the identity doesn't need to remember another separate id and password.

PKI Authentication

Public key infrastructure (PKI) authentication, is another way of doing identity authentication. An identity is given a digital certificate by an Certificate Authority (CA). This is then presented during the authentication process to verify an identity is who they say they are. The level of authentication trust varies for digital certificates depending on the level of identity verification done during the identity registration process as well as the digital certificate revocation process. Digital certificates are becoming more important to authenticate and verify an identity in single sign on systems, document management systems and in web services.

Security Token Authentication

Security token authentication, such as RSA secureID tokens, are used to authenticate an identity (something that user have). During the login process, or if required by a single sign on system for a higher risk application, the identity is required to enter in the numbers appearing on the token screen along with their id. Since the numbers change randomly to the user viewing the screen (but is understood by the central authentication server), there is a higher degree of trust associated with this form of authentication. However, operating costs for security authentication tokens are higher than the use of password and id since they must be physically issued, replaced and recovered.

Smart Card Authentication

Smart cards are another form of authentication token (something user have). Often they contain a digital certificate as well as additional identity attribute information. Smart card authentication is becoming wide spread. The same smart cards used in an authentication process are now commonly used as well for access control mechanisms to enter physical facilities, buildings, floors and rooms.

Authentication Management

Authentication management is the overall process of managing identities and their authentication mechanisms. In most enterprise authentication management involves authentication policies and processes to manage passwords, digital certificates, security tokens, access control, biometrics, smart cards, LDAP directories, transaction authentication, single sign on and identity authentication federation. Strong business cases can be made to lower authentication costs while at the same time strengthening overall enterprise security.

Wireless Authentication

Authenticating wireless devices is today becoming a main enterprise security issue. Often, the authentication used is very insecure or easily breached. There are however ways to increase reliability that the user is who they claim to be by using multi-factor authentication.

Document Authentication

Formerly separate document authentication systems are now becoming intertwined with enterprise identity and authentication mechanisms. Gone are the days of relying upon mostly passwords to authenticate users trying to open document. Formerly separate document authentication systems are now becoming intertwined with enterprise identity and authentication mechanisms. Gone are the days of relying upon mostly passwords to authenticate users trying to open documents.

Outsourcing Authentication

Many modern enterprises have outsourced portions of their authentication development, maintenance and troubleshooting. If done well it can save the enterprise money. If done poorly, it can create security holes or, cause enterprise failures.

Firewalls implement the authentication process:

Most operating systems are equipped with authentication schemes. Web servers can be configured to authenticate clients who want to access certain protected content. Firewalls, too, can perform user authentication. In fact, many organizations depend on firewalls to provide more secure authentication than conventional systems. Authentication is a key function because firewalls exist to give external users access to protected resources.

A firewalls uses authentication to identify individuals so that it can apply rules that have been associated with those individuals. Some firewalls use authentication to give employees access to common resources such as the web or file transfer protocol(FTP).Some identify the user associated with a particular IP address ;after the user is authorized, the IP address can then be used to send and receive information with hosts on the internal network.

The exact steps that firewalls follow to authenticate users may vary, but the general process is the same:

1. Client makes request to access a resource
2. Firewall intercepts the request and prompts the user for name and password
3. User submits information to firewall
4. User is authenticated
5. Request is checked against firewall’s rule base
6. If request matches existing allow rule, user is granted access
7. User accesses desired resources

The “plain English” version of the exchange between external client and authenticating firewall is illustrated in figure

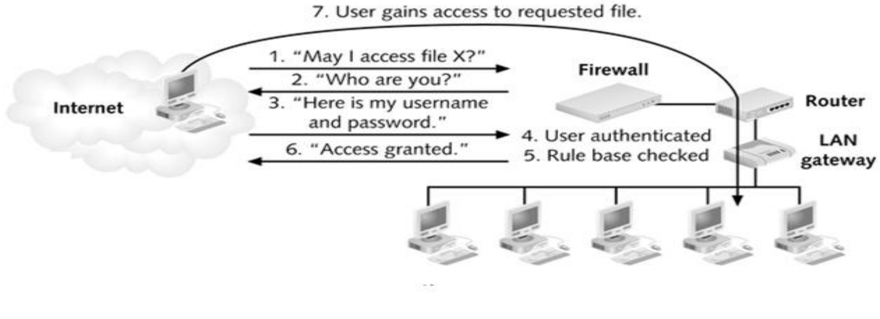


Fig 3.2 Basic external authentication

Strong Authentication

Passkeys: User password is mapped to a one-way has-function to generate a cryptographic key. Such password-derived keys are known as passkeys.The passkey is used to secure communication link between user and the system.

One time passwords: A special equipment generates a pseudorandom number which is used as password. The password is changed every minute and is time synchronized to the database stored in the computer. This method is expensive because of the additional hardware.

Challenge response protocol: In proof of knowledge method using passwords, the user discloses the passwords to prove the knowledge of the shared secrete. Whereas, in the challenge-response method, a user provides his/her identity by responding correctly to the challenge asked by the verifier. For example, the user and the system agree on function f=x2+5.when the user logs in, the system randomly selects a number say 10 and sends it to user ,the user has to reply with number 105 for valid authentication.

Protecting Password

A strong password is one that's hard to crack. A strong password must have all of the following:

- User password must be no fewer than eight (8) characters in length. **However, a good choice is a "pass phrase" composed of four (4) words and punctuation.** A pass phrase is a longer version of a password and is therefore more secure. A pass phrase is typically composed of multiple words.
  - Note: Though technology constraints may impose maximum length or other restrictions, use of pass phrases shall be supported where possible and practical.
  - Examples of pass phrases:
    - I like ice cream.
    - Turn Off Cell Phones!
    - It was hot today.
    - Cal Poly Broncos rule!
- At least three of the following four types of characters:
  - It must have at least one number.
  - It must have at least one uppercase letter.
  - It must have at least one lowercase letter.
  - It must have at least one symbol (!,@,#,$,^).

Examples of Extremely Bad Passwords

- The name in any form - first, middle, last, maiden, spelled backwards, nickname or initials
- The user ID spelled backwards
- Part of user ID or name
- Any common name, such as Joe
- The name of a close relative, friend or pet
- The phone number, office number or address, birthday or anniversary date
- Simple variants of names or words (even foreign words), simple patterns, famous equations or well-known values
- The favorite sports team (NFL, NBA, MLB, etc.)
- The license plate number, user social security number or any all-numeral password
- Names from popular culture (e.g.: Beatles, Spiderman, etc.)

Creating a Stronger Password

The user should follow these guidelines when creating a password:

- Do not use user name or any part of user real name.
- Do not use a single word in a common language. There are tools for hackers that search through electronic dictionaries, trying every word.
- Avoid characters other than those above, such as accented characters (áèôü) or characters from other alphabets (Ρωσικά, Греческий). The basic system will handle these passwords, but user may not be able to enter them correctly on web pages.
- Spell a word backwards (anomopyloplac1#).
- Insert a number (calpo7lyPomona) or punctuation (go!Broncos).
- Use weird capitalization (remember that it counts), or combine words (broNCOsrOOL!)).

- Use the first letters of each word in a phrase (“I can never remember my stupid password!” = Icnrmsp!).
- Combine things user will remember ("I like to eat broccoli and listen to Beethoven = broCColi@bEEthoven).
- Consider using a pass phrase instead of a password.

Viruses

According to Webster's *Collegiate Dictionary*, a computer virus is "a computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs or files, and that usually performs a malicious action (such as destroying data)". Computer viruses are never naturally occurring; they are always man-made. Once created and released, however, their spread is not directly under human control.

- **Macro viruses:** A macro is a piece of code that can be embedded in a data file. A macro virus is thus a virus that exists as a macro attached to a data file. In most respects, macro viruses are like all other viruses. The main difference is that they are attached to data files (i.e., documents) rather than executable programs.
  Document-based viruses are, and will likely continue to be, more prevalent than any other type of virus.
- **Worms:** Worms are very similar to viruses in that they are computer programs that replicate functional copies of themselves (usually to other computer systems via network connections) and often, but not always, contain some functionality that will interfere with the normal use of a computer or a program. Unlike viruses, however, worms exist as separate entities; they do not attach themselves to other files or programs. Because of their similarity to viruses, worms also are often referred to as viruses.
- **Trojan horses:** A Trojan horse is a program that does something undocumented which the programmer intended, but that users would not accept if they knew about it. By some definitions, a virus is a particular case of a Trojan horse, namely, one which is able to spread to other programs (i.e., it turns them into Trojans too). According to others, a virus that does not do any deliberate damage (other than merely replicating) is not a Trojan. Finally, despite the definitions, many people use the term "Trojan" to refer only to a non-replicating malicious program.

Program Threats

- There are many common threats to modern systems. Only a few are discussed here.

Trojan Horse

- A ***Trojan Horse*** is a program that secretly performs some maliciousness in addition to its visible actions.
- Some Trojan horses are deliberately written as such, and others are the result of legitimate programs that have become infected with ***viruses,*** (see below.)
- One dangerous opening for Trojan horses is long search paths, and in particular paths which include the current directory (".") as part of the path. If a dangerous program having the same name as a legitimate program (or a common mis-spelling, such as "sl" instead of "ls") is placed anywhere on the path, then an unsuspecting user may be fooled into running the wrong program by mistake.
- Another classic Trojan Horse is a login emulator, which records a users account name and password, issues a "password incorrect" message, and then logs off the system. The user then tries again (with a proper login prompt), logs in successfully, and doesn't realize that their information has been stolen.
- Two solutions to Trojan Horses are to have the system print usage statistics on logouts, and to require the typing of non-trappable key sequences such as Control-Alt-Delete in order to log in. (This is why modern Windows systems require the Control-Alt-Delete

sequence to commence logging in, which cannot be emulated or caught by ordinary programs. I.e. that key sequence always transfers control over to the operating system.)

