A Course Material on

Information Security

By

Mr.S.R.VALAN PRADEEP

ASSISTANT PROFESSOR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SASURIE COLLEGE OF ENGINEERING

VIJAYAMANGALAM – 638 056

QUALITY CERTIFICATE

This is to certify that the e-course material

Subject Code : **IT2042**

Scubject : INFORMATION SECURITY

Class : IV Year IT

being prepared by me and it meets the knowledge requirement of the university curriculum.

Signature of the Author

Name: Mr.S.R.VALAN PRADEEP

Designation: AP

This is to certify that the course material being prepared by Mr.S.R.VALAN PRADEEP is of adequate quality. He has referred more than five books amont them minimum one is from aborad author.

Signature of HD

Name: Mr. J. SATHISH KUMAR

SEAL

S.No.	Date	Title of Contents	Page No.
UNIT 1 - INTRODUCTION			
1.1		History	1
1.2		What is Security?	2
1.3		Critical Characteristics of Information	3
1.4		NSTISSC Security Model	6
1.5		Components of an Information System	7
1.6		Securing Components	9
1.7		Balancing Information Security and Access	10
1.8		The Systems Development Life Cycle (SDLC)	11
1.9		1.9 The Security Systems Development Life Cycle (Sec SDLC)	13
UNIT II - SECURITY INVESTIGATION			
2.1		Need for Security	19
2.2		Business Needs First	19
2.3		Threats	20
2.4		Attacks	28
2.5		Legal, Ethical, and Professional Issues in Information Security	33
UNIT III - SECURITY ANALYSIS			
3.1		Risk Management	39
3.2		Risk Identification	42
3.3		Risk Assessment	53
3.4		Risk Control Strategies	57
UNIT IV - LOGICAL DESIGN			
4.1		Information Security Policy	75

4.2		The Information Security Blueprint	79
4.3		Standard and Practice - Security Models	80
4.4		NIST Security Models	81
4.5		VISA International Security Model	86
4.6		Design of Security Architecture	87
4.7		Contingency Planning (CP)	96
UNIT V – PHYSICAL DESIGN			
5.1		Security Technology	102
5.2		Intrusion Detection System	112
5.3		Scanning and Analysis Tools	122
5.4		Cryptography	125
5.5		Access Control Devices	134
5.6		Physical Security	142
5.7		Security and Personnel	147
APPENDICES			
6.1		Glossary	152
6.2		Question Bank	160
6.3		University Question Papers	189

SYLLABUS

UNIT I INTRODUCTION 9

History, what is Information Security, Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC

UNIT II SECURITY INVESTIGATION 9

Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues

UNIT III SECURITY ANALYSIS 9

Risk Management : Identifying and Assessing Risk, Assessing and Controlling Risk

UNIT IV LOGICAL DESIGN 9

Blueprint for Security, Information Security Poicy, Standards and Practices, ISO 17799/BS 7799, NIST Models, VISA International Security Model, Design of Security Architecture,PlanningforContinuity.

UNIT V PHYSICAL DESIGN 9

Security Technology, IDS, Scanning and Analysis Tools, Cryptography, Access Control Devices, Physical Security, Security and Personnel

TOTAL : 45 PERIODS

UNIT I- INTRODUCTION

History, what is Information Security, Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC

HISTORY OF IS

ARPA
ARPANET
1970's and 80's
MULTICS
1990's
Present

Pre Requisite Discussion

The history of information security begins with the history of computer security.The need to secure physical locations, hardware and software, from outside threats.

Concepts

The department of defense's advanced research project agency (ARP) begin examining the feasibility of redundant networked communications systems to support the military exchange information.

The larry Roberts as the founder of the internet, developed the project from its inception, This project called ARPANET.

1970 and 1980's. ARPANET grew in popularity and use so did the potential for its misuse.

The Rand report R-609 which is attempted to define the multiple controls and mechanisms necessary for the protection of a multilevel computer system.

The Rand Report was the first widely recognized published document to identify the role of management and policy issues in computer security.

Multics

Multiplexed information and computing service was the first and only operating system created with the primary goal.

It implemented multiple security level and passwords, the unix system does not.

The need for resource sharing increased during th e1980's.

Present

The internets have brought many millions of unsecured computer networks into communication with each other.

The security of each computers stored information is now contingent on the level of security every other computer connected.

WHAT IS IS?

Contents

Security, Multiple layers of security, CIA Triangle.

Pre Requisite Discussion

Security: The quality or state of being secure of being to be free from danger.

Concepts: The following multiple layers of security in place to protect its operation are,

Physical security, Personal security, operational security, Communication security, network security and Information security.

The NSTISSC model of information security evolved from concept C.I.A triangle.

C.I.A Triangle

It is a computer security standard for industry, it is based on three characteristics.

Confidentiality, Integrity, Availability.

C.I.A triangle model no longer adequately addresses the constantly changing the environment of the computer industry.

CRITICAL CHARACTERISTICS OF INFORMATION

Content:

Availability

Accuracy

Authenticity

Confidentiality

Integrity

Utility & Possession

Pre requisite Discussion

When a characteristic of information changes, the value of that information either increases or more commonly decreases.

The timelines of information can be critical factor because information often loses all value when it is delivered too late.

Availability	- Access information without interference.
Accuracy	- When it is free from mistakes or errors.
Authenticity	- Information is the quality or state of being genuine or original.
Confidentiality	- Prevent exposure of confidential information
Integrity	- Information has integrity when it is whole complete and uncorrupted.
Utility	- The quality or state of having value for some purpose.
Possession	- Quality or state having ownership or content of some object or item.

NSTISSC SECURITY MODEL

Content:

Dimensions,

Dimension1: Confidentiality, Integrity, Authenticity.
Dimension2: Storage, Processing, Transmission.
Dimension3: Policy, Technology, Education.

Pre-Requisite Discussion:

NSTISSC Security Model provides the model for information security. It provides the standard policy for information security.

It presents a comprehensive model for information security, it is represented by three dimensions of each axis become a 3* 3 *3 cube with 27 cells representing areas that must be addressed to secure today's information systems.

The each cells must be addressed during the security process, the control would be a system for detecting host intrusion that protects the integrity of information by alerting the security administrators to the potential modification of critical file.

COMPONENTS OF INFORMATION SYSTEMS

Pre requisite discussion

IS (Information System is much more than computer hardware it is the entire set of hardware, data, people, procedures and networks)**.**These six critical components that enable information to be input, processed, output and stored. Each components of IS has own Security Requirements.

- Software
- Hardware
- Data
- People
- Procedures
- Networks

SECURING COMPONENTS

Content:

- Subject of an attack
- Object of an attack
- Direct attack
- Indirect attack

Pre-Requisite Discussion

Securing all components and protecting them from potential misuse and abuse by unauthorized users.

Subject of an attack - It is used as an active tool to conduct the attack.

Object of an attack - It is an entity being attack.

Direct attack - When a hacker uses his personal computer to break into a system, Originate threat itself.

Indirect attack - When a system is compromised and used to attack other systems, originate system or resource it.

BALANCING INFORMATION SECURITY AND ACCESS

Pre-requisite Discussion

The best Planning and Implementation, it is impossible to obtain perfect information security. It is a process or goal.

Concept:

Information security should balance protection and availability.

It is possible to allow a system to have unrestricted access

It poses a danger to the integrity of information.

To achieve balance that is to operate an information system to the satisfication of the user and security Professional.

SDLC (SYSTEM DEVELOPMENT LIFE CYCLE)

Pre-requisite Discussion

Information security must be managed in a manner similar to any other major system, implemented in an organization.

Methodology-Formal approach for solving the problem, based structured sequence procedures, it increase probability of success.

The phases are,

Investigation

Analysis

Logical Design

Physical Design

Implementation

Maintenance

SECURITY SYSTEM DEVELOPMENT LIFE CYCLE

Content

The same phases used in the system development life cycle.

Pre-Requisite Discussion

Implementing information security involves identifying specific threats and creating specific controls to counter those threats.

Concepts

Investigation - Management defines program security policy
Analysis - Analyze existing , current threats & security policy
Logical Design - Develop or select technology

Physical Design - Measures to support technological solutions
Implementation - Buy or develop security solutions at end present tested package to management for approval.
Maintenance - Constantly, monitor, test, modify, update and repair to meet changing threats.

UNIT II SECURITY INVESTIGATION

Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues

CONTENTS

- Need for security-Introduction
- Business needs-Protecting function, enabling safe operation, Protecting Data, Safeguarding technology assets.
- Threats- Act of human error, Intellectual Property, Acts of trespass, acts of information extortion, acts of theft, software attacks, forces of nature, deviations in Q o S, Technical Hardware failures or errors, Technical software failures or error, Technical obsolesce.
- Attacks-Malicious code, Hoaxes, Back doors, Brute force, Dictionary, Denial of Service (D o S), Spoofing, Man in middle, Spam, mail bombing, sniffers, social engineering, buffer overflow, timing attack.
- Legal, ethical, professional issues in information security.

Pre-Requisite Discussion

- To understand the business need for IS.
- To understand that successful information security program.
- Identify the threats to the information security.
- Differentiate between laws and ethics.
- Identify major national law.
- Understand the role of culture as it applies to ethics in IS.

Concepts

- Need for security
- Business needs first
- Enabling safe operation
- Protecting Data
- Safe guarding Technology Assets

Attacks – it is an act or action, It accomplished by threat agent damages an organisation information or physical asset.

Malicious code-includes the execution of virus, worm, Trojan horse and active web scripts.

Hoaxes-It is a approach to attacking the computer system is the transmission of a virus hoax with a real virus attached.

Backdoors- using a known or previously unknown and newly discovered access mechanism, attacker can gain access to a system or network resource through a back door.

Password crack-attempting to reverse calculate password is often called cracking, using same algorithm

Brute force-combination of options of a password is called a brute force attack.

Dictionary-another form of brute force for guessing passwords, it uses a list of commonly used passwords instead of random combinations.

Denial of Service- attacker sends number of connection for the request of target.

Spoofing-a technique used the IP address to unauthorized access to computer, hacker use a variety of techniques to find an IP address of a trusted host and then modify the parallel address of router.

Man in middle-also called as Hijacking TCP attack, uses IP Spoofing, and attacker monitors packet from the network, modifies them and inserts back into the network.

Spam-used to make malicious code attacks more effective.

Mail Bombing- attacker sends more number of emails to an address.

Sniffers- a program or device that can monitor data traveling over a network.

LEGAL, ETHICAL AND PROFESSIONAL ISSUES IN IS

Concept

Laws are rule that mandate or prohibit certain behaviour in society.

Pre-Requisite Discussion

Types of law:

Civil law, Criminal law, Tort law.

General computer crime laws
Privacy
Export and Esionage Laws
U.S Copyright law
Financial Reporting
Freedom of information Act of 1966

International laws and legal Bodies

Digital millennium copyright act-used to reduce the impact of copyright trademark and privacy infringement.

United nation character-makes provision for information security during information warfare.

Policy versus Law

Policy-describe acceptable and unacceptable employee behaviours in the workplace.

Law-Complete with penalities, judicial practice and sanctions of require compliance.

Ethics and Information security

It deals with conflicts about the art of ethics and morality in workplace.

Deterrence to unethical and illegal behaviour

Illegal is a immortal or unethical behaviour, there are general categories include, ignorance ,Accident and intent

Deterrence

Three conditions, Fear of penality, probability of being caught, Probability of penalty being administrated.

Code of ethics and Professional organizations

Association of computer machinery
Computer security institute
Internet society
IS audit and control association
IS system security association
International information system security certification consortium.

Other security organizations are,

Internet society
Computer Security Division
CERT Coordination center
Computer professional for social Responsibility.

Due Diligence
Jurisdiction

UNIT III - SECURITY ANALYSIS

Risk Management : Identifying and Assessing Risk, Assessing and Controlling Risk

Contents

An overview of risk managaement
Risk identification
Risk assessment
Risk control strategies
Selecting a risk control strategies

Pre-requisite Discussion

- It defines the risk management, risk identification, and risk control
- Understand how risk is identified and assessed
- Describe the risk mitigation strategy options for controlling risks
- Identifying the categories that can be used to classify control
- Assess risk based on probability of occurrence.

Overview

- The formal process of identifying and controlling risk involves, know yourself, know the enemy.
- There are three steps,
    - Risk identification-process of examining and document the security of an organizations
    - Risk assessment-assigns a risk rating or score the information asset
    - Risk control-four basic strategies to control risk from vulnerabilities
- The iterative process and data asset identification involves people, procedure, data
- Hardware, software, and network asset identification
- Automated risk management tools
- Information asset classification
- Information asset valuation
- Data classification-Confidential, internal, external
- Security clearances
- Management of classified data includes storage, distribution, valuable proper care should be taken to destroy them.
- Threat identification because they are danger to the organization.
- Vulnerability identification are specific that threat agent can be exploit to attack an information asset.

Risk identification

- Risk assessment includes risk rating or score to information asset
- Likelihood is the probability of specific vulnerability with organization.
- Valuation of information asset assigns weighted scores for the value of organization asset
  - ✓ Risk determination =[(likelihood of vulnerability occurrence)*(value of
    - information asset)-[% of risk mitigation by current controls]+uncertainity of current]
- Identify possible controls (for residual risk) is the risk that remains to the information
- even after the existing control has been applied.
- Three general categories of controls are, Policies, programs, technologies.
- Access control are particular application of control in access.
- Types of access controls are mandatory access control, Non discretionary control,
- discretionary control, Latice based access control.

Risk assessment and Risk control strategies

- Apply safeguards that eliminate the remaining
- Transfer the risk to other areas or to outside
- Reduce the impact should be vulnerability be exploited
- Understand the consequences and accept the risk
- Three common methods of risk avoidance are,
  - Application of policy
  - Application of training
  - Application of technology
- Transference is the control application to shift the risk to other asset
- Mitigation is control approach that attempts to reduce the impact caused by the other asset, they are,
- Incident response plan-it provides answers to questions such as what to do now, what should the administrator do first, whom should they contact, what should they document.

Disaster recovery plan – to limit loses before and during the disaster, it focuses more or preparations completed before actions taken after the incident.

Business continuity plan –it is the most strategic and long term of the three phases.

Selecting a risk control strategies

The level of threat and value of asset play major role selection of strategy,

- Evaluation assessment and maintenance of risk controls
- Categories of controls are, control function, architecture layer,

- organization policy, strategic layer.
- Characteristics of secure information are, confidentiality, integrity, availability, authenticity, authorization, accountability, Privacy.
- Feasibility studies include, deciding before the strategy.
- Cost avoidance
- Cost benefit analysis
- Bench marking
- Applying best policies
- Base lining
- Residual risk
- Documenting risk
- Quality measure and recommended practices in risk.

UNIT IV LOGICAL DESIGN

Blueprint for Security, Information Security Poicy, Standards and Practices, ISO 17799/BS 7799, NIST Models, VISA International Security Model, Design of Security Architecture,PlanningforContinuity.

Contents

Definitions
Enterprise information security
Issue specific security policy
System specific policy
Policy management
Information classification

Prerequisite discussion

Describe management role in the development maintenance and enforcement of information security policy standard practices,guidelines.

Understand what is information security blueprint

Understand how organization institutionalizes its policies,standards,and practices.

Explain what contingency planning is and how incident reponse planning diasaster recovery planning and continuity are related to contigency planning.

Information security policy standards and practices

Planning for security
Why policy
Types of policies
Issues specific security policy
Components of policy
Systems specific policy
ACL policies
Responsible individual

Schedule of reviews
Review procedures and policies
Policy and revision date
Automated policy management

Security model

ISO 17799/BS 7799

It is one most widely used and often discussed security model for IT which is published as British model.

Objectives of ISO 17799

1. Organisational security policy
2. Organisational security infra structure
3. Personal security
4. System access control
5. System development and maintenance
6. Compliance

NIST SECURITY MODEL

It refers to national security telecommunications and IS security committee, which assist the design of a security framework

NIST SP 800-12
NIST SP 800-14
NIST SP 800-18
NIST SP 800-26
NIST SP 800-30

VISA INTERNATIONAL SECURITY MODEL

It promotes security measures in its business associates where,

Security asasesment process
Agreed upon procedures

Base lining and best business practices
Hybrid framework for a blueprint of an information security system

Design of security architecture

Defence in depth requires that the organization establish sufficient security controls
Layers organized into policy,training, education
Implemented by firewall,proxy servers.

Security perimeter

Key technolony components

Firewall,gateway router, dm2s,intrusion detection system

CONTINUING STRATEGIES

To assure the continous availability of IS
Business continuity plans
Disaster recovery plans

Incident response plans
Champion
Project manager
Team members
Business impact analysis(BIA)
Incident recovery
Law enforcement involvement
Model for consolidated involvement

UNIT V PHYSICAL DESIGN

Security Technology, IDS, Scanning and Analysis Tools, Cryptography, Access Control Devices, Physical Security, Security and Personnel

Content

Security technology
Intrusion detection systems
Scanning and analysis tools
Access control devices
Cryptography
Physical security
Security personnel

Pre requisite discussion

Identify and describe the categories and operating mode of intrusion detection systems.
List and define major categories of scanning tools used within each categories.
Major protocols for secure communication
Various approach to access control including use of biometric access mechanisms
Tools and describe the specific tools used within each categories.

Security technology

Intrusion is a type of attack on information asset it distrup normal operation on system.
IDS Terminology
Why use an IDS?

Types of IDS and detection methods

Network based IDS
NIDS signature matching
Protocol Stack Verification
Host based IDS
Signature based IDS
Statistical anomaly based IDS
Deployment and Implementation of IDS
IDS control strategies

Measuring the effectiveness of IDS
Active Intrusion Prevention

Scanning & analysis tools

Port scanners
Firewall analysis tools
Vulnerability scanners
Packet sniffers
Wireless security tools

Access control devices

What a supplicant knows
What a supplicant has
Who supplicant
What a supplicant procedures

Cryptography

Encryption
Decryption
Principles of cryptography
Cryptography tools
Protocols for secure communication
Attacks on crptosystems

Employment policies practices

Job descriptions,interviews,background,checks,employment contracts,new hire orientation, new hire orientation,performance evaluation,termination

Security considerations for non employees

Temporary employees
Contract employees
Consultants

Security and personnel

Positioning and staffing the security function
Credentials of IS

Failure of supporting utilities and structural collapse

Heating,ventilation, air conditioning
Temperature and filtration
Humidity and static electricity
Ventilation shafts
Water problems
Structural collapse
Remote computing security

Special considerations for physical security threats

Networking,applications,development,administrativeserver,insurance,risk management,legal department.

APPLICATION AREAS OF INFORMATION SECURITY

All private and government organizations.

SIGNIFICANCE

Port scanners

Firewall analysis tools

Packet sniffers

Wireless security tools and other scanning and analysis tools.

UNIT 1 - INTRODUCTION

1.1 HISTORY

- ✓ Julius Caesar-Caesar Cipher c50 B.C., which was created in order to prevent his secret messages from being, read should a message fall into the wrong hands.
- ✓ The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption.

Introduction

Information technology is the vehicle that stores and transports information—a company's most valuable resource—from one business unit to another. But what happens if the vehicle breaks down, even for a little while? As businesses have become more fluid, the concept of computer security has been replaced by the concept of information security.

Because this new concept covers a broader range of issues, from the protection of data to the protection of human resources, information security is no longer the sole responsibility of a discrete group of people in the company; rather, it is the responsibility of every employee, and especially managers.

Organizations must realize that information security funding and planning decisions involve more than just technical managers: Rather, the process should involve three distinct groups of decision makers, or communities of interest:

- ✓ Information security managers and professionals
- ✓ Information technology managers and professionals
- ✓ Nontechnical business managers and professionals

These communities of interest fulfill the following roles:

- ✓ The information security community protects the organization's information assets from the many threats they face.
- ✓ The information technology community supports the business objectives of the organization by supplying and supporting information technology appropriate to the business' needs.
- ✓ The nontechnical general business community articulates and communicates organizational policy and objectives and allocates resources to the other groups.

1.2 WHAT IS SECURITY?

Understanding the technical aspects of information security requires that you know the definitions of certain information technology terms and concepts. In general, security is defined as "the quality or state of being secure—to be free from danger."

Security is often achieved by means of several strategies usually undertaken simultaneously or used in combination with one another.

Specialized areas of security

- ✓ **Physical security**, which encompasses strategies to protect people, physical assets, and the workplace from various threats including fire, unauthorized access, or natural disasters
- ✓ **Personal security**, which overlaps with physical security in the protection of the people within the organization
- ✓ **Operations security**, which focuses on securing the organization's ability to carry out its operational activities without interruption or compromise

- ✓ **Communications security**, which encompasses the protection of an organization's communications media, technology, and content, and its ability to use these tools to achieve the organization's objectives

- ✓ **Network security**, which addresses the protection of an organization's data networking devices, connections, and contents, and the ability to use that network to accomplish the organization's data communication functions

- ✓ **Information security** includes the broad areas of information security management, computer and data security, and network security.

Where it has been used?

- ✓ Governments, military, financial institutions, hospitals, and private businesses.

- ✓ Protecting confidential information is a business requirement.

1.2.1 Information Security components:

- ✓ Confidentiality

- ✓ Integrity

- ✓ Availability(CIA)

CIA Triangle

The C.I.A. triangle - confidentiality, integrity, and availability - has expanded into a more comprehensive list of critical characteristics of information. At the heart of the study of information security is the concept of policy. Policy, awareness, training, education, and technology are vital concepts for the protection of information and for keeping information systems from danger.

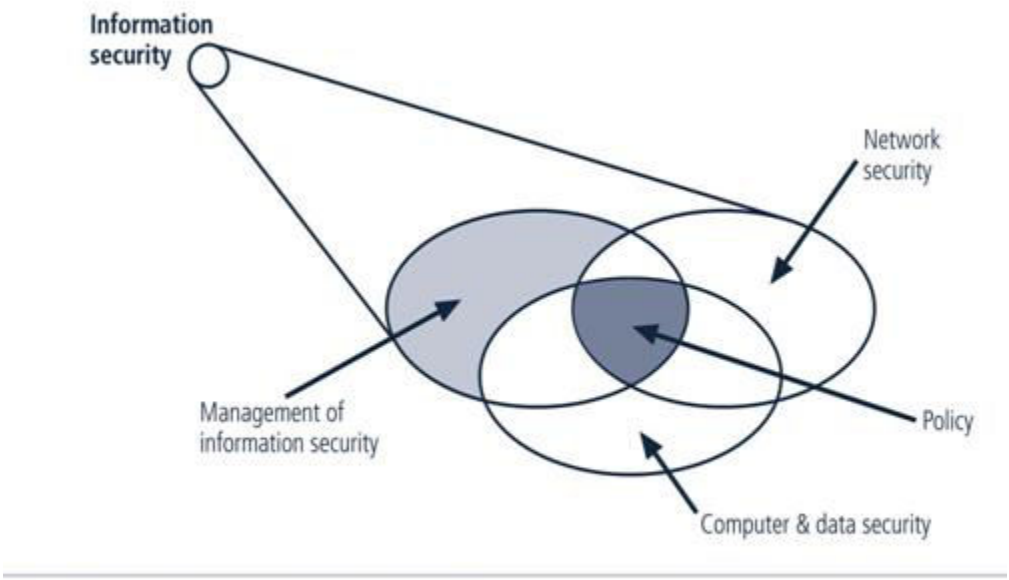


Figure 1.2.1.1 Components of Information Security

1.3 CRITICAL CHARACTERISTICS OF INFORMATION

- ✓ Confidentiality
  - Integrity
- ✓ Availability
  - Privacy
  - Identification
  - Authentication
  - Authorization
  - Accountability
- ✓ Accuracy

Utility

Possession

1.3.1 Confidentiality

Confidentiality of information ensures that only those with sufficient privileges may access certain information. When unauthorized individuals or systems can access information, confidentiality is breached. To protect the confidentiality of information, a number of measures are used:

- ✓ Information classification
- ✓ Secure document storage
- ✓ Application of general security policies
- ✓ Education of information custodians and end users

Example, a credit card transaction on the Internet.

- ✓ The system attempts to enforce confidentiality by encrypting the card number during transmission, by limiting the places where it might appear (in data bases, log files, backups, printed receipts, and so on), and by restricting access to the places where it is stored.
- ✓ Giving out confidential information over the telephone is a breach of confidentiality if the caller is not authorized to have the information, it could result in a breach of confidentiality.

Integrity

Integrity is the quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when it is exposed to corruption, damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being compiled, stored, or transmitted.

- ✓ Integrity means that data cannot be modified without authorization.
- ✓ Eg: Integrity is violated when an employee deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a website, when someone is able to cast a very large number of votes in an online poll, and so on.

1.3.2 Availability

Availability is the characteristic of information that enables user access to information without interference or obstruction and in a required format. A user in this definition may be either a person or another computer system. Availability does not imply that the information is accessible to any user; rather, it means availability to authorized users.

- ✓ For any information system to serve its purpose, the information must be available when it is needed.
- ✓ Eg: High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.

Privacy

The information that is collected, used, and stored by an organization is to be used only for the purposes stated to the data owner at the time it was collected. This definition of privacy does focus on freedom from observation (the meaning usually associated with the word), but rather means that information will be used only in ways known to the person providing it.

Identification

An information system possesses the characteristic of identification when it is able to recognize individual users. Identification and authentication are essential to establishing the level of access or authorization that an individual is granted.

Authentication

Authentication occurs when a control provides proof that a user possesses the identity that he or she claims.

- ✓ In computing, e-Business and information security it is necessary to ensure that the data, transactions, communications or documents(electronic or physical) are genuine(i.e. they have not been forged or fabricated)

Authorization

After the identity of a user is authenticated, a process called authorization provides assurance that the user (whether a person or a computer) has been specifically and explicitly authorized by the proper authority to access, update, or delete the contents of an information asset.

Accountability

The characteristic of accountability exists when a control provides assurance that every activity undertaken can be attributed to a named person or automated process. For example, audit logs that track user activity on an information system provide accountability.

1.3.3 Accuracy

Information should have accuracy. Information has accuracy when it is free from mistakes or errors and it has the value that the end users expects. If information contains a value different from the user's expectations, due to the intentional or unintentional modification of its content, it is no longer accurate.

Utility

Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful 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.

1.4 NSTISSC SECURITY MODEL

'National Security Telecommunications & Information systems security committee' document.

It is now called **the National Training Standard for Information security professionals.**

The NSTISSC Security Model provides a more detailed perspective on security.

While the NSTISSC model covers the three dimensions of information security, it omits discussion of detailed guidelines and policies that direct the implementation of controls.

Another weakness of using this model with too limited an approach is to view it from a single perspective.

- ✓ The 3 dimensions of each axis become a 3x3x3 cube with 27 cells representing areas that must be addressed to secure today's Information systems.
- ✓ To ensure system security, each of the 27 cells must be properly addressed during the security process.
- ✓ For example, the intersection between technology, Integrity & storage areas requires a control or safeguard that addresses the need to use technology to protect the Integrity of information while in storage.

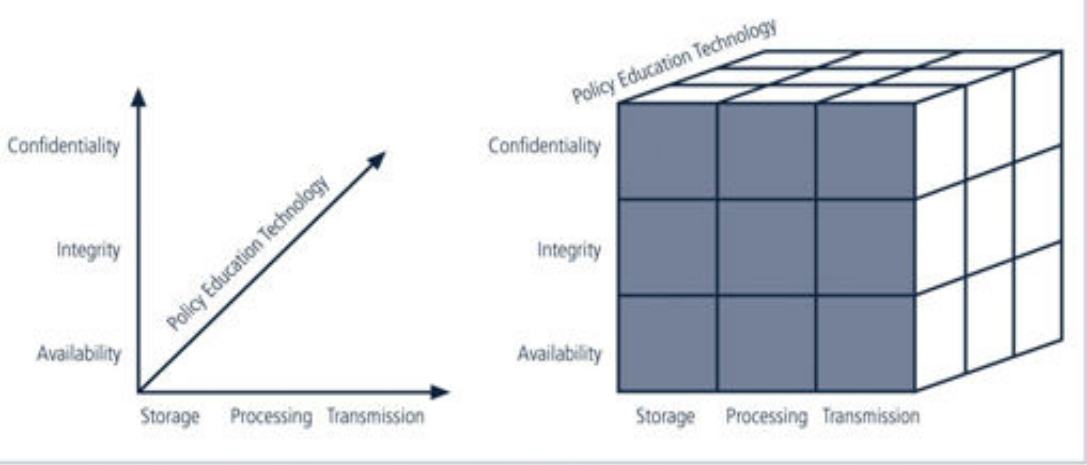


Figure 1.4.1 NSTISSC Security Model

1.5 COMPONENTS OF AN INFORMATION SYSTEM

- ✓ Software
- ✓ Hardware
- ✓ Data
- ✓ People
- ✓ Procedures
- ✓ Networks

1.5.1 Software

- ✓ The software components of IS comprises applications, operating systems, and assorted command utilities.
- ✓ Software programs are the vessels that carry the lifeblood of information through an organization. These are often created under the demanding constraints of project management, which limit time, cost, and manpower.

1.5.2 Hardware

- ✓ Hardware is the physical technology that houses and executes the software, stores and carries the data, and provides interfaces for the entry and removal of information from the system.
- ✓ Physical security policies deal with hardware as a physical asset and with the protection of these physical assets from harm or theft. Applying the traditional tools of physical

security, such as locks and keys, restricts access to and interaction with the hardware components of an information system.

- ✓ Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

1.5.3 Data

- ✓ Data stored, processed, and transmitted through a computer system must be protected.
- ✓ Data is often the most valuable asset possessed by an organization and is the main target of intentional attacks.
- ✓ The raw, unorganized, discrete(separate, isolated) potentially-useful facts and figures that are later processed(manipulated) to produce information.

1.5.4 People

There are many roles for people in information systems. Common ones include

- ✓ Systems Analyst
- ✓ Programmer
- ✓ Technician
- ✓ Engineer
- ✓ Network Manager
- ✓ MIS (Manager of Information Systems)
- ✓ Data entry operator

1.5.5 Procedures

A procedure is a series of documented actions taken to achieve something. A procedure is more than a single simple task. A procedure can be quite complex and involved, such as performing a backup, shutting down a system, patching software.

1.5.6 Networks

- ✓ When information systems are connected to each other to form Local Area Network (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.

- ✓ Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

1.6 SECURING COMPONENTS

Protecting the components from potential misuse and abuse by unauthorized users.

- ✓ **Subject of an attack**

  Computer is used as an active tool to conduct the attack.

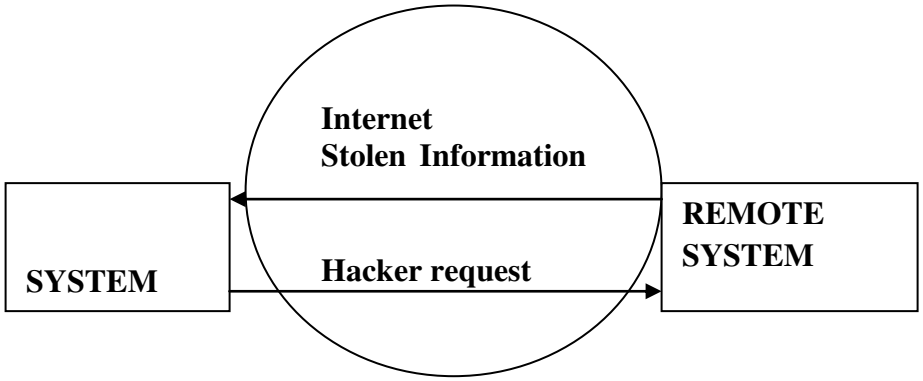
- ✓ **Object of an attack**

  Computer itself is the entity being attacked

Two types of attacks:

1. Direct attack

2. Indirect attack



Hacker using a computer as the subject of attack

Remote system that is the object of an attack

Figure 1.6.1 Attack

1. Direct attack

When a Hacker uses his personal computer to break into a system.[Originate from the threat itself]

2. Indirect attack

When a system is compromised and used to attack other system.

[Originate from a system or resource that itself has been attacked, and is malfunctioning or working under the control of a threat].

A computer can, therefore, be both the subject and object of an attack when ,for example, it is first the object of an attack and then compromised and used to attack other systems, at which point it becomes the subject of an attack.

1.7 BALANCING INFORMATION SECURITY AND ACCESS

- ✓ Has to provide the security and is also feasible to access the information for its application.
- ✓ Information Security cannot be an absolute: it is a process, not a goal.
- ✓ Should balance protection and availability.

Approaches to Information Security Implementation

- ✓ Bottom- up- approach.
- ✓ Top-down-approach
  - ✓ Has higher probability of success.
  - ✓ Project is initiated by upper level managers who issue policy & procedures & processes.
  - ✓ Dictate the goals & expected outcomes of the project.
  - ✓ Determine who is suitable for each of the required action.

1.8 THE SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

SDLC Waterfall Methodology

SDLC-is a methodology for the design and implementation of an information system in an organization.

- ✓ A methodology is a formal approach to solving a problem based on a structured sequence of procedures.
- ✓ SDLC consists of 6 phases.

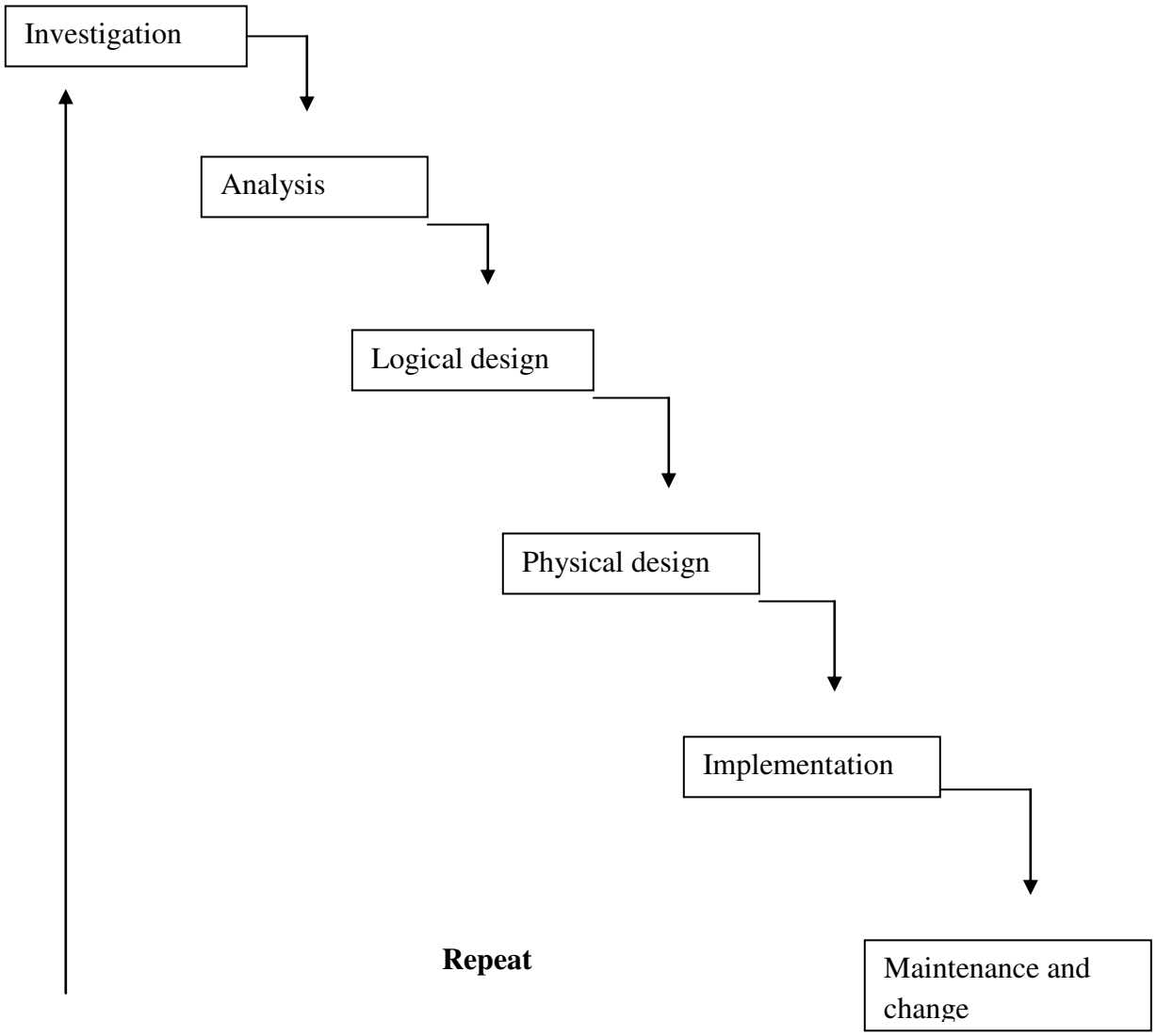


Figure 1.8.1 Systems Development Life Cycle

1.8.1 Investigation

- ✓ It is the most important phase and it begins with an examination of the event or plan that initiates the process.
- ✓ During this phase, the objectives, constraints, and scope of the project are specified.
- ✓ At the conclusion of this phase, a feasibility analysis is performed, which assesses the economic, technical and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

1.8.2 Analysis

- ✓ It begins with the information gained during the investigation phase.
- ✓ It consists of assessments (quality) of the organization, the status of current systems, and the capability to support the proposed systems.
- ✓ Analysts begin by determining what the new system is expected to do, and how it will interact with existing systems.
- ✓ This phase ends with the documentation of the findings and an update of the feasibility analysis.

1.8.3 Logical Design

- ✓ In this phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem.
- ✓ Based on the business need, applications are selected that are capable of providing needed services.
- ✓ Based on the applications needed, data support and structures capable of providing the needed inputs are then chosen.
- ✓ In this phase, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits.
- ✓ At the end of this phase, another feasibility analysis is performed.

