UNIVERSITY OF GONDAR

COLLEGE OF INFORMATICS

DEPARTMENT OF INFORMATION SYSTEMS

INTRODUCTION TO INFORMATION SECURITY

Chapter One
Introduction to Information Security What is Security?

- **Security** is the quality or state of being secure to be free from danger
- **Physical security :** Product the Physical item, object or areas from unauthorized access and misuse
- **Operations security** : Protection of the details of particular operation or activities
- **Communications security** : Protection of organizations communication media, technology and content
- **Network security:** Protection of Networking Components, connections and contents
- **Information security:** Protection of Information and its Critical elements

What is Information Security?

- Information security: a "well-informed sense of assurance that the information risks and controls are in balance."
- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Necessary tools: policy, awareness, training, education, technology
- The NSTISSC (National Security Telecommunications and Information Systems Security Committee) model of information security is known as the **C.I.A. triangle (C**onfidentiality, Integrity, and Availability) – these are characteristics that describe the utility/value of information

C.I.A. triangle now expanded into list of critical characteristics of information

- **Confidentiality, integrity and availability**, also known as the **CIA triad**, is a model designed to guide policies for information security within an organization.
- The model is also sometimes referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the Central Intelligence Agency.

Critical concepts of Information Security

The value of information comes from the characteristics it possesses:

- **Confidentiality**
- **Authentication**
- **Integrity**
- **Non repudiation**
- **Access control**
- **Availability**

- **Confidentiality:** Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties.
- **Authentication:** Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
- **Integrity:** Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
- **Non repudiation:** Requires that neither the sender nor the receiver of a message be able to deny the transmission.
- **Access control:** Requires that access to information resources may be controlled by the target system.

- **Availability:** Requires that computer system assets be available to authorized parties when needed.

The History of Information Security

- Began immediately after the first mainframes were developed
- Groups developing code-breaking computations during World War II created the first modern computers
- Physical controls to limit access to sensitive military locations to authorized personnel
- Rudimentary in defending against physical theft, espionage, and sabotage

The 1960s

- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception

The 1970s and 80s

- ARPANET grew in popularity as did its potential for misuse
- Fundamental problems with ARPANET security were identified
- No safety procedures for dial-up connections to ARPANET
- Non-existent user identification and authorization to system
- Late 1970s: microprocessor expanded computing capabilities and security threats

R-609

- Information security began with Rand Report R-609 (paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
- Safety of data
- Limiting unauthorized access to data
- Involvement of personnel from multiple levels of an organization

The 1990s

- Networks of computers became more common; so too did the need to interconnect networks
- Internet became first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority

The Present

- The Internet brings millions of computer networks into communication with each other—many of them unsecured
- Ability to secure a computer's data influenced by the security of every computer to which it is connected

Security Attacks, Services and Mechanisms

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

Security attack – Any action that compromises the security of information owned by an organization.

Security mechanism – A mechanism that is designed to detect, prevent or recover from a security attack.

Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

CHAPTER TWO

Fundamentals of IS Security

IS Security Fundamentals

The Elements of Security

Vulnerability

- It is a software, hardware, or procedural weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment.
- Vulnerability characterizes the absence or weakness of a safeguard that could be exploited.

E.g.: a service running on a server, unpatched applications or operating system software, unrestricted modem dial-in access, an open port on a firewall, lack of physical security etc.

Threat

- Any potential danger to information or systems.
- A threat is a possibility that someone (person, s/w) would identify and exploit the vulnerability.
- The entity that takes advantage of vulnerability is referred to as a threat agent.
- E.g.: A threat agent could be an intruder accessing the network through a port on the firewall

Risk

- Risk is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact.
- Reducing vulnerability and/or threat reduces the risk.

Exposure

- An exposure is an instance of being exposed to losses from a threat agent.
- Vulnerability exposes an organization to possible damages.
- E.g.: If password management is weak and password rules are not enforced, the company is exposed to the possibility of having users' passwords captured and used in an unauthorized manner.

Countermeasure or Safeguard

- It is an application or a s/w configuration or h/w or a procedure that mitigates the risk.
- E.g.: strong password management, a security guard, access control mechanisms within an operating system, the implementation of basic input/output system (BIOS) passwords, and security-awareness training

The Relation Between the Security Elements

- Example: If a company has antivirus software but does not keep the virus signatures up-to-date, this is vulnerability. The company is vulnerable to virus attacks.
- The threat is that a virus will show up in the environment and disrupt productivity.
- The likelihood of a virus showing up in the environment and causing damage is the risk.
- If a virus infiltrates the company's environment, then vulnerability has been exploited and the company is exposed to loss.
- The countermeasures in this situation are to update the signatures and install the antivirus software on all computers

Principles of Information Systems Security

The three fundamental principles of security are availability, integrity, and confidentiality and are commonly referred to as CIA or AIC triad which also form the main objective of any security program.