- ***Spyware*** is a version of a Trojan Horse that is often included in "free" software downloaded off the Internet. Spyware programs generate pop-up browser windows, and may also accumulate information about the user and deliver it to some central site. (This is an example of ***covert channels,*** in which surreptitious communications occur.) Another common task of spyware is to send out spam e-mail messages, which then purportedly come from the infected user.

Trap Door

- A ***Trap Door*** is when a designer or a programmer (or hacker) deliberately inserts a security hole that they can use later to access the system.
- Because of the possibility of trap doors, once a system has been in an untrustworthy state, that system can never be trusted again. Even the backup tapes may contain a copy of some cleverly hidden back door.
- A clever trap door could be inserted into a compiler, so that any programs compiled with that compiler would contain a security hole. This is especially dangerous, because inspection of the code being compiled would not reveal any problems.

Logic Bomb

- A ***Logic Bomb*** is code that is not designed to cause havoc all the time, but only when a certain set of circumstances occurs, such as when a particular date or time is reached or some other noticeable event.
- A classic example is the ***Dead-Man Switch***, which is designed to check whether a certain person (e.g. the author) is logging in every day, and if they don't log in for a long time (presumably because they've been fired), then the logic bomb goes off and either opens up security holes or causes other problems.

Stack and Buffer Overflow

- This is a classic method of attack, which exploits bugs in system code that allows buffers to overflow. Consider what happens in the following code, for example, if argv[1] exceeds 256 characters:
  - The strcpy command will overflow the buffer, overwriting adjacent areas of memory.
  - (The problem could be avoided using str***n***cpy, with a limit of 255 characters copied plus room for the null byte.)

```
#include
#define BUFFER_SIZE 256

int main( int argc, char * argv[ ] )
{
   char buffer[ BUFFER_SIZE ];

   if( argc < 2 )
      return -1;
   else {
      strcpy( buffer, argv[ 1 ] );
      return 0;
   }
}
```

Figure 2 - C program with buffer-overflow condition.

- So how does overflowing the buffer cause a security breach? Well the first step is to understand the structure of the stack in memory:
    - The "bottom" of the stack is actually at a high memory address, and the stack grows towards lower addresses.
    - However the address of an array is the lowest address of the array, and higher array elements extend to higher addresses. (I.e. an array "grows" towards the bottom of the stack.
    - In particular, writing past the top of an array, as occurs when a buffer overflows with too much input data, can eventually overwrite the return address, effectively changing where the program jumps to when it returns.

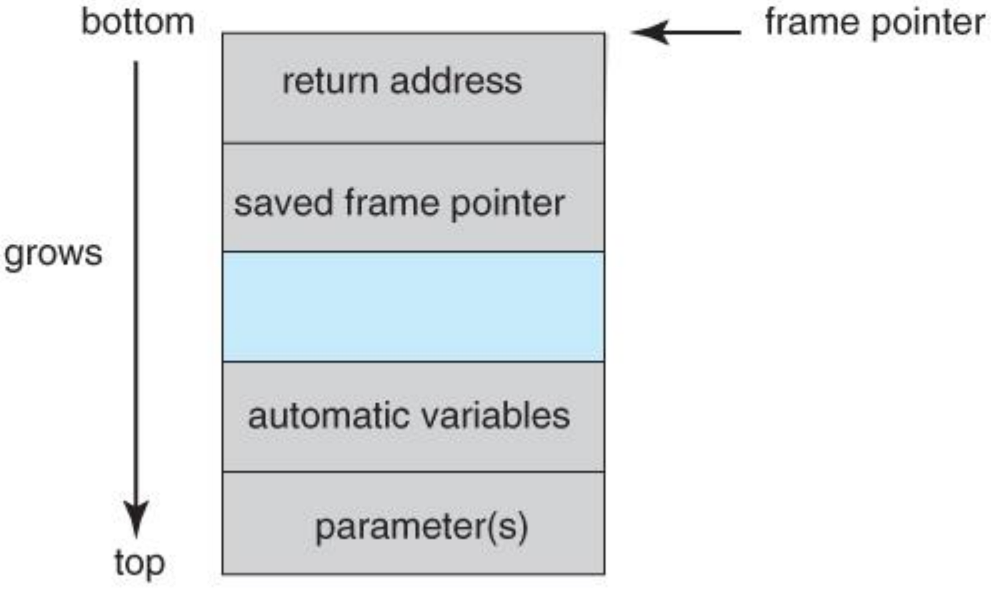


Figure.3 - The layout for a typical stack frame.

- Now that we know how to change where the program returns to by overflowing the buffer, the second step is to insert some nefarious code, and then get the program to jump to our inserted code.
- Our only opportunity to enter code is via the input into the buffer, which means there isn't room for very much. One of the simplest and most obvious approaches is to insert the code for "exec(/bin/sh)". To do this requires compiling a program that contains this instruction, and then using an assembler or debugging tool to extract the minimum extent that includes the necessary instructions.
- The bad code is then padded with as many extra bytes as are needed to overflow the buffer to the correct extent, and the address of the buffer inserted into the return address location. (Note, however, that neither the bad code or the padding can contain null bytes, which would terminate the strcpy.)
- The resulting block of information is provided as "input", copied into the buffer by the original program, and then the return statement causes control to jump to the location of the buffer and start executing the code to launch a shell.

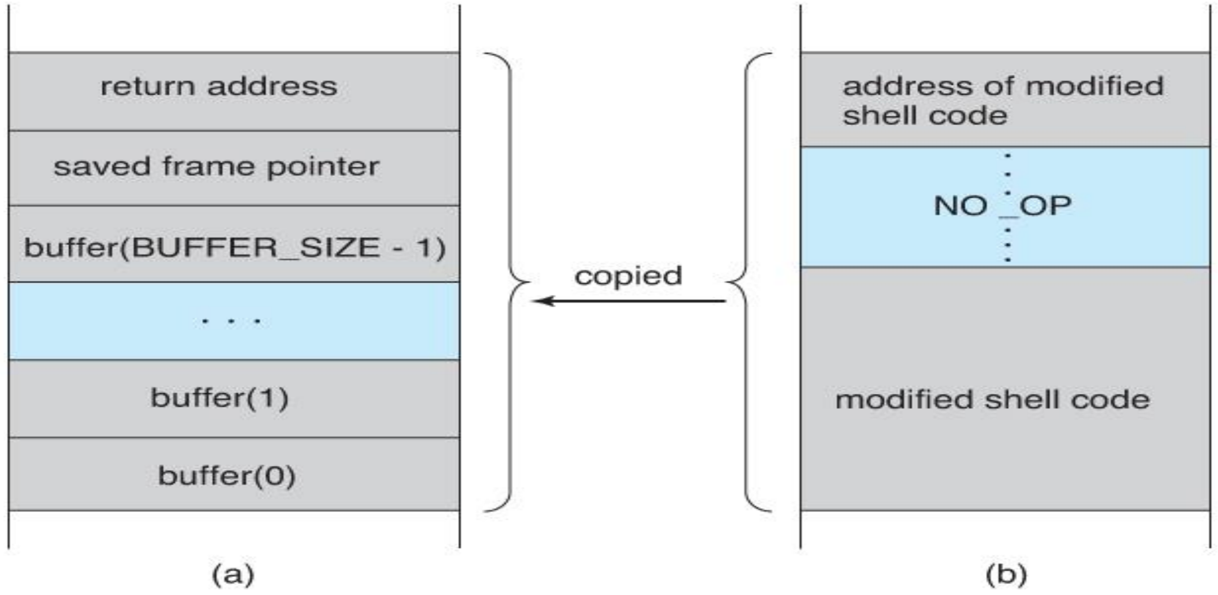


Figure - Hypothetical stack frame for Figure 15.2, (a) before and (b) after.

- Unfortunately famous hacks such as the buffer overflow attack are well published and well known, and it doesn't take a lot of skill to follow the instructions and start attacking lots of systems until the law of averages eventually works out. (***Script Kiddies*** are those hackers with only rudimentary skills of their own but the ability to copy the efforts of others.)
- Fortunately modern hardware now includes a bit in the page tables to mark certain pages as non-executable. In this case the buffer-overflow attack would work up to a point, but as soon as it "returns" to an address in the data space and tries executing statements there, an exception would be thrown crashing the program.
- (More details about stack-overflow attacks are available on-line from http://www.insecure.org/stf/smashstack.txt)

Viruses

- A virus is a fragment of code embedded in an otherwise legitimate program, designed to replicate itself (by infecting other programs), and (eventually) wreaking havoc.
- Viruses are more likely to infect PCs than UNIX or other multi-user systems, because programs in the latter systems have limited authority to modify other programs or to access critical system structures (such as the boot block.)
- Viruses are delivered to systems in a ***virus dropper,*** usually some form of a Trojan Horse, and usually via e-mail or unsafe downloads.
- Viruses take many forms (see below.) Figure 15.5 shows typical operation of a boot sector virus:

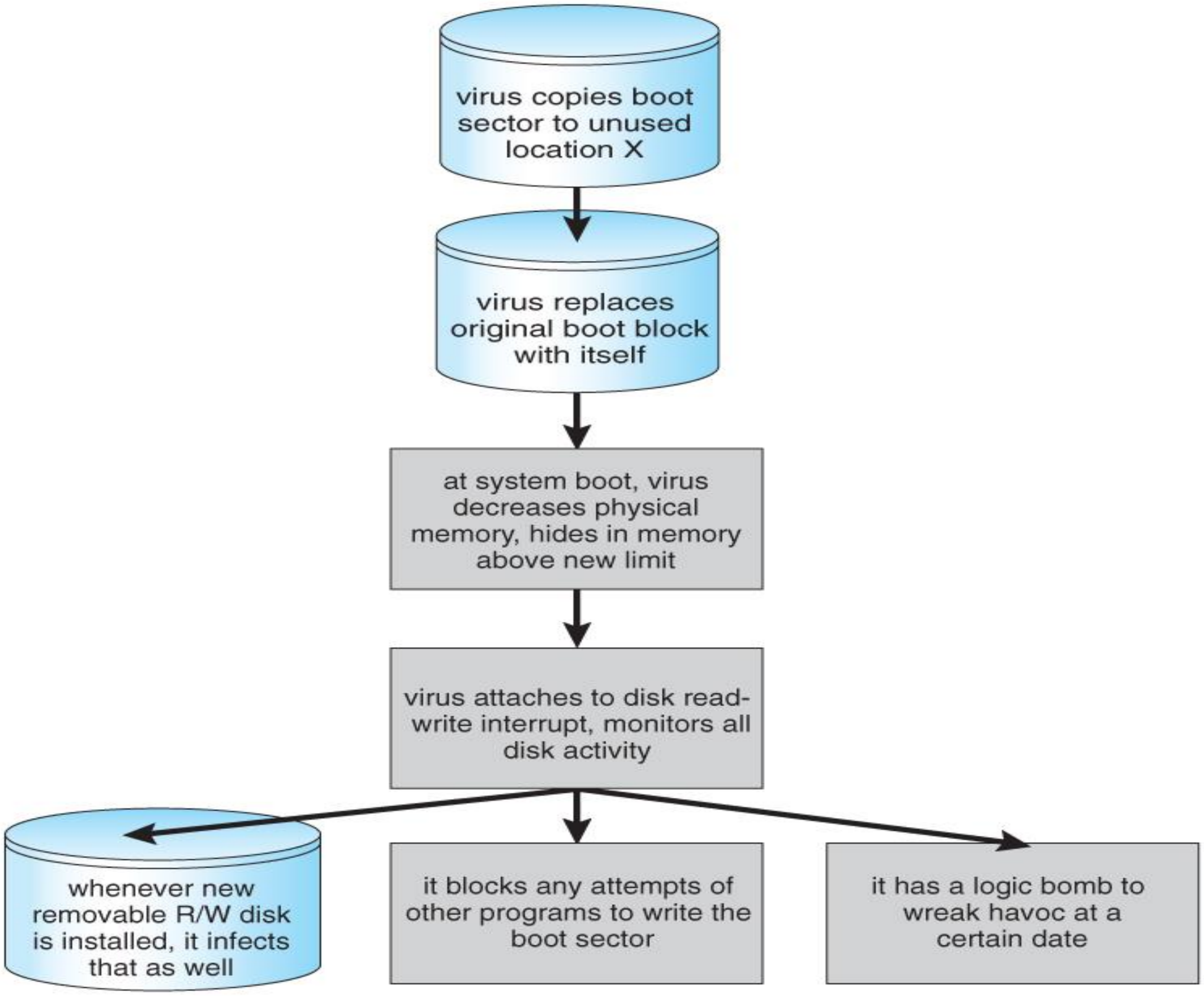

virus copies boot sector to unused location X
virus replaces original boot block with itself
at system boot, virus decreases physical memory, hides in memory above new limit
virus attaches to disk read-write interrupt, monitors all disk activity
whenever new removable R/W disk is installed, it infects that as well
it blocks any attempts of other programs to write the boot sector
it has a logic bomb to wreak havoc at a certain date

Figure 5 - A boot-sector computer virus.

- Some of the forms of viruses include:
  - **File -** A file virus attaches itself to an executable file, causing it to run the virus code first and then jump to the start of the original program. These viruses are termed ***parasitic,*** because they do not leave any new files on the system, and the original program is still fully functional.
  - **Boot -** A boot virus occupies the boot sector, and runs before the OS is loaded. These are also known as ***memory viruses***, because in operation they reside in memory, and do not appear in the file system.
  - **Macro -** These viruses exist as a macro (script) that are run automatically by certain macro-capable programs such as MS Word or Excel. These viruses can exist in word processing documents or spreadsheet files.
  - **Source code** viruses look for source code and infect it in order to spread.
  - **Polymorphic** viruses change every time they spread - Not their underlying functionality, but just their ***signature,*** by which virus checkers recognize them.
  - **Encrypted** viruses travel in encrypted form to escape detection. In practice they are self-decrypting, which then allows them to infect other files.
  - **Stealth** viruses try to avoid detection by modifying parts of the system that could be used to detect it. For example the read( ) system call could be modified so that if an infected file is read the infected part gets skipped and the reader would see the original unadulterated file.

- **Tunneling** viruses attempt to avoid detection by inserting themselves into the interrupt handler chain, or into device drivers.
- **Multipartite** viruses attack multiple parts of the system, such as files, boot sector, and memory.
- **Armored** viruses are coded to make them hard for anti-virus researchers to decode and understand. In addition many files associated with viruses are hidden, protected, or given innocuous looking names such as "...".

- In 2004 a virus exploited three bugs in Microsoft products to infect hundreds of Windows servers (including many trusted sites) running Microsoft Internet Information Server, which in turn infected any Microsoft Internet Explorer web browser that visited any of the infected server sites. One of the back-door programs it installed was a ***keystroke logger,*** which records users keystrokes, including passwords and other sensitive information.
- There is some debate in the computing community as to whether a ***monoculture,*** in which nearly all systems run the same hardware, operating system, and applications, increases the threat of viruses and the potential for harm caused by them.

System and Network Threats

- Most of the threats described above are termed ***program threats***, because they attack specific programs or are carried and distributed in programs. The threats in this section attack the operating system or the network itself, or leverage those systems to launch their attacks.

Worms

- A ***worm*** is a process that uses the fork / spawn process to make copies of itself in order to wreak havoc on a system. Worms consume system resources, often blocking out other, legitimate processes. Worms that propagate over networks can be especially problematic, as they can tie up vast amounts of network resources and bring down large-scale systems.
- One of the most well-known worms was launched by Robert Morris, a graduate student at Cornell, in November 1988. Targeting Sun and VAX computers running BSD UNIX version 4, the worm spanned the Internet in a matter of a few hours, and consumed enough resources to bring down many systems.
- This worm consisted of two parts:
  1. A small program called a ***grappling hook,*** which was deposited on the target system through one of three vulnerabilities, and
  2. The main worm program, which was transferred onto the target system and launched by the grappling hook program.

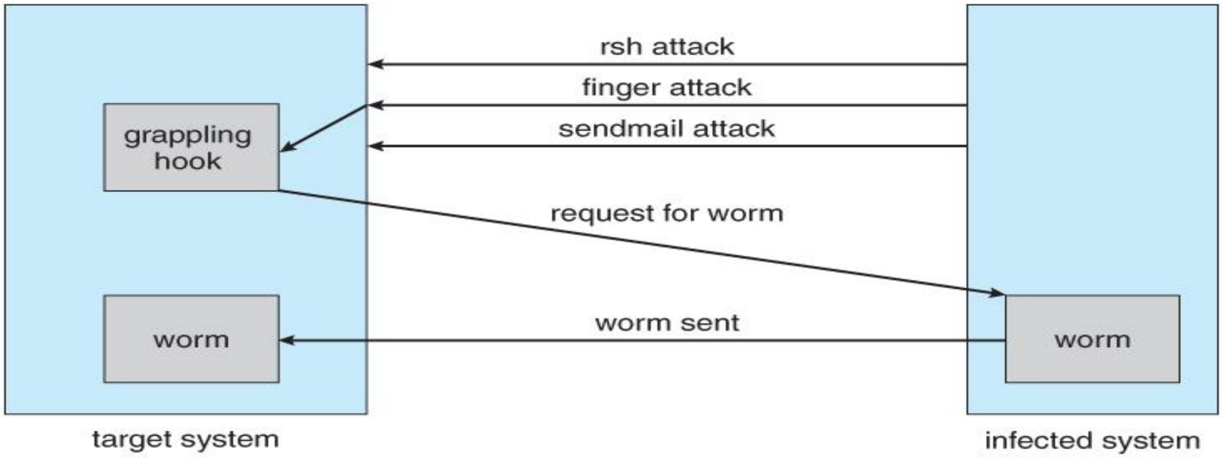


Figure.6 - The Morris Internet worm.

- The three vulnerabilities exploited by the Morris Internet worm were as follows:
    1. **rsh (remote shell)** is a utility that was in common use at that time for accessing remote systems without having to provide a password. If a user had an account on two different computers (with the same account name on both systems), then the system could be configured to allow that user to remotely connect from one system to the other without having to provide a password. Many systems were configured so that ***any*** user (except root) on system A could access the same account on system B without providing a password.
    2. **finger** is a utility that allows one to remotely query a user database, to find the true name and other information for a given account name on a given system. For example "finger joeUser@somemachine.edu" would access the finger daemon at somemachine.edu and return information regarding joeUser. Unfortunately the finger daemon (which ran with system privileges) had the buffer overflow problem, so by sending a special 536-character user name the worm was able to fork a shell on the remote system running with root privileges.
    3. **sendmail** is a routine for sending and forwarding mail that also included a debugging option for verifying and testing the system. The debug feature was convenient for administrators, and was often left turned on. The Morris worm exploited the debugger to mail and execute a copy of the grappling hook program on the remote system.
- Once in place, the worm undertook systematic attacks to discover user passwords:
    1. First it would check for accounts for which the account name and the password were the same, such as "guest", "guest".
    2. Then it would try an internal dictionary of 432 favorite password choices. (I'm sure "password", "pass", and blank passwords were all on the list.)
    3. Finally it would try every word in the standard UNIX on-line dictionary to try and break into user accounts.
- Once it had gotten access to one or more user accounts, then it would attempt to use those accounts to rsh to other systems, and continue the process.
- With each new access the worm would check for already running copies of itself, and 6 out of 7 times if it found one it would stop. (The seventh was to prevent the worm from being stopped by fake copies.)
- Fortunately the same rapid network connectivity that allowed the worm to propagate so quickly also quickly led to its demise - Within 24 hours remedies for stopping the worm propagated through the Internet from administrator to administrator, and the worm was quickly shut down.
- There is some debate about whether Mr. Morris's actions were a harmless prank or research project that got out of hand or a deliberate and malicious attack on the Internet. However the court system convicted him, and penalized him heavy fines and court costs.
- There have since been many other worm attacks, including the W32.Sobig.F@mm attack which infected hundreds of thousands of computers and an estimated 1 in 17 e-mails in August 2003. This worm made detection difficult by varying the subject line of the infection-carrying mail message, including "Thank You!", "user details", and "Re: Approved".