1.8.4 Physical design

- ✓ In this phase, specific technologies are selected to support the solutions developed in the logical design.

- ✓ The selected components are evaluated based on a make-or-buy decision.
- ✓ Final designs integrate various components and technologies.

1.8.5 Implementation

- ✓ In this phase, any needed software is created.
- ✓ Components are ordered, received and tested.
- ✓ Afterwards, users are trained and supporting documentation created.
- ✓ Once all the components are tested individually, they are installed and tested as a system.
- ✓ Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test.

1.8.6 Maintenance and change

- ✓ It is the longest and most expensive phase of the process.
- ✓ It consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle.
- ✓ Periodically, the system is tested for compliance, with business needs.
- ✓ Upgrades, updates, and patches are managed.
- ✓ As the needs of the organization change, the systems that support the organization must also change.
- ✓ When a current system can no longer support the organization, the project is terminated and a new project is implemented.

1.9 THE SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE (SEC SDLC)

The same phases used in the traditional SDLC can be adapted to support the implementation of an information security project.

1.9.1 Sec SDLC phases

Investigation

- ✓ This phase begins with a directive from upper management, dictating the process, outcomes, and goals of the project, as well as its budget and other constraints.

- ✓ Frequently, this phase begins with an **enterprise information security policy**, which outlines the implementation of a security program within the organization.
- ✓ Teams of responsible managers, employees, and contractors are organized.
- ✓ Problems are analyzed.
- ✓ Scope of the project, as well as specific goals and objectives, and any additional constraints not covered in the program policy, are defined.
- ✓ Finally, an organizational feasibility analysis is performed to determine whether the organization has the resources and commitment necessary to conduct a successful security analysis and design.

Analysis

- ✓ In this phase, the documents from the investigation phase are studied.
- ✓ The developed team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls.
- ✓ The risk management task also begins in this phase.

Risk management is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization.

Logical design

- ✓ This phase creates and develops the blueprints for information security, and examines and implements key policies.
- ✓ The team plans the incident response actions.
- ✓ Plans business response to disaster.
- ✓ Determines feasibility of continuing and outsourcing the project.

Physical design

- ✓ In this phase, the information security technology needed to support the blueprint outlined in the logical design is evaluated.
- ✓ Alternative solutions are generated.
- ✓ Designs for physical security measures to support the proposed technological solutions are created.

- ✓ At the end of this phase, a feasibility study should determine the readiness of the organization for the proposed project.
- ✓ At this phase, all parties involved have a chance to approve the project before implementation begins.

Implementation

- ✓ Similar to traditional SDLC
- ✓ The security solutions are acquired (made or bought), tested, implemented, and tested again
- ✓ Personnel issues are evaluated and specific training and education programs are conducted.
- ✓ Finally, the entire tested package is presented to upper management for final approval.

Maintenance and change

- ✓ Constant monitoring, testing, modification, updating, and repairing to meet changing threats have been done in this phase.

1.9.2 Security Professionals and the organization

Senior management

Chief information Officer (CIO) is the responsible for

- ✓ Assessment
- ✓ Management
- ✓ And implementation of information security in the organization

Information Security Project Team

- ✓ **Champion**
  - Promotes the project
  - Ensures its support, both financially & administratively.
- ✓ **Team Leader**
  - Understands project management
  - Personnel management

- And information Security technical requirements.

✓ **Security policy developers**

- individuals who understand the organizational culture,
- existing policies
- Requirements for developing & implementing successful policies.

✓ **Risk assessment specialists**

- Individuals who understand financial risk assessment techniques.
- The value of organizational assets,
- and the security methods to be used.

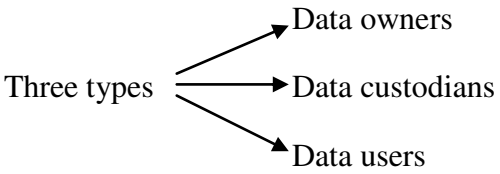
✓ **Security Professionals**

- Dedicated
- Trained, and well educated specialists in all aspects of information security from both a technical and non technical stand point.

✓ **System Administrators**

- Administrating the systems that house the information used by the organization.

✓ **End users**



Data Owners

- Responsible for the security and use of a particular set of information.
- Determine the level of data classification
- Work with subordinate managers to oversee the day-to-day administration of the data.

Data Custodians

- Responsible for the storage, maintenance, and protection of the information.

- Overseeing data storage and backups
- Implementing the specific procedures and policies.

Data Users (End users)

- Work with the information to perform their daily jobs supporting the mission of the organization.
- Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

1.9.3 Key Terms in Information Security Terminology

✓ **Asset**

-An asset is the organizational resource that is being protected.

-An Asset can be logical ,such as

➔ Website, information or data

- Asset can be physical, such as

➔ person , computer system

✓ **Attack**

- An attack is an intentional or unintentional attempt to cause damage to or otherwise compromise the information and /or the systems that support it. If someone casually reads sensitive information not intended for his use, this is considered a passive attack. If a hacker attempts to break into an information system, the attack is considered active.

✓ **Risk**

- Risk is the probability that something can happen. In information security, it could be the probability of a threat to a system.

✓ **Security Blueprint**

- It is the plan for the implementation of new security measures in the organization. Sometimes called a frame work, the blueprint presents an organized approach to the security planning process.

✓ **Security Model**

- A security model is a collection of specific security rules that represents the implementation of a security policy.

✓ **Threats**

- A threat is a category of objects, persons, or other entities that pose a potential danger to an asset. Threats are always present. Some threats manifest themselves in accidental occurrences, while others are purposeful. For example, all hackers represent potential danger or threat to an unprotected information system. Severe storms are also a threat to buildings and their contents.

✓ **Threat agent**

- A threat agent is the specific instance or component of a threat. For example, you can think of all hackers in the world as a collective threat, and Kevin Mitnick, who was convicted for hacking into phone systems, as a specific threat agent. Likewise, a specific lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.

✓ **Vulnerability**

- Weaknesses or faults in a system or protection mechanism that expose information to attack or damage are known as vulnerabilities. Vulnerabilities that have been examined, documented, and published are referred to as **well-known vulnerabilities.**

✓ **Exposure**

- The exposure of an information system is a single instance when the system is open to damage. Vulnerabilities can cause an exposure to potential damage or attack from a threat. Total exposure is the degree to which an organization's assets are at risk of attack from a threat..

UNIT II - SECURITY INVESTIGATION

2.1 NEED FOR SECURITY

The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents. The Audit Commission Update report (1998) shows that fraud or cases of IT abuse often occur due to the absence of basic controls, with one half of all detected frauds found by accident. An Information Security Management System (ISMS) enables information to be shared, whilst ensuring the protection of information and computing assets.

At the most practical level, securing the information on your computer means:

- ✓ Ensuring that your information remains confidential and only those who *should* access that information, *can*.
- ✓ Knowing that no one has been able to change your information, so you can depend on its accuracy (information integrity).
- ✓ Making sure that your information is available when you need it (by making back-up copies and, if appropriate, storing the back-up copies off-site).

2.2 BUSINESS NEEDS FIRST

Information security performs four important functions for an organization:

1. Protects the organization's ability to function
2. Enables the safe operation of applications implemented on the organization's IT systems.
3. Protects the data the organization collects and uses.
4. Safeguards the technology assets in use at the organization.

1. Protecting the functionality of an organization

- ✓ Decision makers in organizations must set policy and operate their organizations in compliance with the complex, shifting legislation that controls the use of technology.

2. Enabling the safe operation of applications

- ✓ Organizations are under immense pressure to acquire and operate integrated, efficient, and capable applications
- ✓ The modern organization needs to create an environment that safeguards applications using the organization's IT systems, particularly those applications that serve as important elements of the infrastructure of the organization.

3. Protecting data that organizations collect & use

- ✓ Protecting data in motion
- ✓ Protecting data at rest
- ✓ Both are critical aspects of information security.
- ✓ The value of data motivates attackers to seal, sabotage, or corrupt it.
- ✓ It is essential for the protection of integrity and value of the organization's data

4. Safeguarding Technology assets in organizations

- ✓ Must add secure infrastructure services based on the size and scope of the enterprise.
- ✓ Organizational growth could lead to the need for **public key infrastructure,** PKI, an integrated system of software, encryption methodologies.

2.3 THREATS

To protect an organization's information, you must

1. Know yourself

(i.e) be familiar wit the information to be protected, and the systems that store, transport and process it.

2. Know the threats you face

To make sound decisions about information security, management must be informed about the various threats facing the organization, its application, data and information systems.

A threat is an object, person, or other entity, that represents a constant danger to an asset.

2.3.1 Threats to Information Security

Categories of threat		Examples
Acts of human error or failure	--	Accidents, employee mistakes
Compromises to intellectual property	--	Piracy, copyright infringement
Deliberate acts of espionage or trespass	--	Unauthorized access and/or/data collection
Deliberate acts of information extortion	--	Blackmail or information disclosure
Deliberate acts of sabotage or vandalism	--	Destruction of systems or information
Deliberate acts of theft	--	Illegal confiscation of equipment or information
Deliberate software attacks	--	Viruses, worms, macros, denial-of-service
Forces of nature	--	Fire, flood, earthquake, lightning
Deviations in quality of service	--	ISP, power ,or WAN service providers
Technical hardware failures or errors	--	Equipment failure
Technical software failures or errors	--	Bugs, code problems, unknown loopholes
Technological obsolescence	--	Antiquated or outdated technologies

2.3.2 Threats

1. Acts of Human Error or Failure:

- ✓ Acts performed without intent or malicious purpose by an authorized user.
- ✓ because of in experience ,improper training,
- ✓ Making of incorrect assumptions.

One of the greatest threats to an organization's information security is the organization's own employees.

- ✓ Entry of erroneous data

- ✓ accidental deletion or modification of data
- ✓ storage of data in unprotected areas.
- ✓ Failure to protect information can be prevented with

  - Training

  - Ongoing awareness activities

  -Verification by a second party

  - Many military applications have robust, dual- approval controls built in .

2. Compromises to Intellectual Property

- ✓ **Intellectual Property** is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas.
- ✓ Intellectual property includes trade secrets, copyrights, trademarks, and patents.
- ✓ Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information.
- ✓ Organization purchases or leases the IP of other organizations.
- ✓ Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as **software Piracy**.
- ✓ Software Piracy affects the world economy.
- ✓ U.S provides approximately 80% of world's software.

In addition to the laws surrounding software piracy, two watch dog organizations investigate allegations of software abuse.

1. Software and Information Industry Association (SIIA)

   (i.e)Software Publishers Association

2. Business Software Alliance (BSA)

   - Another effort to combat (take action against) piracy is the online registration process.

3. Deliberate Acts of Espionage or Trespass

- ✓ Electronic and human activities that can breach the confidentiality of information.
- ✓ When an unauthorized individual's gain access to the information an organization is trying to protect is categorized as act of espionage or trespass.
- ✓ Attackers can use many different methods to access the information stored in an information system.

1. Competitive Intelligence[use web browser to get information from market research]
2. Industrial espionage(spying)
3. Shoulder Surfing(ATM)

Trespass

- ✓ Can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.
- ✓ Sound principles of authentication & authorization can help organizations protect valuable information and systems.
- ✓ **Hackers->** "People who use and create computer software to gain access to information illegally"
- ✓ There are generally two skill levels among hackers.
- ✓ **Expert Hackers**-> Masters of several programming languages, networking protocols, and operating systems .
- ✓ **Unskilled Hackers**

4. Deliberate Acts of information Extortion (obtain by force or threat)

- ✓ Possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement not to disclose the information.

5. Deliberate Acts of sabotage or Vandalism

- ✓ Destroy an asset or
- ✓ Damage the image of organization
- ✓ Cyber terrorism-Cyber terrorists hack systems to conduct terrorist activities through network or internet pathways.

6. Deliberate Acts of Theft

- ✓ Illegal taking of another's property-- is a constant problem.
- ✓ Within an organization, property can be physical, electronic, or intellectual.
- ✓ Physical theft can be controlled by installation of alarm systems.
- ✓ Trained security professionals.
- ✓ Electronic theft control is under research.

7. Deliberate Software Attacks

- ✓ Because of **malicious code** or **malicious software** or sometimes **malware.**
- ✓ These software components are designed to damage, destroy or deny service to the target system.
- ✓ More common instances are
    - Virus, Worms, Trojan horses, Logic bombs, Backdoors.
- ✓ "The British Internet Service Provider Cloudnine" be the first business "hacked out of existence"

7.1 Virus

- ✓ Segments of code that performs malicious actions.
- ✓ Virus transmission is at the opening of Email attachment files.
- ✓ **Macro virus**-> Embedded in automatically executing macrocode common in word processors, spreadsheets and database applications.
- ✓ **Boot Virus**-> infects the key operating files located in the computer's boot sector.

7.2 Worms

- ✓ A worm is a malicious program that replicates itself constantly, without requiring another program to provide a safe environment for replication.
- ✓ Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.
- ✓ Eg: MS-Blaster, MyDoom, Netsky, are multifaceted attack worms.
- ✓ Once the worm has infected a computer , it can redistribute itself to all e-mail addresses found on the infected system.
- ✓ Furthermore, a worm can deposit copies of itself onto all Web servers that the infected systems can reach, so that users who subsequently visit those sites become infected.

7.3 Trojan Horses

- ✓ Are software programs that hide their true nature and reveal their designed behavior only when activated.

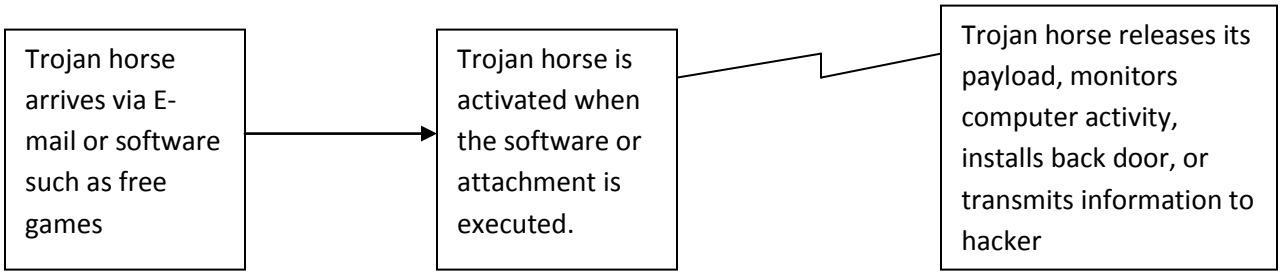


Figure 7.3.1 Trojan horse Attack

7.4 Back Door or Trap Door

- ✓ A Virus or Worm has a payload that installs a backdoor or trapdoor component in a system, which allows the attacker to access the system at will with special privileges.

Eg: Back Orifice

Polymorphism

- ✓ A **Polymorphic threat** is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures.
- ✓ These viruses and Worms actually evolve, changing their size, and appearance to elude detection by antivirus software programs.

7.5 Virus & Worm Hoaxes

Types of Trojans

- ✓ Data Sending Trojans
- ✓ Proxy Trojans
- ✓ FTP Trojans
- ✓ Security software disabler Trojans
- ✓ Denial of service attack Trojans(DOS)

Virus

- ✓ A program or piece of code that be loaded on to your computer, without your knowledge and run against your wishes.

Worm

- ✓ A program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Trojan Horse

- ✓ A destructive program that masquerade on beginning application, unlike viruses, Trojan horse do not replicate themselves.

Blended threat

- ✓ Blended threats combine the characteristics of virus, worm, Trojan horses & malicious code with server and Internet Vulnerabilities.

Antivirus Program

- ✓ A Utility that searches a hard disk for viruses and removes any that found.

7.8 Forces of Nature

- ✓ **Fire:** Structural fire that damages the building. Also encompasses smoke damage from a fire or water damage from sprinkles systems.
- ✓ **Flood:** Can sometimes be mitigated with flood insurance and/or business interruption Insurance.
- ✓ **Earthquake:** Can sometimes be mitigated with specific causality insurance and/or business interruption insurance, but is usually a separate policy.
- ✓ **Lightning**: An Abrupt, discontinuous natural electric discharge in the atmosphere.
- ✓ **Landslide/Mudslide**: The downward sliding of a mass of earth & rocks directly damaging all parts of the information systems.
- ✓ **Tornado/Severe Windstorm**
- ✓ **Huricane/typhoon**
- ✓ **Tsunami**
- ✓ **Electrostatic Discharge (ESD)**
- ✓ **Dust Contamination**

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage.

- ✓ They must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, to limit losses in the face of these threats.

7.9 Deviations in Quality of Service

- ✓ A product or service is not delivered to the organization as expected.
- ✓ The Organization's information system depends on the successful operation of many interdependent support systems.
- ✓ It includes power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff & garbage haulers.
- ✓ This degradation of service is a form of **availability disruption.**

Internet Service Issues

- ✓ Internet service Provider(ISP) failures can considerably undermine the availability of information.
- ✓ The web hosting services are usually arranged with an agreement providing minimum service levels known as a **Service level Agreement (SLA).**
- ✓ When a Service Provider fails to meet SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

Communications & Other Service Provider Issues

- ✓ Other utility services can affect the organizations are telephone, water, waste water, trash pickup, cable television, natural or propane gas, and custodial services.
- ✓ The loss of these services can impair the ability of an organization to function.
- ✓ For an example, if the waste water system fails, an organization might be prevented from allowing employees into the building.
- ✓ This would stop normal business operations.

Power Irregularities

- ✓ Fluctuations due to power excesses.
- ✓ Power shortages &
- ✓ Power losses

This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.

- ✓ When voltage levels **spike** (experience a momentary increase),or **surge** (experience prolonged increase), the extra voltage can severely damage or destroy equipment.
- ✓ The more expensive uninterruptible power supply (UPS) can protect against spikes and surges.

7.10 Technical Hardware Failures or Errors

- ✓ Resulting in unreliable service or lack of availability
- ✓ Some errors are terminal, in that they result in unrecoverable loss of equipment.
- ✓ Some errors are intermittent, in that they resulting in faults that are not easily repeated.

7.11 Technical software failures or errors

- ✓ This category involves threats that come from purchasing software with unknown, hidden faults.
- ✓ Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.
- ✓ These failures range from bugs to untested failure conditions.

7.12 Technological obsolescence

- ✓ Outdated infrastructure can lead to unreliable and untrustworthy systems.
- ✓ Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks.

2.4 ATTACKS

- ✓ An attack is an act of or action that takes advantage of a vulnerability to compromise a controlled system.
- ✓ It is accomplished by a **threat agent** that damages or steals an organization's information or physical asset.
- ✓ **Vulnerability** is an identified weakness in a controlled system, where controls are not present or are no longer effective.
- ✓ Attacks exist when a specific act or action comes into play and may cause a potential loss.

2.4.1 Malicious code

- ✓ The malicious code attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.
- ✓ The state –of-the-art malicious code attack is the polymorphic or multivector, worm.
- ✓ These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

2.4.2 Attack Replication Vectors

1. IP scan & attack
2. Web browsing
3. Virus

4. Unprotected shares
5. Mass mail
6. Simple Network Management Protocol(SNMP)

1. IP scan & attack

- ✓ The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers.

2. Web browsing

- ✓ If the infected system has write access to any Web pages, it makes all Web content files (.html,.asp,.cgi & others) infectious, so that users who browse to those pages become infected.

3. Virus

- ✓ Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.

4. Unprotected shares

- ✓ Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.

5. Mass Mail

- ✓ By sending E-mail infections to addresses found in the address book, the infected machine infects many users, whose mail -reading programs also automatically run the program & infect other systems.

6. Simple Network Management Protocol (SNMP)

- ✓ By using the widely known and common passwords that were employed in early versions of this protocol, the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

2.4.3 Examples

Hoaxes

- ✓ A more devious approach to attacking the computer systems is the transmission of a virus hoax with a real virus attached.
- ✓ Even though these users are trying to avoid infection, they end up sending the attack on to their co-workers.

Backdoors

- ✓ Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door.
- ✓ Sometimes these entries are left behind by system designers or maintenance staff, and thus referred to as trap doors.
- ✓ A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

Password Crack

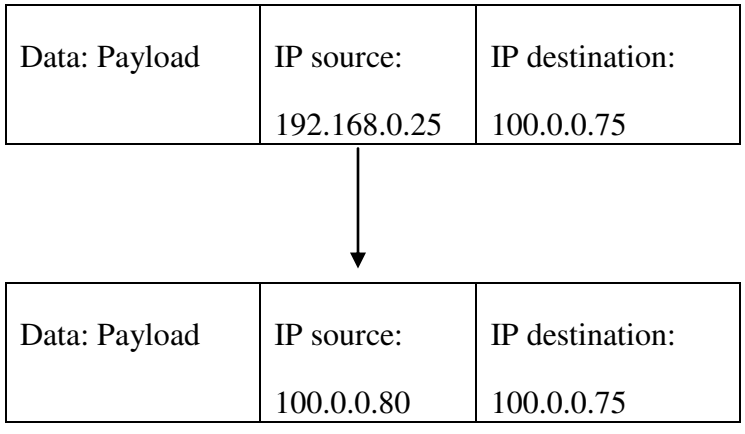
- ✓ Attempting to reverse calculate a password is often called **cracking.**
- ✓ A password can be hashed using the same algorithm and compared to the hashed results, If they are same, the password has been cracked.
- ✓ The (SAM) Security Account Manager file contains the hashed representation of the user's password.

Brute Force

- ✓ The application of computing & network resources to try every possible combination of options of a password is called a **Brute force attack.**
- ✓ This is often an attempt to repeatedly guess passwords to commonly used accounts, it is sometimes called a **password attack.**

Spoofing

- ✓ It is a technique used to gain unauthorized access to computers, where in the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host.

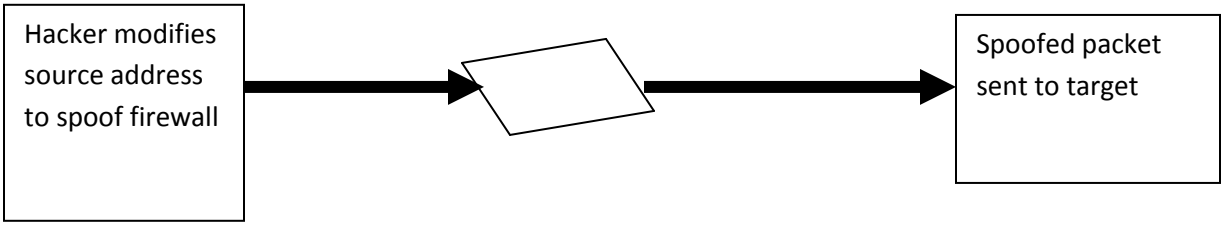


Original IP packet

From hacker's system

Spoofed (modified)

IP packet



Firewall allows packet in, mistaking it for legitimate traffic

Figure 2.4.3.1 IP spoofing

Dictionary

- ✓ This is another form of the brute force attack noted above for guessing passwords.
- ✓ The **dictionary attack** narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords instead of random combinations.

Denial –of- Services(DOS) & Distributed Denial –of- Service(DDOS)

- ✓ The attacker sends a large number of connection or information requests to a target.
- ✓ This may result in the system crashing, or simply becoming unable to perform ordinary functions.
- ✓ DDOS is an attack in which a coordinated stream of requests is launched dagainst a target from many locations at the same.

Man-in-the –Middle

- ✓ Otherwise called as **TCP hijacking attack**.
- ✓ An attacker monitors packets from the network, modifies them, and inserts them back into the network.
- ✓ This type of attack uses IP spoofing.
- ✓ It allows the attacker to change, delete, reroute, add, forge or divert data.
- ✓ TCP hijacking session, the spoofing involves the interception of an encryption key exchange.

SPAM

- ✓ Spam is unsolicited commercial E-mail.

- ✓ It has been used to make malicious code attacks more effective.
- ✓ Spam is considered as a trivial nuisance rather than an attack.
- ✓ It is the waste of both computer and human resources it causes by the flow of unwanted E-mail.

Mail Bombing

- ✓ Another form of E-mail attack that is also a DOS called a **mail bomb**.
- ✓ Attacker routes large quantities of e-mail to the target.
- ✓ The target of the attack receives unmanageably large volumes of unsolicited e-mail.
- ✓ By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.
- ✓ The target e-mail address is buried under thousands or even millions of unwanted e-mails.

Sniffers

- ✓ A **sniffer** is a program or device that can monitor data traveling over a network.
- ✓ Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.
- ✓ Sniffer often works on TCP/IP networks, where they are sometimes called **"packet Sniffers".**

Social Engineering

- ✓ It is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.
- ✓ An attacker gets more information by calling others in the company and asserting his/her authority by mentioning chief's name.

Buffer Overflow

- ✓ A buffer overflow is an application error that occurs when more data is sent to a buffer than it can handle.
- ✓ Attacker can make the target system execute instructions.

Timing Attack

- ✓ Works by exploring the contents of a web browser's cache.
- ✓ These attacks allow a Web designer to create a malicious form of cookie, that is stored on the client's system.
- ✓ The cookie could allow the designer to collect information on how to access password-protected sites.

2.5 LEGAL, ETHICAL, AND PROFESSIONAL ISSUES IN INFORMATION SECURITY

2.5.1 Law and Ethics in Information Security

- ✓ **Laws** are rules that mandate or prohibit certain behavior in society; they are drawn from **ethics**, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the sanctions of a governing authority and ethics do not. Ethics in turn are based on **Cultural mores.**
- ✓ **Types of Law**
    - ✓ **Civil law**
    - ✓ **Criminal law**
    - ✓ **Tort law**
    - ✓ **Private law**
    - ✓ **Public law**

2.5.2 Relevant U.S. Laws – General

- ✓ Computer Fraud and Abuse Act of 1986
- ✓ National Information Infrastructure Protection Act of 1996
- ✓ USA Patriot Act of 2001
- ✓ Telecommunications Deregulation and Competition Act of 1996
- ✓ Communications Decency Act (CDA)
- ✓ Computer Security Act of 1987

Privacy

- ✓ The issue of privacy has become one of the hottest topics in information
- ✓ The ability to collect information on an individual, combine facts from separate sources, and merge it with other information has resulted in databases of information that were previously impossible to set up
- ✓ The aggregation of data from multiple sources permits unethical organizations to build databases of facts with frightening capabilities

Privacy of Customer Information

- ✓ Privacy of Customer Information Section of Common Carrier Regulations
- ✓ Federal Privacy Act of 1974
- ✓ The Electronic Communications Privacy Act of 1986

- ✓ The Health Insurance Portability & Accountability Act Of 1996 (HIPAA) also known as the Kennedy-Kassebaum Act
- ✓ The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999

Table 2.5.2.1 Key U.S Laws of Interest to Information Security Professionals

ACT	SUBJECT	DATE	DESCRIPTION
Communications Act of 1934,updated by Telecommunications Deregulation & Competition Act	Telecommunications	1934	Regulates interstate and foreign Telecommunications.
Computer Fraud & Abuse Act	Threats to computers	1986	Defines and formalizes laws to counter threats from computer related acts and offenses.
Computer Security Act of 1987	Federal Agency Information Security	1987	Requires all federal computer systems that contain classified information to have surety plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems.
Economic Espionage Act of 1996	Trade secrets.	1996	Designed to prevent abuse of information gained by an individual working in one company and employed by another.
Electronic Communications Privacy Act of 1986	Cryptography	1986	Also referred to as the Federal Wiretapping Act; regulates interception and disclosure of electronic information.
Federal Privacy Act	Privacy	1974	Governs federal agency use

of 1974			of personal information.
Gramm-Leach-Bliley Act of 1999	Banking	1999	Focuses on facilitating affiliation among banks, insurance and securities firms; it has significant impact on the privacy of personal information used by these industries.
Health Insurance Portability and Accountability Act	Health care privacy	1996	Regulates collection, storage, and transmission of sensitive personal health care information.
National Information Infrastructure protection Act of 1996	Criminal intent	1996	Categorized crimes based on defendant's authority to access computer and criminal intent.
Sarbanes-Oxley Act of 2002	Financial Reporting	2002	Affects how public organizations and accounting firms deal with corporate governance, financial disclosure, and the practice of public accounting.
Security and Freedom through Encryption Act of 1999	Use and sale of software that uses or enables encryption.	1999	Clarifies use of encryption for people in the United states and permits all persons in the U.S. to buy or sell any encryption product and states that the government cannot require the use of any kind of key escrow system for encryption products.
U.S.A. Patriot Act of 2001	Terrorism	2001	Defines stiffer penalties for prosecution of terrorist crimes.

Export and Espionage Laws

- ✓ **Economic Espionage Act** (EEA) of 1996
- ✓ **Security and Freedom Through Encryption Act of 1997** (SAFE)

US Copyright Law

- ✓ Intellectual property is recognized as a protected asset in the US
- ✓ US copyright law extends this right to the published word, including electronic formats
- ✓ Fair use of copyrighted materials includes
  - the use to support news reporting, teaching, scholarship, and a number of other related permissions
  - the purpose of the use has to be for educational or library purposes, not for profit, and should not be excessive

Freedom of Information Act of 1966 (FOIA)

- ✓ The **Freedom of Information Act** provides any person with the right to request access to federal agency records or information, not determined to be of national security
  - US Government agencies are required to disclose any requested information on receipt of a written request
- ✓ There are exceptions for information that is protected from disclosure, and the Act does not apply to state or local government agencies or to private businesses or individuals, although many states have their own version of the FOIA

State & Local Regulations

- ✓ In addition to the national and international restrictions placed on an organization in the use of computer technology, each state or locality may have a number of laws and regulations that impact operations

It is the responsibility of the information security professional to understand state laws and regulations and insure the organization's security policies and procedures comply with those laws and regulations

2.5.3 International Laws and Legal Bodies

- ✓ Recently the Council of Europe drafted the **European Council Cyber-Crime Convention,** designed
  - to create an international task force to oversee a range of security functions associated with Internet activities,
  - to standardize technology laws across international borders

- ✓ It also attempts to improve the effectiveness of international investigations into breaches of technology law
- ✓ This convention is well received by advocates of intellectual property rights with its emphasis on copyright infringement prosecution

Digital Millennium Copyright Act (DMCA) Digital Millennium Copyright Act (DMCA)

- ✓ The Digital Millennium Copyright Act (DMCA) is the US version of an international effort to reduce the impact of copyright, trademark, and privacy infringement
- ✓ The European Union Directive 95/46/EC increases protection of individuals with regard to the processing of personal data and limits the free movement of such data
- ✓ The United Kingdom has already implemented a version of this directive called the Database Right

United Nations Charter

- ✓ To some degree the **United Nations Charter** provides provisions for information security during Information Warfare
- ✓ Information Warfare (IW) involves the use of information technology to conduct offensive operations as part of an organized and lawful military operation by a sovereign state
- ✓ IW is a relatively new application of warfare, although the military has been conducting electronic warfare and counter-warfare operations for decades, jamming, intercepting, and spoofing enemy communications

Policy Versus Law

- ✓ Most organizations develop and formalize a body of expectations called policy
- ✓ Policies function in an organization like laws
- ✓ For a policy to become enforceable, it must be:
  - Distributed to all individuals who are expected to comply with it
  - Readily available for employee reference
  - Easily understood with multi-language translations and translations for visually impaired, or literacy-impaired employees
  - Acknowledged by the employee, usually by means of a signed consent form
- ✓ Only when all conditions are met, does the organization have a reasonable expectation of effective policy

2.5.4 Ethical Concepts in Information Security

Cultural Differences in Ethical Concepts

- ✓ Differences in cultures cause problems in determining what is ethical and what is not ethical
- ✓ Studies of ethical sensitivity to computer use reveal different nationalities have different perspectives

- ✓ Difficulties arise when one nationality's ethical behavior contradicts that of another national group

Ethics and Education

- ✓ Employees must be trained and kept aware of a number of topics related to information security, not the least of which is the expected behaviors of an ethical employee
- ✓ This is especially important in areas of information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal
- ✓ Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user

Deterrence to Unethical and Illegal Behavior

- ✓ Deterrence - preventing an illegal or unethical activity
- ✓ Laws, policies, and technical controls are all examples of deterrents
- ✓ Laws and policies only deter if three conditions are present:
    - Fear of penalty
    - Probability of being caught
    - Probability of penalty being administered

UNIT III - SECURITY ANALYSIS

Risk Management: Identifying and Assessing Risk, Assessing and Controlling Risk

3.1 RISK MANAGEMENT

3.1.1 Definition:

- ✓ The formal process of identifying and controlling the risks facing an organization is called risk management. It is the probability of an undesired event causing damage to an asset. There are three steps

    1. Risk Identification.
    2. Risk Assessment
    3. Risk Control

        1. **Risk Identification**: It is the process of examining and documenting the security posture of an organization's information technology and the risk it faces.

        2. **Risk Assessment**: It is the documentation of the results of risk identification.

        3. **Risk Control**: It is the process of applying controls to reduce the risks to an organization's data and information systems.

- ✓ To keep up with the competition, organizations must design and create safe environments in which business process and procedures can function.
- ✓ These environments must maintain Confidentiality & Privacy and assure the integrity of organizational data-objectives that are met through the application of the principles of risk management

3.1.2 Components of Risk Management

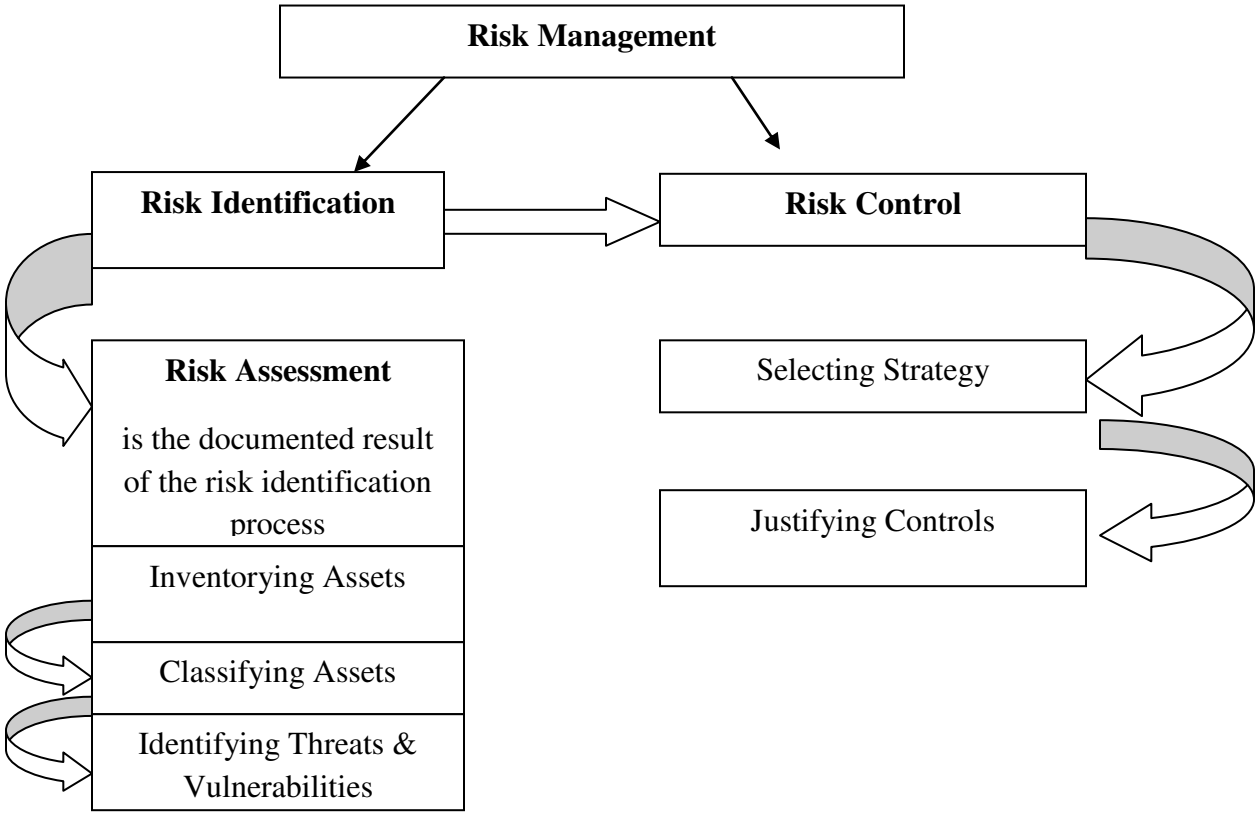


Figure 3.1.2.1 Components of Risk Management

3.1.3 An Overview of Risk Management

Over 2,400 years ago by Chinese General Sun Tzu said

"1.If you know the enemy & know yourself, you need not fear the result of a hundred battles.

2. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

3. If you know neither the enemy nor yourself, you will succumb in every battle"

Know Yourself

- ✓ Identify, Examine & Understand the information systems.
- ✓ To protect assets, you must understand what they are? How they add value to the organization, and to which vulnerabilities they are susceptible.
- ✓ The policies, Education and training programs, and technologies that protect information must be carefully maintained and administered to ensure that they are still effective.

Know the Enemy

- ✓ Identifying, Examining & Understanding the threats facing the organization.

The Roles of the Communities of Interest

- ✓ It is the responsibility of each community of interest to manage the risks that organization encounters.

Information Security

- ✓ Understand the threats and attacks that introduce risk into the organization.
- ✓ Take a leadership role in addressing risk.

Management & Users

- ✓ Management must ensure that sufficient resource are allocated to the information security & Information technology groups to meet the security needs of the organization.
- ✓ Users work with the systems and the data and are therefore well positioned to understand the value of the information assets.

Information Technology

- ✓ Must build secure systems and operate them safely.