The level of security required to accomplish these principles differs per company, because each has its own unique combination of business and security goals and requirements.

All security controls, mechanisms, and safeguards are implemented to provide one or more of these principles.

All risks, threats, and vulnerabilities are measured for their potential capability to compromise one or all of the AIC principles

Introduction to IS Security Policy

A security policy is an overall general statement produced by senior management (or a selected policy board or committee) that dictates what role security plays within the organization.

A well designed policy addresses:

1. What is being secured?
   - Typically an asset.
2. Who is expected to comply with the policy?
   - Typically employees.
3. Where is the vulnerability, threat or risk?
   - Typically an issue of integrity or responsibility.

Types of Security Policies

1. Organizational

- Management establishes how a security program will be set up, lays out the program's goals, assigns responsibilities, shows the strategic and tactical value of security, and outlines how enforcement should be carried out.
- Provides scope and direction for all future security activities within the organization.
- This policy must address relative laws, regulations, and liability issues and how they are to be satisfied.
- It also describes the amount of risk senior management is willing to accept.

2. Issue-specific

- Addresses specific security issues that management feels need more detailed explanation and attention to make sure a comprehensive structure is built and all employees understand how they are to comply with these security issues
- E.g.: An e-mail policy might state that management can read any employee's e-mail messages that reside on the mail server, but not when they reside on the user's workstation

3.System-specific

- Presents the management's decisions that are specific to the actual computers, networks, applications, and data.
- This type of policy may provide an approved software list, which contains a list of applications that may be installed on individual workstations.
- E.g.: This policy may describe how databases are to be used and protected, how computers are to be locked down, and how firewalls, IDSs, and scanners are to be employed.

Plan, Design and Implement IS Security

The Security Systems Development Life Cycle

- The same phases used in traditional SDLC may be adapted to support specialized implementation of an IS project
- Identification of specific threats and creating controls to counter them
- SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

Analysis:

- Documents from investigation phase are studied Analysis of existing security policies or programs, along with documented current threats and associated controls.
- Includes analysis of relevant legal issues that could impact design of the security solution.
- Risk management task begins.

Logical Design :

- Creates and develops blueprints for information security
- Incident response actions planned:
  - –Continuity planning
  - –Incident response
  - –Disaster recovery

- Feasibility analysis to determine whether project should be continued or outsourced

Physical Design:

- Needed security technology is evaluated, alternatives are generated, and final design is selected
- At end of phase, feasibility study determines readiness of organization for project

Implementation:

- Security solutions are acquired, tested, implemented, and tested again.
- Personnel issues evaluated; specific training and education programs conducted.
- Entire tested package is presented to management for final approval.

Maintenance and Change:

- Perhaps the most important phase, given the everchanging threat environment.
- Often, reparation and restoration of information is a constant duel with an unseen adversary.
- Information security profile of an organization requires constant adaptation as new threats emerge and old threats evolve.

Chapter Three

Attack Types and Protection Schemes

SECURITY ATTACKS:

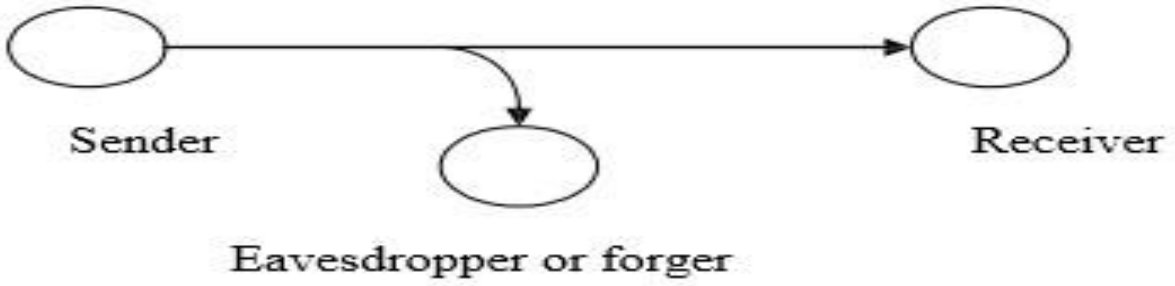
There are four general categories of attack which are listed below.