Port Scanning

- ***Port Scanning*** is technically not an attack, but rather a search for vulnerabilities to attack. The basic idea is to systematically attempt to connect to every known (or common or possible) network port on some remote machine, and to attempt to make contact. Once it is determined that a particular computer is listening to a particular port, then the next step is to determine what daemon is listening, and whether or not it is a version containing a known security flaw that can be exploited.
- Because port scanning is easily detected and traced, it is usually launched from ***zombie systems,*** i.e. previously hacked systems that are being used without the knowledge or permission of their rightful owner. For this reason it is important to protect "innocuous" systems and accounts as well as those that contain sensitive information or special privileges.
- There are also port scanners available that administrators can use to check their own systems, which report any weaknesses found but which do not exploit the weaknesses or cause any problems. Two such systems are ***nmap*** (http://www.insecure.org/nmap) and ***nessus*** (http://www.nessus.org). The former identifies what OS is found, what firewalls are in place, and what services are listening to what ports. The latter also contains a database of known security holes, and identifies any that it finds.

Denial of Service

- ***Denial of Service (DOS)*** attacks do not attempt to actually access or damage systems, but merely to clog them up so badly that they cannot be used for any useful work. Tight loops that repeatedly request system services are an obvious form of this attack.
- DOS attacks can also involve social engineering, such as the Internet chain letters that say "send this immediately to 10 of their friends, and then go to a certain URL", which clogs up not only the Internet mail system but also the web server to which everyone is directed. (Note: Sending a "reply all" to such a message notifying everyone that it was just a hoax also clogs up the Internet mail service, just as effectively as if user had forwarded the thing.)
- Security systems that lock accounts after a certain number of failed login attempts are subject to DOS attacks which repeatedly attempt logins to all accounts with invalid passwords strictly in order to lock up all accounts.
- Sometimes DOS is not the result of deliberate maliciousness. Consider for example:
  - A web site that sees a huge volume of hits as a result of a successful advertising campaign.
  - CNN.com occasionally gets overwhelmed on big news days, such as Sept 11, 2001.
  - CS students given their first programming assignment involving fork( ) often quickly fill up process tables or otherwise completely consume system resources.

Firewalls

A firewall is a system designed to prevent unauthorized access to or from a private network. 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.

Need of Firewalls

Without a firewall, user computer is operating with an "open door" policy. Bank account information, passwords, credit card numbers, virtually any sensitive information on their computer becomes available to hackers. Hackers can get in, take what they want, and even leave one of their own "back doors" in place for ongoing access to computer whenever they like. Firewalls have a wide range of capabilities. Types of firewalls include:

- Packet filtering firewalls
- Stateful inspection firewalls
- Proxy firewalls
- Guards
- Personal firewalls

Packet filter

Packet filtering is “controlling access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination. Packet filtering is one technique, among many, for implementing security firewalls. ”i Packet filtering is both a tool and a technique that is a basic building block of network security. It is a tool in that it is an instrument that aids in accomplishing a task. It is a technique because it is a method of accomplishing a task. In the context of a TCP/IP network, a packet filter watches each individual IP datagram, decodes the header information of in-bound and out-bound traffic and then either blocks the datagram from passing or allows the datagram to pass based upon the contents of the source address, destination address, source port, destination port and/or connection status. This is based upon certain criteria defined to the packet filtering tool. The leading IP routers, including Cisco, Bay, and Lucent, can be configured to filter IP datagrams. Many operating systems can be configured for packet filtering. Packet filtering can be added to *nix operating systems. Support for packet filtering via ipchains is included by default in the Linux kernel. Windows NT and Windows 2000 support packet filtering. Virtually all commercial firewalls support packet filtering. Some commercial firewalls also have the capability of filtering packets based upon the state of previous packets (stateful inspection).

Purpose of Packet Filter

Packet filtering generally is inexpensive to implement. However it must be understood that a packet filtering device does not provide the same level of security as an application or proxy firewall. All except the most trivial of IP networks is composed of IP subnets and contain routers. Each router is a potential filtering point. Because the cost of the router has already been absorbed, additional cost for packet filtering is not required. Packet filtering is appropriate where there are modest security requirements. The internal (private) networks of many organizations are not highly segmented. Highly sophisticated firewalls are not necessary for isolating one part of the organization from another. However it is prudent to provide some sort of protection of the production network from a lab or experimental network. A packet filtering device is a very appropriate measure for providing isolation of one subnet from another.

Functionality

All packet filters function in the same general fashion. Operating at the network layer and transport layer of the TCP/IP protocol stack, every packet is examined as it enters the protocol stack. The network and transport headers are examined closely for the following information:

protocol (IP header, network layer) – In the IP header, byte 9 (remember the byte count begins with zero) identifies the protocol of the packet. Most filter devices have the capability to differentiate between TCP, UPD, and ICMP.(TCP-Transmission Control Protocol,UDP-User Datagram Protocol,Internet Control Message Control)

source address (IP header, network layer) – The source address is the 32-bit IP address of the host which created the packet.

Destination address (IP header, network layer) – The destination address is the 32-bit IP address of the host the packet is destined for

Source port (TCP or UDP header, transport layer) – Each end of a TCP or UDP network connection is bound to a port. TCP ports are separate and distinct from UDP ports. Ports numbered below 1024 are reserved – they have a specifically defined use. Ports numbered above 1024 (inclusive) are known as ephemeral ports. They can be used however a vendor chooses. For a list of “well known” ports, refer to RFP1700. The source port is a pseudo-randomly assigned ephemeral port number. Thus it is often not very useful to filter on the source port.

Destination port (TCP or UDP header, transport layer) – The destination port number indicates a port that the packet is sent to. Each service on the destination host listens to a port. Some well-known ports that might be filtered are 20/TCP and 21/TCP - ftp connection/data, 23/TCP - telnet, 80/TCP - http, and 53/TCP - DNS zone transfers.

Connection status (TCP header, transport layer) – The connection status tells whether the packet is the first packet of the network session. The ACK bit in the TCP header is set to “false” or 0 if this is the first packet in the session. It is simple to disallow a host from establishing a connection by rejecting or discarding any packets which have the ACK bit set to “false” or 0.

The filtering device compares the values of these fields to rules that have been defined, and based upon the values and the rules the packet is either passed or discarded. Many filters also allow additional criteria from the link layer to be defined, such as the network interface where the filtering is to occur.

Types of Packet Filtering

Packet filtering firewall allows only those packets to pass, which are allowed as per their firewall policy. Each packet passing through is inspected and then the firewall decides to pass it or not. The packet filtering can be divided into two parts:

1. Stateless packet filtering.
2. Stateful packet filtering.

The data travels through the internet in the form of packets. Each packet has a header which provides the information about the packet, its source and destination etc. The packet filtering firewalls inpects these packets to allow or deny them. The information may or may not be remembered by the firewall.

Stateless Packet Filtering

If the information about the passing packets is not remembered by the firewall, then this type of filtering is called stateless packet filtering. This type of firewalls are not smart enough and can be fooled very easily by the hackers. These are especially dangerous for UDP type of data packets. The reason is that, the allow/deny decisions are taken on packet by packet basis and these are not related to the previous allowed/denied packets.

Stateful Packet Filtering

If the firewall remembers the information about the previously passed packets, then that type of filtering is stateful packet filtering. These can be termed as smart firewalls. This type of filtering is also known as Dynamic packet filtering.

Stateful Inspection Firewall

Stateful Inspection Firewall is a firewall that keeps track of the state of network connections travelling across it.

Functionality

Firewall protection uses stateful inspection to track current connections. Stateful inspection tracks source and destination IP addresses, ports, applications, and other connection information. Before the client inspects the firewall rules, it makes the traffic flow decisions that are based on the connection information.

For example, if a firewall rule allows a computer to connect to a Web server, the firewall logs the connection information. When the server replies, the firewall discovers that a response from the Web server to the computer is expected. It permits the Web server traffic to flow to the initiating computer without inspecting the rule base. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection eliminates the need to create new rules. For the traffic that is initiated in one direction, they do not have to create the rules that permit the traffic in both directions. The client traffic that is initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443). The client computers initiate this outbound traffic; they create a rule that permits the outbound traffic for these protocols. Stateful inspection automatically permits the return traffic that responds to the outbound traffic. Because the firewall is stateful in nature, they only need to create the rules that initiate a connection, not the characteristics of a particular packet. All packets that belong to an allowed connection are implicitly allowed as being an integral part of that same connection.Stateful inspection supports all rules that direct TCP traffic. Stateful inspection does not support the rules that filter ICMP traffic. For ICMP traffic, they must create the rules that permit the traffic in both directions. For example, for the clients to use the ping command and receive replies, they must create a rule that permits ICMP traffic in both directions.