Three communities of interest are also responsible for the following

- ✓ Evaluating the risk controls.
- ✓ Determining which control options are cost effective.
- ✓ Acquiring or installing the needed controls.
- ✓ Overseeing that the controls remain effective.

3.1.4 Important Risk Factors of information Security are

1. Understand the threats and attacks that introduce risk into the organization.
2. Taking asset inventory.
3. Verify the threats and vulnerabilities that have been identified as dangerous to the asset inventory, as well as the current controls and mitigation strategies.
4. Review the cost effectiveness of various risk control measures.

3.2 RISK IDENTIFICATION

- ✓ IT professionals to know their organization's information assets through identifying, classifying and prioritizing them.
- ✓ Assets are the targets of various threats and threat agents, and the goal is to protect the assets from the threats.
- ✓ Once the organizational assets have been identified, a threat identification process is undertaken.
- ✓ The circumstances and settings of each information asset are examined to identify vulnerabilities.
- ✓ When vulnerabilities are found, controls are identified and assessed as to their capability to limit possible losses in the eventuality of attack.
- ✓ The process of Risk Identification begins with the identification of the organization's information assets and an assessment of their value.
- ✓ The Components of this process are shown in figure

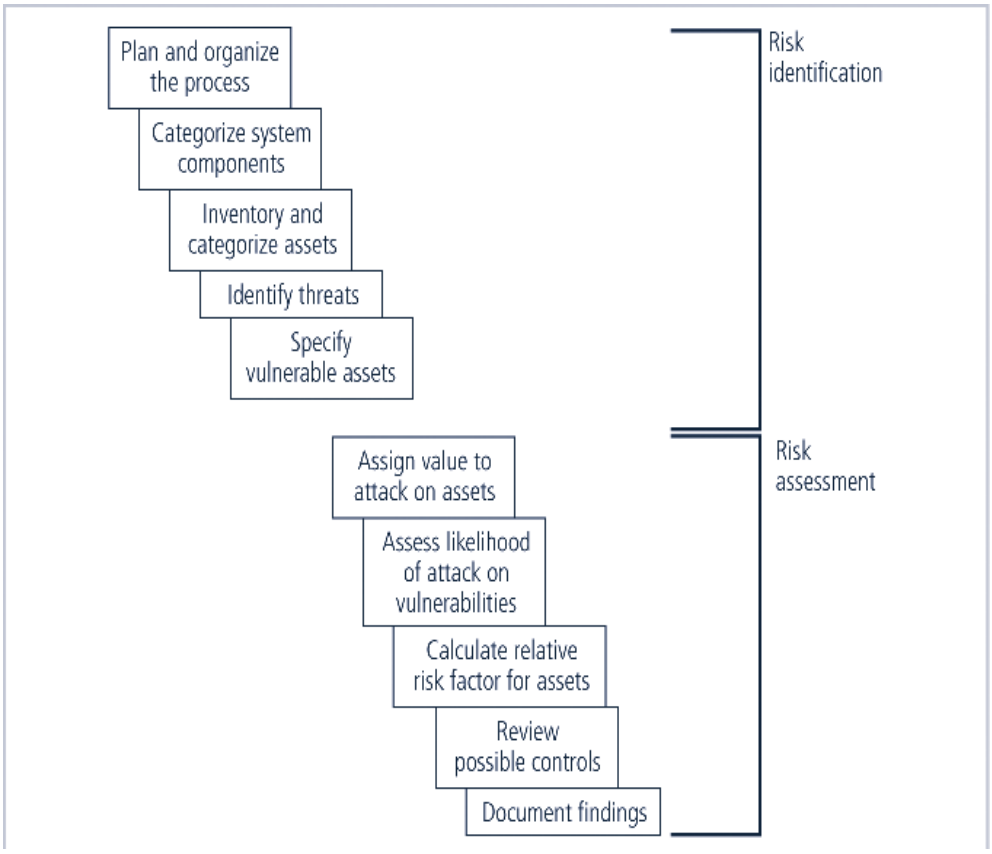


Figure 3.2.1 Components of Risk Identification

3.2.1 Asset Identification & Valuation

- ✓ Includes all the elements of an organization's system, such as people, procedures, data and information, software, hardware, and networking elements.
- ✓ Then, you classify and categorize the assets, adding details.

3.2.1.1 Components of Information System

Table 3.2.2.1 Categorization of IT Components

Traditional system components	SecSDLC and risk management system components	
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

People include employees and nonemployees. There are two categories of employees: those who hold trusted roles and have correspondingly greater authority and accountability, and other staff who have assignments without special privileges. Nonemployees include contractors and consultants, members of other organizations with which the organization has a trust relationship, and strangers.

- ✓ Procedures fall into two categories: IT and business standard procedures, and IT and business sensitive procedures. The business sensitive procedures are those that may assist

a threat agent in crafting an attack against the organization or that have some other content or feature that may introduce risk to the organization.

- ✓ Data Components have been expanded to account for the management of information in all stages: Transmission, Processing, and Storage.

- ✓ Software Components can be assigned to one of three categories: Applications, Operating Systems, or security components. Software Components that provide security controls may span the range of operating systems and applications categories, but are differentiated by the fact that they are the part of the information security control environment and must be protected more thoroughly than other system components.

- ✓ **Hardware** is assigned to one of two categories: the usual systems devices and their peripherals, and the devices that are part of information security control systems. The latter must be protected more thoroughly than the former.

3.2.1.2 People, Procedures,& Data Asset Identification

- ✓ **People :** Position name/number/ID: Supervisor; Security clearance level; special skills.
- ✓ **Procedures :** Description/intended purpose/relationship to software / hardware and networking elements; storage location for update; storage location for reference.
- ✓ **Data :** Classification; owner; Creator; Manager; Size of data structure; data structure used; online/offline/location/backup procedures employed.

3.2.1.3 Hardware, Software, and Network Asset Identification

Depends on the needs of the organization and its risk management efforts.

- ✓ **Name**: Should adopt naming standards that do not convey information to potential system attackers.

- ✓ **IP address**: Useful for network devices & Servers. Many organizations use the dynamic host control protocol (DHCP) within TCP/IP that reassigns IP numbers to devices as needed, making the use of IP numbers as part of the asset identification process problematic. IP address use in inventory is usually limited to those devices that use static IP addresses.
- ✓ **Media Access Control (MAC) address**: Electronic serial numbers or hardware addresses. All network interface hardware devices have a unique number. The MAC address number is used by the network operating system as a means to identify a specific network device. It is used by the client's network software to recognize traffic that it must process.

- ✓ **Element Type**: Document the function of each Element by listing its type. For hardware, a list of possible element types, such as servers, desktops, networking devices or test equipment.

One server might be listed as

- Device class= S (Server)
- Device OS= W2K (Windows 2000)
- Device Capacity = AS (Advanced Server)

- ✓ **Serial Number**: For hardware devices, the serial number can uniquely identify a specific device.

- ✓ **Manufacturer Name**: Record the manufacturer of the device or software component. This can be useful when responding to incidents that involve these devices or when certain manufacturers announce specific vulnerabilities.

- ✓ **Manufacturer's Model No or Part No:** Record the model or part number of the element. This record of exactly what the element is can be very useful in later analysis of vulnerabilities, because some vulnerability instances only apply to specific models of certain devices and software components.

- ✓ **Software Version, Update revision, or FCO number**: Document the specific software or firmware revision number and, for hardware devices, the current field change order (FCO) number. An FCO is an authorization issued by an organization for the repair, modification, or update of a piece of equipment. Documenting the revision number and FCO is particularly important for networking devices that function mainly through the software running on them. For example, firewall devices often have three versions: an operating system (OS) version, a software version, and a basic input/output system (BIOS) firmware version.

- ✓ **Physical location**: Note where this element is located physically (Hardware)

- ✓ **Logical Location**: Note where this element can be found on the organization's network. The logical location is most useful for networking devices and indicates the logical network where the device is connected.

- ✓ **Controlling Entity**: Identify which organizational unit controls the element.

3.2.1.4 Automated Risk Management Tools

- ✓ Automated tools identify the system elements that make up the hardware, software, & network components.
- ✓ Many organizations use automated asset inventory systems.

- ✓ The inventory listing is usually available in a data base.
- ✓ Once stored, the inventory listing must be kept current, often by means of a tool that periodically refreshes the data.

3.2.2 Information Asset Classification

- ✓ In addition to the categories, it is advisable to add another dimension to represent the sensitivity & Security priority of the data and the devices that store, transmit & process the data.
- ✓ Eg: Kinds of classifications are confidential data, internal data and public data.

3.2.3 Information Asset Valuation

- ✓ As each asset is assigned to its category, posing a number of questions assists in developing the weighting criteria to be used for information asset valuation or impact evaluation. Before beginning the inventory process, the organization should determine which criteria can best be used to establish the value of the information assets. Among the criteria to be considered are:

    - Which information Asset is the most critical to the success of the organization.
    - Which information asset generates the most revenue?
    - Which information asset generates the most probability?
    - Which Information asset would be the expensive to replace?

System Name: SLS E-Commerce
Date Evaluated: February 2003
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 —Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (Outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Figure 3.2.3.1 Sample Inventory Worksheet

3.2.4 Data Classification

1. Confidential
2. Internal
3. External

- ✓ **Confidential**: Access to information with this classification is strictly on a need-to-know basis or as required by the terms of a contract.
- ✓ **Internal**: Used for all internal information that does not meet the criteria for the confidential category and is to be viewed only by authorized contractors, and other third parties.
- ✓ **External:** All information that has been approved by management for public release.

The military uses five level classifications

1. Unclassified data
2. Sensitive But Unclassified data (SBU)
3. Confidential data
4. Secret data
5. Top Secret data

1. **Unclassified data**: Information that can generally be distributed to the public without any threat to U.S. National interests.

2. **Sensitive But Unclassified data (SBU)** : Any information of which the loss, misuse, or unauthorized access to, or modification of might adversely affect U.S. national interests, the conduct of Department of Defense(DoD) programs, or the privacy of DoD personnel.

3. **Confidential data**: Any information or material the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

4. **Secret**: Any information or material the unauthorized disclosure of which reasonably could be cause serious damage to the national security.

5. **Top Secret Data:** Any information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

Organization may have

1. Research data
2. Personnel data
3. Customer data
4. General Internal Communications

Some organization may use

1. Public data
2. For office use only
3. Sensitive data
4. Classified data

- ✓ **Public**: Information for general public dissemination, such as an advertisement or public release.
- ✓ **For Official Use Only**: Information that is not particularly sensitive, but not for public release, such as internal communications.
- ✓ **Sensitive**: Information important to the business that could embarrass the company or cause loss of market share if revealed.
- ✓ **Classified**: Information of the utmost secrecy to the organization, disclosure of which could severely impact the well-being of the organization.

Security Clearances

- ✓ The other side of the data classification scheme is the personnel security clearance structure.
- ✓ Each user of data must be assigned a single authorization level that indicates the level of classification he or she is authorized to view.

  - Eg: Data entry clerk, development Programmer, Information Security Analyst, or even CIO.
  - Most organizations have a set of roles and the accompanying security clearances associated with each role.
  - Overriding an employee's security clearance is the fundamental principle of "need-to-know".

Management of classified data

- ✓ Includes its storage, distribution, portability, and destruction.
- ✓ Military uses color coordinated cover sheets to protect classified information from the casual observer.
- ✓ Each classified document should contain the appropriate designation at the top and bottom of each page.
- ✓ A clean desk policy requires that employees secure all information in appropriate storage containers at the end of each day.

    - When Information are no longer valuable, proper care should be taken to destroy them by means of shredding, burning or transferring to a service offering authorized document destruction.
- ✓ **Dumpster diving→** to retrieve information that could embarrass a company or compromise information security.

3.2.5 Threat Identification

- ✓ After identifying the information assets, the analysis phase moves on to an examination of the threats facing the organization.

Identify and Prioritize Threats and Threat Agents

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Figure 3.2.5.1 Threats to Information Security

- ✓ This examination is known as a threat assessment. You can address each threat with a few basic questions, as follows:
- ✓ Which threats present a danger to an organization's assets in the given environment?
- ✓ Which threats represent the most danger to the organization's information?
- ✓ How much would it cost to recover from a successful attack?
- ✓ Which of the threats would require the greatest expenditure to prevent?

Threat	Mean	Standard Deviation	Weight	Weighted Rank
Deliberate software attacks	3.99	1.03	546	2178.3
Forces of Nature	2.80	1.09	218	610.9
Acts of human error or failure	3.15	1.11	350	1101.0
Deliberate acts of theft	3.07	1.30	226	694.5
Technological obsolescence	2.71	1.11	158	427.9
Technical software failures or errors	3.16	1.13	358	1129.9
Compromises to intellectual property	2.72	1.21	181	494.8

Table 3.2.5.1 Weighted Ranks of Threats to Information Security

3.2.6 Vulnerability Identification:

- ✓ Create a list of Vulnerabilities for each information asset.
- ✓ Groups of people work iteratively in a series of sessions give best result.
- ✓ At the end of Identification process, you have a list of assets and their vulnerabilities.

Table 3.2.6.1 Vulnerability Assessment of a Hypothetical DMZ Router

Threat	Possible Vulnerabilities
Deliberate software attacks	Internet protocol is vulnerable to denial of service.
Acts of human error or failure	Employees may cause outage if configuration errors are made.
Technical software failures or errors	Vendor-supplied routing software could fail and cause an outage.

Technical hardware failures or errors	Hardware can fail and cause an outage.
Deviations in Quality of service	Power system failures are always possible.
Deliberate acts of sabotage or vandalism	Internet protocol is vulnerable to denial of service.
Deliberate acts of theft	This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.
Technological obsolescence	If this asset is not reviewed and periodically updated, it may fall too far behind its vendor support model to be kept in service.
Forces of nature	All information assets in the organization are subject to forces of nature, unless suitable controls are provided.
Compromises to intellectual property	This information asset has little intrinsic value, but other assets protected by this device could be attacked if it is compromised.

3.3 RISK ASSESSMENT

- ✓ Assigns a risk rating or score to each Information asset.
- ✓ It is useful in gauging the relative risk to each Vulnerable asset.

3.3.1 Valuation of Information assets

- ✓ Assign weighted scores for the value to the organization of each Information asset.
- ✓ National Institute of Standards & Technology (NIST) gives some standards.
- ✓ To be effective, the values must be assigned by asking he following questions.

- ✓ Which threats present a danger to an organization's assets in the given environment?
- ✓ Which threats represent the most danger to the organization's Information?
- ✓ How much would it cost to recover from a successful attack?
- ✓ Which of the threats would require the greatest expenditure to prevent?

3.3.2 Likelihood

- ✓ It is the probability of specific vulnerability within an organization will be successfully attacked.
- ✓ NIST gives some standards.
- ✓ 0.1 = Low 1.0 = High
- ✓ Eg: Number of network attacks can be forecast based on how many network address the organization has assigned.

3.3.3 Risk Determination

Risk = [(Likelihood of vulnerability occurrence) X (Value of information Asset)] __ (% of risk mitigated by current controls) + uncertainty of current knowledge of the Vulnerability

- For the purpose of relative risk assessment, risk equals:
  - Likelihood of vulnerability occurrence TIMES value (or impact)
  - MINUS percentage risk already controlled
  - PLUS an element of uncertainty

Eg: Information Asset A has a value score of 50 & has one vulnerability: Vulnerability 1 has a likelihood of 1.0 with no current controls, estimate that assumptions and data are 90% accurate.

Solution:

Risk = [(1.0) x 50] – 0% + 10%

= (50 x 1.0) – ((50 x 1.0)x 0.0) + ((50 x 1.0) x 0.1)

= 50 – 0 + 5

= 55

3.3.4 Identify Possible Controls (For Residual Risk)

- ✓ Residual risk is the risk that remains to the information asset even after the existing control has been applied.
- ✓ Three general categories of controls

1. Policies
2. Programs
3. Technologies

1. Policies
   - General Security Policy
   - Program Security Policy
   - Issue Specific Policy
   - Systems Specific Policy
2. Programs
   - Education
   - Training
   - Awareness
3. Security Technologies
   - Technical Implementation Policies

Access Controls

- ✓ Specially addresses admission of a user into a trusted area of the organization.
- ✓ Eg: Computer rooms, Power Rooms.
- ✓ Combination of policies , Programs, & Technologies

Types of Access controls

Mandatory Access Controls (MACs)

- Give users and data owners limited control over access to information resources.

Nondiscretionary Controls

- Managed by a central authority in the organization; can be based on individual's role (role-based controls) or a specified set of assigned tasks (task-based controls)

Discretionary Access Controls (DAC)

- Implemented at discretion or option of the data user

Lattice-based Access Control

- Variation of MAC - users are assigned matrix of authorizations for particular areas of access.

3.3.5 Documenting the Results of Risk Assessment

- ✓ By the end of the Risk Assessment process, you probably have a collection of long lists of information assets with data about each of them.
- ✓ The goal of this process is to identify the information assets that have specific vulnerabilities and list them, ranked according to those most needing protection. You should also have collected some information about the controls that are already in place.
- ✓ The final summarized document is the ranked vulnerability risk worksheet, a sample of which is shown in the following table.

Table 3.3.5.1 Ranked vulnerability risk worksheet

Asset	Asset Impact or Relative value	Vulnerability	Vulnerability Likelihood	Risk Rating Factor
Customer Service Request via e-mail(inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL - (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL - (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer Service Request via e-mail(inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer Service Request via e-mail(inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL - (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL - (inbound)SSL-Secure Sockets Layer	100	Lost orders due to Web server software failure	0.01	1

3.4 RISK CONTROL STRATEGIES

Four basic strategies to control each of the risks that result from these vulnerabilities.

1. Apply safeguards that eliminate the remaining uncontrolled risks for the vulnerability [Avoidance]
2. Transfer the risk to other areas (or) to outside entities[transference]
3. Reduce the impact should the vulnerability be exploited[Mitigation]
4. Understand the consequences and accept the risk without control or mitigation[Acceptance]

3.4.1 Avoidance

- ✓ It is the risk control strategy that attempts to prevent the exploitation of the vulnerability, and is accomplished by means of
    1. Countering threats
    2. Removing Vulnerabilities in assets
    3. Limiting access to assets
    4. Adding protective safeguards.
- ✓ Three common methods of risk avoidance are
    1. Application of policy
    2. Application of Training & Education
    3. Application of Technology

3.4.2 Transference

- ✓ Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations.
- ✓ It may be accomplished through rethinking how services are offered, revising deployment models, outsourcing to other organizations, purchasing Insurance, Implementing Service contracts with providers.
- ✓ Top 10 Information Security mistakes made by individuals.

    1. Passwords on Post-it-Notes
    2. Leaving unattended computers on.
    3. Opening e-mail attachments from strangers.
    4. Poor Password etiquette
    5. Laptops on the loose (unsecured laptops that are easily stolen)
    6. Blabber mouths (People who talk about passwords)
    7. Plug & Play[Technology that enables hardware devices to be installed and configured without the protection provided by people who perform installations]
    8. Unreported Security Violations
    9. Always behind the times.
    10. Not watching for dangers inside the organization

3.4.3 Mitigation

- ✓ It is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning & preparation.

- ✓ Mitigation begins with the early detection that an attack is in progress and the ability of the organization to respond quickly, efficiently and effectively.
- ✓ Includes 3 types of plans.

1. Incident response plan (IRP) -Actions to take while incident is in progress

2. Disaster recovery plan (DRP) - Most common mitigation procedure.

3. Business continuity plan (BCP) - Continuation of business activities if catastrophic event occurs.

1. Incident Response Plan (IRP)

- ✓ This IRP Plan provides answers to questions such as

1. What do I do now?
2. What should the administrator do first?
3. Whom should they contact?
4. What should they document?

2.The IRP Supplies answers.

- ✓ For example, a system's administrator may notice that someone is copying information from the server without authorization, signaling violation of policy by a potential hacker or an unauthorized employee.
- ✓ **The IRP** also enables the organization to take coordinated action that is either predefined and specific or ad hoc and reactive.

3.Disaster Recovery Plan (DRP)

- ✓ Can include strategies to limit losses before and during the disaster.
- ✓ Include all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when the smoke clears, the dust settles, or the floodwater recede.
- ✓ DRP focuses more on preparations completed before and actions taken after the incident, whereas the IRP focuses on intelligence gathering, information analysis, coordinated decision making, and urgent, concrete actions.

4.Business Continuity Plan (BCP)

- ✓ BCP is the most strategic and long term of the three plans.
- ✓ It encompasses the continuation of business activities if a catastrophic event occurs, such as the loss of an entire database, building or operations center.

- ✓ The BCP includes planning the steps necessary to ensure the continuation of the organization when the scope or scale of a disaster exceeds the ability of the DRP to restore operations.
- ✓ Many companies offer this service as a contingency against disastrous events such as fires. Floods, earthquakes, and most natural disasters.

3.4.4 Acceptance

- ✓ It is the choice to do nothing to protect a vulnerability and do accept the outcome of its exploitation.
- ✓ This strategy occurs when the organization has:

  - Determined the level of risk.
  - Assessed the probability of attack.
  - Estimated the potential damage that could occur from attacks.
  - Performed a thorough cost benefit analysis.
  - Evaluated controls using each appropriate type of feasibility.
  - Decided that the particular function, service, information, or asset did not justify the cost of protection.

3.4.5 Selecting a Risk Control Strategy

- ✓ Level of threat and value of asset play major role in selection of strategy
- ✓ Rules of thumb on strategy selection can be applied:

  - When vulnerability (flaw or weakness) exists: Implement security controls to reduce the likelihood of a vulnerability being exercised.

  - When vulnerability can be exploited: Apply layered protections, architectural designs, and administrative controls to minimize the risk.

  - When the attacker's cost is less than his potential gain: Apply protections to increase the attacker's cost.

  - When potential loss is substantial: Apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attack, thereby reducing the potential for loss.

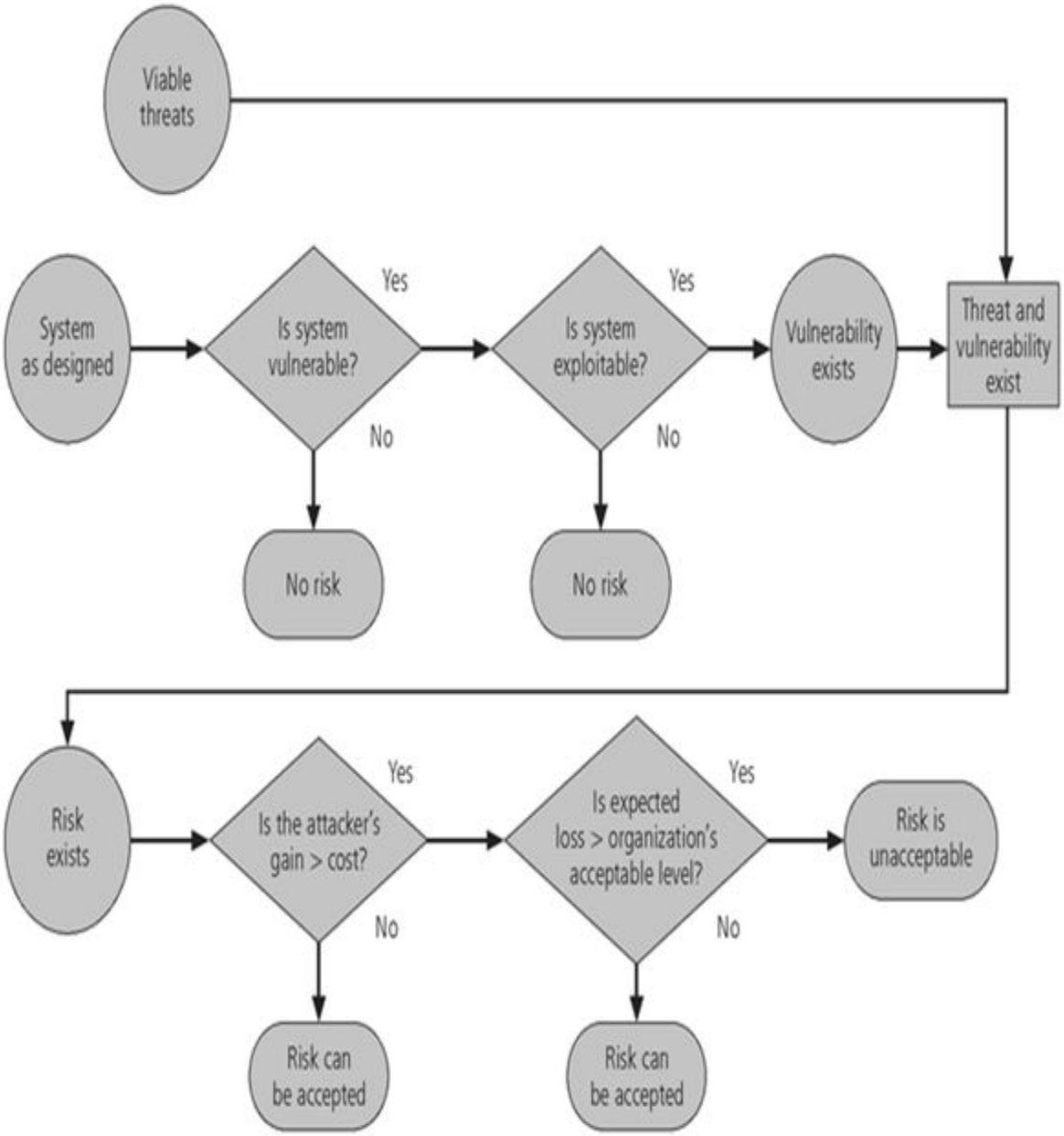


Figure 3.4.5.1 Risk handing dicision points

3.4.6 Evaluation, Assessment & Maintenance of Risk Controls

- ✓ Once a control strategy has been implemented, it should be monitored, & measured on an ongoing basis to determine the effectiveness of the security controls and the accuracy of the estimate of the Residual risk
- ✓ There is no exit from this cycle; it is a process that continues for as long as the organization continues to function.

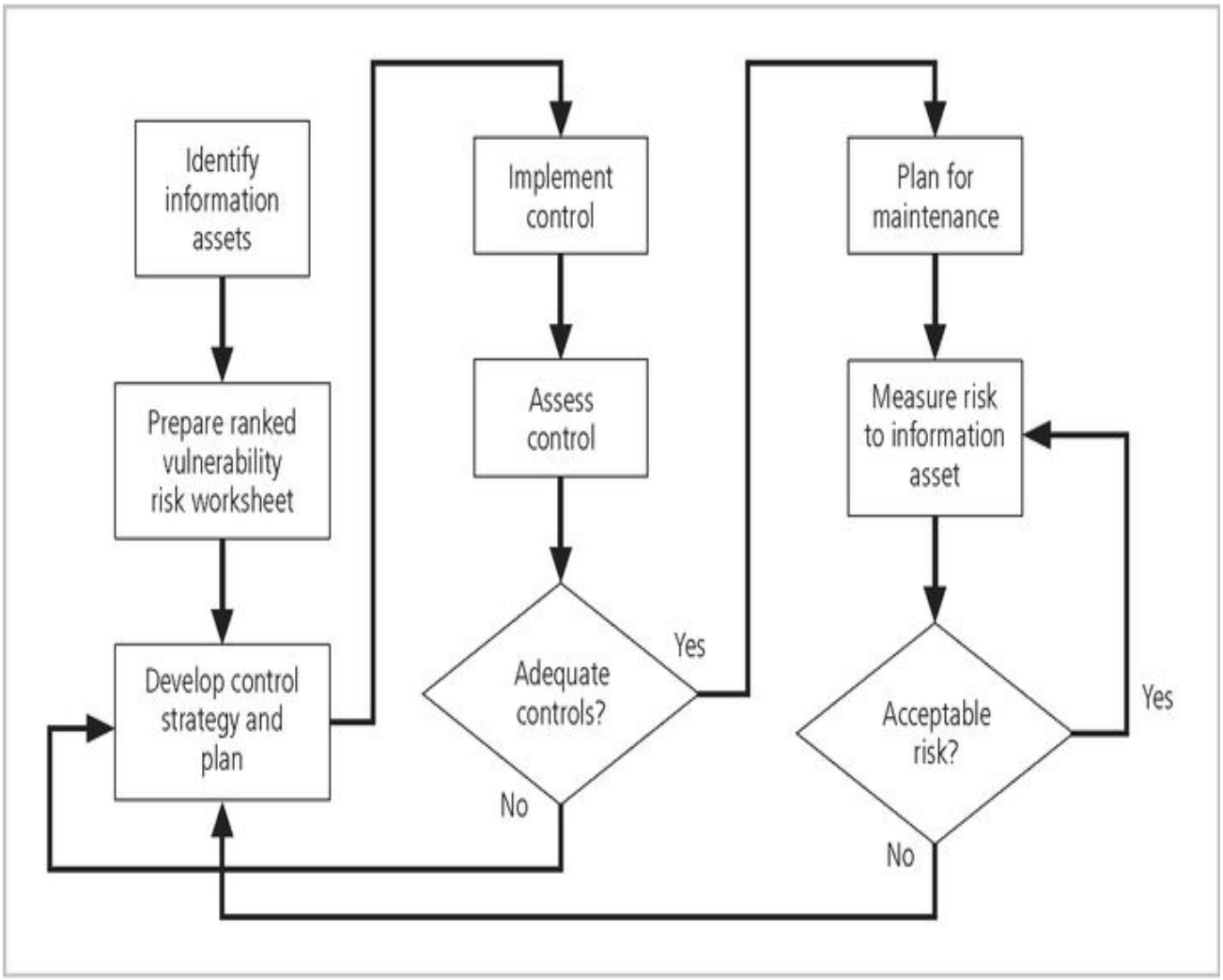


Figure 3.4.5.2 Risk Control Cycle

Categories of Controls

- ✓ Controlling risk through avoidance, Mitigation or Transference may be accomplished by implementing controls or safeguards.
- ✓ Four ways to categorize controls have been identified.

  - **Control function**
    - Preventive or detective
  - **Architectural layer**
    - One or more layers of technical architecture
  - **Strategy layer**
    - Avoidance, mitigation …
  - **Information security principle**

Control Function

- ✓ Safeguards designed to defend systems are either preventive or detective.
- ✓ Preventive controls stop attempts to exploit a vulnerability by implementing a security principle, such as authentication, or Confidentiality.
- ✓ Preventive controls use a technical procedure, such as encryption, or some combination of technical means and enforcement methods.
- ✓ Detective controls – warn organizations of violations of security principles, organizational policies, or attempts to exploit vulnerabilities.
- ✓ Detective controls use techniques such as audit trails, intrusion detection and configuration monitoring.

Architectural Layer

- ✓ Controls apply to one or more layers of an organization's technical architecture.
- ✓ The following entities are commonly regarded as distinct layers in an organization's Information architecture.

1. Organizational policy.
2. External Networks.
3. Extranets (or demilitarized zones)
4. Intranets (WANs and LANs)

5. Network devices that interface network zones.(Switches, Routers, firewalls and hubs)
6. Systems [Mainframe, Server, desktop]
7. Applications.

Strategy Layer

- ✓ Controls are sometimes classified by the risk control strategy they operate within:

1. Avoidance
2. Mitigation
3. transference

Characteristics of Secure Information

1. Confidentiality
2. Integrity
3. Availability
4. Authentication
5. Authorization
6. Accountability
7. Privacy

Confidentiality: The control assures the confidentiality of data when it is stored, processed, or transmitted. An example of this type of control is the use of Secure Sockets Layer (SSL) encryption technology to secure Web content as it moves from Web server to browser.

Integrity: The control assures that the information asset properly, completely, and correctly receives, processes, stores, and retrieves data in a consistent and correct manner .Ex: Use of parity or cyclical redundancy checks in data transmission protocols.

Availability: The control assures ongoing access to critical information assets. Ex: Deployment of a network operations center using a sophisticated network monitoring toolset.

Authentication: The control assures that the entity (person or computer) accessing information assets is in fact the stated entity. Ex: The use of cryptographic certificates to establish SSL connections, or the use of cryptographic hardware tokens such as SecurID cards as a second authentication of identity.

Authorization: The control assures that a user has been specifically and explicitly authorized to access, update, or delete the contents of an information asset. Ex: Use of access control lists and authorization groups in the Windows networking environment. Another example is the use of a database authorization scheme to verify the designated users for each function.

Accountability: The control assures that every activity undertaken can be attributed to a specific named person or automated process. Ex: Use of audit logs to track when each user logged in and logged out of each computer.

Privacy: The control assures that the procedures to access, update, or remove personally identifiable information comply with the applicable laws and policies for that kind of information.

3.4.7 Feasibility Studies

- ✓ Before deciding on the strategy (Avoidance, transference, mitigation, or acceptance), for a specific vulnerability, all the economic and non-economic consequences of the vulnerability facing the information asset must be explored.
- ✓ **Cost Avoidance**- It is the process of avoiding the financial impact of an incident by implementing a control.
- ✓ Includes

1. Cost Benefit analysis
2. Organizational feasibility
3. Operational Feasibility
4. Technical Feasibility
5. Political feasibility.

Cost Benefit Analysis (CBA)

- ✓ Organizations are urged to begin the cost benefit analysis by evaluating the worth of the information assets to be protected and the loss in value if those information assets were compromised by the exploitation of a specific vulnerability.
- ✓ The formal process to document this decision making process is called a Cost Benefit analysis or an economic feasibility study.

Cost Benefit Analysis or an Economic Feasibility study

- ✓ Some of the items that affect the cost of a control or safeguard include:

1. Cost of development or acquisition [purchase cost] of hardware, software and services.
2. Training Fees(cost to train personnel)
3. Cost of Implementation[Cost to install, Configure, and test hardware, software and services]
4. service Costs[Vendor fees for maintenance and upgrades]
5. Cost of maintenance[Labor expense to verify and continually test, maintain and update]

- ✓ Benefit is the value that an organization realizes by using controls to prevent losses associated with a specific vulnerability.

Amount of benefit = Value of the Information asset and Value at risk.

- ✓ Asset Valuation is the process of assigning financial value or worth to each information asset.
- ✓ Some of the components of asset valuation include:

1. Value retained from the cost of creating the information asset.
2. Value retained from past maintenance of the information asset.
3. Value implied by the cost of replacing the information.
4. Value from providing the information.
5. Value incurred from the cost of protecting the information.
6. Value to owners.
7. Value of intellectual property.
8. Value to adversaries.
9. Loss of Productivity while the information assets are unavoidable.
10. Loss of revenue while information assets are unavailable.

- ✓ The organization must be able to place a dollar value on each collection of information and the information assets it owns. This value is based on the answers to these questions:
  - How much did it cost to create or acquire this information?
  - How much would it cost to recreate or recover this information?
  - How much does it cost to maintain this information?
  - How much is this information worth to the organization?
  - How much is this information worth to the competition?

- ✓ **A Single loss expectancy (SLE)** is the calculation of the value associated with the most likely loss from an attack. It is a calculation based on the value of the asset and the **exposure factor (EF),** which is the expected percentage of loss that would occur from a particular attack, as follows:

Single Loss Expectancy (SLE) = Asset value x Exposure factor [EF]

- ✓ EF → Expected percentage of loss that would occur from a particular attack.
- ✓ The probability of threat occurring is usually a loosely derived table indicating the probability of an attack from each threat type within a given time frame (for example, once every 10 years). This value is commonly referred to as the **annualized rate of occurrence (ARO)**
- ✓ The expected value of a loss can be stated in the following equation:
- ✓ **Annualized loss Expectancy (ALE)** which is calculated from the ARO and SLE.

ALE = SLE x ARO

Cost Benefit Analysis (CBA)Formula

- ✓ CBA is whether or not the control alternative being evaluated is worth the associated cost incurred to control the specific vulnerability.
- ✓ The CBA is most easily calculated using the ALE from earlier assessments before the implementation of the proposed control, which is known as ALE (prior).

- ✓ Subtract the revised ALE, estimated based on control being in place, known as ALE (post). Complete the calculation by subtracting the annualized cost of the safeguard (ACS).

CBA = ALE (Prior) - ALE (Post) - ACS

Where:

- ✓ ALE prior is the Annualized Loss Expectancy of the risk before the implementation of the control.
- ✓ ALE post is the ALE examined after the control has been in place for a period of time.
- ✓ ACS is the Annual Cost of the Safeguard.

3.4.8 Bench Marking

- ✓ An alternative approach to risk management
- ✓ Process of seeking out and studying the practices used in other organizations that produce results you would like to duplicate in your organization.
- ✓ One of two measures typically used to compare practices:

  - **Metrics-based measures**

  - **Process-based measures**

- ✓ Good for potential legal protection.
- ✓ **Metrics-based measures** are comparisons based on numerical standards, such as:

1. Numbers of successful attacks.
2. Staff-hours spent on systems protection.
3. Dollars spent on protection.
4. Numbers of Security Personnel.
5. Estimated value in dollars of the information lost in successful attacks.
6. Loss in productivity hours associated with successful attacks.

- ✓ The difference between an organization's measures and those of others is often referred to as a performance gap. The other measures commonly used in benchmarking

are process-based measures. **Process-based measures** are generally less focused on numbers and more strategic than metrics-based-measures.

Due Care/Due Diligence

- ✓ When organizations adopt levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances - this is referred to as a standard of due care
- ✓ Due diligence is the demonstration that the organization is diligent in ensuring that the implemented standards continue to provide the required level of protection
- ✓ Failure to support a standard of due care or due diligence can open an organization to legal liability

Best Business Practices

- ✓ Security efforts that provide a superior level of protection of information are referred to as best business practices
- ✓ Best security practices (BSPs) are security efforts that are among the best in the industry
- ✓ When considering best practices for adoption in your organization, consider the following:
  - Does your organization resemble the identified target?
  - Are the resources you can expend similar?
  - Are you in a similar threat environment?