Interruption

An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or disabling of file management system.

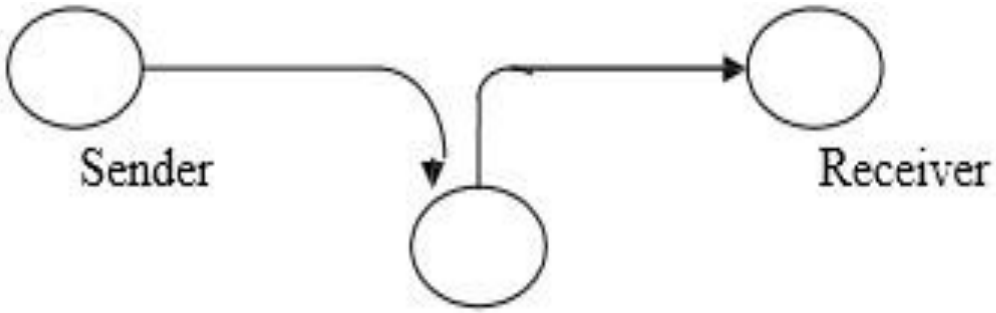
Interception

An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer. e.g., wire tapping to capture data in the network, illicit copying of files



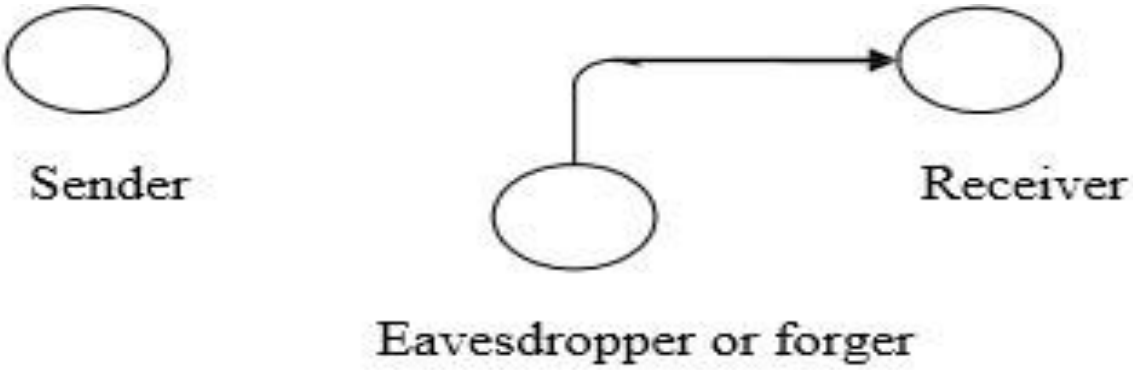
Modification

An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifyingthe contents of messages being transmitted in a network



Fabrication

An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.



Vulnerabilities of Information Systems

Why systems are vulnerable

- Accessibility of networks
- Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
- Software problems (programming errors, installation errors, unauthorized changes)
- Disasters
- Loss and theft of portable devices

Internet vulnerabilities

- Network open to anyone
- Size of Internet means abuses can have wide impact
- Use of fixed Internet addresses with cable or DSL modems creates fixed targets hackers

Security Threats

Spoofing

- Hackers attempting to hide true identities often spoof, or misrepresenting oneself by using fake e-mail addresses or masquerading as someone else.
- Redirecting Web link to address different from intended one, with site masquerading as intended destination.

Sniffer

- Eavesdropping program that monitors information traveling over network.
- Enables hackers to steal proprietary information such as e-mail, company files, etc.

Denial-of-service attacks (DoS)

- Flooding server with thousands of false requests to crash the network.

Phishing

- Setting up fake Web sites or sending e-mail messages that look like legitimate businesses to ask

users for confidential personal data.

Pharming

- Redirects users to a bogus Web page, even when individual types correct Web page address into his or her browser

Malware (malicious software)

✓ Viruses

- Rogue software program that attaches itself to other software programs or data files in order to be executed

✓ Worms

- Independent computer programs that copy themselves from one computer to other computers over a network.

✓ Trojan horses

- Software program that appears to be benign but then does something other than expected.

✓ SQL injection attacks

- Hackers submit data to Web forms that exploits site's unprotected software and sends rogue SQL query to database Spyware
- Small programs install themselves surreptitiously on computers to monitor user Web surfing activity and serve up advertising

✓ Key loggers

- Record every keystroke on computer to steal serial numbers, passwords, launch Internet attacks

Categories of Security controls

CONTROLS: Methods, policies, procedures to protect assets; accuracy & reliability of records; adherence to management standards.