The state table that maintains the connection information may be periodically cleared. For example, it is cleared when a Firewall policy update is processed or if Symantec Endpoint Protection services are restarted.

Proxy Firewalls

A Proxy is a central machine on the network that allows other machines in that network to use a shared Internet connection. Proxy servers are intermediate servers which accept requests from clients and forward them to other proxy servers, a source server, or service the request from their own cache. The proxy is also called 'server' or 'gateway'. Proxy allows users on a network to browse the Web, send files over FTP, and work with E-mail and other Internet services.

A Firewall Proxy provides Internet access to other computers on the network but is mostly deployed to provide safety or security. It controls the information going in and out the network. Firewalls are often used to keep the network safe and free of intruders and viruses. Firewall proxy servers filter, cache, log, and control requests coming from a client. A firewall proxy is one that is used for restricting connections from a proxy to the outside world or to the source server inside of the LAN. This is different from a conventional firewall, in that a conventional firewall restricts connections coming from the outside world.

Functionality

Simply put, proxy are gateway applications used to route Internet and web access from within a firewall. Proxy servers work by opening a socket on the server and allowing the connection to pass through. There is often only one computer in a company with direct Internet connection. Other computers have access to the Internet using that computer as gateway.

A proxy basically does the following:

- Receives a request from a client inside the firewall
- Sends this request to the remote server outside of the firewall
- Reads the response
- Sends it back to the client

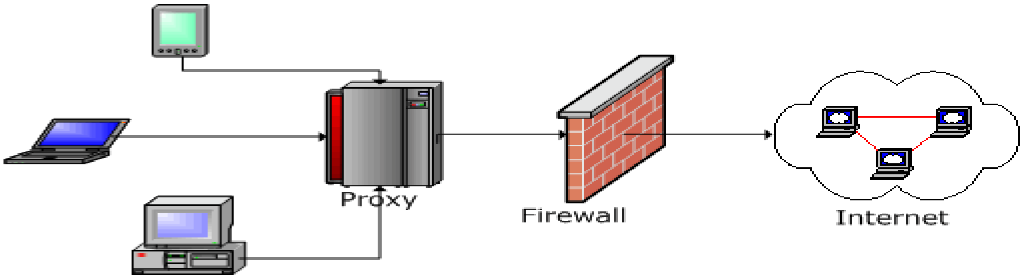


Fig3.1Proxy Firewalls

Usually, the same proxy is used by all of the clients on the network. This enables the proxy to efficiently cache documents that are requested by several clients.

SOCKS4 or SOCKS5 Proxy

In a SOCKS network, all network application data flows through SOCKS, enabling SOCKS to collect, audit, screen, filter and control the network data, and create a network application data warehouse.

It is recommended to use SOCKS5 proxy with PostCast Server. SOCKS4 performed three functions: connection request, proxy server setup and application data relay. SOCKS5 brings authentication to the table. With authentication, SOCKS5 adds two messages. SOCKS5 makes configuring clients easier and includes support for UDP and TCP applications such as SNMP and audio/video applications such as RealAudio. It supports communications among networks with different IP addressing schemes, and supports authentication and encryption.

Tunneling Proxy

Tunneling allows users to perform various Internet tasks despite the restrictions imposed by firewalls. This is made possible by sending data through HTTP (port 80). Additionally, Tunneling protocol is very secure, making it indispensable for both average and business communications. SSL (Secure Sockets Layer) tunneling protocol allows a web proxy server to act as a tunnel for SSL enhanced protocols. The client makes an HTTP Request to the proxy and asks for an SSL tunnel. A Tunneling Proxy operates on port 443.

Guard

In information security, a guard is a device or system for allowing computers on otherwise separate networks to communicate, subject to configured constraints. In many respects a guard is like a firewall and guards may have similar functionality to a gateway.

Whereas a firewall is designed to limit traffic to certain services, a guard aims to control the information exchange that the network communication is supporting at the business level. Further, unlike a firewall a guard provides assurance that it is effective in providing this control even under attack and failure conditions.

A guard will typically sit between a protected network and an external network, and ensure the protected network is safe from threats posed by the external network and from leaks of sensitive information to the external network.

A guard is usually dual-homed, though guards can connect more than two networks, and acts as a full application layer proxy, engaging in separate communications on each interface. A guard will pass only the business information carried by the protocols from one network to another, and then only if the information passes configured checks which provide the required protection.

Guards were initially designed to control the release of information from classified systems, protecting the confidentiality of the sensitive information handled by the protected system. Since then their scope has been extended to cover controls over the import of data, in order to protect the integrity of information and availability of services in the protected network.

Guards generally provide the following functionality:

- Source and destination address authentication
- Source and destination address white listing
- Security label checks against source and destination clearances
- Data format whitelisting
- Data format consistency and validity checking
- Scanning data for known malware
- Validation of digital signatures
- Inspection of encrypted content
- Checking text against a blacklist of phrases
- Removal of redundant data

- Generation of logs recording security relevant events
- Self-test mechanisms

Personal firewall

A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. Typically it works as an application layer firewall.

A personal firewall differs from a conventional firewall in terms of scale. A personal firewall will usually protect only the computer on which it is installed, as compared to a conventional firewall which is normally installed on a designated interface between two or more networks, such as a router or proxy server. Hence, personal firewalls allow a security policy to be defined for individual computers, whereas a conventional firewall controls the policy between the networks that it connects.

The per-computer scope of personal firewalls is useful to protect machines that are moved across different networks. For example, a laptop computer may be used on a trusted intranet at a workplace where minimal protection is needed as a conventional firewall is already in place, and services that require open ports such as file and printer sharing are useful. The same laptop could be used at public Wi-Fi hotspots, where strict security is required to protect from malicious activity. Most personal firewalls will prompt the user when a new network is connected for the first time to decide the level of trust, and can set individual security policies for each network.

Unlike network firewalls, many personal firewalls are able to control network traffic allowed to programs on the firewalled computer. When an application attempts an outbound connection, the firewall may block it if blacklisted, or ask the user whether to blacklist it if it is not yet known. This protects against malware implemented as an executable program. Personal firewalls may also provide some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted.

Common personal firewall features:

- Block or alert the user about all unauthorized inbound or outbound connection attempts[1]
- Allows the user to control which programs can and cannot access the local network and/or Internet and provide the user with information about an application that makes a connection attempt
- Hide the computer from port scans by not responding to unsolicited network traffic
- Monitor applications that are listening for incoming connections
- Monitor and regulate all incoming and outgoing Internet users
- Prevent unwanted network traffic from locally installed applications
- Provide information about the destination server with which an application is attempting to communicate.

Security for smart cards

Smart cards provide computing and business systems the enormous benefit of portable and secure storage of data and value. At the same time, the integration of smart cards into their system introduces its own security management issues, as people access card data far and wide in a variety of applications.

The following is a basic discussion of system security and smart cards, designed to familiarize user with the terminology and concepts user need in order to start their security planning.

Types of Smart Cards

Smart cards are tamper resistant, credit card size devices that include an integrated circuit chip to provide data storage and processing. Most smart cards require an external interface to provide communications, power, and clock cycles. There are many different types of cards and card characteristics by which they can be distinguished. In this paper, the cards will be broken up into two major categories: memory cards and microprocessor cards.

Memory Cards

Memory cards are ICCs designed to store and protect information on the card. The cards can hold considerably more data than the magnetic stripes currently on credit cards and provide enough logic to protect that data from unauthorized read and/or write access.

Microprocessor Cards

Microprocessor cards contain a true CPU and RAM to allow for data processing other than just the protection of the data from unauthorized access. Some of these cards specialize in the math calculations required for cryptography functions, others are made to support specific programming languages such as Java cards, and others are made to do both.

USB Tokens6

According to Rainbow Technologies, USB tokens are “technologically identical to Smart Cards, with the exception of their form factor and interface”. These tokens often contain the same type of ICCs that are in Smart Cards, but interface through a USB port instead of requiring a separate reader. These physical and interface differences provide both pros and cons in terms of the security of these devices.

Contact vs. Contactless Smart Cards

The main difference between contact and contactless Smart Cards is that contact Smart Cards must have a physical connection to a reader in order to work. Contactless Smart Cards communicates with the reader and derives its power from radio frequencies7Contactless Smart Cards normally need to be within 10cm of the reader to operate and communicate. The cost of the contactless Smart Cards has prevented them from becoming widely popular. Since these do not represent a significant market share and most of the security implications are the same as contact smart cards.

Security

Smart cards provide computing and business systems the enormous benefit of portable and secure storage of data and value. At the same time, the integration of smart cards into their system introduces its own security management issues, as people access card data far and wide in a variety of applications.

The following is a basic discussion of system security and smart cards, designed to familiarize user with the terminology and concepts user need in order to start their security planning.

Security is basically the protection of something valuable to ensure that it is not stolen, lost, or altered. The term "data security" governs an extremely wide range of applications and touches everyone's daily life. Concerns over data security are at an all-time high, due to the rapid advancement of technology into virtually every transaction, from parking meters to national defense.