Microsoft's Ten Immutable Laws of Security

1. If a bad guy can persuade you to run his program on your computer, it's not your computer anymore
2. If a bad guy can alter the operating system on your computer, it's not your computer anymore
3. If a bad guy has unrestricted physical access to your computer, it's not your computer anymore
4. If you allow a bad guy to upload programs to your web site, it's not your web site anymore
5. Weak passwords trump strong security
6. A machine is only as secure as the administrator is trustworthy
7. Encrypted data is only as secure as the decryption key

8. An out of date virus scanner is only marginally better than no virus scanner at all
9. Absolute anonymity isn't practical, in real life or on the web
10. Technology is not a panacea

Problems

- ✓ The biggest problem with benchmarking in information security is that organizations don't talk to each other.
- ✓ Another problem with benchmarking is that no two organizations are identical
- ✓ A third problem is that best practices are a moving target.
- ✓ One last issue to consider is that simply knowing what was going on a few years ago, as in benchmarking, doesn't necessarily tell us what.

Baselining

- ✓ Baselining is the analysis of measures against established standards,
- ✓ In information security, baselining is comparing security activities and events against the organization's future performance.
- ✓ When baselining it is useful to have a guide to the overall process

Feasibility Studies and the Cost Benefit analysis

- ✓ Before deciding on the strategy for a specific vulnerability all information about the economic and non-economic consequences of the vulnerability facing the information asset must be explored.
- ✓ Fundamentally we are asking "What are the actual and perceived advantages of implementing a control contrasted with the actual and perceived disadvantages of implementing the control?"

Cost Benefit Analysis (CBA)

- ✓ The most common approach for a project of information Security controls and safeguards is the economic feasibility of implementation.
- ✓ Begins by evaluating the worth of information assets are compromised.
- ✓ It is only common sense that an organization should not spend more to protect an asset than it is worth.
- ✓ The formal process to document this is called a cost benefit analysis or an economic feasibility study.

CBA: Cost Factors

- ✓ Some of the items that the cost of a control or safeguard include:
- ✓ Cost of Development or Acquisition
- ✓ Training Fees
- ✓ Cost of implementation.

- ✓ Service Costs
- ✓ Cost of Maintenance

CBA: Benefits

- ✓ Benefit is the value that the organization recognizes by using controls to prevent losses associated with a specific vulnerability.
- ✓ This is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk.

CBA: Asset Valuation

- ✓ Asset Valuation is the process of assigning financial value or worth to each information asset.
- ✓ The valuation of assets involves estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against market loss and litigation.
- ✓ These estimates are calculated for each set of information bearing systems or information assets.
- ✓ There are many components to asset valuation.

CBA: Loss Estimates

- ✓ Once the worth of various assets is estimated examine the potential loss that could occur from the exploitation of vulnerability or a threat occurrence.
- ✓ This process results in the estimate of potential loss per risk.
- ✓ The questions that must be asked here include:

  - What damage could occur, and what financial impact would it have?
  - What would it cost to recover from the attack, in addition to the costs above?
  - What is the single loss expectancy for each risk?

Organizational Feasibility

- ✓ Organizational Feasibility examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization.

- ✓ Above and beyond the impact on the bottom line, the organization must determine how the proposed alternatives contribute to the business objectives of the organization.

Operational feasibility

- ✓ Addresses user acceptance and support, management acceptance and support, and the overall requirements of the organization's stake holders.

- ✓ Sometimes known as behavioral feasibility, because it measures the behavior of users.
- ✓ One of the fundamental principles of systems development is obtaining user buy in on a project and one of the most common methods for obtaining user acceptance and support is through user involvement obtained through three simple steps:
    - Communicate
    - Educate
    - Involve

Technical Feasibility

- ✓ The project team must also consider the technical feasibilities associated with the design, implementation, and management of controls.
- ✓ Examines whether or not the organization has or can acquire the technology necessary to implement and support the control alternatives.

Political feasibility

- ✓ For some organizations, the most significant feasibility evaluated may be political
- ✓ Within Organizations, political feasibility defines what can and cannot occur based on the consensus and relationships between the communities of interest.
- ✓ The limits placed on an organization's actions or a behavior by the information security controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources.

Risk Management Discussion Points

- ✓ Not every organization has the collective will to manage each vulnerability through the application of controls
    - Depending on the willingness to assume risk, each organization must define its risk appetite
    - Risk appetite defines the quantity and nature of risk that organizations are willing to accept as they evaluate the tradeoffs between perfect security and unlimited accessibility

Residual Risk

- ✓ When we have controlled any given vulnerability as much as we can, there is often risk that has not been completely removed or has not been completely shifted or planned for this remainder is called residual risk.

- ✓ To express it another way, "Residual risk is a combined function of
    1. A threat less the effect of some threat –reducing safeguards.
    2. Vulnerability less the effect of some vulnerability- reducing safeguards.
    3. an asset less the effect of some asset value-reducing safeguards "

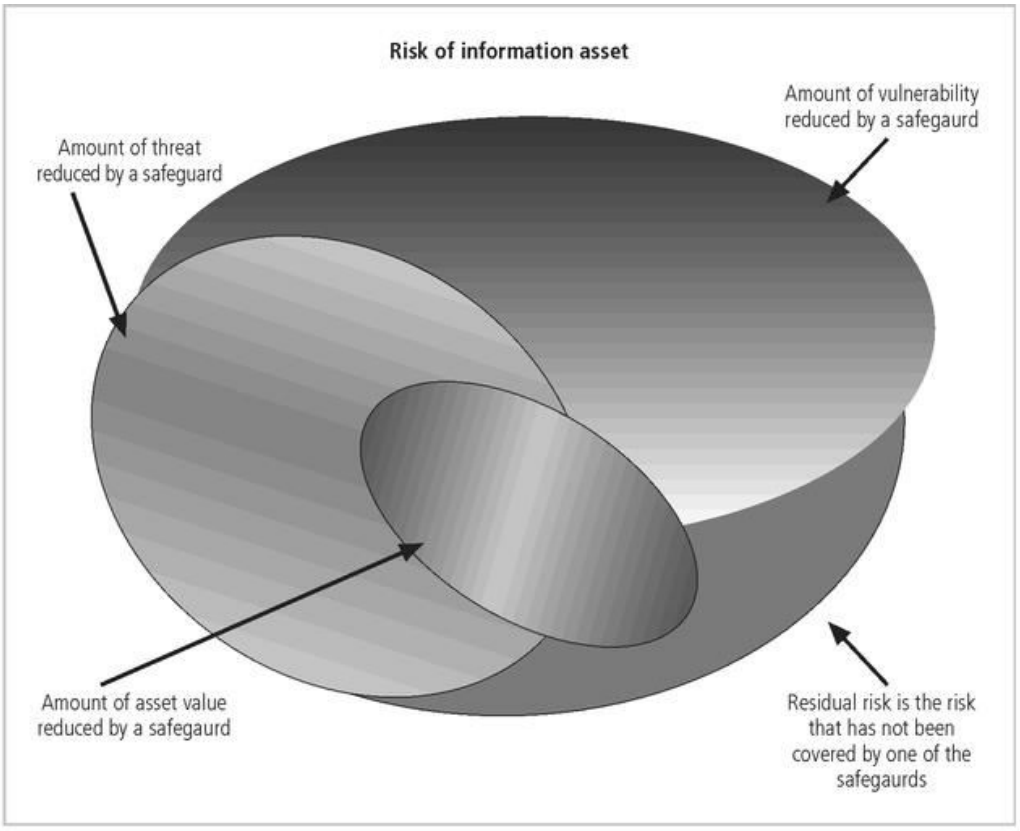


FIGURE 5-4 Risk Residual

Documenting Results

- ✓ At minimum, each information asset-vulnerability pair should have a documented control strategy that clearly identifies any residual risk remaining after the proposed strategy has been executed.
- ✓ Some organizations document the outcome of the control strategy for each information asset-vulnerability pair as an action plan
- ✓ This action plan includes concrete tasks, each with accountability assigned to an organizational unit or to an individual

Recommended Practices in Controlling Risk

- ✓ We must convince budget authorities to spend up to the value of the asset to protect a particular asset from an identified threat
- ✓ Each and every control or safeguard implemented will impact more than one threat-asset pair

Qualitative Measures

- ✓ The spectrum of steps described above was performed with real numbers or best guess estimates of real numbers-this is known as a quantitative assessment.
- ✓ However, an organization could determine that it couldn't put specific numbers on these values.
- ✓ Fortunately, it is possible to repeat these steps using estimates based on a qualitative assessment.
- ✓ Instead of using specific numbers, ranges or levels of values can be developed simplifying the process

Delphi Technique

- ✓ One technique for accurately estimating scales and values is the Delphi Technique.
- ✓ The Delphi Technique, named for the Oracle at Delphi, is a process whereby a group of individuals rate or rank a set of information
- ✓ The individual responses are compiled and then returned to the individuals for another iteration
- ✓ This process continues until the group is satisfied with the result.

UNIT IV - LOGICAL DESIGN

4.1 INFORMATION SECURITY POLICY

PLANNING FOR SECURITY

- ✓ Creation of information security program begins with creation and/or review of organization's information security policies, standards, and practices
- ✓ Then, selection or creation of information security architecture and the development and use of a detailed information security blueprint creates plan for future success
- ✓ Security education and training to successfully implement policies and ensure secure environment

4.1.1 Why Policy?

- ✓ A quality information security program begins and ends with policy
- ✓ Policies are least expensive means of control and often the most difficult to implement
- ✓ Some basic rules must be followed when shaping a policy:
  - Never conflict with law
  - Stand up in court
  - Properly supported and administered
  - Contribute to the success of the organization
  - Involve end users of information systems

Definitions

- ✓ **Policy**: course of action used by an organization to convey instructions from management to those who perform duties
  - Organizational rules for acceptable/unacceptable behavior
  - Penalties for violations
  - Appeals process
- ✓ **Standards**: more detailed statements of what must be done to comply with policy

- ✓ **Practices, procedures and guidelines** effectively explain how to comply with policy
- ✓ For a policy to be effective it must be
  - Properly disseminated
  - Read
  - Understood
  - Agreed to by all members of organization

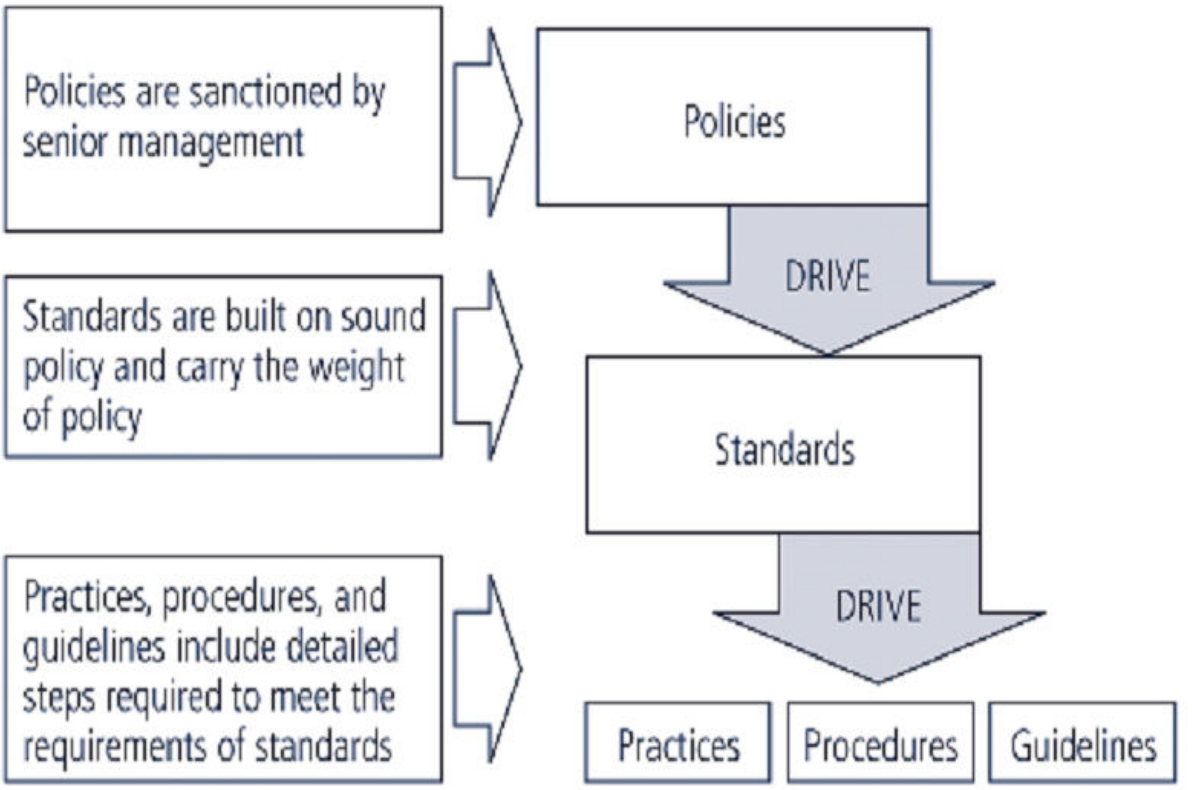


Figure 4.1.1.1 Polices, Standards and Practice

4.1.2 Types of Policies

1. Enterprise information Security program Policy(EISP)
2. Issue-specific information Security Policy (ISSP)
3. Systems-specific information Security Policy (SysSP)

1.Enterprise Information Security Policy (EISP)

- ✓ Also Known as a general Security policy, IT security policy, or information security policy.
- ✓ Sets strategic direction, scope, and tone for all security efforts within the organization
- ✓ Assigns responsibilities to various areas of information security
- ✓ Guides development, implementation, and management of information security program

2.Issue-Specific Security Policy (ISSP)

- ✓ The ISSP:
  - Addresses specific areas of technology
  - Requires frequent updates
  - Contains statement on position on specific issue
- ✓ Approaches to creating and managing ISSPs:
  - Create number of independent ISSP documents
  - Create a single comprehensive ISSP document
  - Create a modular ISSP document
- ✓ ISSP topics could include:
  - E-mail, use of Web, configurations of computers to defend against worms and viruses, prohibitions against hacking or testing organisation security controls, home use of company-owned computer equipment, use of personal equipment on company networks, use of telecommunications technologies(FAX and phone), use of photocopiers

Components of the ISSP

- ✓ Statement of Policy
  - Scope and Applicability
  - Definition of Technology Addressed
  - Responsibilities

- ✓ Authorized Access and Usage of Equipment
  - User Access
  - Fair and Responsible Use
  - Protection of Privacy
- ✓ Prohibited Usage of Equipment
  - Disruptive Use or Misuse
  - Criminal Use
  - Offensive or Harassing Materials
  - Copyrighted, Licensed or other Intellectual Property
  - Other Restrictions
- ✓ Systems Management
  - Management of Stored Materials
  - Employer Monitoring
  - Virus Protection
  - Physical Security
  - Encryption
- ✓ Violations of Policy
  - Procedures for Reporting Violations
  - Penalties for Violations
- ✓ Policy Review and Modification
  - Scheduled Review of Policy and Procedures for Modification
- ✓ Limitations of Liability
  - Statements of Liability or Disclaimers

3.Systems-Specific Policy (SysSP)

- ✓ SysSPs are frequently codified as standards and procedures to be used when configuring or maintaining systems
- ✓ Systems-specific policies fall into two groups:
- ✓ **Access control lists (ACLs)** consist of the access control lists, matrices, and capability tables governing the rights and privileges of a particular user to a particular system
- ✓ **Configuration rules** comprise the specific configuration codes entered into security systems to guide the execution of the system

ACL Policies

- ✓ Both Microsoft Windows NT/2000 and Novell Netware 5.x/6.x families of systems translate ACLs into sets of configurations that administrators use to control access to their respective systems
- ✓ ACLs allow a configuration to restrict access from anyone and anywhere
- ✓ ACLs regulate:
  - Who can use the system
  - What authorized users can access
  - When authorized users can access the system
  - Where authorized users can access the system from
  - How authorized users can access the system

4.2 THE INFORMATION SECURITY BLUEPRINT

- ✓ It is the basis for the design, selection, and implementation of all security policies, education and training programs, and technological controls.
- ✓ More detailed version of **security framework**, which is an outline of overall information security strategy for organization and a road map for planned changes to the information security environment of the organization.
- ✓ Should specify tasks to be accomplished and the order in which they are to be realized.
- ✓ Should also serve as a scalable, upgradeable, and comprehensive plan for the information security needs for coming years.

4.3 STANDARD AND PRACTICE - SECURITY MODELS

4.3.1 ISO 17799/BS 7799

- ✓ One of the most widely referenced and often discussed security models is the Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- ✓ In 2000, this Code of Practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799.

4.3.2 Drawbacks of ISO 17799/BS 7799

- ✓ Several countries have not adopted 17799 claiming there are fundamental problems:
  - The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
  - 17799 lacks "the necessary measurement precision of a technical standard"
  - There is no reason to believe that 17799 is more useful than any other approach currently available
  - 17799 is not as complete as other frameworks available
  - 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

4.3.3 Objectives of ISO 17799

- ✓ Organizational Security Policy is needed to provide management direction and support.

4.3.4 Ten Sections of ISO/IEC 17799

1. Organizational Security Policy
2. Organizational Security Infrastructure
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security

6. Communications and Operations Management
7. System Access Control
8. System Development and Maintenance
9. Business Continuity Planning
10. Compliance

- ✓ Alternate Security Models available other than ISO 17799/BS 7799

4.4 NIST SECURITY MODELS

- ✓ This refers to "The National Security Telecommunications and Information systems Security Committee" document. This document presents a comprehensive model for information security. The model consists of three dimensions.
- ✓ Another possible approach available is described in the many documents available from the Computer Security Resource Center of the National Institute for Standards and Technology (csrc.nist.gov).
- ✓ The following NIST documents can assist in the design of a security framework:
  - **NIST SP 800-12 :** An Introduction to Computer Security: The NIST Handbook
  - **NIST SP 800-14 :** Generally Accepted Security Principles and Practices for Securing IT Systems
  - **NIST SP 800-18** : The Guide for Developing Security Plans for IT Systems
  - **NIST SP 800-26**: Security Self-Assessment Guide for IT systems.
  - **NIST SP 800-30**: Risk Management for IT systems.

4.4.1 NIST Special Publication SP 800-12

- ✓ **SP 800-12** is an excellent reference and guide for the security manager or administrator in the routine management of information security.
- ✓ It provides little guidance, however, on design and implementation of new security systems, and therefore should be used only as a valuable precursor to understanding an information security blueprint.

4.4.2 NIST Special Publication SP 800-14

- ✓ Generally accepted Principles and practices for Security Information Technology Systems.
- ✓ Provides best practices and security principles that can direct the security team in the development of **Security Blue Print**.
- ✓ The scope of NIST SP 800-14 is broad. It is important to consider each of the security principles it presents, and therefore the following sections examine some of the more significant points in more detail:
  - Security Supports the Mission of the Organization
  - Security is an Integral Element of Sound Management
  - Security Should Be Cost-Effective
  - Systems Owners Have Security Responsibilities Outside Their Own Organizations
  - Security Responsibilities and Accountability Should Be Made Explicit
  - Security Requires a Comprehensive and Integrated Approach
  - Security Should Be Periodically Reassessed
  - Security is Constrained by Societal Factors
  - 33 Principles enumerated

4.4.3 NIST SP 800-18

- ✓ The Guide for Developing Security plans for Information Technology Systems can be used as the foundation for a comprehensive security blueprint and framework.
- ✓ It provides detailed methods for assessing, and implementing controls and plans for applications of varying size.
- ✓ It can serve as a useful guide to the activities and as an aid in the planning process.
- ✓ It also includes templates for major application security plans.
- ✓ The table of contents for Publication 800-18 is presented in the following.

System Analysis

- System Boundaries
- Multiple similar systems

- System Categories

Plan Development- All Systems

- Plan control
- System identification
- System Operational status
- System Interconnection/ Information Sharing
- Sensitivity of information handled
- Laws, regulations and policies affecting the system

Management Controls

- Risk Assessment and Management
- Review of Security Controls
- Rules of behavior
- Planning for security in the life cycle
- Authorization of Processing (Certification and Accreditation)
- System Security Plan

Operational Controls

1. Personnel Security
2. Physical Security
3. Production, Input/Output Controls
4. Contingency Planning
5. Hardware and Systems Software
6. Data Integrity
7. Documentation
8. Security Awareness, Training, and Education

9. Incident Response Capability

Technical Controls

- Identification and Authentication
- Logical Access Controls
- Audit Trails

4.4.4 NIST SP 800-26: Security Self-Assessment Guide for IT systems

NIST SP 800-26 Table of contents

Management Controls

1. Risk Management
2. Review of Security Controls
3. Life Cycle Maintenance
4. Authorization of Processing (Certification and Accreditation)
5. System Security Plan

Operational Controls

6. Personnel Security
7. Physical Security
8. Production, Input/Output Controls
9. Contingency Planning
10. Hardware and Systems Software
11. Data Integrity
12. Documentation
13. Security Awareness, Training, and Education
14. Incident Response Capability

Technical Controls

15. Identification and Authentication

16. Logical Access Controls

17. Audit Trails

Management controls

- ✓ It address the design and implementation of the security planning process and security program management.
- ✓ They also address risk management and security control reviews. They further describe the necessity and scope of legal compliance and the maintenance of the entire security life cycle.

Operational controls

- ✓ It deal with the operational functionality of security in the organization. They include management functions and lower level planning, such as disaster recovery and incident response planning.
- ✓ They also address personnel security, physical security, and the protection of production inputs and outputs.
- ✓ They guide the development of education, training and awareness programs for users, administrators, and management. Finally, they address hardware and software systems maintenance and the integrity of data.

Technical controls

- ✓ It address the tactical and technical issues related to designing and implementing security in the organization, as well as issues related to examining and selecting the technologies appropriate to protecting information.
- ✓ They address the specifics of technology selection and the acquisition of certain technical components. They also include logical access controls, such as identification, authentication, authorization, and accountability.
- ✓ They cover cryptography to protect information in storage and transit. Finally, they include the classification of assets and users, to facilitate the authorization levels needed.

Using the three sets of controls, the organization should be able to specify controls to cover the entire spectrum of safeguards, from strategic to tactical, and from managerial to technical.

4.5 VISA INTERNATIONAL SECURITY MODEL

- ✓ It promotes strong security measures in its business associates and has established guidelines for the security of its information systems.
- ✓ It has developed two important documents
    1. Security Assessment Process
    2. Agreed Upon Procedures.
- ✓ Both documents provide specific instructions on the use of the VISA Cardholder Information Security Program.
- ✓ The Security Assessment Process document is a series of recommendations for the detailed examination of an organization's systems with the eventual goal of integration into the VISA systems.
- ✓ The Agreed upon Procedures document outlines the policies and technologies required for security systems that carry the sensitive card holder information to and from VISA systems.
- ✓ Using the two documents, a security team can develop a sound strategy for the design of good security architecture.
- ✓ The only downside to this approach is the specific focus on systems that can or do integrate with VISA's systems with the explicit purpose of carrying the aforementioned cardholder information.

Baselining & Best Business Practices

- ✓ Baselining and best practices are solid methods for collecting security practices, but provide less detail than a complete methodology
- ✓ Possible to gain information by baselining and using best practices and thus work backwards to an effective design
- ✓ The Federal Agency Security Practices (FASP) site (fasp.nist.gov) designed to provide best practices for public agencies and adapted easily to private institutions.
- ✓ The documents found in this site include specific examples of key policies and planning documents, implementation strategies for key technologies, and position descriptions for key security personnel.
- ✓ Of particular value is the section on program management, which includes the following:

- A summary guide: public law, executive orders, and policy documents
- Position description for computer system security officer.
- Position description for information security officer
- Position description for computer specialist.
- Sample of an information technology(IT) security staffing plan for a large service application(LSA)
- Sample of an information technology(IT) security program policy
- Security handbook and standard operating procedures.
- Telecommuting and mobile computer security policy.

4.6 DESIGN OF SECURITY ARCHITECTURE

4.6.1 Hybrid Framework for a Blueprint of an Information Security System

- ✓ The framework of security includes philosophical components of the Human Firewall Project, which maintain that people, not technology, are the primary defenders of information assets in an information security program, and are uniquely responsible for their protection.
- ✓ The spheres of security are the foundation of the security framework.
- ✓ The sphere of use, at the left in fig, explains the ways in which people access information; for example, people read hard copies of documents and can also access information through systems.
- ✓ The sphere of protection at the right illustrates that between each layer of the sphere of use there must exist a layer of protection to prevent access to the inner layer from the outer layer.
- ✓ Each shaded band is a layer of protection and control.

4.6.2 Sphere of Protection

- ✓ The “sphere of protection” overlays each of the levels of the “sphere of use” with a layer of security, protecting that layer from direct or indirect use through the next layer
- ✓ The people must become a layer of security, a **human firewall** that protects the information from unauthorized access and use
- ✓ Information security is therefore designed and implemented in three layers

- policies
- people (education, training, and awareness programs)
- technology

✓ As illustrated in the sphere of protection, a variety of controls can be used to protect the information.

✓ The items of control shown in the figure are not intended to be comprehensive but rather illustrate individual safeguards that can protect the various systems that are located closer to the center of the sphere.

✓ However, because people can directly access each ring as well as the information at the core of the model, the side of the sphere of protection that attempt to control access by relying on people requires a different approach to security than the side that uses technology.

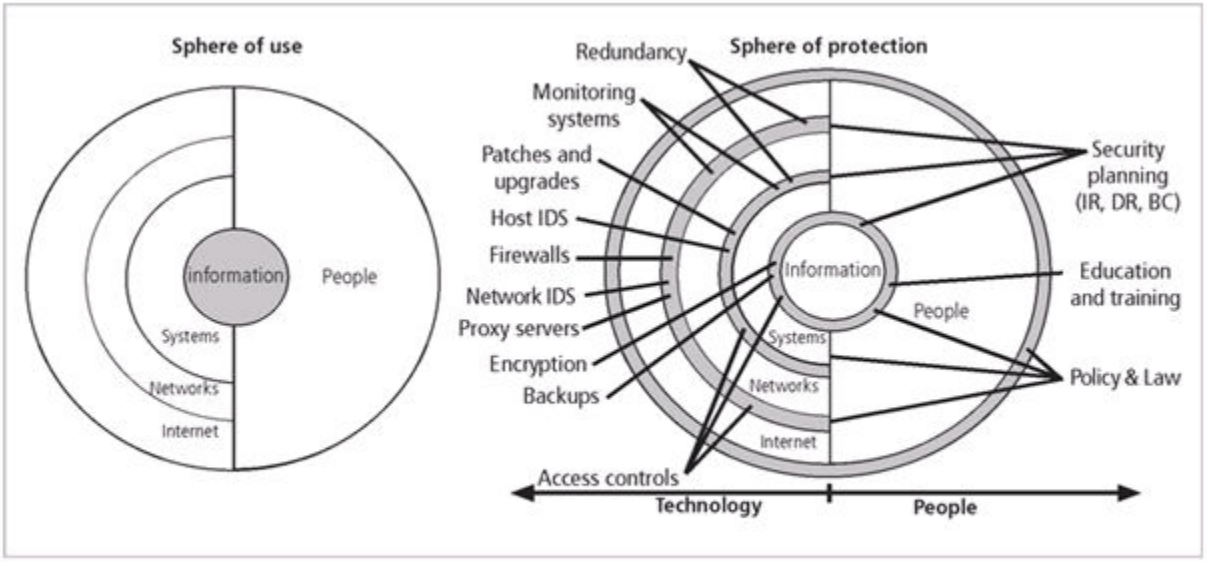


Figure 4.6.2.1 Spheres of security

4.6.3 Level of Control

Management Controls

1. Risk Management
2. Review of Security Controls
3. Life Cycle Maintenance

4. Authorization of Processing (Certification and Accreditation)
5. System Security Plan

Operational Controls

1. Personnel Security
2. Physical Security
3. Production, Input/Output Controls
4. Contingency Planning
5. Hardware and Systems Software
6. Data Integrity
7. Documentation
8. Security Awareness, Training, and Education
9. Incident Response Capability

Technical Controls

1. Identification and Authentication
2. Logical Access Controls
3. Audit Trails

Management controls

- ✓ It address the design and implementation of the security planning process and security program management.
- ✓ They also address risk management and security control reviews. They further describe the necessity and scope of legal compliance and the maintenance of the entire security life cycle.

Operational controls

- ✓ It deal with the operational functionality of security in the organization. They include management functions and lower level planning, such as disaster recovery and incident response planning.
- ✓ They also address personnel security, physical security, and the protection of production inputs and outputs.

- ✓ They guide the development of education, training and awareness programs for users, administrators, and management. Finally, they address hardware and software systems maintenance and the integrity of data.

Technical controls

- ✓ It address the tactical and technical issues related to designing and implementing security in the organization, as well as issues related to examining and selecting the technologies appropriate to protecting information.
- ✓ They address the specifics of technology selection and the acquisition of certain technical components. They also include logical access controls, such as identification, authentication, authorization, and accountability.
- ✓ They cover cryptography to protect information in storage and transit. Finally, they include the classification of assets and users, to facilitate the authorization levels needed.

Using the three sets of controls, the organization should be able to specify controls to cover the entire spectrum of safeguards, from strategic to tactical, and from managerial to technical.

4.6.4 Defense in Depth

- ✓ One of the basic foundations of security architectures is the implementation of security in layers. This layered approach is called **defense in depth**.
- ✓ Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls.
- ✓ These layers of control can be organized into policy, training and education and technology as per the NSTISSC model.
- ✓ While policy itself may not prevent attacks, they coupled with other layers and deter attacks.
- ✓ Training and Education are similar.
- ✓ Technology is also implemented in layers, with detection equipment, all operating behind access control mechanisms.
- ✓ Implementing multiple types of technology and thereby preventing the failure of one system from compromising the security of the information is referred to as **redundancy**.
- ✓ Redundancy can be implemented at a number of points throughout the security architecture, such as firewalls, proxy servers, and access controls. The figure shows the use of firewalls and intrusion detection systems(IDS) that use both packet-level rules and data content.

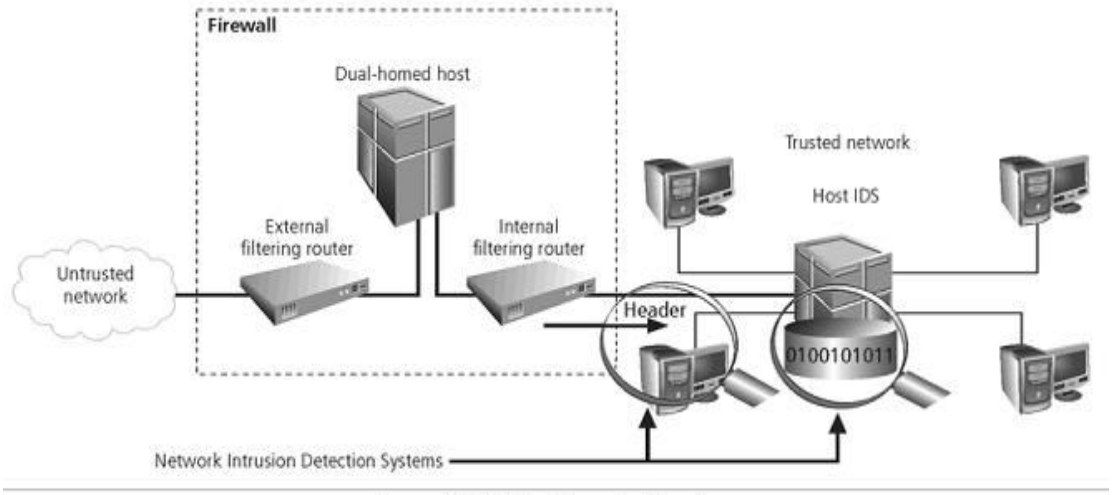


Figure 4.6.4.1 Defense in Depth

4.6.5 Security Perimeter

- ✓ A Security Perimeter is the first level of security that protects all internal systems from outside threats.
- ✓ Unfortunately, the perimeter does not protect against internal attacks from employee threats, or on-site physical threats.
- ✓ Security perimeters can effectively be implemented as multiple technologies that segregate the protected information from those who would attack it.
- ✓ Within security perimeters the organization can establish security domains, or areas of trust within which users can freely communicate.
- ✓ The presence and nature of the security perimeter is an essential element of the overall security framework, and the details of implementing the perimeter make up a great deal of the particulars of the completed security blueprint.
- ✓ The key components used for planning the perimeter are presented in the following sections on firewalls, DMZs, proxy servers, and intrusion detection systems.

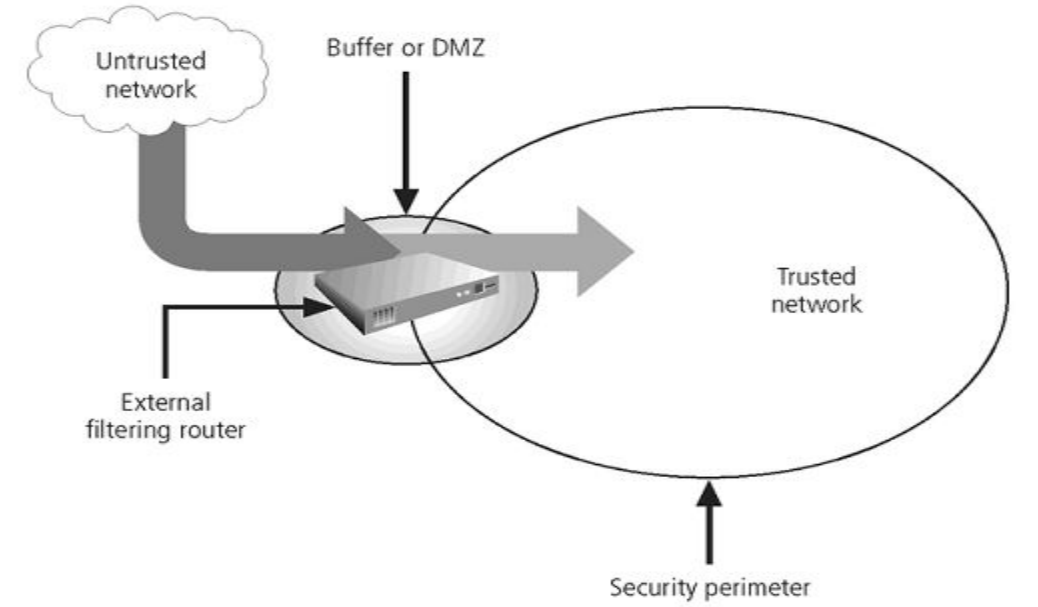


Figure 4.6.5.1 Security Perimeter and Domain

4.6.6 Key Technology Components

- ✓ Other key technology components

  - A **firewall** is a device that selectively discriminates against information flowing into or out of the organization.

  - Firewalls are usually placed on the security perimeter, just behind or as part of a **gateway router**.

  - Firewalls can be packet filtering, stateful packet filtering, proxy, or application level.

  - A Firewall can be a single device or a **firewall subnet**, which consists of multiple firewalls creating a buffer between the outside and inside networks.

  - The **DMZ** (demilitarized zone) is a no-man's land, between the inside and outside networks, where some organizations place Web servers

  - These servers provide access to organizational web pages, without allowing Web requests to enter the interior networks.

  - **Proxy server-** An alternative approach to the strategies of using a firewall subnet or a DMZ is to use a **proxy server**, or **proxy firewall**.

- When an outside client requests a particular Web page, the proxy server receives the request as if it were the subject of the request, then asks for the same information from the true Web server(acting as a proxy for the requestor), and then responds to the request as a proxy for the true Web server.

- For more frequently accessed Web pages, proxy servers can cache or temporarily store the page, and thus are sometimes called **cache servers.**

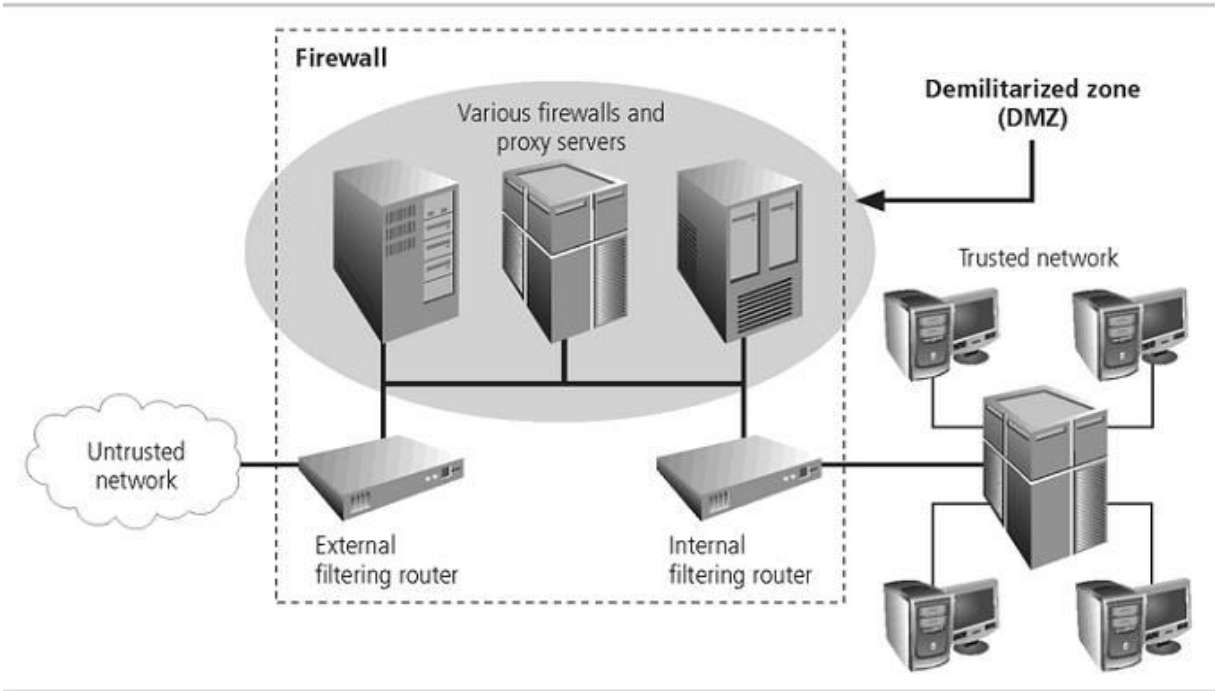


Figure 4.6.6.1 FirewalsProxy servers and DMZs

- **Intrusion Detection Systems (IDSs).** In an effort to detect unauthorized activity within the inner network, or on individual machines, an organization may wish to implement **Intrusion Detection Systems or IDS**.