Data is created, updated, exchanged and stored via networks. A network is any computing system where users are highly interactive and interdependent and by definition, not all in the same physical place. In any network, diversity abounds, certainly in terms of types of data, but also types of users. For that reason, a system of security is essential to maintain computing and network functions, keep sensitive data secret, or simply maintain worker safety. Any one company might provide an example of these multiple security concerns: Take, for instance, a pharmaceutical manufacturer:

Type of Data	Security Concern	Type of Access
Drug Formula	Basis of business income. Competitor spying	Highly selective list of executives
Accounting, Regulatory	Required by law	Relevant executives and departments
Personnel Files	Employee privacy	Relevant executives and departments
Employee ID	Non-employee access. Inaccurate payroll, benefits assignment	Relevant executives and departments
Facilities	Access authorization	Individuals per function and clearance such as customers, visitors, or vendors
Building safety, emergency response	All employees	Outside emergency response

Information Security

Information security is the application of measures to ensure the safety and privacy of data by managing its storage and distribution. Information security has both technical and social implications. The first simply deals with the 'how' and 'how much' question of applying secure measures at a reasonable cost. The second grapples with issues of individual freedom, public concerns, legal standards and how the need for privacy intersects them. This discussion covers a range of options open to business managers, system planners and programmers that will contribute to their ultimate security strategy. The eventual choice rests with the system designer and issuer.

The Elements of Data Security

In implementing a security system, all data networks deal with the following main elements:

- **Hardware**, including servers, redundant mass storage devices, communication channels and lines, hardware tokens (**smart cards**) and remotely located devices (e.g., thin clients or Internet appliances) serving as interfaces between users and computers
- **Software**, including operating systems, database management systems, communication and security application programs
- **Data**, including databases containing customer - related information.
- **Personnel**, to act as originators and/or users of the data; professional personnel, clerical staff, administrative personnel, and computer staff

Safe Payments

The online payment ecosystem is a prime target for cybercriminals. Security 7 Award winner, Steven Elefant, formerly of Heartland Payment Systems, explains why end-to-end encryption is needed to maintain the integrity of transactions carried out online.

The old saying is true: Money really does make the world go ‘round. What many people don’t realize is what it takes to make the money go ‘round, so to speak.

When it comes to credit and debit card payments, several entities are required to process a transaction from start to finish: consumers and their payment cards, merchants and their point-of-sale (POS) payment systems, the card brands (i.e. Visa, MasterCard, Discover Network, American Express), issuing banks, and card processors like Heartland Payment Systems, the nation’s fifth largest payments processor. Enormous amounts of electronic data and digital currency flow through this payment ecosystem as billions of transactions are processed each year.

With access to the sensitive information that enables the exchange of billions of dollars in transactions each year, the payments infrastructure is a red-hot target for hackers. I have been entrenched in the electronic commerce industry for more than 30 years and never before have we been at a more critical juncture in our fight against cybercrime than now. It’s us good guys against the bad guys, and we are determined to win.

Pay User Way has released some security guide and advice for online banking, after its research revealed a widespread new phobia of the latest payment methods.

Pay user Way’s research revealed peoples fear of using the latest ways to pay, such as mobile phone banking and contactless cards, because of concerns around security.

The research also showed that one in seven people surveyed felt their life was being held back by their fear of technology, with one in ten actively avoiding internet banking due to their fears.

Banks take many measures to ensure that online banking is safe and secure. These include making sure their websites are encrypted, having timed log outs, deactivation of their login details if a number of incorrect attempts are made, and many authentication processes.

Top Ten guide for safe online banking

- Keep user computer up-to-date with antivirus software, operating system patches, firewalls etc and ensure their browser is set to the highest level of security.
- Be wary of unsolicited emails or phone calls asking user for PINs or passwords –user bank or the police would never ask for these in full.
- Always type user bank’s address into user web browser – never follow a link in an email and then enter personal details.
- A locked padlock or unbroken key symbol should always appear in user browser window when banking online. The ‘http’ at the beginning of the website address will change to ‘https’ when a secure connection is made.
- When making a payment, always double check that user have entered the correct account number and sort code.
- Never leave their computer unattended when logged in and log off as soon as they’re finished, especially on any public computer.
- Check user statements regularly – if user notice anything strange, contact their bank immediately.
- Be wary of any unexpected or suspicious looking ‘pop-up’ windows that appear during their online banking session.
- Stop and think about the process user normally go through to make a payment to someone – be suspicious if it differs from the last time user used it.
- Fraudsters sometimes try to trick people into making a real payment by claiming “it’s just a test”

Electronic Banking

For many people, **electronic banking** means 24-hour access to cash through an automated teller machine (ATM) or Direct Deposit of paychecks into checking or savings accounts.

But **electronic banking** involves many different types of transactions, rights, responsibilities — and sometimes, fees.Some are listed as follow as

- Electronic Fund Transfers
- Disclosures
- Errors
- Lost or Stolen ATM or Debit Cards
- Overdrafts for One-Time Debit Card Transactions and ATM Cards
- Limited Stop-Payment Privileges
- Additional Rights
- For More Information and Complaints

Electronic Fund Transfers

Electronic banking, also known as electronic fund transfer (EFT), uses computer and electronic technology in place of checks and other paper transactions. EFTs are initiated through devices like cards or codes that let user, or those user authorize, access their account. Many financial institutions use ATM or debit cards and Personal Identification Numbers (PINs) for this purpose. Some use other types of debit cards that require their signature or a scan. For example, some use radio frequency identification (RFID) or other forms of "contactless" technology that scan their information without direct contact with user. The federal Electronic Fund Transfer Act (EFT Act) covers some electronic consumer transactions.

Here are some common EFT services:

ATMs are electronic terminals that let their bank almost virtually any time. To withdraw cash, make deposits, or transfer funds between accounts, user generally insert an ATM card and enter their PIN. Some financial institutions and ATM owners charge a fee, particularly if user don't have accounts with them or if their transactions take place at remote locations. Generally, ATMs must tell user they charge a fee and the amount on or at the terminal screen before user complete the transaction. Check with their institution and at ATMs user use for more information about these fees.

Direct Deposit lets user authorize specific deposits — like paychecks, Social Security checks, and other benefits — to their account on a regular basis. User also may pre-authorize direct withdrawals so that recurring bills — like insurance premiums, mortgages, utility bills, and gym memberships — are paid automatically. Be cautious before user pre-authorize recurring withdrawals to pay companies user aren't familiar with; funds from their bank account could be withdrawn improperly. Monitor user bank account to make sure direct recurring payments take place and are for the right amount.

Pay-by-Phone Systems let user call their financial institution with instructions to pay certain bills or to transfer funds between accounts. User must have an agreement with their institution to make these transfers.

Personal Computer Banking lets user handle many banking transactions using their personal computer. For example, user may use their computer to request transfers between accounts and pay bills electronically.

Debit Card Purchase or Payment Transactions let user make purchases or payments with a debit card, which also may be their ATM card. Transactions can take place in-person, online, or by phone. The process is similar to using a credit card, with some important exceptions: a debit card purchase or payment transfers money quickly from their bank account to the company's account, so user have to have sufficient funds in their account to cover their purchase. This means user need to keep accurate records of the dates and amounts of their debit card purchases, payments, and ATM withdrawals. Be sure user know the store or business before user provide their debit card information to avoid the possible loss of funds through fraud. User liability for unauthorized use, and their rights for dealing with errors, may be different for a debit card than a credit card.

Electronic Check Conversion converts a paper check into an electronic payment in a store or when a company gets user check in the mail.

When user give their check to a cashier in a store, the check is run through an electronic system that captures user banking information and the amount of the check. User sign a receipt and user get a copy for their records. When user check is given back to user, it should be voided or marked by the merchant so that it can't be used again. The merchant electronically sends information from the check (but not the check itself) to their bank or other financial institution, and the funds are transferred into the merchant's account.

When user mail a check for payment to a merchant or other company, they may electronically send information from their check (but not the check itself) through the system; the funds are transferred from their account into their account. For a mailed check, user still should get notice from a company that expects to send their check information through the system electronically. For example, the company might include the notice on their monthly statement. The notice also should state if the company will electronically collect a fee from user account — like a "bounced check" fee — if user don't have enough money to cover the transaction.

Be careful with online and telephone transactions that may involve the use of their bank account information, rather than a check. A legitimate merchant that lets user use their bank account information to make a purchase or pay on an account should post information about the process on its website or explain the process on the phone. The merchant also should ask for their permission to electronically debit their bank account for the item they're buying or paying on. However, because online and telephone electronic debits don't occur face-to-face, be cautious about sharing their bank account information. Don't give out this information when user have no experience with the business, when user didn't initiate the call, or when the business seems reluctant to discuss the process with user. Check their bank account regularly to be sure that the right amounts were transferred.

Not all electronic fund transfers are covered by the EFT Act. For example, some financial institutions and merchants issue cards with cash value stored electronically on the card itself. Examples include prepaid phone cards, mass transit passes, general purpose reloadable cards, and some **gift cards**. These "stored-value" cards, as well as transactions using them, may not be covered by the EFT Act, or they may be subject to different rules under the EFT Act. This means user may not be covered for the loss or misuse of the card. Ask their financial institution or merchant about any protections offered for these cards.

Disclosures

To understand their rights and responsibilities for their EFTs, read the documents user get from the financial institution that issued their"access device" – the card, code or other way user access their account to transfer money electronically. Although the method varies by institution, it often involves a card and/or a PIN. No one should know their PIN but user and select employees at their financial institution. User also should read the documents user receive for their bank account, which may contain more information about EFTs.

Before user contract for EFT services or make their first electronic transfer, the institution must give user the following information in a format user can keep.

- A summary of their liability for unauthorized transfers
- The phone number and address for a contact if you think an unauthorized transfer has been or may be made, the institution's "business days" (when the institution is open to the public for normal business), and the number of days you have to report suspected unauthorized transfers
- The type of transfers user can make, fees for transfers, and any limits on the frequency and dollar amount of transfers

- A summary of their right to get documentation of transfers and to stop payment on a pre-authorized transfer, and how user stop payment
- a notice describing how to report an error on a receipt for an EFT or their statement, to request more information about a transfer listed on their statement, and how long user have to make their report
- a summary of the institution's liability to they if it fails to make or stop certain transactions
- circumstances when the institution will share information about their account with third parties
- a notice that user may have to pay a fee charged by operators of ATMs where user don't have an account, for an EFT or a balance inquiry at the ATM, and charged by networks to complete the transfer.

They also will get two more types of information for most transactions: terminal receipts and periodic statements. Separate rules apply to deposit accounts from which pre-authorized transfers are drawn. For example, pre-authorized transfers from their account need they written or similar authorization, and a copy of that authorization must be given to user. Additional information about pre-authorized transfers is in their contract with the financial institution for that account. They're entitled to a terminal receipt each time user initiate an electronic transfer, whether user use an ATM or make a point-of-sale electronic transfer, for transfers over $15. The receipt must show the amount and date of the transfer, and its type, like "from savings to checking." It also must show a number or code that identifies the account, and list the terminal location and other information. When they make a point-of-sale transfer, They'll probably get their terminal receipt from the salesperson.

They won't get a terminal receipt for regularly occurring electronic payments that they've pre-authorized, like insurance premiums, mortgages, or utility bills. Instead, these transfers will appear on their statement. If the pre-authorized payments vary, however, they should get a notice of the amount that will be debited at least 10 days before the debit takes place.

They're also entitled to a periodic statement for each statement cycle in which an electronic transfer is made. The statement must show the amount of any transfer, the date it was credited or debited to their account, the type of transfer and type of account(s) to or from which funds were transferred, the account number, the amount of any fees charged, the account balances at the beginning and end of the statement cycle, and the address and phone number for inquiries. They're entitled to a quarterly statement whether or not electronic transfers were made.

Keep and compare their EFT receipts with their periodic statements the same way user compare their credit card receipts with their monthly credit card statement. This will help user make the best use of their rights under federal law to dispute errors and avoid liability for unauthorized transfers.

Errors

User have 60 days from the date a periodic statement containing a problem or error was sent to user to notify their financial institution. The best way to protect theirself if an error occurs is to notify the financial institution by certified letter. Ask for a return receipt so user can prove that the institution got their letter. Keep a copy of the letter for their records.

Under federal law, the institution has no obligation to conduct an investigation if user miss the 60-day deadline.

Once they've notified the financial institution about an error on their statement, it has 10 business days to investigate. The institution must tell user the results of its investigation within three business days after completing it, and must correct an error within one business day after determining that the error has occurred. An institution usually is permitted to take more time — up to 45 days — to complete the investigation, but only if the money in dispute is returned to their account and they're notified promptly of the credit. At the end of the investigation, if no error has been found, the institution may take the money back if it sends user written explanation.

An error also may occur in connection with a point-of-sale purchase with a debit card. For example, an oil company might give user debit card that lets user pay for gas directly from their bank account. Or user may have a debit card that can be used for a various types of retail purchases. These purchases will appear on their bank statement. In case of an error on their account, however, user should contact the card issuer (for example, the oil company or bank) at the address or phone number provided by the company for errors. Once they've notified the company about the error, it has 10 business days to investigate and tell user the results. In this situation, it may take up to 90 days to complete an investigation, if the money in dispute is returned to their account and they're notified promptly of the credit. If no error is found at the end of the investigation, the institution may take back the money if it sends user written explanation.

Lost or Stolen ATM or Debit Cards

If their credit card is lost or stolen, user can't lose more than $50. If someone uses their ATM or debit card without your permission, you can lose much more.

If you report an ATM or debit card missing to the institution that issues the card before someone uses the card without your permission, you can't be responsible for any unauthorized withdrawals. But if unauthorized use occurs before you report it, the amount you can be responsible for depends on how quickly you report the loss to the card issuer.

- If you report the loss within two business days after you realize your card is missing, you won't be responsible for more than $50 of unauthorized use.
- If you report the loss within 60 days after your statement is mailed to you, you could lose as much as $500 because of an unauthorized transfer.
- If you don’t report an unauthorized use of your card within 60 days after the card issuer mails your statement to you, you risk unlimited loss; you could lose all the money in that account, the unused portion of your maximum line of credit established for overdrafts, and maybe more.

If an extenuating circumstance, like lengthy travel or illness, keeps you from notifying the card issuer within the time allowed, the notification period must be extended. In addition, if state law or your contract imposes lower liability limits than the federal EFT Act, the lower limits apply.

Once you report the loss or theft of your ATM or debit card to the card issuer, you're not responsible for additional unauthorized use. Because unauthorized transfers may appear on your statements, though, read each statement you receive after you've reported the loss or theft. If the statement shows transfers that you didn't make or that you need more information about, contact the card issuer immediately, using the special procedures it provided for reporting errors.

Overdrafts for One-Time Debit Card Transactions and ATM Cards

If you make a one-time purchase or payment with your debit card or use your ATM card and don't have sufficient funds, an overdraft can occur. Your bank must get your permission to charge you a fee to pay for your overdraft on a one-time debit card transaction or ATM transaction. They also must send you a notice and get your opt-in agreement before charging you.

For accounts that you already have, unless you opt-in, the transaction will be declined if you don't have the funds to pay it, and you can't be charged an overdraft fee. If you open a new account, the bank can't charge you an overdraft fee for your one-time debit card or ATM transactions, either, unless you opt-in to the fees. The bank will give you a notice about opting-in when you open the account, and you can decide whether to opt-in. If you opt-in, you can cancel any time; if you don’t opt-in, you can do it later.

These rules do not apply to recurring payments from your account. For those transactions, your bank can enroll you in their usual overdraft coverage. If you don’t want the coverage (and the fees), contact your bank to see if they will let you discontinue it for those payments.

Limited Stop-Payment Privileges

When you use an electronic fund transfer, the EFT Act does not give you the right to stop payment. If your purchase is defective or your order isn't delivered, it's as if you paid cash: It's up to you to resolve the problem with the seller and get your money back.

One exception: If you arranged for recurring payments out of your account to third parties, like insurance companies or utilities, you can stop payment if you notify your institution at least three business days before the scheduled transfer. The notice may be written or oral, but the institution may require a written follow-up within 14 days of your oral notice. If you don’t follow-up in writing, the institution's responsibility to stop payment ends.

Although federal law provides limited rights to stop payment, financial institutions may offer more rights or state laws may require them. If this feature is important to you, shop around to be sure you're getting the best "stop-payment" terms available.

Additional Rights

The EFT Act protects your right of choice in two specific situations: First, financial institutions can't require you to repay a loan by preauthorized electronic transfers. Second, if you're required to get your salary or government benefit check by EFT, you can choose the institution where those payments will be deposited.

For More Information and Complaints

If you decide to use EFT, keep these tips in mind:

- Take care of your ATM or debit card. Know where it is at all times; if you lose it, report it as soon as possible.
- Choose a PIN for your ATM or debit card that's different from your address, telephone number, Social Security number, or birth date. This will make it more difficult for a thief to use your card.
- Keep and compare your receipts for all types of EFT transactions with your statements so you can find errors or unauthorized transfers and report them.
- Make sure you know and trust a merchant or other company before you share any bank account information or pre-authorize debits to your account. Be aware that some merchants or companies may process your check information electronically when you pay by check.
- Read your monthly statements promptly and carefully. Contact your bank or other financial institution immediately if you find unauthorized transactions and errors.

If you think a financial institution or company hasn’t met its responsibilities to you under the EFT Act, you can complain to the appropriate federal agency. Visit the **Consumer Financial Protection Bureau** or**HelpWithMyBank.gov**, a site maintained by the Office of the Comptroller of the Currency, for answers to frequently-asked questions on topics like bank accounts, deposit insurance, credit cards, consumer loans, insurance, mortgages, identity theft, and safe deposit boxes, and for other information about federal agencies that have responsibility for financial institutions

Mobile Information Security

In today’s scenario where technology is getting very much advance day by day, and people are getting used to the mobile or wireless application, the key message is anytime anywhere communication and transferring of any information. Many technological Considerations need to be examined in order to actualize such a message. Integral to enabling anytime-anywhere communication and transmission of data and information is a sound secure system. Hence a robust trust model in any mobile transaction becomes significant.

Generally a mobile transaction occurs when a client accesses the web-enabled services of a merchant and after necessary negotiations and communications, decides to place an order and make payment. The order and payment information is transmitted from the mobile device to a base wireless station and from there, through the mobile communication infrastructure of the service operator, to the wireless application gateway of the merchant. In a typical mobile computing environment, one or more of the transacting parties are based on some wireless handheld devices.

However, security over the mobile platform is more critical due to the open nature of Wireless networks. Furthermore, security is more difficult to implement on the mobile Platform because of the resource limitation of mobile handheld devices. Therefore, security mechanisms for protecting traditional computer communications need to be revisited so as to ensure that electronic transactions involving mobile devices can be secured and implemented in an effective manner.

Modern day smart phones offer wireless internet connectivity and other advanced computing applications to mobile users, and as a result more and more people are using portable mobile devices for performing official and other works. For this reason, most of the handheld mobile devices store valuable user information, and proper security arrangements must be adopted to secure the user data both in transit as well as in storage. Wireless internet imposes several threats to user information being transmitted via internet. The username/password can be guessed during transmission using dictionaries. Eavesdropping on the unsecured network connection can reveal usernames, passwords or other sensitive information. Hackers can attack social engineering sites to gather password or other private information. Websites containing active contents and plug-ins may inject viruses, malwares and may cause disruption of services of the mobile device. Spoofing can hijack the mobile user to a fake website and force to perform illegal business transactions. Spam messages are injected that consume valuable programming resources and block the system with large amount of garbage messages and also cause distribution of malware over the network connection. Hackers can break into the mobile devices and gain access to private database and other resources causing damage and loss to the organization. In order to prevent above-mentioned security risks, proper security arrangements in the form of firewalls, proxy servers and NAT (Network Access Translation) are adopted. NAT hides the inner network in such a manner that outsider's only see the IP address of the proxy server. Various filters, such as content sensitive firewalls and spam filters are used to protect the information from hackers and malwares.