- **IDs** come in two versions. Host-based & Network-based IDSs.

- **Host-based IDSs** are usually installed on the machines they protect to monitor the status of various files stored on those machines.

- **Network-based IDSs** look at patterns of network traffic and attempt to detect unusual activity based on previous baselines.

- This could include packets coming into the organization's networks with addresses from machines already within the organization (IP spoofing).
- It could also include high volumes of traffic going to outside addresses (as in cases of data theft) or coming into the network (as in a denial of service attack).
- Both host-and network based IDSs require a database of previous activity.

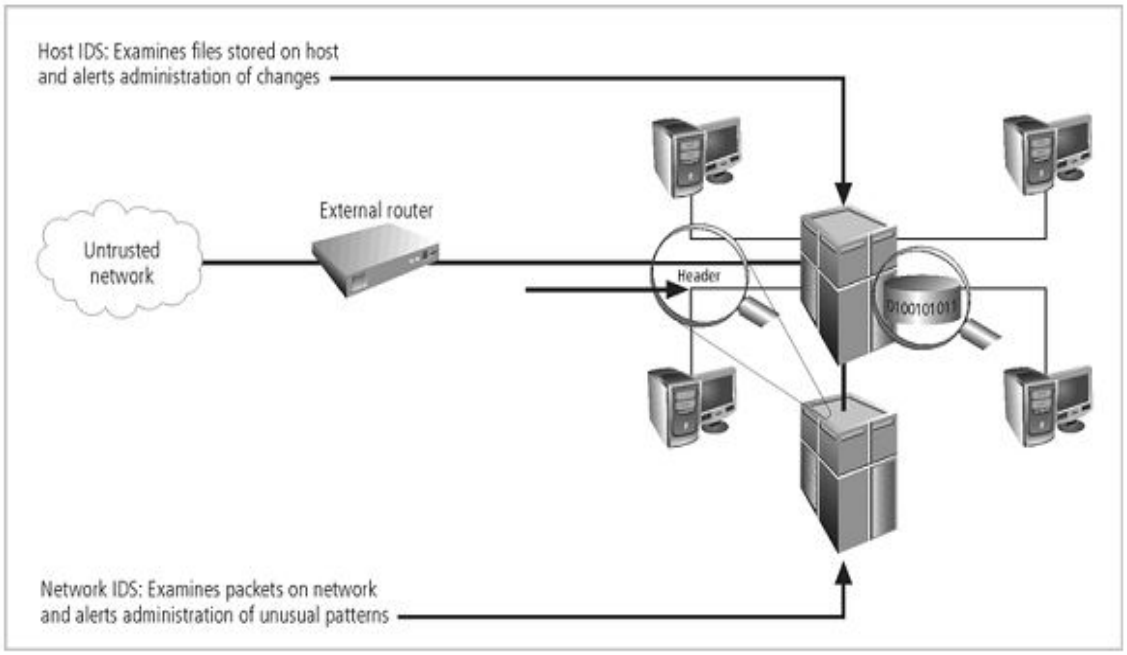


Figure 4.6.6.2 Intrusion detection system

4.6.7 Security Education, Training, and Awareness Program

- ✓ As soon as general security policy exists, policies to implement **security education, training and awareness (SETA)** program should follow.
- ✓ SETA is a control measure designed to reduce accidental security breaches by employees.
- ✓ Security education and training builds on the general knowledge the employees must possess to do their jobs, familiarizing them with the way to do their jobs securely

- ✓ The SETA program consists of three elements: security education; security training; and security awareness
- ✓ The purpose of SETA is to enhance security by:
    - Improving awareness of the need to protect system resources.
    - Developing skills and knowledge so computer users can perform their jobs more securely.
    - Building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

Security Education

- ✓ Everyone in an organization needs to be trained and aware of information security, but not every member of the organization needs a formal degree or certificate in information security.
- ✓ A number of universities have formal coursework in information security.
- ✓ For those interested in researching formal information security programs, there are resources available, such as the NSA-identified Centers of Excellence in Information Assurance Education.

Security Training

- ✓ It involves providing members of the organization with detailed information and hands-on instruction to prepare them to perform their duties securely.
- ✓ Management of information security can develop customized in-house training or outsource the training program.

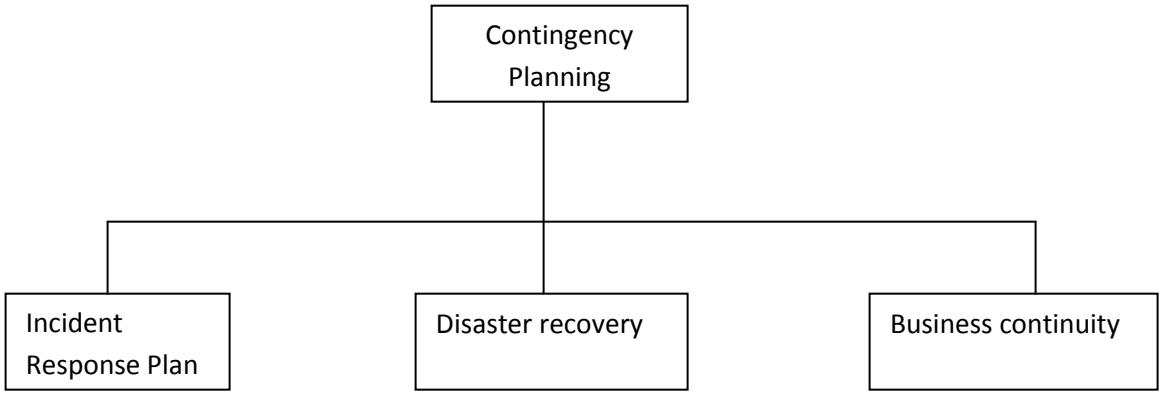
Security Awareness

- ✓ One of the least frequently implemented, but most beneficial programs is the security awareness program
- ✓ Designed to keep information security at the forefront of users' minds
- ✓ Need not be complicated or expensive
- ✓ If the program is not actively implemented, employees may begin to "tune out" and risk of employee accidents and failures increases

4.7 CONTINGENCY PLANNING (CP)

- ✓ Contingency Planning (CP) comprises a set of plans designed to ensure the effective reaction and recovery from an attack and the subsequent restoration to normal modes of business operations.
- ✓ Organizations need to develop disaster recovery plans, incident response plans, and business continuity plans as subsets of an overall CP.
- ✓ An **incident response plan (IRP)** deals with the identification, classification, response, and recovery from an incident, but if the attack is disastrous(e.g., fire, flood, earthquake) the process moves on to disaster recovery and BCP
- ✓ A **disaster recovery plan (DRP)** deals with the preparation for and recovery from a disaster, whether natural or man-made and it is closely associated with BCP.
- ✓ A **Business continuity plan (BCP)** ensures that critical business functions continue, if a catastrophic incident or disaster occurs. BCP occurs concurrently with DRP when the damage is major or long term, requiring more than simple restoration of information and information resources.

4.7.1 Components of Contingency Planning



There are six steps to contingency planning. They are

1. Identifying the mission-or business-critical functions,
2. Identifying the resources that support the critical functions,
3. Anticipating potential contingencies or disasters,
4. Selecting contingency planning strategies,

5. Implementing the contingencies strategies,

6. and Testing and revising the strategy.

4.7.2 Business Impact Analysis (BIA)

- ✓ A BIA is an investigation and assessment of the impact that various attacks can have on the organization.
- ✓ The contingency planning team conducts the BIA in the following stages,
    1. Threat attack indentification and prioritization
    2. Business unit analysis
    3. Attack success scenario development
    4. Potential damage assessment
    5. Subordinate plan classification

4.7.3 Incident response plan (IRP)

- ✓ It is the set of activities taken to plan for, detect, and correct the impact of an incident on information assets.
- ✓ IRP consists of the following 4 phases:
    1. Incident Planning
    2. Incident Detection
    3. Incident Reaction
    4. Incident Recovery

Incident Planning

- ✓ Planning for an incident is the first step in the overall process of incident response planning.
- ✓ The planners should develop a set of documents that guide the actions of each involved individual who reacts to and recovers from the incident.
- ✓ These plans must be properly organized and stored to be available when and where needed, and in a useful format.

Incident Detection

- ✓ Incident Detection relies on either a human or automated system, which is often the help desk staff, to identify an unusual occurrence and to classify it properly as an incident.
- ✓ The mechanisms that could potentially detect an incident include intrusion detection systems (both host-based and network based), virus detection software, systems administrators, and even end users.
- ✓ Once an attack is properly identified, the organization can effectively execute the corresponding procedures from the IR plan. Thus, **incident classification** is the process of examining a potential incident, or **incident candidate**, and determining whether or not the candidate constitutes an actual incident.
- ✓ **Incident Indicators**- There is a number of occurrences that could signal the presence of an incident candidate.
- ✓ **Donald Pipkin**, an IT security expert, identifies three categories of incident indicators: **Possible, Probable, and Definite Indicators**.
- ✓ **Possible Indicators**- There are 4 types of possible indicators of events ,they are,

  1. Presence of unfamiliar files.
  2. Presence or execution of unknown programs or processes.
  3. Unusual consumption of computing resources
  4. Unusual system crashes

- ✓ **Probable Indicators**- The four types of probable indicators of incidents are

  1. Activities at unexpected times.
  2. Presence of new accounts
  3. Reported attacks
  4. Notification from IDS

- ✓ **Definite Indicators-** The five types of definite indicators of incidents are

  1. Use of Dormant accounts
  2. Changes to logs

3. Presence of hacker tools
4. Notifications by partner or peer
5. Notification by hacker

Incident Reaction

- ✓ It consists of actions outlined in the IRP that guide the organization in attempting to stop the incident, mitigate the impact of the incident, and provide information for recovery from the incident.
- ✓ These actions take place as soon as the incident itself is over.
- ✓ In reacting to the incident there are a number of actions that must occur quickly, including notification of key personnel and documentation of the incident.
- ✓ These must have been prioritized and documented in the IRP for quick use in the heat of the moment.

Incident Recovery

- ✓ The recovery process involves much more than the simple restoration of stolen, damaged, or destroyed data files. It involves the following steps.

1. Identify the Vulnerabilities
2. Address the safeguards.
3. Evaluate monitoring capabilities
4. Restore the data from backups.
5. Restore the services and processes in use.
6. Continuously monitor the system
7. Restore the confidence of the members of the organization's communities of interest.

4.7.4 Disaster Recovery Plan (DRP)

- ✓ DRP provides detailed guidance in the event of a disaster and also provides details on the roles and responsibilities of the various individuals involved in the disaster recovery effort, and identifies the personnel and agencies that must be notified.
- ✓ At a minimum, the DRP must be reviewed during a walk-through or talk-through on a periodic basis.
- ✓ Many of the same precepts of incident response apply to disaster recovery:

1. There must be a clear establishment of priorities
2. There must be a clear delegation of roles and responsibilities
3. Someone must initiate the alert roster and notify key personnel.
4. Someone must be tasked with the documentation of the disaster.
5. If and only if it is possible, attempts must be made to mitigate the impact of the disaster on the operations of the organization.

4.7.5 Business Continuity Plan (BCP)

- ✓ It prepares an organization to reestablish critical business operations during a disaster that affects operations at the primary site.
- ✓ If a disaster has rendered the current location unusable for continued operations, there must be a plan to allow the business to continue to function.

Developing Continuity Programs

- ✓ Once the incident response plans and disaster recovery plans are in place, the organization needs to consider finding temporary facilities to support the continued viability of the business in the event of a disaster.
- ✓ The development of the BCP is simpler than that of the IRP and DRP ,in that it consists of selecting a continuity strategy and integrating the off-site data storage and recovery functions into this strategy.

Continuity Strategies

- ✓ There are a number of strategies from which an organization can choose when planning for business continuity.
- ✓ The determining factor in selection between these options is usually cost.
- ✓ In general there are three exclusive options: Hot sites, Warm Sites, and Cold sites; and three shared functions: Time-share, Service bureaus, and Mutual Agreements.

Hot sites: A hot site is a fully configured facility, with all services, communications links, and physical plant operations including heating and air conditioning. It is the pinnacle of contingency planning, a duplicate facility that needs only the latest data backups and the personnel to function as a fully operational twin of the original. Disadvantages include the need to provide maintenance for all the systems and equipment in the hot site, as well as physical and information security.

Warm sites: A warm site includes computing equipment and peripherals with servers but not client work stations. It has many of the advantages of a hot site, but at a lower cost.

Cold Sites: A cold site provides only rudimentary services and facilities, No computer hardware or peripherals are provided. Basically a cold site is an empty room with heating, air conditioning, and electricity. The main advantage of cold site is in the area of cost.

Time-shares: It allows the organization to maintain a disaster recovery and business continuity option, but at a reduced overall cost. The advantages are identical to the type of site selected(hot, warm, or cold). The disadvantages are the possibility that more than one organization involved in the time share may need the facility simultaneously and the need to stock the facility with the equipment and data from all organizations involved, the negotiations for arranging the time-share, and associated arrangements, should one or more parties decide to cancel the agreement or to sublease its options.

Service bureaus: A service bureau is an agency that provides a service for a fee. In the case of disaster recovery and continuity planning, the service is the agreement to provide physical facilities in the event of a disaster. These types of agencies also provide off-site data storage for a fee. The disadvantage is that it is a service, and must be renegotiated periodically. Also, using a service bureau can be quite expensive.

Mutual Agreements: A mutual agreement is a contract between two or more organizations that specifies how each will assist the other in the event of a disaster.

UNIT V – PHYSICAL DESIGN

5.1 Security Technology

5.1.1 What is Security?

- ✓ quality or state of being secure—to be free from danger"
- ✓ A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

Physical Design

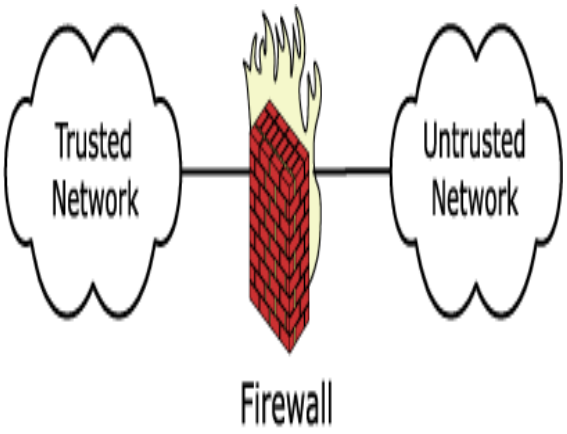
- ✓ Physical design of an information security program is made up of two parts:
  1. **Security technologies**
  2. **Physical security**
- ✓ Physical design process:
  - Identifies complete technical solutions based on these technologies (deployment, operations and maintenance elements)
  - Design physical security measures to support the technical solution.

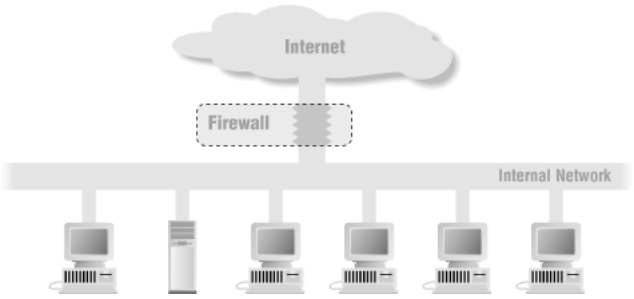
5.1.2 Firewalls

- ✓ A software or hardware component that restricts network communication between two computers or networks.
  - In buildings, a firewall is a fireproof wall that restricts the spread of a fire.
  - Network firewall prevents threats from spreading from one network to another
- ✓ Prevent specific types of information from moving between the outside world (untrusted networks) and the inside world (trusted networks)

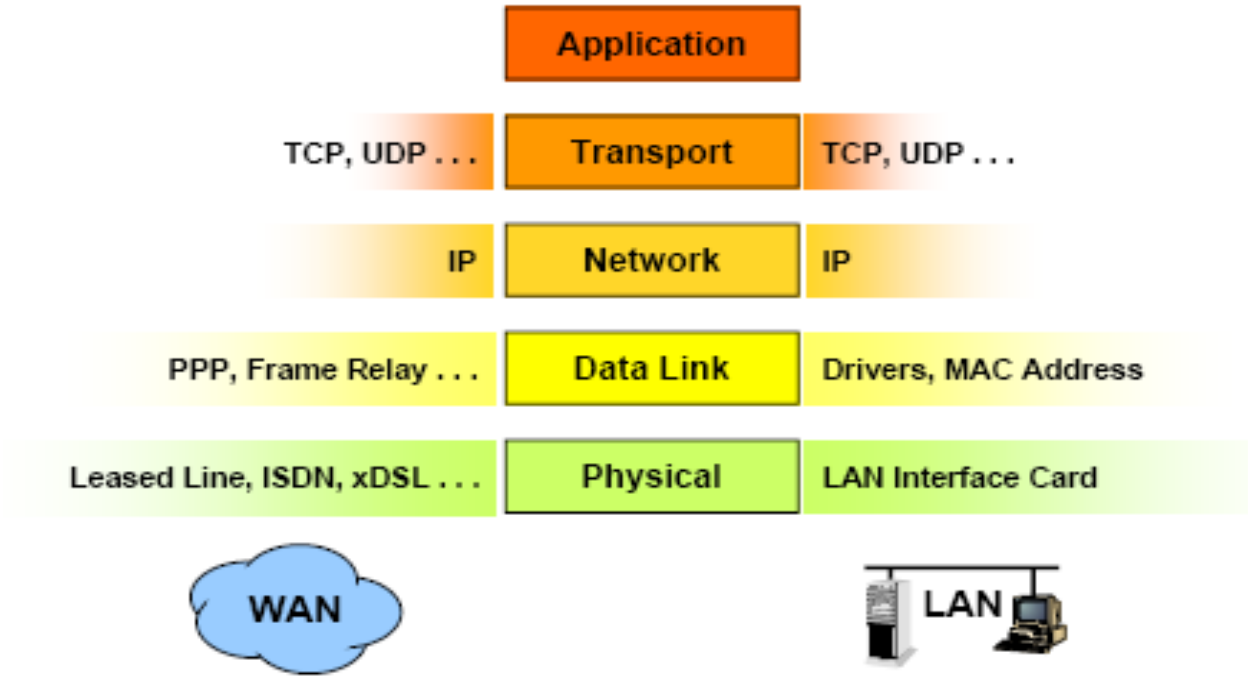
- ✓ The firewall may be a separate computer system, a software service running on an existing router all server, or a separate network containing a number of supporting devices.

Internet Firewalls





The Internet Protocol Stack



5.1.2.1 What Firewalls do

- ✓ Protects the resources of an internal network.
    - Restrict external access.
    - Log Network activities.
- Intrusion detection
- DoS
    - Act as intermediary
    - Centralized Security Management
    - Carefully administer one firewall to control internet traffic of many machines.
    - Internal machines can be administered with less care.

5.1.2.2 Types of Firewalls (General)

- ✓ Firewalls types can be categorized depending on:
    - The Function or methodology the firewall use
    - Whether the communication is being done between a single node and the network, or between two or more networks.
    - Whether the communication state is being tracked at the firewall or not.
- ✓ **With regard to the scope of filtered communications the done between a single node and the network, or between two or more networks there exist :**
    - Personal Firewalls, a software application which normally filters traffic entering or leaving a single computer.
    - Network firewalls, normally running on a dedicated network device or computer positioned on the boundary of two or more networks.

5.1.2.3 Firewall categorization methods

The Function or methodology the firewall use

- ✓ Five processing modes that firewalls can be categorized by are :
    1. packet filtering

2. application gateways
3. circuit gateways
4. MAC layer firewalls
5. hybrids

1.Packet filtering:

- ✓ examine the header information of data packets that come into a network.
- ✓ a packet filtering firewall installed on TCP/IP based network and determine wether to drop a packet or forward it to the next network connection based on the rules programmed in the firewall.
- ✓ Packet filtering firewalls scan network data packets looking for violation of the rules of the firewalls database.
- ✓ Filtering firewall inspect packets on at the network layers.
- ✓ If the device finds a packet that matches a restriction it stops the packet from traveling from network to another.
- ✓ filters packet-by-packet, decides to *Accept/Deny/Discard* packet based on certain/configurable criteria – *Filter Rule sets*.
- ✓ Typically stateless: do not keep a table of the connection *state* of the various traffic that flows through them
  - Not dynamic enough to be considered true firewalls.
  - Usually located at the boundary of a network.
  - Their main strength points: ***Speed*** and ***Flexibility***.

There are three subsets of packet filtering firewalls:

1. static filtering
2. dynamic filtering
3. stateful inspection

1. static filtering:

- ✓ requires that the filtering rules governing how the firewall decides which packets are allowed and which are denied.

- ✓ This type of filtering is common in network routers and gateways.

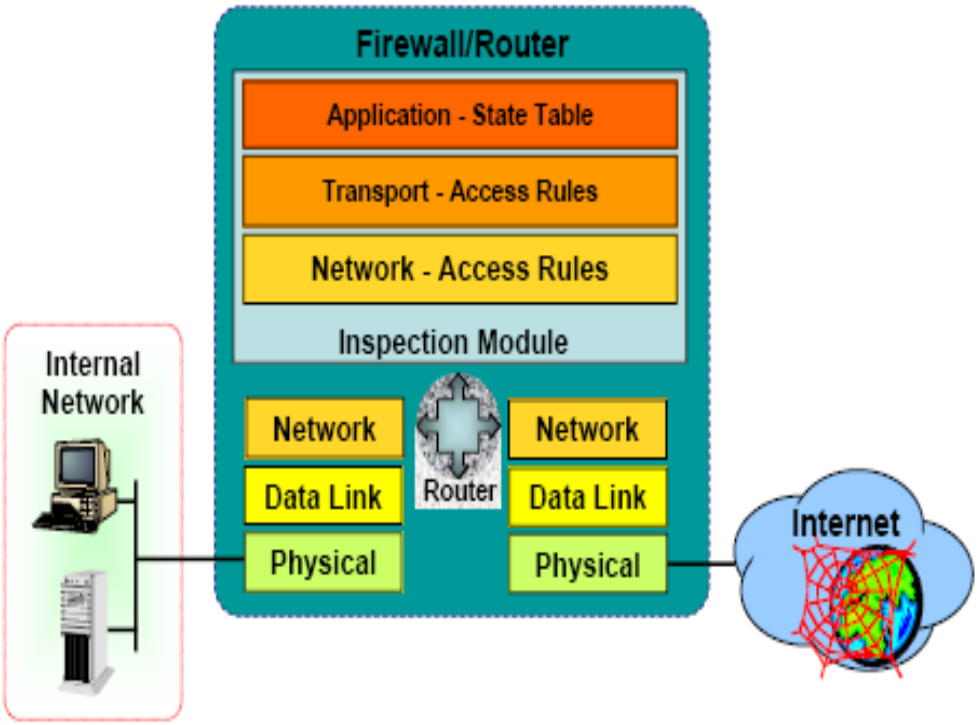
2. Dynamic filtering

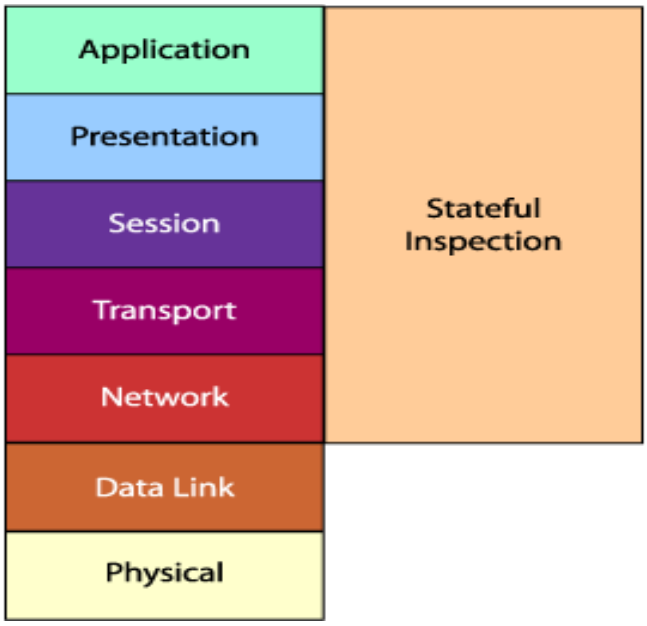
- ✓ allows the firewall to create rules to deal with event.
- ✓ This reaction could be positive as in allowing an internal user to engage in a specific activity upon request or negative as in dropping all packets from a particular address

3. Stateful inspection

- ✓ keep track of each network connection between internal and external systems using a state table.
- ✓ A state table tracks the state and context of each packet in the conversation by recording which station send , what packet and when.
- ✓ More complex than their constituent component firewalls
- ✓ Nearly all modern firewalls in the market today are staful

Stateful Inspection Firewalls





Basic Weaknesses Associated with Packet Filters\ Statful

- They cannot prevent attacks that employ application-specific vulnerabilities or functions.
- Logging functionality present in packet filter firewalls is limited
- Most packet filter firewalls do not support advanced user authentication schemes.
- Vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing.
- Susceptible to security breaches caused by improper configurations.

✓ **Advantages**:

- One packet filter can protect an entire network
- Efficient (requires little CPU)
- Supported by most routers

✓ **Disadvantages**:

- Difficult to configure correctly

✓ Must consider rule set in its entirety

- Difficult to test completely

- Performance penalty for complex rulesets

✓ Stateful packet filtering much more expensive

- Enforces ACLs at layer 3 + 4, without knowing any application details

Packet Filtering Firewalls

✓ The original firewall

✓ Works at the network level of the OSI

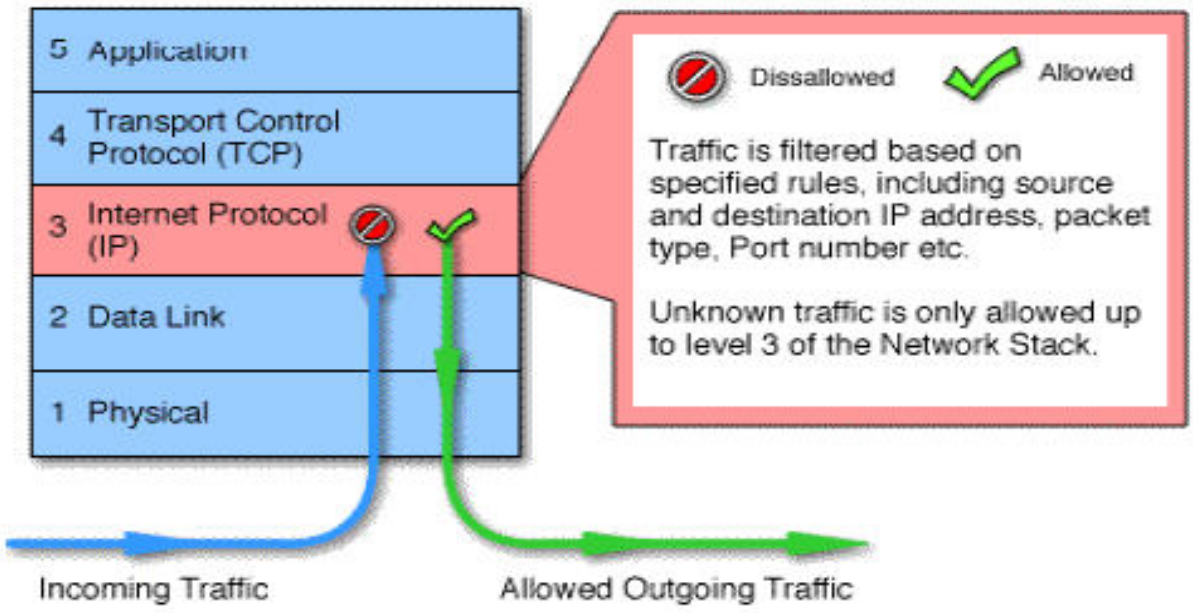
✓ model

✓ Applies packet filters based on access

✓ Rules:

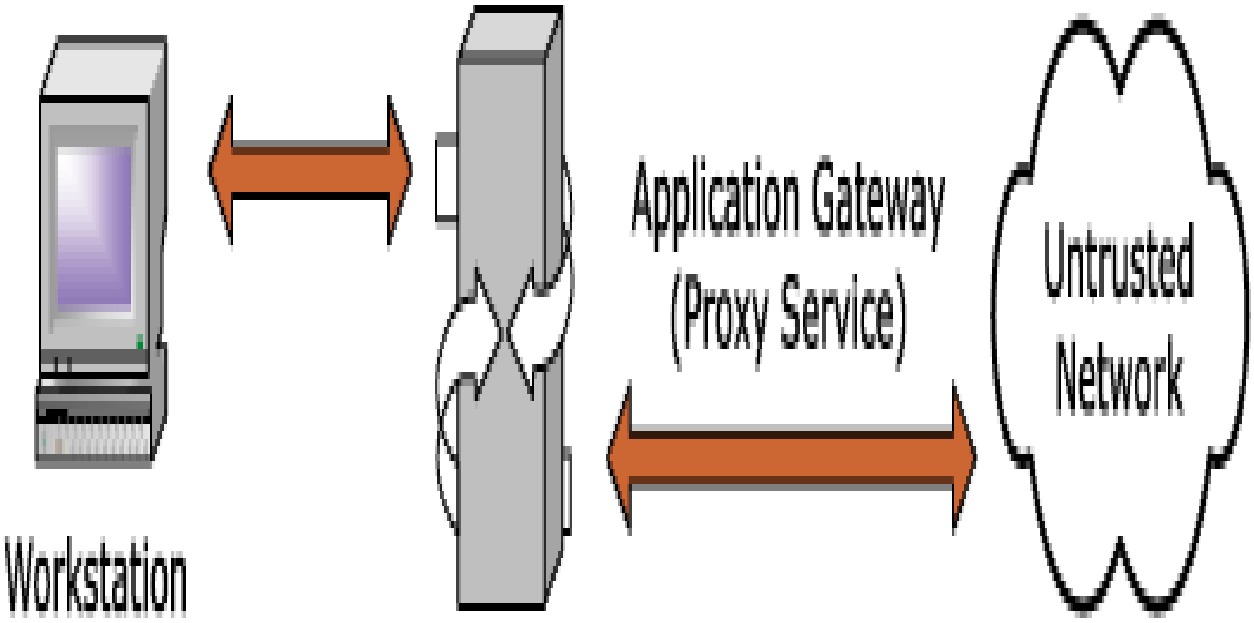
- Source IP address
- Destination IP address
- Application or protocol
- Source port number
- Destination port number

Packet Filtering Firewalls



2. Application gateways:

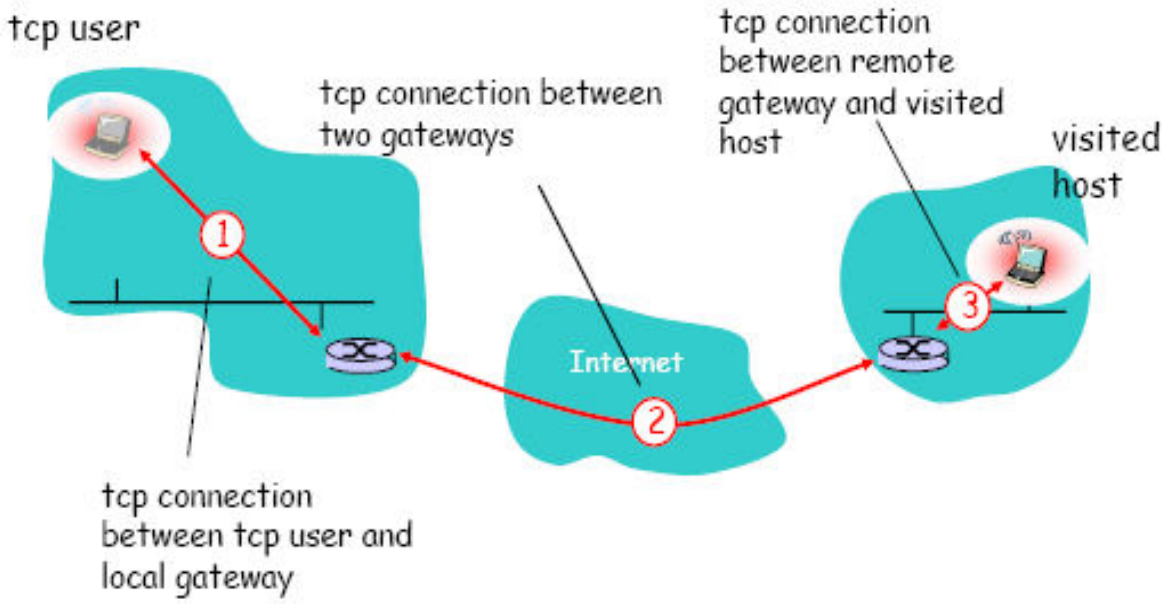
- ✓ is also known as proxy server since it runs special software that acts as a proxy for a service request.
- ✓ One common example of proxy server is a firewall that blocks or requests for and responses to request for web pages and services from the internal computers of an organization.
- ✓ The primary disadvantage of application level firewalls is that they are designed for a specific protocols and cannot easily be reconfigured to protect against attacks in other protocols.
- ✓ Application firewalls work at the application layer.
- ✓ Filters packets on application data as well as on IP/TCP/UDP fields.
- ✓ The interaction is controlled at the application layer
- ✓ A proxy server is an application that mediates traffic between two network segments.
- ✓ With the proxy acting as mediator, the source and destination systems never actually "connect".
- ✓ Filtering Hostile Code: Proxies can analyze the payload of a packet of data and make decision as to whether this packet should be passed or dropped.



4.Circuit gateways:

- ✓ operates at the transport layer.
- ✓ Connections are authorized based on addresses , they prevent direct connections between network and another.
- ✓ They accomplish this prevention by creating channels connecting specific systems on each side of the firewall and then allow only authorized traffic.
- ✓ relays two TCP connections (session layer)
- ✓ imposes security by limiting which such connections are allowed
- ✓ once created usually relays traffic without examining contents
- ✓ Monitor handshaking between packets to decide whether the traffic is legitimate
- ✓ typically used when trust internal users by allowing general outbound connections
- ✓ SOCKS commonly used for this

Circuit Level Firewalls Example



4.MAC layer firewalls:

- ✓ design to operate at the media access control layer.

- ✓ Using this approach the MAC addresses of specific host computers are linked to ACL entries that identify the specific types of packets that can be send to each host and all other traffic is blocked.

5.Hybrids firewalls:

- ✓ companied the elements of other types of firewalls , example the elements of packet filtering and proxy services, or a packet filtering and circuit gateways.

- ✓ That means a hybrids firewalls may actually of two separate firewall devices; each is a separate firewall system, but they are connected so that they work together.

5.1.2.3 Types of Firewalls

- ✓ Finally, Types depending on whether the firewalls keeps track of the state of network connections or treats each packet in isolation, two additional categories of firewalls exist:

  - Stateful firewall

  - Stateless firewall

Stateful firewall

- ✓ keeps track of the state of network connections (such as TCP streams) traveling across it.

- ✓ Stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection.

Stateless firewall

- ✓ Treats each network frame (Packet) in isolation. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.

- ✓ The classic example is the File Transfer Protocol, because by design it opens new connections to random ports.