Mobile devices cannot store large databases as they have limited storage area. They need to download databases from base stations, and data access security is an important factor in mobile information security. The security and privacy of data can be compromised during transfer from mobile base station to mobile device and hackers can issue false queries to central databases which lead to information leakage to unwanted users. The attackers can pretend to be a mobile support station and can retrieve portions of data from base station on behalf of the authorized user. In order to prevent such malpractices, sufficient authentication and identification verification are required for both mobile user and mobile support stations. User authentication and identification is usually based on encryption algorithms (keys), and attackers tent to break the encryption algorithms in order to gain access to personal data stored in encrypted form in the mobile devices. The secret encryption key stored in SIM card can be stolen (copied) leading to potential information and other losses to the mobile user. In order to prevent such security breaches, authority should use strong 256 bit encryption which is virtually impossible to crack as it takes trillions of years to guess the correct encryption key. Another potential security threats to mobile information arises due to disconnection or degradation of access time at the cell boarders. A roaming user when comes near the cell boarder may face service degradation or even disconnection due to problems in cell coverage. Proper cell handover techniques must be adopted to avoid services discontinuity at cell boarder for roaming subscribers. Digital contents transmitted across mobile networks are sometimes copyrighted, and unlawful copying of these materials without the consent of the owner can lead to digital copyright violation. In order to protect copyrighted materials, manufactures implement Digital Rights Management (DRM) mechanism provided by Open Mobile Alliance (OMA). It includes use of forward lock and other hardware independent solutions that prevent more-than-one use of the copyrighted materials.

Bluetooth Security

Bluetooth is a short range wireless communication technology developed by Bluetooth Special Interest Group' and is mainly used by computer peripheral devices' such as printer or modems for exchange of data wirelessly within a short area, such as inside a room. Bluetooth employs encryption of transmission data and exchange-response protocol for user authentication. When the connecting devices do not share a common key, they have to utilize a PIN that must be entered in both the devices beforehand. However, Bluetooth networks are free of security risks as the encryption key can be cracked with the help of a bugging device that can listen to the conversation in a Bluetooth network and can gather enough information to determine the encryption key. Another weakness of Bluetooth system is the generation of the PIN code. Moreover the privacy of Bluetooth users are often compromised as it is possible to track users based on their Bluetooth device addresses.

WLAN Security

Wireless Local Area Networks (WLAN) are used for short range wireless data transfer between Access Points and mobile devices or other fixed IP based networks (such as internet). The main security attacks in WLAN are eavesdropping whereby a mobile attacker can gain access and manipulate all the wireless traffic transmitted through the network. In order to protect the network from unwanted intruders, WLAN adopts WEP (Wired Equivalent Privacy) protocol of IEEE 802.11 standard that secures confidentiality and integrity of data to be transmitted across WLAN. WEP employs encryption (RC4 104 bit chipper) technique to prevent misuse of transmission data as well as employs checksum to maintain the integrity.

Mobile Social Networking

Mobile social networking allows users to connect to their friends through various social networking sites, such as Face book, Twitter, LinkedIn, MySpace or Fraudster from their mobile devices. All major social networking sites have added mobile modules which can conveniently be accessed from user mobile devices for connecting to friends any time and irrespective of the physical location of the user. Thus, people have the liberty to socialize with friends and relatives even if they are travelling on some official trip to some remote corner of the globe. mobile social networking have become very popular in recent past as more and more people get internet-enabled 3G or 4G smart phones that allow fast internet connectivity and easy multimedia download. Another important aspect of mobile social networking is the opportunity it creates for online retailers for advertising their products. As a large number of mobile users nowadays remain engaged in social networking, the product promotions are done directly on mobile social networking sites. The user while logging into a mobile networking site can catch up the advertising message on one of their favourite products and may instantly ask friends about the feedback regarding the product in the form of thumbs up or thumbs down and the user decide to buy or reject the item. At the same time the product gets wide circulation among a large number of users and the promotional purpose is served. The future of mobile commerce will be greatly influenced by mobile social networking as more and more people will be linked to the social media and the retailers will get instant return on their investments in product promotions. mobile social networking will influence mobile purchase and the combination of social networking and mobile purchasing will give rise to a new model called social commerce, i.e., enhancing mobile transactions through social networking sites, Mobile payments, mobile shopping and mobile social networking together will revolutionize consumer experience and will determine the future of mobile commerce to a great extent. another important aspect of social networking sites are they store user identity information in huge databases, and this valuable user information can very well be used for validating user identity at the time of making mobile payments. Sophisticated data mining tools will be utilized in targeted advertisements. Advertisements in social networking sites will become more and more innovative and will introduce various user-friendly buttons that will help customer to purchase and /or share information with friends if they decide to do so. Thus, mobile commerce when combined with social networking will increase the sales revenue to a large extend and will bring more and more people under the purview of mobile commerce.

As more and more people have started performing mobile commerce transactions, various types of mobile applications are being developed by mobile application developers in various application areas. App developers are developing mobile payment applications, mobile banking applications, and mobile ticketing applications and so on. Retailers are launching newer applications in their mobile websites to attract customers in spot purchasing and spot payments. Various mobile coupons and other offers are sent in the form of SMS/MMS through a number of innovative, but simple user-friendly mobile apps. The main criteria of future mobile apps would be fast download and attractive graphics to engage customer attention. As social networks store valuable user information, special mobile applications will be required to collect and analyze user data and use it in strategic planning or in new product launch. Customer preference or customer buying pattern will be tracked, and accordingly targeted advertisements will be sent through customised mobile apps. Mobile gaming applications will also become predominant as smart phones with powerful processor and larger screens will become suitable for playing more complex and adventours games with rich multimedia graphics. More and more app stores will be introduced by different networks or device manufacturers, which will offer both free and paid apps in a number of application areas. This will create huge opportunities for mobile app developers who can exploit the app market and achieve considerable financial gains.

Measures for secured transaction

It is no secret that the Internet and the emergence of mobile or m-Commerce have thoroughly revolutionized traditional commerce. Developments in wireless and mobile network technologies are ensuring that this revolution continues. The constant state of change means that new vulnerabilities will continue to provide opportunities for hackers and fraudsters and security will continue to be a top priority for mobile enterprises, mobile service providers and mobile app developers alike. It is useful to consider secure m-Commerce solutions as incorporating the managerial and technological procedures and processes that are applied to mobile commerce to provide the following properties:

1. Confidentiality
2. Authentication
3. Integrity
4. Authorization
5. Availability
6. Non-repudiation

These six areas form the basis of all secure m-commerce solutions.

1. Confidentiality

States that all information must not be divulged to unauthorized persons, devices or processes. It has two types; forward and backward confidentiality.

2. Authentication

Means that each of the communicating partners are able to identify each other. The purpose of authentication is to ensure that each party to a transaction is 100% verified, trusted and is not an impostor.

3. Integrity

Maintains the protection of data and makes sure it is not altered, corrupted or changed in any way during transmission by outside unauthorized parties. The successful assurance of in-process integrity during an m-Commerce transaction greatly adds to the overall security.

4. Authorization

Steps to verify that the user is allowed to make purchases must also be facilitated.

5. Availability

Availability is where the authorized user has reliable and timely access to personal information so that he/she can adequately perform transactions. Unlike wired services, mobile unavailability of services is a big problem, if not handled properly.

6. Non--repudiation

Non--repudiation is basically the assurance that a user cannot deny that they have carried out a transaction. With m-Commerce transactions, a digital signature is commonly used to ensure that down the line a person cannot later deny that they did not carry out a given transaction. Digital signature is commonly used to ensure that down the line a person cannot later deny that they did not carry out a given transaction. Credit card fraud can be a significant problem for customers, merchants, and credit card issuers [5]. Liability for fraudulent transactions belongs to the credit card issuer for a card present, in-store transaction, but shifts to the merchant for "card not present" transactions, including transactions conducted online. This means that the merchant does not receive payment for a fraudulent online transaction. Fortunately, there are steps you can take to significantly limit your risk as an online merchant. The following important fraud prevention steps should be adhered to:

- Choose a payment services provider that is well-established and credible. Your provider should also have in-depth experience in and a strong track record for transaction security.
- Make sure your payment gateway provider offers real-time credit card authorization results. This ensures that the credit card has not been reported as lost or stolen and that it is a valid card number.
- One of the simplest ways to reduce the risk of a fraudulent transaction is to use Address Verification Service (AVS). This matches the card holder billing address on file with the billing address submitted to ensure that the card holder is the card owner.
- Use Card Security Codes, known as CVV2 for Visa, CVVC for MasterCard, and CID for American Express®. For American Express, the code is a four-digit number that appears on the front of the card above the account number. For Visa and MasterCard, the code is a three-digit number that appears at the end of the account number on the back of the card. The code is not printed on any receipts and provides additional assurance that the actual card is in possession of the person submitting the transaction.
- Watch for multiple orders for easily resold items such as electronic goods purchased on the same credit card.
- Develop a negative card and shipping address list and cross-check transactions against it. Many perpetrators will go back to the same merchant again and again to make fraudulent transactions.

"IF PRIVACY IS OUTLAWED, ONLY OUTLAWS WILL HAVE PRIVACY"

- PHILIP ZIMMERMANN