5.1.2.4 Advantages of a Firewall

- ✓ Stop incoming calls to insecure services

- ✓ such as rlogin and NFS

- ✓ Control access to other services

- ✓ Control the spread of viruses

- ✓ Cost Effective
- ✓ More secure than securing every
- ✓ system

5.1.2.5 Disadvantages of a Firewall

- ✓ Central point of attack
- ✓ Restrict legitimate use of the Internet
- ✓ Bottleneck for performance
- ✓ Does not protect the 'back door'
- ✓ Cannot always protect against
- ✓ smuggling
- ✓ Cannot prevent insider attacks

5.2 INTRUSION DETECTION SYSTEM

5.2.1 Introduction

- ✓ **Intrusion:** type of attack on information assets in which instigator attempts to gain entry into or disrupt system with harmful intent
- ✓ **Intrusion detection:** consists of procedures and systems created and operated to detect system intrusions
- ✓ **Intrusion reaction:** encompasses actions an organization undertakes when intrusion event is detected
- ✓ **Intrusion correction activities:** finalize restoration of operations to a normal state
- ✓ **Intrusion prevention:** consists of activities that seek to deter an intrusion from occurring

5.2.2 Intrusion Detection Systems (IDSs)

- ✓ Detects a violation of its configuration and activates alarm
- ✓ Many IDSs enable administrators to configure systems to notify them directly of trouble via e-mail or pagers

- ✓ Systems can also be configured to notify an external security service organization of a "break-in"

5.2.3 IDS Terminology

- ✓ Alert or alarm
- ✓ False negative
  - The failure of an IDS system to react to an actual attack event.
- ✓ False positive
  - An alarm or alert that indicates that an attack is in progress or that an attack has successfully occurred when in fact there was no such attack.
- ✓ Confidence value
- ✓ Alarm filtering

5.2.4 IDSs Classification

- ✓ All IDSs use one of two detection methods:
  - Signature-based
  - Statistical anomaly-based
- ✓ IDSs operate as:
  - network-based
  - host-based
  - application-based systems

5.2.4.1 Signature-Based IDS

- ✓ Examine data traffic in search of patterns that match known signatures
- ✓ Widely used because many attacks have clear and distinct signatures
- ✓ Problem with this approach is that as new attack strategies are identified, the IDS's database of signatures must be continually updated

5.2.4.2 Statistical Anomaly-Based IDS

- ✓ The statistical anomaly-based IDS (stat IDS) or behavior-based IDS sample network activity to compare to traffic that is known to be normal

- ✓ When measured activity is outside baseline parameters or clipping level, IDS will trigger an alert
- ✓ IDS can detect new types of attacks
- ✓ Requires much more overhead and processing capacity than signature-based
- ✓ May generate many false positives

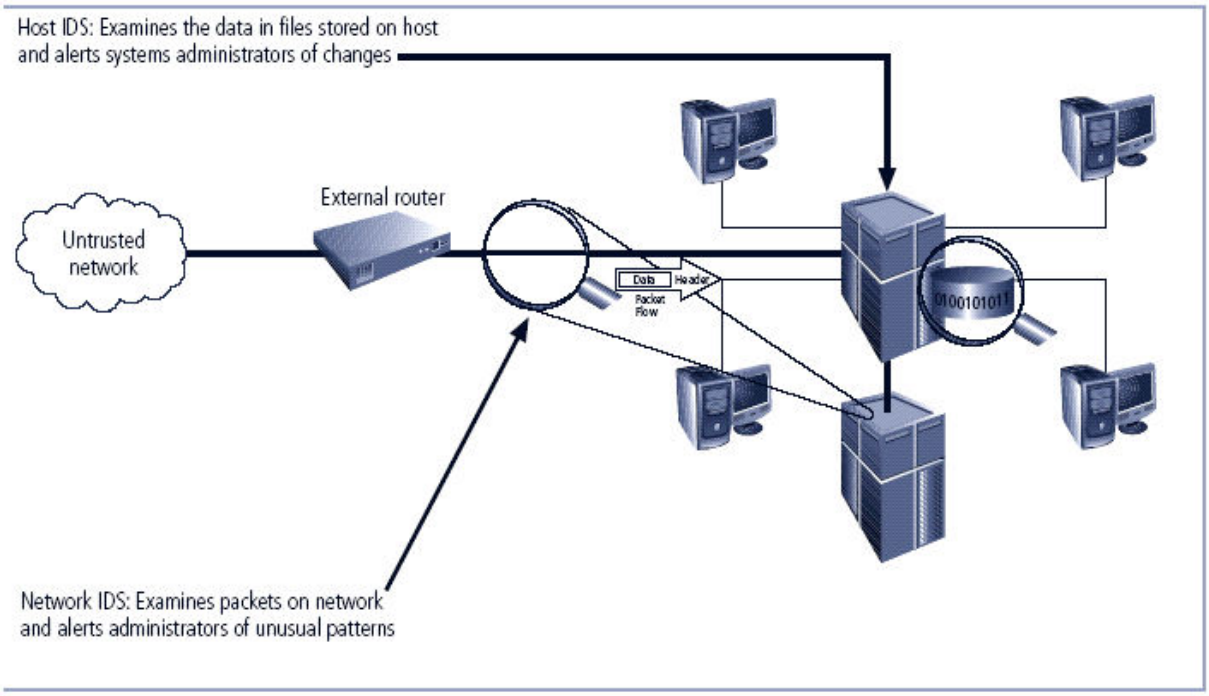


FIGURE 7-1 Intrusion Detection Systems

5.2.4.3 Network-Based IDS (NIDS)

- ✓ Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks
- ✓ When examining packets, a NIDS looks for attack patterns
- ✓ Installed at specific place in the network where it can watch traffic going into and out of particular network segment

NIDS Signature Matching

- ✓ To detect an attack, NIDSs look for attack patterns
- ✓ Done by using special implementation of TCP/IP stack:

- In process of protocol stack verification, NIDSs look for invalid data packets
- In application protocol verification, higher-order protocols are examined for unexpected packet behavior or improper use

Advantages and Disadvantages of NIDSs

- ✓ Good network design and placement of NIDS can enable organization to use a few devices to monitor large network
- ✓ NIDSs are usually passive and can be deployed into existing networks with little disruption to normal network operations
- ✓ NIDSs not usually susceptible to direct attack and may not be detectable by attackers
- ✓ Can become overwhelmed by network volume and fail to recognize attacks
- ✓ Require access to all traffic to be monitored
- ✓ Cannot analyze encrypted packets
- ✓ Cannot reliably ascertain if attack was successful or not
- ✓ Some forms of attack are not easily discerned by NIDSs, specifically those involving fragmented packets

5.2.4.4 Host-Based IDS

- ✓ Host-based IDS (HIDS) resides on a particular computer or server and monitors activity only on that system
- ✓ Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
- ✓ Most HIDSs work on the principle of configuration or change management
- ✓ Advantage over NIDS: can usually be installed so that it can access information encrypted when traveling over network
- ✓ Advantages and Disadvantages of HIDSs
- ✓ Can detect local events on host systems and detect attacks that may elude a network-based IDS
- ✓ Functions on host system, where encrypted traffic will have been decrypted and is available for processing
- ✓ Not affected by use of switched network protocols

- ✓ Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs
- ✓ Pose more management issues
- ✓ Vulnerable both to direct attacks and attacks against host operating system
- ✓ Does not detect multi-host scanning, nor scanning of non-host network devices
- ✓ Susceptible to some denial-of-service attacks
- ✓ Can use large amounts of disk space
- ✓ Can inflict a performance overhead on its host systems

5.2.4.5 Application-Based IDS

- ✓ Application-based IDS (AppIDS) examines application for abnormal events
- ✓ AppIDS may be configured to intercept requests:
  - File System
  - Network
  - Configuration
  - Execution Space

Advantages and Disadvantages of AppIDSs

- ✓ Advantages
  - Aware of specific users; can observe interaction between application and user
  - Able to operate even when incoming data is encrypted
- ✓ Disadvantages
  - More susceptible to attack
  - Less capable of detecting software tampering
  - May be taken in by forms of spoofing

Selecting IDS Approaches and Products

- ✓ Technical and policy considerations
  - What is your systems environment?

- What are your security goals and objectives?
- What is your existing security policy?

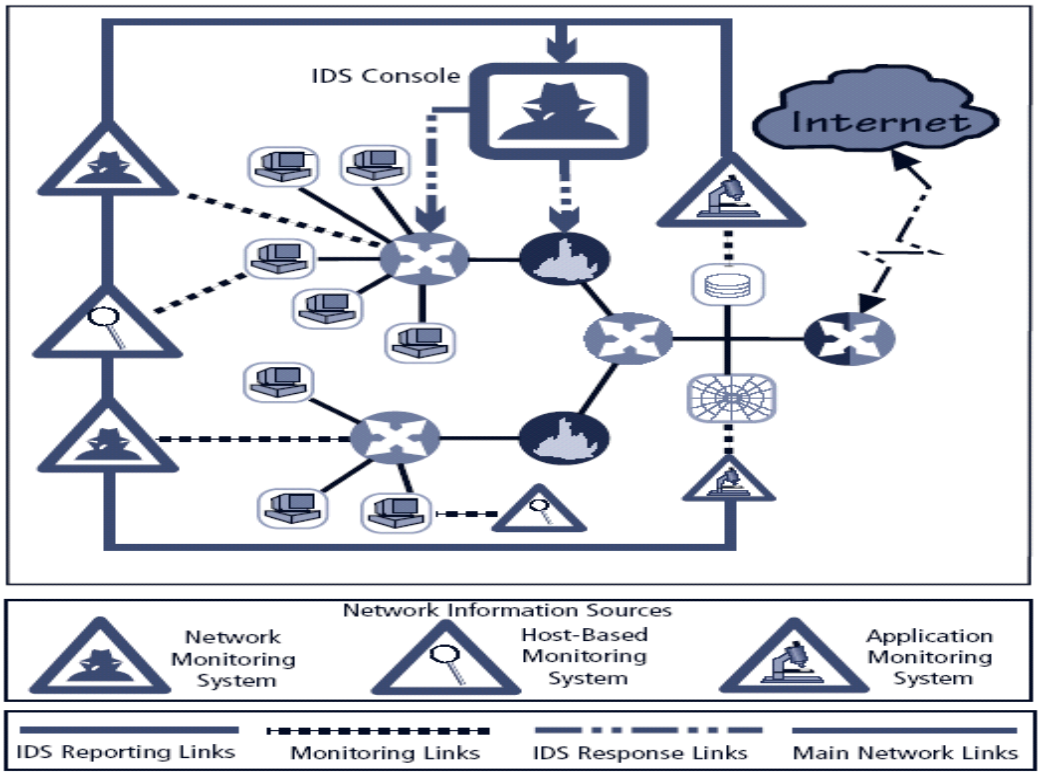
✓ Organizational requirements and constraints

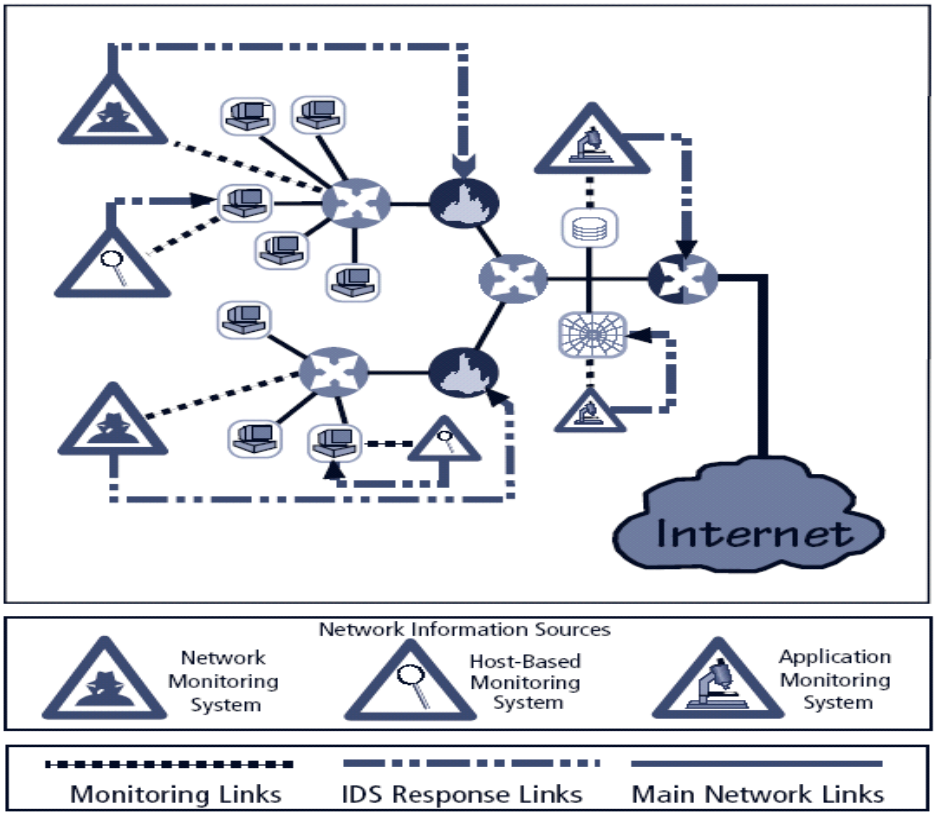
- What are requirements that are levied from outside the organization?
- What are your organization's resource constraints?

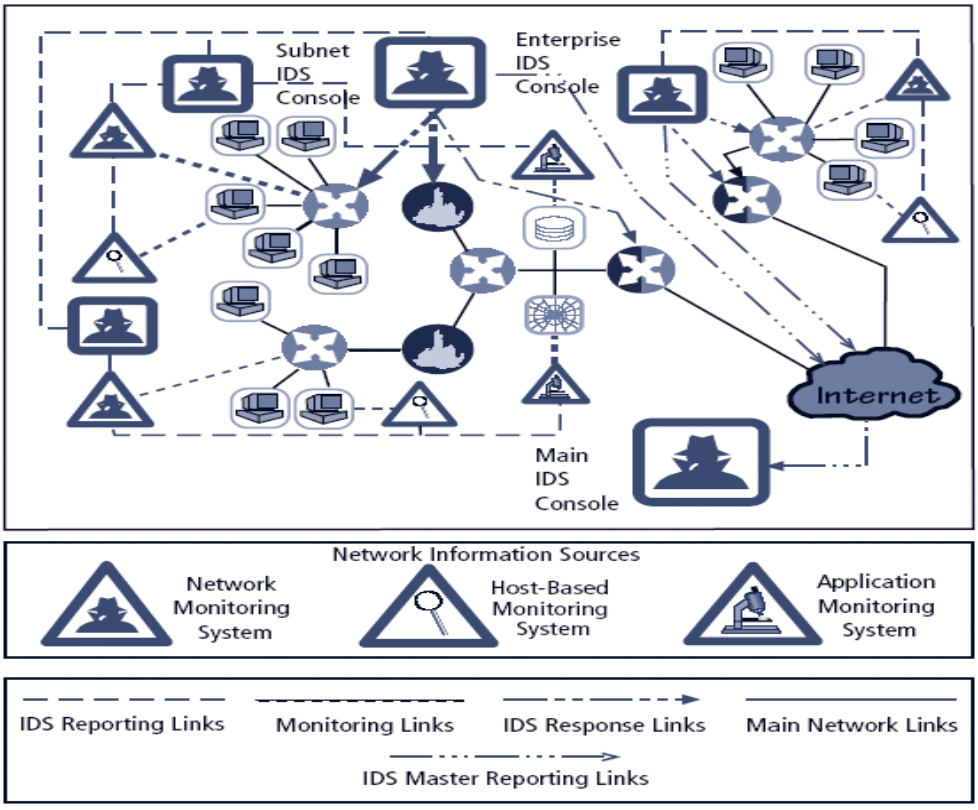
5.2.5 IDS Control Strategies

✓ An IDS can be implemented via one of three basic control strategies

- Centralized: all IDS control functions are implemented and managed in a central location
- Fully distributed: all control functions are applied at the physical location of each IDS component
- Partially distributed: combines the two; while individual agents can still analyze and respond to local threats, they report to a hierarchical central facility to enable organization to detect widespread attacks




Internet
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
Monitoring Links
IDS Response Links
Main Network Links


Subnet IDS Console
Enterprise IDS Console
Internet
Main IDS Console
Network Information Sources
Network Monitoring System
Host-Based Monitoring System
Application Monitoring System
IDS Reporting Links
Monitoring Links
IDS Response Links
Main Network Links
IDS Master Reporting Links

IDS Deployment Overview

- ✓ Like decision regarding control strategies, decisions about where to locate elements of intrusion detection systems can be art in itself
- ✓ Planners must select deployment strategy based on careful analysis of organization's information security requirements but, at the same time, causes minimal impact
- ✓ NIDS and HIDS can be used in tandem to cover both individual systems that connect to an organization's networks and networks themselves

Deploying Network-Based IDSs

- ✓ NIST recommends four locations for NIDS sensors
  - Location 1: behind each external firewall, in the network DMZ
  - Location 2: outside an external firewall
  - Location 3: On major network backbones
  - Location 4: On critical subnets

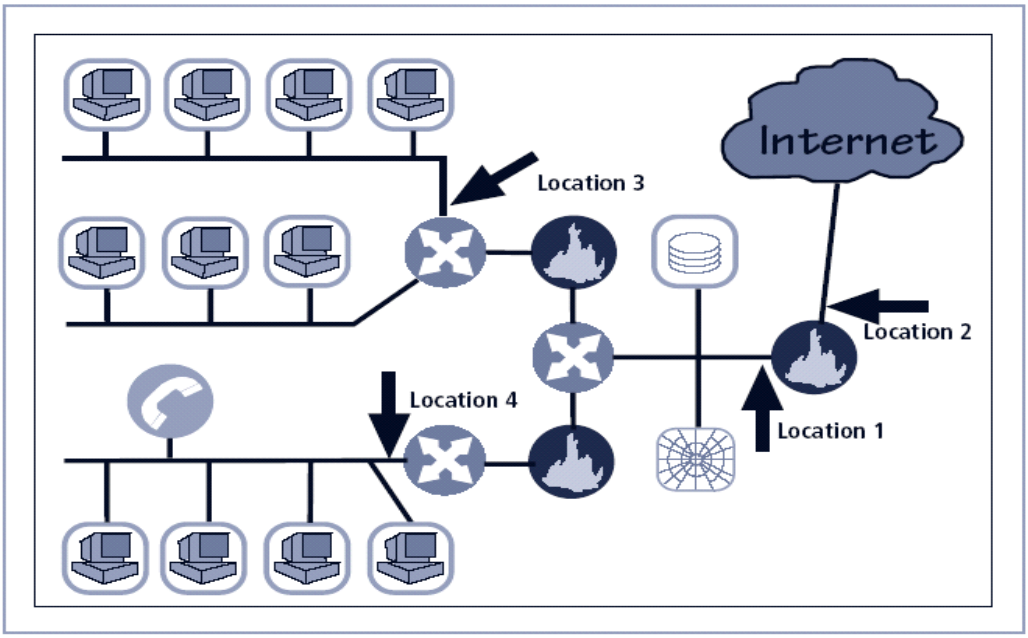


FIGURE 7-7 Network IDS Sensor Locations[17]

Deploying Host-Based IDSs

- ✓ Proper implementation of HIDSs can be painstaking and time-consuming task
- ✓ Deployment begins with implementing most critical systems first
- ✓ Installation continues until either all systems are installed, or the organization reaches planned degree of coverage it is willing to live with

Measuring the Effectiveness of IDSs

- ✓ IDSs are evaluated using two dominant metrics:
  - Administrators evaluate the number of attacks detected in a known collection of probes
  - Administrators examine the level of use at which IDSs fail
- ✓ Evaluation of IDS might read: *at 100 Mb/s, IDS was able to detect 97% of directed attacks*
- ✓ Since developing this collection can be tedious, most IDS vendors provide testing mechanisms that verify systems are performing as expected
- ✓ Some of these testing processes will enable the administrator to:
  - Record and retransmit packets from real virus or worm scan
  - Record and retransmit packets from a real virus or worm scan with incomplete TCP/IP session connections (missing SYN packets)
  - Conduct a real virus or worm scan against an invulnerable system

5.2.6 Honey Pots, Honey Nets, and Padded Cell Systems

- ✓ Honey pots: decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves
- ✓ Honey nets: collection of honey pots connecting several honey pot systems on a subnet
- ✓ Honey pots designed to:
  - Divert attacker from accessing critical systems
  - Collect information about attacker's activity
  - Encourage attacker to stay on system long enough for administrators to document event and, perhaps, respond

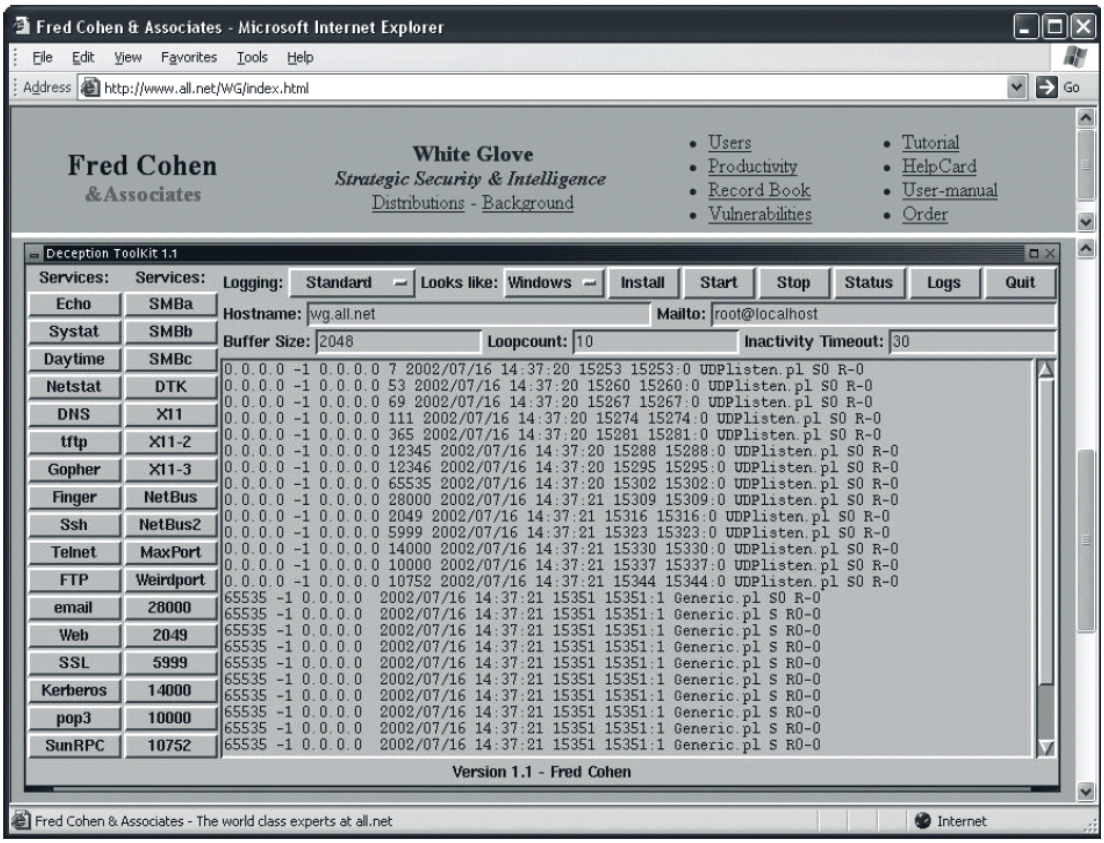


FIGURE 7-8 Deception Toolkit

- ✓ Padded cell: honey pot that has been protected so it cannot be easily compromised
- ✓ In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDS
- ✓ When the IDS detects attackers, it seamlessly transfers them to a special simulated environment where they can cause no harm—the nature of this host environment is what gives approach the name padded cell
- ✓ Advantages
  - Attackers can be diverted to targets they cannot damage
  - Administrators have time to decide how to respond to attacker
  - Attackers' actions can be easily and more extensively monitored, and records can be used to refine threat models and improve system protections
  - Honey pots may be effective at catching insiders who are snooping around a network

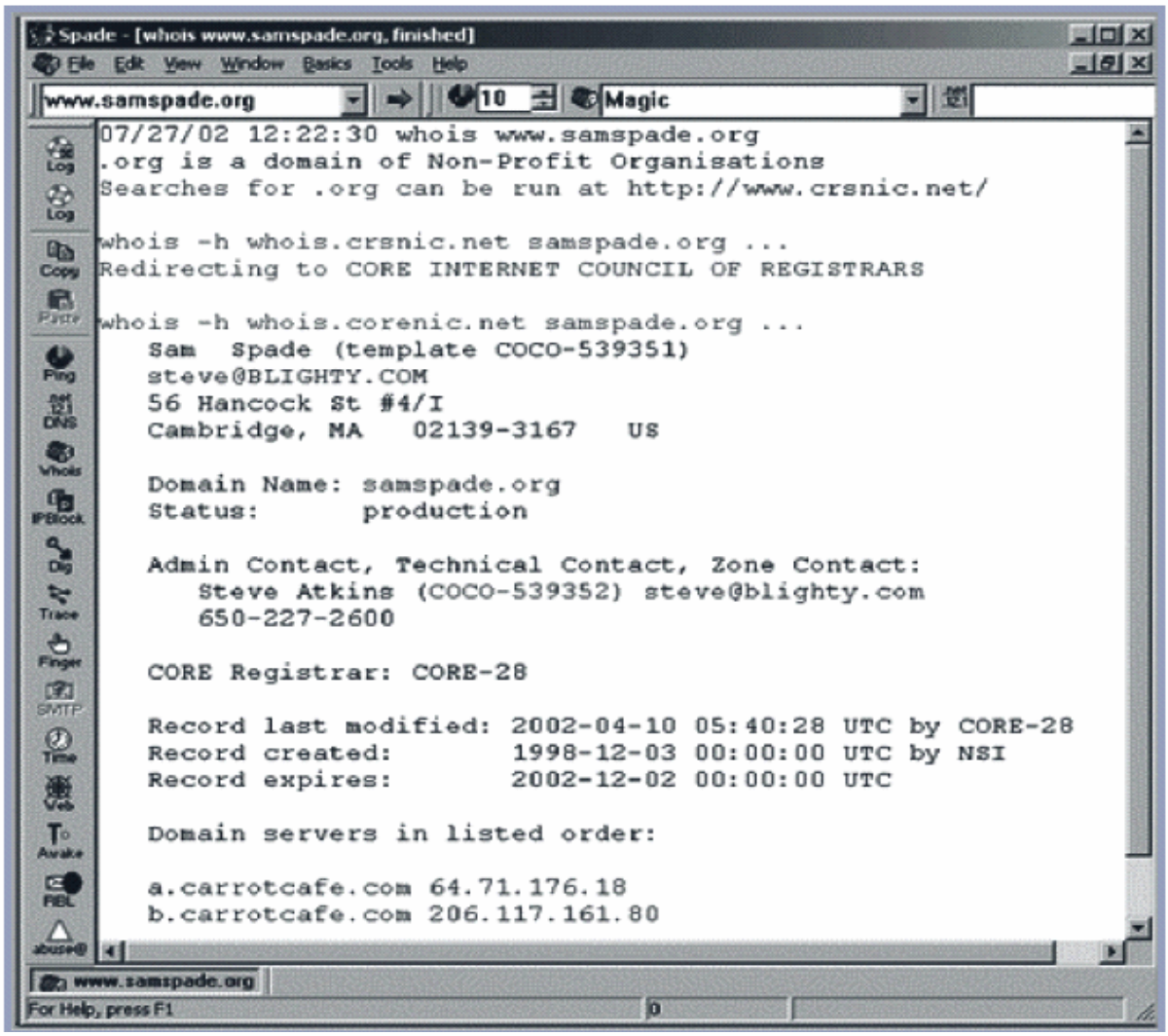
- ✓ Disadvantages
    - Legal implications of using such devices are not well defined
    - Honey pots and padded cells have not yet been shown to be generally useful security technologies
    - Expert attacker, once diverted into a decoy system, may become angry and launch a more hostile attack against an organization's systems
    - Administrators and security managers will need a high level of expertise to use these systems

5.2.7 Trap and Trace Systems

- ✓ Use combination of techniques to detect an intrusion and trace it back to its source
- ✓ Trap usually consists of honey pot or padded cell and alarm
- ✓ Legal drawbacks to trap and trace
    - Enticement: process of attracting attention to system by placing tantalizing bits of information in key locations
    - Entrapment: action of luring an individual into committing a crime to get a conviction.
    - Enticement is legal and ethical, whereas entrapment is not

5.3 SCANNING AND ANALYSIS TOOLS

- ✓ Typically used to collect information that attacker would need to launch successful attack
- ✓ Attack protocol is series of steps or processes used by an attacker, in a logical sequence, to launch attack against a target system or network
- ✓ Footprinting: the organized research of Internet addresses owned or controlled by a target organization



- ✓ Fingerprinting: systematic survey of all of target organization's Internet addresses collected during the footprinting phase
- ✓ Fingerprinting reveals useful information about internal structure and operational nature of target system or network for anticipated attack
- ✓ These tools are valuable to network defender since they can quickly pinpoint the parts of the systems or network that need a prompt repair to close the vulnerability

5.3.1 Port Scanners

- ✓ Tools used by both attackers and defenders to identify computers active on a network, and other useful information

- ✓ Can scan for specific types of computers, protocols, or resources, or their scans can be generic
- ✓ The more specific the scanner is, the better it can give attackers and defenders useful information

5.3.2 Firewall Analysis Tools

- ✓ Several tools automate remote discovery of firewall rules and assist the administrator in analyzing the rules
- ✓ Administrators who feel wary of using same tools that attackers use should remember:
  - It is intent of user that will dictate how information gathered will be used
  - In order to defend a computer or network well, necessary to understand ways it can be attacked
- ✓ A tool that can help close up an open or poorly configured firewall will help network defender minimize risk from attack

5.3.3 Packet Sniffers

- ✓ Network tool that collects copies of packets from network and analyzes them
- ✓ Can provide network administrator with valuable information for diagnosing and resolving networking issues
- ✓ In the wrong hands, a sniffer can be used to eavesdrop on network traffic
- ✓ To use packet sniffer legally, administrator must be on network that organization owns, be under direct authorization of owners of network, and have knowledge and consent of the content creators

5.3.4 Wireless Security Tools

- ✓ Organization that spends its time securing wired network and leaves wireless networks to operate in any manner is opening itself up for security breach
- ✓ Security professional must assess risk of wireless networks
- ✓ A wireless security toolkit should include the ability to sniff wireless traffic, scan wireless hosts, and assess level of privacy or confidentiality afforded on the wireless network

5.4 CRYPTOGRAPHY

5.4.1 Security goals

- ✓ We will first discuss three security goals: *confidentiality*, *integrity* and availability (Figure 16.1).

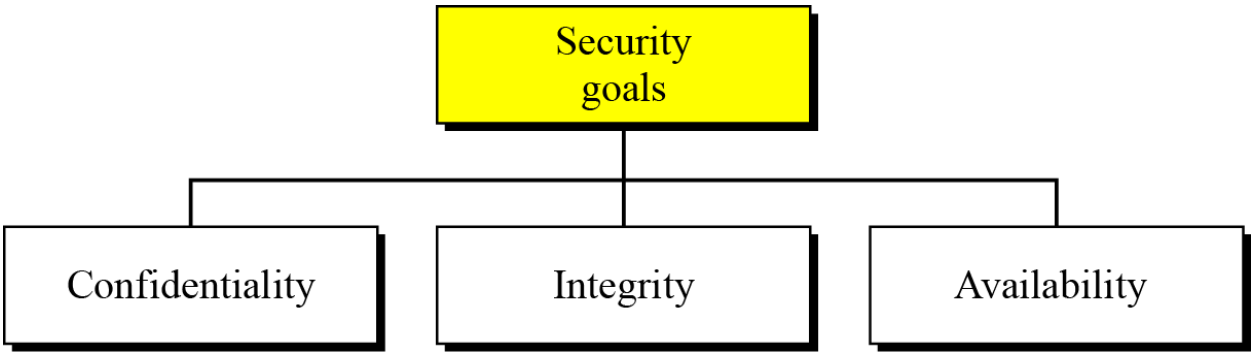


Figure 5.4.1.1 Taxonomy of security goals

Confidentiality

- ✓ Confidentiality, keeping information secret from unauthorized access, is probably the most common aspect of information security: we need to protect confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Integrity

- ✓ Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of their account needs to be changed. Integrity means that changes should be done only by authorized users and through authorized mechanisms.

Availability

- ✓ The third component of information security is availability. The information created and stored by an organization needs to be available to authorized users and applications. Information is useless if it is not available. Information needs to be changed constantly, which means that it must be accessible to those authorized to access it. Unavailability of information is just as harmful to an organization as a lack of confidentiality or integrity. Imagine what would happen to a bank if the customers could not access their accounts for transactions.

5.4.2 Attacks

- ✓ The three goals of security—confidentiality, integrity and availability—can be threatened by security attacks. Figure relates the taxonomy of attack types to security goals.

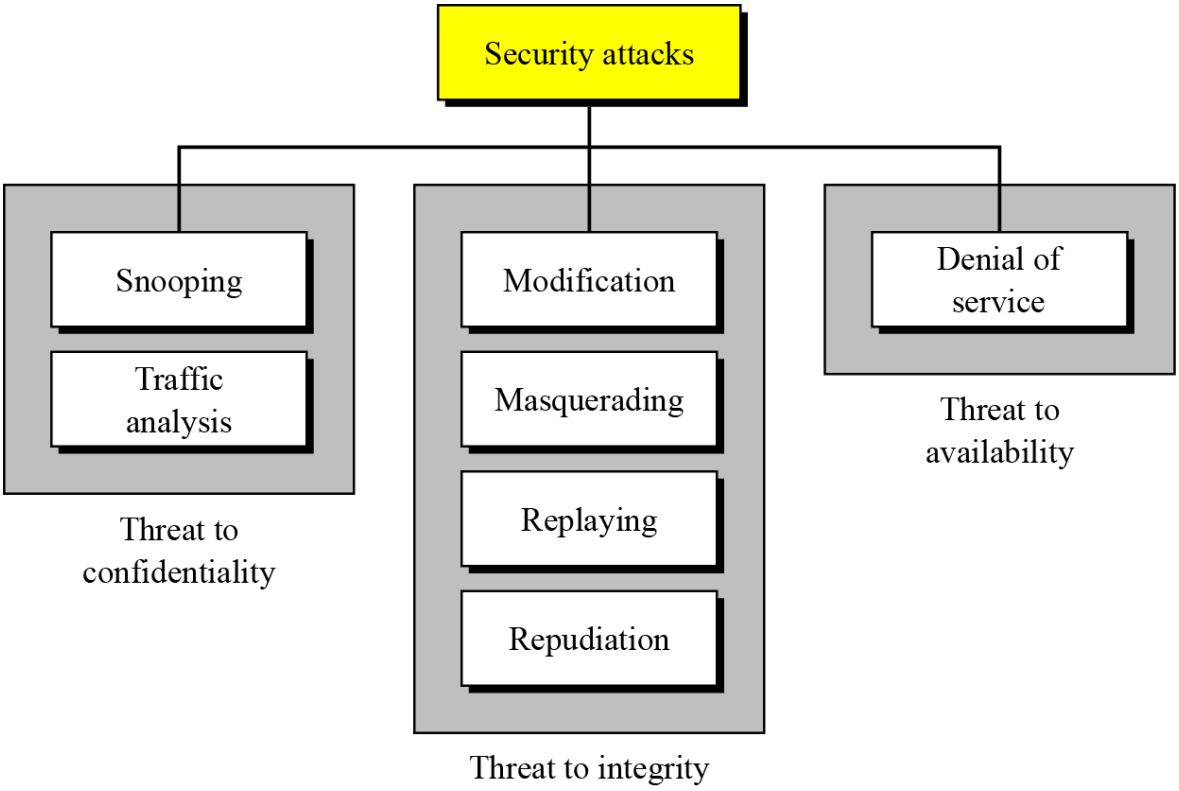


Figure 5.4.2.1 Taxonomy of attacks with relation to security goals

Attacks threatening confidentiality

- ✓ In general, two types of attack threaten the confidentiality of information: snooping and traffic analysis. Snooping refers to unauthorized access to or interception of data. Traffic analysis refers other types of information collected by an intruder by monitoring online traffic.

Attacks threatening integrity

- ✓ The integrity of data can be threatened by several kinds of attack: modification, masquerading, replaying and repudiation.

Attacks threatening availability

- ✓ Denial of service (DoS) attacks may slow down or totally interrupt the service of a system. The attacker can use several strategies to achieve this. They might make the system so busy that it collapses, or they might intercept messages sent in one direction and make the sending system believe that one of the parties involved in the communication or message has lost the message and that it should be resent.

5.4.3 Security services

- ✓ Standards have been defined for security services to achieve security goals and prevent security attacks. Figure 16.3 shows the taxonomy of the five common services.

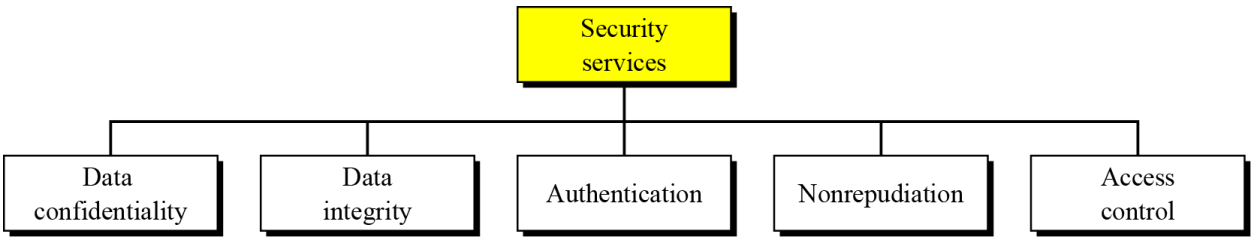


Figure 5.4.3.1 Security services

5.4.4 Techniques

- ✓ The actual implementation of security goals needs some help from mathematics. Two techniques are prevalent today: one is very general—*cryptography*—and one is specific—*steganography*.

Cryptography

- ✓ Some security services can be implemented using cryptography. Cryptography, a word with Greek origins, means "secret writing".

Steganography

- ✓ The word steganography, with its origin in Greek, means "covered writing", in contrast to cryptography, which means
- ✓ "secret writing".

5.4.5 Symmetric-Key Cryptography

- ✓ Figure 16.4 shows the general idea behind symmetric-key cryptography. Alice can send a message to Bob over an insecure channel with the assumption that an adversary, Eve, cannot understand the contents of the message by simply eavesdropping on the channel.
    - The original message from Alice to Bob is referred to as plaintext; the message that is sent through the channel is referred to as the ciphertext. Alice uses an encryption algorithm and a shared secret key. Bob uses a decryption algorithm and the same secret key.

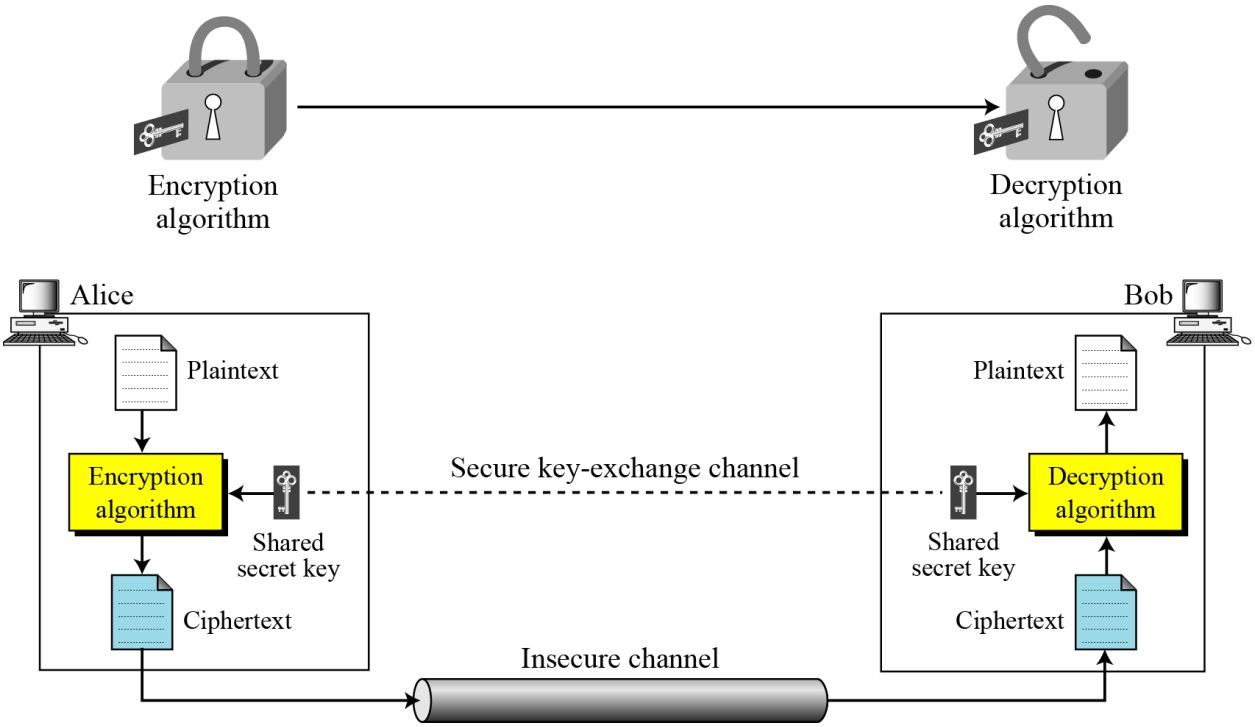


Figure 5.4.5.1 The general idea of symmetric-key cryptography

Traditional ciphers

- ✓ Traditional ciphers used two techniques for hiding information from an intruder: *substitution* and *transposition*.

Substitution ciphers

- ✓ A substitution cipher replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another.

Example 16.1

- ✓ Use the additive cipher with key = 15 to encrypt the message "hello".

Solution

- ✓ We apply the encryption algorithm to the plaintext, character by character:

Plaintext: h	→	Shift 15 characters down	→	Ciphertext: w
Plaintext: e	→	Shift 15 characters down	→	Ciphertext: t
Plaintext: l	→	Shift 15 characters down	→	Ciphertext: a
Plaintext: l	→	Shift 15 characters down	→	Ciphertext: a
Plaintext: o	→	Shift 15 characters down	→	Ciphertext: d

- ✓ The ciphertext is therefore "wtaad".

Transposition ciphers

- ✓ A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols. A symbol in the first position of the plaintext may appear in the tenth position of the ciphertext, while a symbol in the eighth position in the plaintext may appear in the first position of the ciphertext. In other words, a transposition cipher reorders (transposes) the symbols.

Example 16.2

- ✓ Alice needs to send the message "**Enemy attacks tonight**" to Bob. Alice and Bob have agreed to divide the text into groups of five characters and then permute the characters in each group. The following shows the grouping after adding a bogus character (z) at the end to make the last group the same size as the others.
- ✓

```
e n e m y   a t t a c   k s t o n   i g h t z
```

- ✓ The key used for encryption and decryption is a permutation key, which shows how the character are permuted. For this message, assume that Alice and Bob used the following key:

Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

- ✓ The third character in the plaintext block becomes the first character in the ciphertext block, the first character in the plaintext block becomes the second character in the ciphertext block and so on. The permutation yields:

e e m y n t a a c t t k o n s h i t z g

- ✓ Alice sends the ciphertext "eemyntaacttkonshitzg" to Bob. Bob divides the ciphertext into five-character groups and, using the key in the reverse order, finds the plaintext.

5.4.6 Modern symmetric-key ciphers

- ✓ Since traditional ciphers are no longer secure, modern symmetric-key ciphers have been developed during the last few decades. Modern ciphers normally use a combination of substitution, transposition and some other complex transformations to create a ciphertext from a plaintext. Modern ciphers are bit-oriented (instead of character-oriented). The plaintext, ciphertext and the key are strings of bits. In this section we briefly discuss two examples of modern symmetric-key ciphers: DES and AES. The coverage of these two ciphers is short: interested readers can consult the references at the end of the chapter for more details.

DES

- ✓ The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST) in 1977. DES has been the most widely used symmetric-key block cipher since its publication.

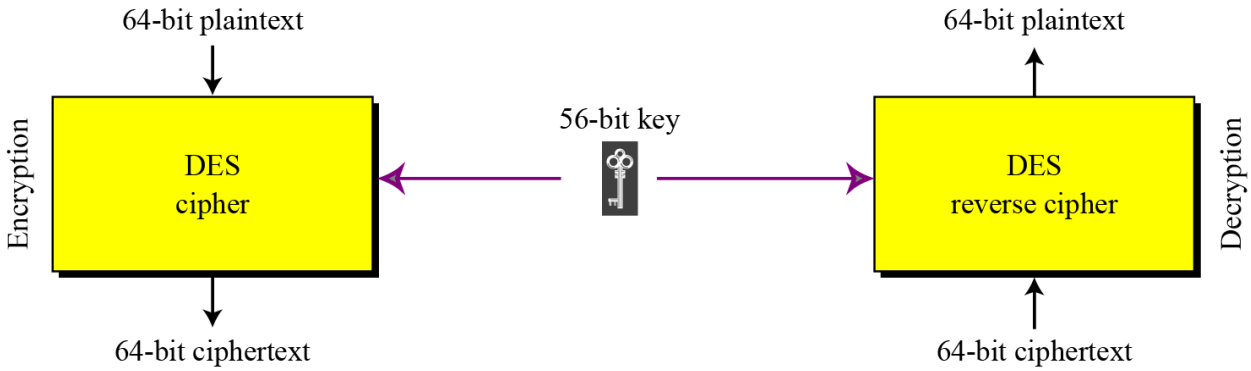


Figure 5.4.6.1 The general design of the DES encryption cipher

AES

- ✓ The Advanced Encryption Standard (AES) is a symmetric-key block cipher published by the US National Institute of Standards and Technology (NIST) in 2001 in response to the shortcoming of DES, for example its small key size. See Figure 16.6.

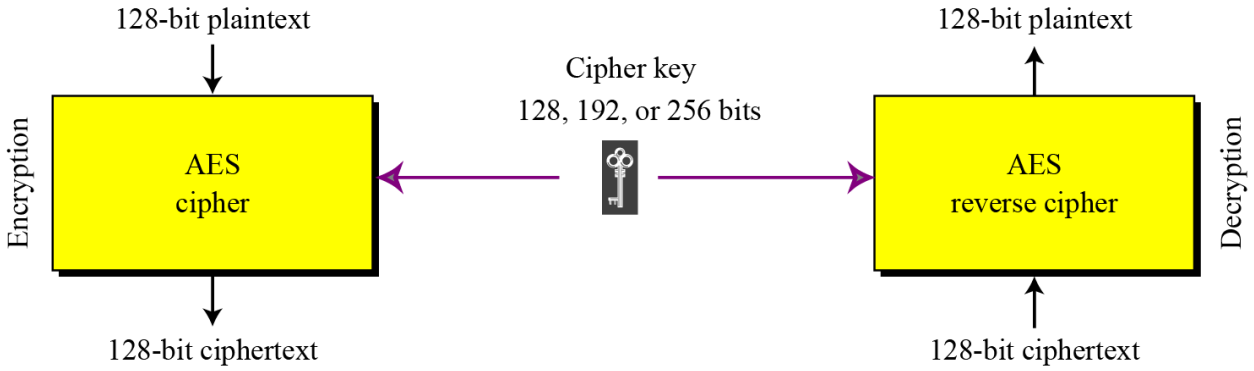


Figure 5.4.6.2 Encryption and decryption with AES

5.4.7 Asymmetric-Key Cryptography

- ✓ Figure shows the general idea of asymmetric-key cryptography as used for confidentiality. The figure shows that, unlike symmetric-key cryptography, there are distinctive keys in asymmetric-key cryptography: a private key and a public key. If encryption and decryption are thought of as locking and unlocking padlocks with keys, then the padlock that is locked with a public key can be unlocked only with the corresponding private key. Eve should not be able to advertise her public key to the community pretending that it is Bob's public key.

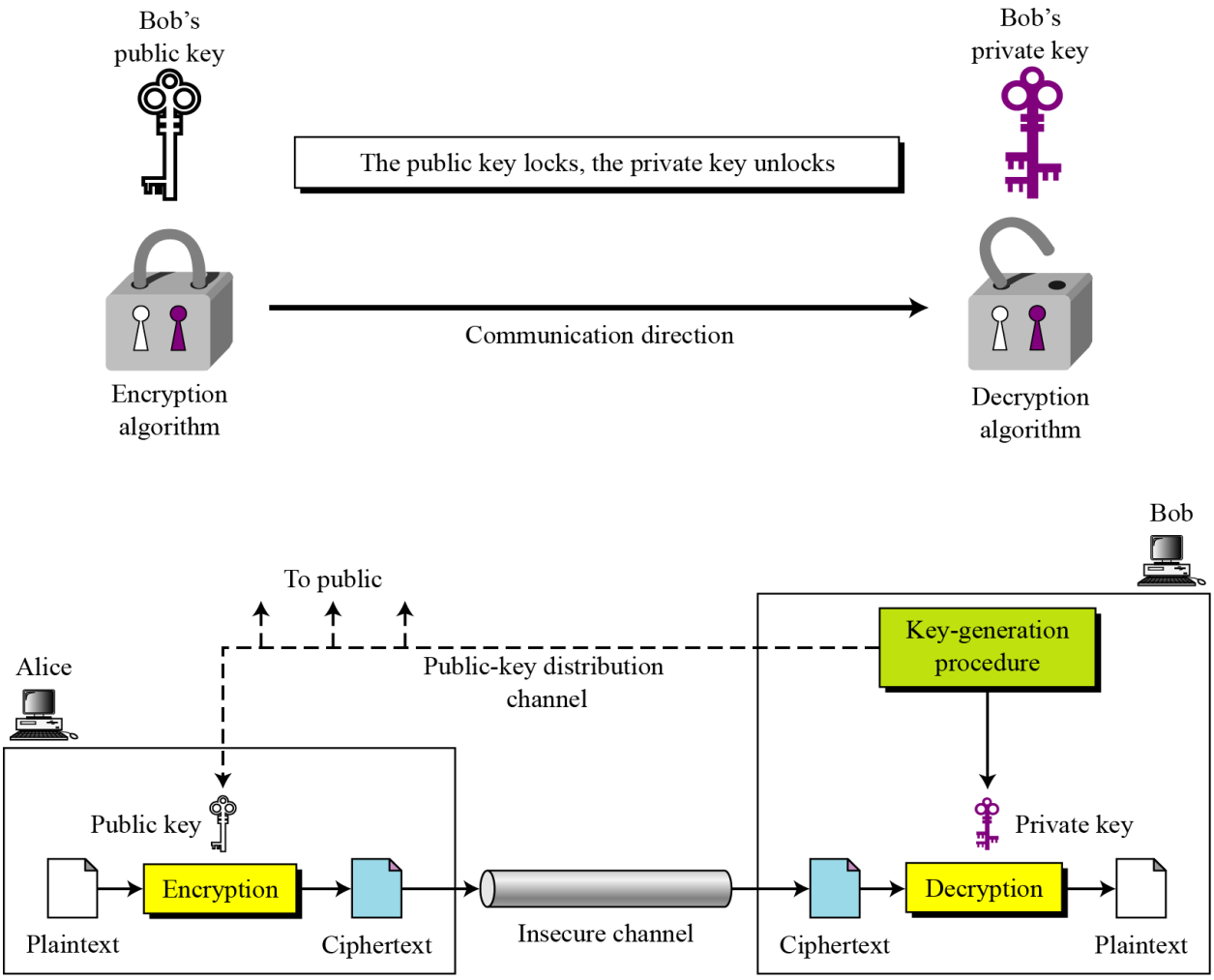


Figure 5.4.7.1 The general idea behind asymmetric-key cryptography

Example 16.3

- ✓ Bob chooses $p = 7$ and $q = 11$ and calculates $n = 7 \times 11 = 77$. Now he chooses two exponents, 13 and 37, using the complex process mentioned before. The public key is ($n = 77$ and $e = 13$) and the private key is ($d = 37$). Now imagine that Alice wants to send the plaintext 5 to Bob. The following shows the encryption and decryption.

Encryption at Alice's site

P:5 → $C = 5^{13} = 26 \bmod 77$

Decryption at Bob's site

C: 26 → $P = 26^{37} = 5 \bmod 77$

5.4.8 Asymmetric-Key Cryptography

- ✓ Both symmetric-key and asymmetric-key cryptography will continue to exist in parallel. We believe that they are complements of each other: the advantages of one can compensate for the disadvantages of the other.

The number of secrets

- ✓ The conceptual differences between the two systems are based on how these systems keep a secret. In symmetric-key cryptography, the secret token must be shared between two parties. In asymmetric-key cryptography, the token is unshared: each party creates its own token.
- ✓ **Symmetric-key cryptography is based on sharing secrecy;**
- ✓ **asymmetric-key cryptography is based on personal secrecy.**

A need for both systems

- ✓ There are other aspects of security besides confidentiality that need asymmetric-key cryptography. These include authentication and digital signatures (discussed later). Whereas symmetric-key cryptography is based on substitution and permutation of symbols, asymmetric-key cryptography is based on applying mathematical functions to numbers.
- ✓ **In symmetric-key cryptography, symbols are permuted or substituted:**
- ✓ **in asymmetric-key cryptography, numbers are manipulated.**

5.5 ACCESS CONTROL DEVICES

- ✓ Successful access control system includes number of components, depending on system's needs for authentication and authorization
- ✓ Strong authentication requires at least two forms of authentication to authenticate the supplicant's identity
- ✓ The technology to manage authentication based on what a supplicant knows is widely integrated into the networking and security software systems in use across the IT industry

Authentication

- ✓ Authentication is validation of a supplicant's identity
- ✓ Four general ways in which authentication is carried out:
  - What a supplicant knows
  - What a supplicant has
  - Who a supplicant is
  - What a supplicant produces

Authorization: Are you allowed to do that?

- Once you have access, what can you do?
- Enforces limits on actions

- ✓ Note: Access control often used as synonym for authorization

5.5.1 Authentication

How to authenticate a human to a machine?

- ✓ Can be based on…
  - Something you **know**
    - For example, a password
  - Something you **have**
    - For example, a smartcard
  - Something you **are**

- For example, your fingerprint

✓ Passwords

✓ Lots of things act as passwords!

- PIN
- Social security number
- Mother's maiden name
- Date of birth
- Name of your pet, etc.

Trouble with Passwords

✓ "Passwords are one of the biggest practical problems facing security engineers today."

✓ "Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. (They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed.)"

Why Passwords?

✓ Why is "something you know" more popular than "something you have" and "something you are"?

✓ **Cost**: passwords are free

✓ **Convenience**: easier for SA to reset pwd than to issue user a new thumb

Keys vs Passwords

Crypto keys

✓ Spse key is 64 bits

✓ Then 2^{64} keys

✓ Choose key at random

✓ Then attacker must try about 2^{63} keys

Passwords

- ✓ Spse passwords are 8 characters, and 256 different characters
- ✓ Then $256^8 = 2^{64}$ pwds
- ✓ Users do **not** select passwords at random
- ✓ Attacker has far less than 2^{63} pwds to try (**dictionary attack**)

Good and Bad Passwords

Bad passwords

- frank
- Fido
- password
- 4444
- Pikachu
- 102560

Good Passwords?

- jfIej,43j-EmmL+y
- 09864376537263
- P0kem0N
- FSa7Yago
- 0nceuP0nAt1m8

Password Experiment

- ✓ Three groups of users — each group advised to select passwords as follows
  - **Group A:** At least 6 chars, 1 non-letter
  - **Group B:** Password based on passphrase
  - **Group C:** 8 random characters
- ✓ Results

- **Group A:** About 30% of pwds easy to crack
- **Group B:** About 10% cracked
  - Passwords easy to remember
- **Group C:** About 10% cracked
  - Passwords hard to remember

✓ User compliance hard to achieve

✓ In each case, 1/3rd did not comply (and about 1/3rd of those easy to crack!)

✓ Assigned passwords sometimes best

✓ If passwords not assigned, best advice is

- Choose passwords based on passphrase
- Use pwd cracking tool to test for weak pwds
- Require periodic password changes?

Attacks on Passwords

✓ Attacker could…

- Target one particular account
- Target any account on system
- Target any account on any system
- Attempt denial of service (DoS) attack

✓ Common attack path

- Outsider → normal user → administrator
- May only require **one** weak password!

Password Retry

✓ Suppose system locks after 3 bad passwords. How long should it lock?

- 5 seconds
- 5 minutes

- Until SA restores service

✓ What are +'s and -'s of each?

Password File

✓ Bad idea to store passwords in a file

✓ But need a way to verify passwords

✓ Cryptographic solution: **hash** the passwords

- Store y = h(password)
- Can verify entered password by hashing
- If attacker obtains password file, he does not obtain passwords
- But attacker with password file can guess x and check whether y = h(x)
- If so, attacker has found password!

Dictionary Attack

✓ Attacker pre-computes h(x) for all x in a **dictionary** of common passwords

✓ Suppose attacker gets access to password file containing hashed passwords

- Attacker only needs to compare hashes to his pre-computed dictionary
- Same attack will work each time

✓ Can we prevent this attack? Or at least make attacker's job more difficult?

Password Cracking:Do the Math

✓ Assumptions

✓ Pwds are 8 chars, 128 choices per character

- Then $128^8 = 2^{56}$ possible passwords

✓ There is a **password file** with 2^{10} pwds

✓ Attacker has **dictionary** of 2^{20} common pwds

✓ Probability of 1/4 that a pwd is in dictionary

✓ **Work** is measured by number of hashes

Password Cracking

- ✓ Attack 1 password without dictionary
  - Must try $2^{56}/2 = 2^{55}$ on average
  - Just like exhaustive key search
- ✓ Attack 1 password with dictionary
  - Expected work is about
    - $1/4\ (2^{19}) + 3/4\ (2^{55}) = 2^{54.6}$
  - But in practice, try all in dictionary and quit if not found — work is at most 2^{20} and probability of success is 1/4
- ✓ Attack any of 1024 passwords in file
- ✓ **Without** dictionary
  - Assume all 2^{10} passwords are distinct
  - Need 2^{55} comparisons before expect to find password
  - If no salt, each hash computation gives 2^{10} comparisons $\Rightarrow$ the expected work (number of hashes) is $2^{55}/2^{10} = 2^{45}$
  - If salt is used, expected work is 2^{55} since each comparison requires a new hash computation
- ✓ Attack any of 1024 passwords in file
- ✓ **With** dictionary
  - Probability at least one password is in dictionary is $1 - (3/4)^{1024} = 1$
  - We ignore case where no pwd is in dictionary
  - If no salt, work is about $2^{19}/2^{10} = 2^9$
  - If salt, expected work is less than 2^{22}
  - Note: If no salt, we can precompute all dictionary hashes and amortize the work

Password cracking is too easy!

- One weak password may break security

- Users choose bad passwords
- Social engineering attacks, etc.

✓ The bad guy has all of the advantages

✓ All of the math favors bad guys

✓ Passwords are a **big** security problem

✓ Password Cracking Tools

✓ Popular password cracking tools

- Password Crackers
- Password Portal
- L0phtCrack and LC4 (Windows)
- John the Ripper (Unix)

✓ Admins should use these tools to test for weak passwords since attackers will!

✓ Good article on password cracking

- Passwords - Conerstone of Computer Security

5.5.1.1 Biometric

- **"You are your key"** — Schneier

✓ Examples

- Fingerprint
- Handwritten signature
- Facial recognition
- Speech recognition

- Gait (walking) recognition
- "Digital doggie" (odor recognition)
- Many more!

Why Biometrics?

- ✓ Biometrics seen as desirable replacement for passwords
- ✓ Cheap and reliable biometrics needed
- ✓ Today, a very active area of research
- ✓ Biometrics are used in security today
  - Thumbprint mouse
  - Palm print for secure entry
  - Fingerprint to unlock car door, etc.
- ✓ But biometrics not too popular
  - Has not lived up to its promise (yet)

Ideal Biometric

- ✓ **Universal** — applies to (almost) everyone
  - In reality, no biometric applies to everyone
- ✓ **Distinguishing** — distinguish with certainty
  - In reality, cannot hope for 100% certainty
- ✓ **Permanent** — physical characteristic being measured never changes
  - In reality, want it to remain valid for a long time
- ✓ **Collectable** — easy to collect required data
  - Depends on whether subjects are cooperative
- ✓ Safe, easy to use, etc., etc.

Biometric Modes

- ✓ **Identification** — Who goes there?

- Compare one to many
- Example: The FBI fingerprint database

✓ **Authentication** — Is that really you?

- Compare one to one
- Example: Thumbprint mouse

✓ Identification problem more difficult

- More "random" matches since more comparisons

✓ Fingerprint Comparison

✓ Examples of loops, whorls and arches

✓ Minutia extracted from these features

5.6 PHYSICAL SECURITY

5.6.1 Introduction

✓ Physical security addresses design, implementation, and maintenance of countermeasures that protect physical resources of an organization.

✓ Most controls can be circumvented if attacker gains physical access

✓ Physical security is as important as logical security

✓ Seven major sources of physical loss

- Extreme temperature
- Gases
- Liquids
- Living organisms
- Projectiles
- Movement

✓ Energy anomalies

✓ Community roles

- General management: responsible for facility security
- IT management and professionals: responsible for environmental and access security
- Information security management and professionals: perform risk assessments and implementation reviews

5.6.2 Physical Access Controls

- ✓ Secure facility: physical location engineered with controls designed to minimize risk of attacks from physical threats
- ✓ Secure facility can take advantage of natural terrain, traffic flow, and degree of urban development; can complement these with protection mechanisms (fences, gates, walls, guards, alarms)

5.6.2.1 Controls for Protecting the Secure Facility

- ✓ Walls, fencing, and gates
- ✓ Guards
- ✓ Dogs
- ✓ ID Cards and badges
- ✓ Locks and keys
- ✓ Mantraps
- ✓ Electronic monitoring
- ✓ Alarms and alarm systems
- ✓ Computer rooms and wiring closets
- ✓ Interior walls and doors

5.6.2.2 ID Cards and Badges

- ✓ Ties physical security with information access control
  - ID card is typically concealed
  - Name badge is visible
- ✓ Serve as simple form of biometrics (facial recognition)

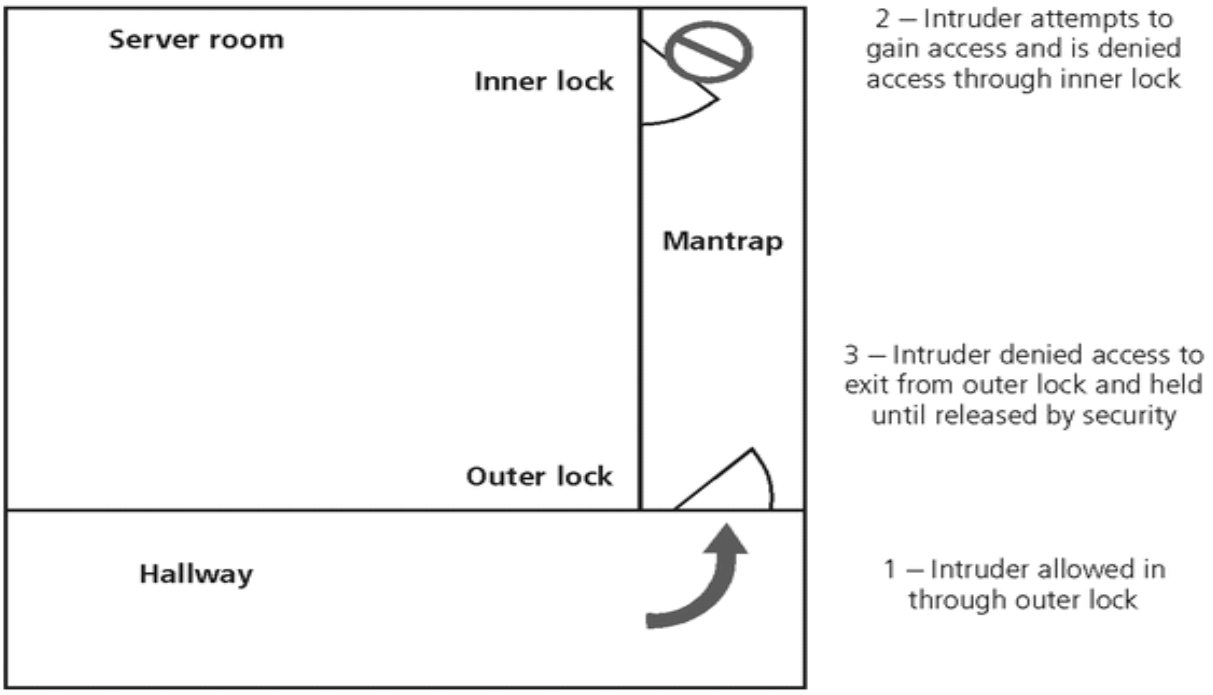
- ✓ Should not be only means of control as cards can be easily duplicated, stolen, and modified
- ✓ Tailgating occurs when unauthorized individual follows authorized user through the control

5.6.2.3 Locks and Keys

- ✓ Two types of locks: mechanical and electromechanical
- ✓ Locks can also be divided into four categories: manual, programmable, electronic, biometric
- ✓ Locks fail and alternative procedures for controlling access must be put in place
- ✓ Locks fail in one of two ways
    - Fail-safe lock
    - Fail-secure lock

5.6.2.4 Mantraps

- ✓ Small enclosure that has entry point and different exit point
- ✓ Individual enters mantrap, requests access, and if verified, is allowed to exit mantrap into facility
- ✓ Individual denied entry is not allowed to exit until security official overrides automatic locks of the enclosure



5.6.2.5 Electronic Monitoring

- ✓ Records events where other types of physical controls are impractical or incomplete
- ✓ May use cameras with video recorders; includes closed-circuit television (CCT) systems
- ✓ Drawbacks
  - Reactive; do not prevent access or prohibited activity
  - Recordings often not monitored in real time; must be reviewed to have any value
- ✓ Alarms and Alarm Systems
- ✓ Alarm systems notify when an event occurs
- ✓ Detect fire, intrusion, environmental disturbance, or an interruption in services
- ✓ Rely on sensors that detect event; e.g., motion detectors, smoke detectors, thermal detectors, glass breakage detectors, weight sensors, contact sensors, vibration sensors

5.6.2.6 Computer Rooms and Wiring Closets

- ✓ Require special attention to ensure confidentiality, integrity, and availability of information
- ✓ Logical controls easily defeated if attacker gains physical access to computing equipment

- ✓ Custodial staff often the least scrutinized persons who have access to offices; are given greatest degree of unsupervised access

5.6.2.7 Interior Walls and Doors

- ✓ Information asset security sometimes compromised by construction of facility walls and doors
- ✓ Facility walls typically either standard interior or firewall
- ✓ High-security areas must have firewall-grade walls to provide physical security from potential intruders and improve resistance to fires
- ✓ Doors allowing access to high security rooms should be evaluated
- ✓ Recommended that push or crash bars be installed on computer rooms and closets

5.6.2.8 Fire Security and Safety

- ✓ Most serious threat to safety of people who work in an organization is possibility of fire
- ✓ Fires account for more property damage, personal injury, and death than any other threat
- ✓ Imperative that physical security plans examine and implement strong measures to detect and respond to fires

5.6.2.9 Fire Detection and Response

- ✓ Fire suppression systems: devices installed and maintained to detect and respond to a fire
- ✓ Deny an environment of heat, fuel, or oxygen
    - Water and water mist systems
    - Carbon dioxide systems
    - Soda acid systems
    - Gas-based systems

5.6.2.10 Fire Detection

- ✓ Fire detection systems fall into two general categories: manual and automatic
- ✓ Part of a complete fire safety program includes individuals that monitor chaos of fire evacuation to prevent an attacker accessing offices
- ✓ There are three basic types of fire detection systems: thermal detection, smoke detection, flame detection

5.6.2.11 Fire Suppression

- ✓ Systems consist of portable, manual, or automatic apparatus
- ✓ Portable extinguishers are rated by the type of fire: Class A, Class B, Class C, Class D
- ✓ Installed systems apply suppressive agents; usually either sprinkler or gaseous systems

5.6.3 Power Management and Conditioning

- ✓ Electrical quantity (voltage level; amperage rating) is a concern, as is quality of power (cleanliness; proper installation)
- ✓ Noise that interferes with the normal 60 Hertz cycle can result in inaccurate time clocks or unreliable internal clocks inside CPU
- ✓ Grounding ensures that returning flow of current is properly discharged to ground
- ✓ Overloading a circuit causes problems with circuit tripping and can overload electrical cable, increasing risk of fire

5.6.4 Inventory Management

- ✓ Computing equipment should be inventoried and inspected on a regular basis
- ✓ Classified information should also be inventoried and managed
- ✓ Physical security of computing equipment, data storage media and classified documents varies for each organization

5.7 SECURITY AND PERSONNEL

5.7.1 Introduction

- ✓ When implementing information security, there are many human resource issues that must be addressed
    - Positioning and naming
    - Staffing
    - Evaluating impact of information security across every role in IT function
    - Integrating solid information security concepts into personnel practices
- ✓ Employees often feel threatened when organization is creating or enhancing overall information security program

5.7.2 Positioning and Staffing the Security Function

- ✓ The security function can be placed within:
  - IT function
  - Physical security function
  - Administrative services function
  - Insurance and risk management function
  - Legal department
- ✓ Organizations balance needs of enforcement with needs for education, training, awareness, and customer service

5.7.3 Staffing The Information Security Function

- ✓ Selecting personnel is based on many criteria, including supply and demand
- ✓ Many professionals enter security market by gaining skills, experience, and credentials
- ✓ At present, information security industry is in period of high demand

Qualifications and Requirements

- ✓ The following factors must be addressed:
  - Management should learn more about position requirements and qualifications
  - Upper management should learn about budgetary needs of information security function
  - IT and management must learn more about level of influence and prestige the information security function should be given to be effective
- ✓ Organizations typically look for technically qualified information security generalist
- ✓ Organizations look for information security professionals who understand:
  - How an organization operates at all levels
  - Information security usually a management problem, not a technical problem
  - Strong communications and writing skills
  - The role of policy in guiding security efforts

- ✓ Organizations look for (continued):
  - Most mainstream IT technologies
  - The terminology of IT and information security
  - Threats facing an organization and how they can become attacks
  - How to protect organization's assets from information security attacks
  - How business solutions can be applied to solve specific information security problems

Entry into the Information Security Profession

- ✓ Many information security professionals enter the field through one of two career paths:
  - Law enforcement and military
  - Technical, working on security applications and processes
- ✓ Today, students select and tailor degree programs to prepare for work in information security
- ✓ Organizations can foster greater professionalism by matching candidates to clearly defined expectations and position descriptions

Information Security Positions

- ✓ Use of standard job descriptions can increase degree of professionalism and improve the consistency of roles and responsibilities between organizations
- ✓ Charles Cresson Wood's book *Information Security Roles and Responsibilities Made Easy* offers set of model job descriptions
- ✓ Chief Information Security Officer (CISO or CSO)
  - Top information security position; frequently reports to Chief Information Officer
  - Manages the overall information security program
  - Drafts or approves information security policies
  - Works with the CIO on strategic plans
- ✓ Chief Information Security Officer (CISO or CSO) (continued)
  - Develops information security budgets

- Sets priorities for information security projects and technology
- Makes recruiting, hiring, and firing decisions or recommendations
- Acts as spokesperson for information security team
- Typical qualifications: accreditation; graduate degree; experience

✓ Security Manager

- Accountable for day-to-day operation of information security program
- Accomplish objectives as identified by CISO
- Typical qualifications: not uncommon to have accreditation; ability to draft middle and lower level policies, standards and guidelines; budgeting, project management, and hiring and firing; manage technicians

5.7.4 Employment Policies and Practices

✓ Management community of interest should integrate solid information security concepts into organization's employment policies and practices

✓ Organization should make information security a documented part of every employee's job description

✓ From information security perspective, hiring of employees is a responsibility laden with potential security pitfalls

✓ CISO and information security manager should provide human resources with information security input to personnel hiring guidelines

✓ Termination

✓ When employee leaves organization, there are a number of security-related issues

✓ Key is protection of all information to which employee had access

✓ Once cleared, the former employee should be escorted from premises

✓ Many organizations use an exit interview to remind former employee of contractual obligations and to obtain feedback

✓ Hostile departures include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting

- Before employee is aware, all logical and keycard access is terminated

- Employee collects all belongings and surrenders all keys, keycards, and other company property
- Employee is then escorted out of the building

✓ Friendly departures include resignation, retirement, promotion, or relocation

- Employee may be notified well in advance of departure date
- More difficult for security to maintain positive control over employee's access and information usage
- Employee access usually continues with new expiration date
- Employees come and go at will, collect their own belongings, and leave on their own

✓ Offices and information used by the employee must be inventoried; files stored or destroyed; and property returned to organizational stores

✓ Possible that employees foresee departure well in advance and begin collecting organizational information for their future employment

✓ Only by scrutinizing systems logs after employee has departed can organization determine if there has been a breach of policy or a loss of information

✓ If information has been copied or stolen, action should be declared an incident and the appropriate policy followed

6.1 GLOSSARY

Security

- ✓ **security** is defined as "the quality or state of being secure—to be free from danger."

Integrity

- ✓ **Integrity** means that data cannot be modified without authorization.

Components of an Information System

- ✓ Software
- ✓ Hardware
- ✓ Data
- ✓ People
- ✓ Procedures
- ✓ Networks

Subject of an attack

- ✓ Computer is used as an active tool to conduct the attack.

Object of an attack

- ✓ Computer itself is the entity being attacked

Direct attack

- ✓ When a Hacker uses his personal computer to break into a system.[Originate from the threat itself]

Indirect attack

- ✓ When a system is compromised and used to attack other system.

[Originate from a system or resource that itself has been attacked, and is malfunctioning or working under the control of a threat].

SDLC

- ✓ **SDLC** is a methodology for the design and implementation of an information system in an organization.

End users

- Work with the information to perform their daily jobs supporting the mission of the organization.

1. Data owners
2. Data custodians
3. Data users

Attack

- ✓ An attack is an intentional or unintentional attempt to cause damage to or otherwise compromise the information and /or the systems that support it.

Risk

- ✓ Risk is the probability that something can happen. In information security, it could be the probability of a threat to a system.

Security Blueprint

- ✓ It is the plan for the implementation of new security measures in the organization. Sometimes called a frame work, the blueprint presents an organized approach to the security planning process.

Security Model

- ✓ A security model is a collection of specific security rules that represents the implementation of a security policy.

Threats

- ✓ A threat is a category of objects, persons, or other entities that pose a potential danger to an asset. Threats are always present.

Threat agent

- ✓ A threat agent is the specific instance or component of a threat.

UNIT II

Intellectual Property

- ✓ It is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas.

Software Piracy

- ✓ Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as **software Piracy**.

Hackers

"People who use and create computer software to gain access to information illegally"

- ✓ **Expert Hackers**-> Masters of several programming languages, networking protocols, and operating systems .
- ✓ **Unskilled Hackers**

Virus

Segments of code that performs malicious actions.

- ✓ **Macro virus**-> Embedded in automatically executing macrocode common in word processors, spreadsheets and database applications.

- ✓ **Boot Virus**-> infects the key operating files located in the computer's boot sector.

Worms

- ✓ A worm is a malicious program that replicates itself constantly, without requiring another program to provide a safe environment for replication.

Worms

- ✓ A worm is a malicious program that replicates itself constantly, without requiring another program to provide a safe environment for replication.

Password Crack

- ✓ Attempting to reverse calculate a password is often called **cracking.**

Brute Force

- ✓ The application of computing & network resources to try every possible combination of options of a password is called a **Brute force attack.**

SPAM

- ✓ Spam is unsolicited commercial E-mail.
- ✓ It has been used to make malicious code attacks more effective.

Mail Bombing

- ✓ Another form of E-mail attack that is also a DOS called a **mail bomb**.
- ✓ **Sniffers**
- ✓ A **sniffer** is a program or device that can monitor data traveling over a network.

UNIT III

Risk Identification:

- ✓ It is the process of examining and documenting the security posture of an organization's information technology and the risk it faces.

Risk Assessment:

- ✓ It is the documentation of the results of risk identification.

Risk Control:

- ✓ It is the process of applying controls to reduce the risks to an organization's data and information systems.

Data Classification

4. Confidential
5. Internal
6. External

- ✓ **Confidential**: Access to information with this classification is strictly on a need-to-know basis or as required by the terms of a contract.
- ✓ **Internal**: Used for all internal information that does not meet the criteria for the confidential category and is to be viewed only by authorized contractors, and other third parties.
- ✓ **External:** All information that has been approved by management for public release.

Risk Determination

- ✓ Risk = [(Likelihood of vulnerability occurrence) X (Value of information Asset)] __ (% of risk mitigated by current controls) + uncertainty of current knowledge of the Vulnerability

Risk Control Strategies

Four basic strategies to control each of the risks that result from these vulnerabilities.

5. Apply safeguards that eliminate the remaining uncontrolled risks for the vulnerability [Avoidance]
6. Transfer the risk to other areas (or) to outside entities[transference]

7. Reduce the impact should the vulnerability be exploited[Mitigation]

8. Understand the consequences and accept the risk without control or mitigation[Acceptance]

Cost Avoidance

- ✓ It is the process of avoiding the financial impact of an incident by implementing a control.

Cost Benefit Analysis (CBA)

- ✓ Organizations are urged to begin the cost benefit analysis by evaluating the worth of the information assets to be protected and the loss in value if those information assets were compromised by the exploitation of a specific vulnerability.
- ✓ The formal process to document this decision making process is called a Cost Benefit analysis or an economic feasibility study.

Baselining

- ✓ Baselining is the analysis of measures against established standards,

Residual Risk

- ✓ When we have controlled any given vulnerability as much as we can, there is often risk that has not been completely removed or has not been completely shifted or planned for this remainder is called residual risk.

UNIT IV

Policy:

- ✓ course of action used by an organization to convey instructions from management to those who perform duties

Types of Policies

4. Enterprise information Security program Policy(EISP)

5. Issue-specific information Security Policy (ISSP)

6. Systems-specific information Security Policy (SysSP)

Defense in Depth

- ✓ One of the basic foundations of security architectures is the implementation of security in layers. This layered approach is called **defense in depth**.

Firewall

- ✓ A **firewall** is a device that selectively discriminates against information flowing into or out of the organization.

Cache servers

- ✓ For more frequently accessed Web pages, proxy servers can cache or temporarily store the page, and thus are sometimes called **cache servers.**

Contingency Planning (CP)

- ✓ Contingency Planning (CP) comprises a set of plans designed to ensure the effective reaction and recovery from an attack and the subsequent restoration to normal modes of business operations.

Incident response plan (IRP)

- ✓ It is the set of activities taken to plan for, detect, and correct the impact of an incident on information assets.

Business Continuity Plan (BCP)

- ✓ It prepares an organization to reestablish critical business operations during a disaster that affects operations at the primary site.

Disaster Recovery Plan (DRP)

- ✓ DRP provides detailed guidance in the event of a disaster and also provides details on the roles and responsibilities of the various individuals involved in the disaster recovery effort, and identifies the personnel and agencies that must be notified.

Redundancy

- ✓ Implementing multiple types of technology and thereby preventing the failure of one system from compromising the security of the information is referred to as **redundancy**.

UNIT V

Stateful firewall

- ✓ keeps track of the state of network connections (such as TCP streams) traveling across it.

- ✓ Stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection.

Stateless firewall

- ✓ Treats each network frame (Packet) in isolation. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.
- ✓ The classic example is the File Transfer Protocol, because by design it opens new connections to random ports.

Intrusion:

- ✓ Type of attack on information assets in which instigator attempts to gain entry into or disrupt system with harmful intent

Intrusion detection:

- ✓ Consists of procedures and systems created and operated to detect system intrusions

Intrusion reaction:

- ✓ Encompasses actions an organization undertakes when intrusion event is detected

Intrusion correction activities:

- ✓ Finalize restoration of operations to a normal state

Intrusion prevention:

- ✓ Consists of activities that seek to deter an intrusion from occurring

Signature-Based IDS

- ✓ Examine data traffic in search of patterns that match known signatures

Statistical Anomaly-Based IDS

- ✓ The statistical anomaly-based IDS (stat IDS) or behavior-based IDS sample network activity to compare to traffic that is known to be normal

Network-Based IDS (NIDS)

- ✓ Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks

Honey pots:

- ✓ Decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves

Honey nets:

- ✓ Collection of honey pots connecting several honey pot systems on a subnet

Mantraps

- ✓ Small enclosure that has entry point and different exit point

6.2 QUESTION BANK

UNIT I

TWO MARKS

1. Define Information Security.

It is a well-informed sense of assurance that the information risks and controls are in balance.

2. What is Security?

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

3. What are the multiple layers of Security?

- Physical Security
- Personal Security
- Operations Security
- Communication Security
- Network Security
- Information Security

4. What are the characteristics of CIA triangle?

- Confidentiality
- Integrity
- Availability

5. What are the characteristics of Information Security?

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

• Possession

6. What is E-mail Spoofing?

It is the process of sending an e-mail with a modified field.

7. What is UDP Packet Spoofing?

User Data Protocol (UDP) Packet Spoofing enables the attacker to get unauthorized access to data stored on computing systems.

8. What are the measures to protect the confidentiality of information?

• Information Classification

• Secure document storage

• Application of general Security Policies.

• Education of information end-users

9. What is Utility of information?

Utility of information is the quality or state of having value for some purpose or end.

10. What are the components of information system?

• Software

• Hardware

• Data

• People

• Procedures

• Networks.

11. What are the functions of Locks & Keys?

Locks & Keys are the traditional tools of physical security, which restricts access to, and interaction with the hardware components of an information system.

12. What is Network Security?

It is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

13. Differentiate Direct and Indirect attacks.

Direct Attack

1. It is when a hacker uses his personal computer to break into the system
2. Originate from the threat itself

Indirect Attack

1. It is when a system is compromised and used to attack other systems, such as in a distributed denial of service attack.
2. Originate from a system or resource that itself has attacked & it is malfunctioning or working under the control of a threat.

14. What is SDLC?

The Systems Development Life Cycle is a methodology for the design and implementation of an information system in an organization.

15. What is a methodology?

Methodology is a formal approach to solve a problem based on a structured sequence of procedures.

16. What are the phases of SDLC Waterfall method?

- ✓ Investigation
- ✓ Analysis
- ✓ Logical Design
- ✓ Physical Design
- ✓ Implementation
- ✓ Maintenance & change.

17. What is enterprise Information Security Policy?

This policy outlines the implementation of a security program within the organization.

18. What is Risk Management?

It is the process of identifying, assessing and evaluating the levels of risk facing the

organization.

19. What are the functions of Information Security?

- ✓ Protects the organization's ability to function
- ✓ Enables the safe operation of applications implemented on the organizations IT systems.
- ✓ Protects the data the organization collects and uses.
- ✓ Safeguards the technology assets in use at the organization.

20. What is PKI?

Public Key Infrastructure is an integrated system of software, encryption methodologies and legal agreements that can be used to support the entire information infrastructure of an organization.

21. What is the use of Digital Certificates?

Digital Certificates are used to ensure the confidentiality of Internet Communications and transactions.

22. What is Firewall?

Firewall is a device that keeps certain kinds of network traffic out of a private network.

23. What are caching network appliances?

Caching network appliances are devices that store legal copies of Internet contents such as WebPages that are frequently referred to by employees.

24. What are appliances?

Appliances display the cached pages to users rather than accessing pages from the server each time.

25 .What is Security? What are the security layers ,a successful organization should have?

Security-"The quality or state of being secure--to be free from danger"

To be protected from adversaries

- ✓ Physical Security – to protect physical items,objects or areas of organization from unauthorized access and misuse
- ✓ Personal Security – involves protection of individuals or group of individuals who are authorized to access the organization and its operations

- ✓ Operations security – focuses on the protection of the details of particular operations or series of activities.
- ✓ Communications security – encompasses the protection of organization's communications media ,technology and content
- ✓ Network security – is the protection of networking components,connections,and contents

Information security – is the protection of information and its critical elements, including the systems and hardware that use ,store, and transmit the information

PART B

1.Explain the Critical Characteristics of Information

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

2. Explain the Components of an Information System

- Software
- Hardware
- People
- Data
- Procedures
- Networks

3. Explain SDLC in detail.
    - Methodology
    - Phases
    - Phases
    - Investigation
    - Analysis
    - Logical Design
    - Physical Design
    - Implementation
    - Maintenance and change
4. Explain SecSDLC in detail
    - Investigation
    - Analysis
    - Logical Design
    - Physical Design
    - Implementation
    - Maintenance and change
5. Explain the functions of an Information security organization
    - Protects the organization’s ability to function
    - Enabling safe operation of applications
    - Protecting data that organizations collect and use
    - Safeguarding technology assets in organizations

UNIT II

1. What is a threat?

Threat is an object, person or other entity that represents a constant danger to an asset.

2. What are Hackers?

Hackers are people who use and create computer software for enjoyment or to gain access to information illegally.

3. What are the levels of hackers?

• Expert Hacker

Develops software codes

• Unskilled Hacker

Uses the codes developed by the experts

4. What are script kiddies?

These are hackers of limited skills who expertly written software to exploit a system but not fully understand or appreciate the systems they hack.

5. What is a Phreaker?

A Phreaker hacks the public telephone network to make free calls.

6. What is Malicious code?

These are programs, which are designed to damage, destroy, or deny service to the target system

7. What are the types of virus?

• Macro virus

• Boot virus

8. What are trojan horses?

They are software programs that hide their true nature and reveal their designed behavior only when activated.

9. What is a polymorphic threat?

It is one that changes its apparent shape over time.

10. What is intellectual propery?

It is the ownership of ideas and control over the tangible or virtual representation of those ideas. 35. What is an attack?

It is a deliberate act that exploits vulnerability.

11. What vulnerability?

It is an identified weakness of a controlled system with controls that are not present or no longer effective.

12. What are the attack replication vectors?

- Ip scan and attack
- Web browsing
- Virus
- Shares
- Mass mail
- SNMP

13. What is a brute force attack?

Trying every possible combination of options of password.

14. What are sniffers?

Sniffers are programs or device that can monitor data traveling over an network.

15. What is social engineering?

It is the process of using social skills to convince people to reveal access credentials to the attackers.

16. What are the types of Laws?

- Civil Law
- Criminal Law
- Tort Law

17. Differentiate Private & Public Laws.

Private Laws:

• This Law regulates the relationship between the individual and the organization.

• Eg: Family Law, Commercial Law, Labor Law Public Law:

• This Law regulates the structure and administration of government agencies and their relationship with the citizens, employees and other governments.

• Eg: Criminal Law, Administrative Law, Constitutional Law.

18. What are the fundamental principles of HIPAA.

1. Consumer control of medical information.

2. Boundaries on the use of medical information.

3. Accountability for the privacy of private information.

4. Security of health information.

19. What are the general categories of unethical and illegal behaviour?

• Ignorance

• Accident

• Intent

20. What is deterrence?

• It is the best method for preventing illegal or unethical activity.

• Examples are laws, Policies and technical controls.

21. What are the forces of Nature affecting information security?

Forces of Nature

- ✓ Forces of nature, force majeure, or acts of God are dangerous because they are unexpected and can occur with very little warning
- ✓ Can disrupt not only the lives of individuals, but also the storage, transmission, and use of information
- ✓ Include fire, flood, earthquake, and lightning as well as volcanic eruption and insect infestation

- ✓ Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations

22. What are technical hardware failures or errors?

Technical Hardware Failures or Errors

- ✓ Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing flaws
- ✓ These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability
- ✓ Some errors are terminal, in that they result in the unrecoverable loss of the equipment
- ✓ Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated

23.What are technical software failures or errors?

Technical Software Failures or Errors

- ✓ This category of threats comes from purchasing software with unrevealed faults
- ✓ Large quantities of computer code are written, debugged, published, and sold only to determine that not all bugs were resolved
- ✓ Sometimes, unique combinations of certain software and hardware reveal new bugs
- ✓ Sometimes, these items aren't errors, but are purposeful shortcuts left by programmers for honest or dishonest reasons

24. What is technological obsolescence?

Technological Obsolescence

- ✓ When the infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems
- ✓ Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity to threats and attacks
- ✓ Ideally, proper planning by management should prevent the risks from technology obsolesce, but when obsolescence is identified, management must take action

25.What is an attack?

Attacks

- ✓ An attack is the deliberate act that exploits vulnerability
- ✓ It is accomplished by a threat-agent to damage or steal an organization's information or physical asset
    - o An exploit is a technique to compromise a system
    - o A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective
    - o An attack is then the use of an exploit to achieve the compromise of a controlled system

26. What is a malicious code?

Malicious Code

- ✓ This kind of attack includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information
- ✓ The state of the art in attacking systems in 2002 is the multi-vector worm using up to six attack vectors to exploit a variety of vulnerabilities in commonly found information system devices

PART B

1. Explain the categories of Threat in detail.

- Acts of human error or failure
- Deviations in QOS by service providers
- Deliberate acts of espionage or trespass
- Deliberate acts of information extortion
- Deliberate acts of Sabotage or vandalism
- Deliberate acts of theft
- Deliberate software attacks
- Compromises to Intellectual Property
- Forces of Nature.

2. Explain the types of Attacks in detail?

- Malicious code
- Hoaxes
- Back Doors
- Password Crack
- Brute Force
- Dictionary

3. Explain General Computer Crime Laws.

- Computer Fraud & abuse Act 0f 1986
- USA Patriot Act of 2001
- Communications Decency Act
- Computer Security Act of 1987

4. Explain Ethical Concepts in Information Security.

- Cultural Differences in Ethical Concepts
- Software License Infringement
- Illicit use
- Misuse of corporate resources

UNIT III

1. What is Risk Management?

Risk Identification is conducted within the larger process of identifying and justifying risk control known as risk management.

2. What are the communities of interest?

- Information Security
- Management and users
- Information Technology

3. What are the responsibilities of the communities of interests?

- Evaluating the risk controls
- Determining which control options are cost effective for the organization
- Acquiring or installing the needed controls.
- Overseeing that the controls remain effective.

4. Write about MAC.

- It is also called as electronic serial number or hardware addresses.
- All network interface hardware devices have a unique number.
- The number is used by the network operating system as a mechanism to identify a specific network device.

5. What is Public key infrastructure certificate authority?

It is a software application that provides cryptographic key management services.

6. What is Clean desk policy?

This requires each employee to secure all information in its appropriate storage container at the end of each day.

7. What is risk assessment?

It is the process of assessing the relative risk for each of the vulnerabilities.

8. What is Likelihood?

Likelihood is the overall rating of the probability that a specific vulnerability within an organization will be successfully attacked.

9. What is Residual Risk?

It is the risk that remains to the information asset even after the existing control has been applied.

10. What are Policies?

Policies are documents that specify an organization's approach to security.

11.What are the types of security policies?

- General Security Policy

- Program Security Policy
- Issue-Specific Policies

12. What are the types of access controls?

- Mandatory Access Controls(MACs)
- Nondiscretionary controls
- Discretionary Controls(DAC)

13. What are the Risk Control Strategies?

- Avoidance – It is the risk control strategy that attempts to prevent the exploitation of the vulnerability.
- Transference – It is the control approach that attempts to shift the risk to other assets,other processes ,or other organizations.
- Mitigation – It is the control approach that attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.
- Acceptance. – It is the choice to do nothingto protect vulnerability and to accept the outcome of an exploited vulnerability.

14. What are the common methods for Risk Avoidance?

- Avoidance through Application of Policy
- Avoidance through Application of training and education
- Avoidance through Application of technology

15. What are the types of plans in Mitigation strategy?

- The Disaster Recovery Plan(DRP)
- Incident Response Plan(IRP)
- Business Continuity Plan(BCP)

16. What is a hot site?

- It is also known as business recovery site.
- It is a remote location with systems identical or similar to the home site.

17. What are the ways to categorize the controls?

- Control function
- Architectural Layer
- Strategy Layer
- Information Security Principle.

18. Differentiate Preventive and Detective controls.

Preventive Controls	Detective Controls
1. Stop attempts to exploit vulnerability by implementing a security principle, such as authentication or confidentiality	2. It warn organizations of violations of security principles, organizational policies or attempts to exploit vulnerability.
3. It uses the technical procedure such as encryption or combination of technical means and enforcement methods.	4. It use techniques such as audit trials, intrusion detection and configuration monitoring.

19.What is the goal of documenting results of the risk assessment?

- ✓ The goal of this process has been to identify the information assets of the organization that have specific vulnerabilities and create a list of them, ranked for focus on those most needing protection first
- ✓ In preparing this list we have collected and preserved factual information about the assets, the threats they face, and the vulnerabilities they experience
- ✓ We should also have collected some information about the controls that are already in place

20. What are risk control strategies?

- ✓ When risks from information security threats are creating a competitive disadvantage
  - o the information technology and information security communities of interest take control of the risks
- ✓ Four basic strategies are used to control the risks that result from vulnerabilities:
  - o Apply safeguards (avoidance)
  - o Transfer the risk (transference)

- Reduce the impact (mitigation)
- Inform themselves of all of the consequences and accept the risk without control or mitigation (acceptance)

PART B

1. Explain Risk Management in detail.
   - Know Yourself
   - Know Your Enemy
   - All Communities of Interest
2. Explain Risk Identification in detail • Asset Identification & Valuation
   - Automated Risk Management tools
   - Information Asset Classification
   - Information Asset Valuation
   - Listing Assets in order of importance
   - Data Classification & Management
   - Threat Identification
3. Explain Risk assessment in detail.
   - Introduction
   - Likelihood
   - Valuation of Information Assets
   - Percentage of Risk Mitigated by Controls
   - Access Controls
4. Explain Risk Control strategies in detail
   - Avoidance
   - Mitigation
   - Acceptance
   - Transference

5. Explain Risk Mitigation strategy Selection

- Evaluation, Assessment and Maintenance of Risk controls
- Categories of controls
- Architectural Layer
- Strategy Layer

UNIT IV

1. What are the commonly accepted information security Principles?

- confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Accountability
- Privacy.

2. What is benefit?

It is the value that the organization recognizes by using controls to prevent loses associated with a specific vulnerability.

3. What is asset valuation?

It is the process of assigning financial value or worth to each information asset.

4. What is a Policy?

It is a plan or course of action, as of a government, political party, intended to influence and determine decisions, actions and other matters.

5. Differentiate mission & Vision.

Mission: Mission of an organization is a written statement of an organization's purpose.

Vision: Vision of an organization is a written statement of an organization's goals.

6. What is Strategic Planning?

It is the process of moving the organization towards its vision by accomplishing its mission.

7. What are the general groups of System-Specific Policy?

- Access Control Lists
- Configuration Rules.

8. What is a Capability table?

- It is a list associated with users and groups
- Specifies which subjects and objects a user or group can access.
- These are frequently complex matrices rather than simple lists or tables.

9. What is "Agreed Upon Procedures"?

It is a document that outlines the policies and technologies necessary to security systems that carry the sensitive cardholder information to and from from VISA systems.

10. What is redundancy?

Implementing multiple types of technology and thereby preventing failure of one system from compromising the security of the information is referred to as redundancy.

11. What is a Firewall?

It is a device that selectively discriminates against information flowing into or out of the organization.

12 . What is Firewall Subnet?

It consists of multiple firewalls creating a buffer between the outside and inside networks.

13. What is DMZs?

- A buffer against outside attack is referred to as Demilitarized Zone.
- It is a no-man's-land between the inside and outside networks where some organizations place Web Servers.
- The servers provide access to organizational Web pages without allowing Web requests to enter the interior networks.

14. What are the 2 versions of IDS? • Hot-based IDS

• Network-based IDS

15. What is Contingency Planning?

It is the entire planning conducted by the organization to prepare for, react to, and recover from events that threaten the security of information and information assets in the organization.

16. Who are the members of the contingency team?

• Champion

• Project Manager

• Team Members.

17. What are the stages in the Business Impact Analysis Step>?

• Threat attack identification

• Business unit analysis

• Attack success scenarios

• Potential damage assessment

• Subordinate plan classification

18. What is an attack profile?

It is a detailed description of activities that occur during an attack.

19. What is an incident?

It is any clearly identified attack on the organization's information assets that would threaten the asset's confidentiality, integrity, or availability.

20. What are the phases of Incident Response?

• Planning

• Detection

• Reaction

• Recovery.

21. What are the 5 testing strategies of Incident Planning?

- Checklist
- Structured walk-through
- Simulation
- Parallel
- Full interruption

22. What is an alert roster?

It is a document containing contact information for individuals to be notified in the event of an incident.

23. What are the 2 ways to activate an alert roster?

- Sequential roster – It is activated as a contact person calls each person on the roster.
- Hierarchical roster – It is activated as the first person calls a few other people on the roster, who in turn call a few people.

24. What is computer forensics?

It is the process of collecting, analyzing and preserving computer related evidence.

25. What are Honey pots?

These are computer servers configured to reassemble production systems, containing rich information just begging to be hacked.

26. What is enticement?

It is the process of attracting attention to a system by placing tantalizing bits of information in key locations.

27. What is entrapment?

It is the action of luring an individual into committing a crime to get a conviction.

28. What is Mutual agreement?

It is a contract between two or more organization's that specifies how each to assist the other in the event of a disaster.

PART B

1. Explain the types of Policies in detail.
    - General security Policy
    - Issue-Specific Policy
    - System-specific Policy
2. Explain NIST Security Models in detail.
    - NIST Special Publication SP 800-12
    - NIST Special Publication SP 800-14
    - NIST Special Publication SP 800-18
3. Explain VISA International Security Model in detail.
    - Baselining and best Business Practises
4. Explain the design of Security Architecture in detail.
    - Defense in Depth
    - Security Perimeter
    - Key Technology Components
5. Explain the Major Steps in Contingency Planning.
    - Business Impact Analysis
    - Incident Response Planning
    - Disaster Recovery Planning
    - Business Continuity Planning.
6. Explain Information Security Policy, Standards and Practices in detail.
    - Definitions
    - Security Program Policy(SPP)
    - Issue-Specific Security Policy(ISSP)
    - Systems-Specific Policy(SysSP)

- ACL Policies
- Policy Management

UNIT V

1. What is intrusion?

An intrusion is a type of attack on information assets in which the instigator attempts to gain entry into a system or disrupt the normal operations of a system with, almost always, the intent to do malicious harm.

2. What is IDS?

IDS stands for Intrusion Detection Systems. It works like a burglar alarm in that it detects a violation of its configuration and activates and alarm. This alarm can be audible and/or visual or it can be silent.

3. What is Signature based IDSs?

Signature based IDSs, also known as knowledge based IDSs, examine data traffic for patterns that match signatures, which are pre-configured, predetermined attack patterns.

4. What are Honey pots?

Honey pots are decoy systems, which means they are designed to lure potential attackers away from critical systems.

In the security industry, these systems are also known as decoys, lures, or flytraps.

5. What is the use of Scanning and analysis tools?

Scanning and analysis tools are used to pinpoint vulnerabilities in systems, holes in security components, and unsecured aspects of the network. Although these tools are used by attackers, they can also be used by an administrator not only to learn more about his/her own system but also identify and repair system weaknesses before they result in losses.

6. What are the factors of authentication?

- What a supplicant knows
- What a supplicant has
- Who a supplicant is

• What a supplicant produces

7. What is Hash function?

Hash functions are mathematical algorithms that generate a message summary or digest that can be used to confirm the identity of a specific message and to confirm that the message has not been altered.

8. What is PKI?

PKI – Public Key Infrastructure

It is an integrated system of software, encryption methodologies, protocols, legal agreements and third party services that enables users to communicate securely. It includes digital certificates and certificate authorities.

9. What is Steganography?

Steganography is the process of hiding information, and while it is not properly a form of cryptography, it is related to cryptography in that both are ways of transmitting information without allowing it to be revealed in transit.

10. What are the protocols used in Secure Internet Communication?

• S-HTTP(Secure Hypertext Transfer Protocol)

• SSL(Secure Socket Layer)

• SSL Record Protocol

• Standard HTTP

11. What is Physical security?

Physical security addresses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization. This means the physical protection of the people, the hardware, and the supporting system elements and resources associated with the control of information in all its states: transmission, storage and processing.

12. What are the controls of protecting the Secure Facility?

• Walls, Fencing, Gates

• Guards

• Dogs

• ID Cards and Badges

- Locks and keys
- Mantraps
- Electronic Monitoring
- Alarms and Alarm Systems
- Computer Rooms and Wiring Closets
- Interior Walls and Doors

13. What are the basic types of Fire Detection Systems?

- Thermal Detection
- Smoke Detection
- Flame Detection

14. What is TEMPEST?

TEMPEST is a technology that prevents the loss of data that may result from the emissions of electromagnetic radiation.

15. What is UPS? What are the types of UPS?

UPS- Uninterruptible Power Supply

It is a electrical device that serves as a battery backup to detect the interruption of power to the power equipment.

The basic configurations are,

- Standby or offline UPS
- Ferroresonant Standby UPS
- Line-interactive UPS
- True online UPS

16. What are the relevant terms for electrical power influence?

- Fault: Momentary Interruption in power
- Blackout: Prolonged Interruption in power
- Sag: Momentary drop in power voltage levels

• Brown out: Prolonged drop in power voltage levels

• Spike: Momentary increase in power voltage levels

• Surge: Prolonged increase in power voltage levels

17. What is fail-safe lock?

It is usually used on an exit, where it is essential for human safety in the event of a fire. It is used when human safety is not a factor.

18. What are the conditions controlled by HVAC Systems? • Temperature

• Filtration

• Humidity

• Static Electricity.

19.How firewalls are categorized by processing mode?

The five processing modes are

1) Packet filtering
2) Application gateways
3) Circuit gateways
4) MAC layer firewalls
5) Hybrids

20. What are the factors to be considered while selecting a right firewall?

Selecting the Right Firewall

- ✓ What type of firewall technology offers the right balance of protection features and cost for the needs of the organization?
- ✓ What features are included in the base price? What features are available at extra cost? Are all cost factors known?
- ✓ How easy is it to set up and configure the firewall? How accessible are staff technicians with the mastery to do it well?
- ✓ Can the candidate firewall adapt to the growing network in the target organization?

21. What are Sock Servers?

SOCKS Servers

- ✓ The SOCKS system is a proprietary circuit-level proxy server that places special SOCKS client-side agents on each workstation
- ✓ Places the filtering requirements on the individual workstation, rather than on a single point of defense (and thus point of failure)
- ✓ This frees the entry router of filtering responsibilities, but then requires each workstation to be managed as a firewall detection and protection device
- ✓ A SOCKS system can require additional support and management resources to configure and manage possibly hundreds of individual clients, versus a single device or set of devices

22. What are the recommended practices in designing firewalls?

Firewall Recommended Practices

- ✓ All traffic from the trusted network is allowed out
- ✓ The firewall device is always inaccessible directly from the public network
- ✓ Allow Simple Mail Transport Protocol (SMTP) data to pass through your firewall, but insure it is all routed to a well-configured SMTP gateway to filter and route messaging traffic securely
- ✓ All Internet Control Message Protocol (ICMP) data should be denied
- ✓ Block telnet (terminal emulation) access to all internal servers from the public networks
- ✓ When Web services are offered outside the firewall, deny HTTP traffic from reaching your internal networks by using some form of proxy access or DMZ architecture

23. What are intrusion detection systems(IDS)?

Intrusion Detection Systems (IDSs)

- ✓ IDSs work like burglar alarms
- ✓ IDSs require complex configurations to provide the level of detection and response desired
- ✓ An IDS operates as either network-based, when the technology is focused on protecting network information assets, or host-based, when the technology is focused on protecting server or host information assets
- ✓ IDSs use one of two detection methods, signature-based or statistical anomaly-based

PART B

1. Explain protocols for Secure communication in detail.
    - S-HTTP & SSL
    - Secure/Multipurpose Internet Mail Extension(S/MIME)
    - Internet Protocol Security(IPSec)
2. Explain Staffing the security in detail.
    - Qualifications and Requirements
    - Entry into the Security Profession
    - Information Security Positions
3. Explain the fire safety in Physical security.
    - Fire Detection & Response
    - Fire Detection
    - Fire Suppression
    - Gaseous Emission Systems
4. Explain the Cryptographic algorithms in detail.
    - Data Encryption Standards(DES)
    - Public Key Infrastructure(PKI)
    - Digital Signatures
    - Pretty Good Privacy(PGP)
5. Explain IDS in detail
    - Host-based Ids
    - Network-based IDS
    - Signature-based IDS
    - Statistical Anomaly-based IDS

6. Explain the type of encryption/decryption method.

Conventional Methods:

• Character-Level Encryption: Substitutional & Transpositional

• Bit-Level Encryption: Encoding/Decoding, Permutation, Substitution, Product, Exclusive-Or & Rotation

Public key Methods

7. Explain about RSA algorithm.

• Public key Encryption technique.

• Encryption algorithm

• Decryption algorithm

• Security in RSA

8.Explain about secret key encryption algorithm.

• Data Encryption Standard

• Algorithm

• Sub key generation

9. Explain Scanning and Analysis Tools in detail

• Footprinting

• Fingerprinting

• Port Scanners

• Vulnerability Scanners

• Packet Sniffers

• Content Filters

10. Explain Firewalls in detail.

• Development of Firewalls(5 generations)

• Firewall Architecture

• Packet Filtering Routers

- Screened Host Firewall Systems
- Dual-homed Host Firewalls
- Screened Subnet Firewalls(with DMZ)
- SOCKS Server
- Configuring and Managing Firewalls

Reg. No. : | | | | | | | | | | | | |

Question Paper Code : 52169

B.E./B.Tech. DEGREE EXAMINATION, MAY/JUNE 2014.

Seventh Semester

Information Technology

IT 2042/IT 706/10177 ITE 33 — INFORMATION SECURITY

(Regulation 2008)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. If the C.I.A triangle is incomplete, why is it so commonly used in security?

2. What does it mean to discover an exploit? How does an exploit differ from vulnerability?

3. Why is information security a management problem? What can management do that technology cannot?

4. What is intellectual property (IP)? Is it offered the same protection in every country of the world?

5. Why do networking components need more examination from an information security perspective than from a systems development perspective?

6. How does a disaster recovery plan different from a business continuity plan?

7. What resources are available on the Web to assist an organization in developing best practices as part of a security framework?

8. What is an after-action review? When is it performed? Why is it done?

9. What is the difference between digital signatures and digital certificates?

10. How do the security considerations for temporary or contract employees differ from those of the regular full-time employee?

PART B — (5 × 16 = 80 marks)

11. (a) (i) List and explain the critical characteristics of information system. (8)

(ii) How is the top-down approach to information security superior to the bottom-up approach? Explain. (8)

Or

(b) Sketch and explain the various components of Systems Development Life Cycle (SDLC) waterfall methodology.

12. (a) How does a threat to information security differ from an attack? Explain the give groups of threats to information security.

Or

(b) Briefly explain about any four information security professional organizations with their role and motivation.

13. (a) Explain the process of risk assessment and documenting the results of risk assessment.

Or

(b) (i) What is cost benefit analysis (CBA)? Explain with suitable formula. (8)

(ii) What is benchmarking? Explain the metrics-based measures used by the organizations to compare practices. (8)

14. (a) Briefly explain the Issue Specific Security Policy and VISA International Security model.

Or

(b) Explain the process of Business Impact Analysis and Incident Response Planning with an real time example.

15. (a) How does a screened host architecture for firewalls differ from a screened subnet firewall architecture? Which offers more security for the information assets that remain on the trusted network? Explain with neat sketch.

Or

(b) Explain the working model of single round DES encryption algorithm with neat sketch. Also compare DES and 3DES.

———————

B.E/B.Tech DEGREE EXAMINATION,NOVEMBER/DECEMBER 2007
Seventh Semester
Computer Science and Engineering
CS1014- INFORMATION SECURITY
(Regulation 2004)

Time :Three hours **Maximum:100 Marks**.

Answer ALL questions
PART A-(10*2=20)

1. State the critical Characteristics of information.

2. List the components used in security models.

3. Name the counter measure on threats.

4. Differentiate between threats and attacks.

5. Mention the benefits of risk management.

6. State the roles involved in risk management.

7. Name the people affected in security policies.

8. State the pros of VISA international security model.

9. List any two IDS. Mention its category of classification.

10. What are the basic functions of access control devices?

PART B-
(5*16=80)

11 (a) Discuss in detail the NSTISSC security model. (16) Or
(b) What is SDLC? Illustrate the security of SDLC. (16)

12 (a) Explain in detail the different types of cryptanalytic attacks. (16) Or
(b) Discuss in detail the Legal, Ethical and Professional issues during the security investigation. (16)

13 (a) What is risk management? State the methods of identifying and assessing risk management. (16) Or
(b) Discuss in detail the process of assessing and controlling risk management issues.

14 (a) (i) Compare and contrast the ISO 17700 with BS 7799 NIST security models. (10)
(ii) Briefly explain the NIST security model. (6) Or

(b) List the styles of architecture security models. Discuss them in detail. (16)

15 (a) (i) What is intrusion detection system? Explain its types in detail. (10)
(ii) Write short notes on scanning and analysis tools used during the security design. (6)
Or
(b) (i) What is cryptography? Discuss the authentication models used in cryptography. (10)
(ii) Write short notes on the control devices used in security design. (6)

B.E/B.Tech DEGREE EXAMINATION,NOVEMBER/DECEMBER 2008
Seventh emester
Computer Science and Engineering
CS 1014- INFORMATION SECURITY
(Regulation 2004)

Time :Three hours **Maximum:100 Marks.**

Answer ALL questions

PART A (10 x 2 =20 marks)

1. Mention the components of Information security.

2.How is the top-down approach to information Security superior to the bottom-up approach?

3.What are the types of password attacks?

4. What is the difference between Criminal law and Civil law?

5.Why do networking components need more examination from an Information Security perspective than from a Systems development perspective?

6.What is a cost-benefit analysis?

7.What is a policy? How does it different from a law?

8.When do we call attacks as incidents?

9.Differentiate Symmetric encryption and Asymmetric encryption.

10. What is a honey pot?

PART B (5 x 16 = 80)

11. (a) (i) How has Computer Security evolved into modern Information security? Explain. (8)
(ii) Why is a methodology important in the implementation of Information Security? How does a methodology improve the process? Explain. (8)(or)

(b) What are the phases in the Security Systems development life cycle? Explain in detail.

12. (a) (i) Describe the three general categories of unethical and illegal behaviour. (8)
(ii) What can be done to deter someone from committing a crime? Explain. (8)(or)

(b)(i) What is a buffer overflow? How is it used against a web server? Explain. (12) (ii) How do worms differ from viruses? (4)

13.(a) Describe Risk mitigation. Explain the planning approaches to mitigate risks. (16)
(or)

(b) Define risk management, risk identification and risk control. Illustrate it with a real time application. (16)

14. (a) Classify each of the following occurrences as an incident or disaster. If an occurrence is a disaster, determine whether business continuity plans would be called into play.
(i) A hacker gets into the network and deletes files from a server.

(ii) A fire breaks out in the storeroom and sets off sprinklers on that floor. Some computers a are damaged, but the fire is controlled.
(iii) Employees go on strike, and the company could be without critical workers for weeks.
(iv) A disgruntled employee takes a critical server home, sneaking it out after hours.
For each of the scenarios above, describe the steps necessary to restore operations. Indicate whether law enforcement would be involved. (4+4+4+4) (or)
(b) What is Contingency planning? Describe its components. How is it different from routine management planning? Explain. (16).

15. (a) (i) How do the security considerations for temporary or contract employees differ from those of regular full-time employees? Explain. (8)

(ii) What is Collusion? How does the separation of duties influence collusion? Explain. (8)
(or)

(b) Describe the categories and operating models of Intrusion Detection Systems (IDS) in detail. (16)

B.E./B.Tech. DEGREE EXAMINATION, NOVEMBER/DECEMBER 2011.

Seventh Semester

Information Technology

IT 2042 — INFORMATION SECURITY

(Regulation 2008)

Time : Three hours Maximum : 100 marks

Answer ALL questions.

PART A — (10 × 2 = 20 marks)

1. What is information security?
2. Why is a methodology important in implementing the information security?
3. Why is information security a management problem?
4. Distinguish between DoS and DDoS.
5. What is risk management?
6. What is the difference between benchmark and baseline?
7. What is information security policy?
8. What are the inherent problems with ISO 17799?
9. Distinguish between symmetric and asymmetric encryption.
10. What are the credentials of information security professionals?

PART B — (5 × 16 = 80 marks)

11. (a) (i) Describe the critical characteristics of information. How are they used in the study of computer security? (8)

(ii) Explain the security system development life cycle in detail. (8)

Or

(b) (i) Explain the NSTISSC security model and the top-down approach to security implementation. (8)

(ii) Briefly explain the components of an information system and their security. (8)

12. (a) (i) Explain the various groups of threats faced by an organization. (8)

(ii) Discuss the ethical concepts in information security and the prevention to illegal and unethical behavior. (8)

Or

(b) (i) Explain the four important functions of information security in an organization. (8)

(ii) Describe the attack replication vectors and the major types of attacks. (8)

13. (a) (i) Describe the process of risk identification in detail. (8)

(ii) Discuss the risk control strategies that guide an organization. (8)

Or

(b) (i) Discuss the risk assessment and the documentation of its results. (8)

(ii) Explain the various feasibility studies considered for a project of information security controls and safeguards. (8)

14. (a) (i) Explain the different types of information security policies. (8)

(ii) Discuss the features of VISA international security model. (8)

Or

(b) (i) Explain the NIST Security model in detail. (8)

(ii) Explain the various components used in designing the security architecture. (8)

15. (a) (i) Discuss the different types of intrusion detection systems. (8)

(ii) Describe the access controls used for providing physical security. (8)

Or

(b) (i) Write notes on scanning and analysis tools used during design. (8)

(ii) Discuss the cryptographic tools used for providing the security. (8)