Categories of Information systems controls

- GENERAL CONTROLS
- APPLICATION CONTROLS

General controls

- Apply to all computerized applications

- Combination of hardware, software, and manual procedures to create overall control environment

Types of general controls

- **IMPLEMENTATION:** Audit system development to assure proper control, management
- **SOFTWARE:** Ensure security, reliability of software
- **PHYSICAL HARDWARE:** Ensure physical security, performance of computer hardware
- **COMPUTER OPERATIONS:** Ensure procedures consistently, correctly applied to data storage, processing
- **DATA SECURITY:** Ensure data disks, tapes protected from wrongful access, change, destruction
- **ADMINISTRATIVE:** Ensure controls properly executed, enforced

Application controls

- Specific controls unique to each computerized application, such as payroll or order processing
- Ensure that only authorized data are completely and accurately processed by that application processing are accurate, complete, and properly distributed.

Types of general controls

1. INPUT
2. PROCESSING
3. OUTPUT
    1- Input controls : check data for accuracy and completeness when they enter the system
    2- Processing controls: establish that data are complete and accurate during updating
    3- Output controls: the results of computer

Social Engineering

What is Social Engineering?

- Manipulate people into doing something, rather than by breaking in using technical means
- Attacker uses **human interaction** to obtain or compromise information

- Attacker my appear **unassuming or respectable** o **Pretend** to be a new employee, repair man, ect o May even **offer credentials**
- By asking questions, the attacker may **piece enough information together** to infiltrate a companies network
    - o May attempt to get information from many sources

Examples of Social Engineering

- Convinced friend that I would help fix their computer
- People inherently want to trust and will believe someone when they want to be helpful
- Fixed minor problems on the computer and secretly installed remote control software
- Now I have total access to their computer through ultravnc viewer

Types of Social Engineering

- Quid Pro Quo
    - Something for something
- Phishing
    - Fraudulently obtaining private information
- Baiting
    - Real world trojan horse
- Pretexting
    - Invented Scenario
- Diversion Theft
    - A con

Quid Pro Quo

• Something for Something

- **Call random numbers** at a company, claiming to be from technical support.
- Eventually, you will reach someone with a **legitamite proble**
- Grateful you called them back, they will **follow your instructions**

- The attacker will "help" the user, but will really have the victim type commands that will allow the attacker to **install malware**

Phishing

- **Fraudulently obtaining private information**

- Send an email that looks like it came from a legitimate business
- Request verification of information and warn of some consequence if not provided
- Usually contains link to a fraudulent web page that looks legitimate
- User gives information to the social engineer

- **Spear Fishing**

- Specific phishing

  Ex: email that makes claims using your name

- **Spear Fishing**
  - **Specific phishing**
    - **Ex**: email that makes claims using your name
- **Vishing**
  - **Phone phishing**
  - Rogue interactive voice system
    - **Ex**:call bank to verify information
- **Real world Trojan horse**
  - **Uses physical media**
  - Attacker leaves a **malware infected cd or usb drive** in a location sure to be found

Pretexting

- **Invented Scenario**

- Prior Research/Setup used to establish legitimacy
  - Give information that a user would normally not divulge

Pretexting Real Example:

- Signed up for Free Credit Report
- Saw Unauthorized charge from another credit company
  - Called to dispute charged and was asked for Credit Card Number
    - They insisted it was useless without the security code
  - Asked for Social Security number
- Talked to Fraud Department at my bank

Diversion Theft

- **A Con**

o Persuade deliver person that **delivery is requested elsewhere**

Ex: Attacker parks **security van outside a bank**. **Victims going to deposit money** into a night safe are told that the **night safe is out of order**. **Victims then give money to attacker** to put in the fake security van

Chapter 4
Security Techniques

- Cryptography is the study of mathematical techniques related to information security aspects such as confidentiality, data integrity, entity authentication, and data authentication.
- Cryptography: process of making and using codes to secure transmission of information
- Cryptography: is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Cryptographic systems are generally classified along 3 independent dimensions:

- **Type of operations used for transforming plain text to cipher text :**All the encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged.

- **The number of keys used :**If the sender and receiver uses same key then it is said to be symmetric key (or) single key (or) conventional encryption. If the sender and receiver use different keys then it is said to be public key encryption.
- **The way in which the plain text is processed :**A block cipher processes the input and block of elements at a time, producing output block for each input block. A stream cipher processes the input elements continuously, producing output element one at a time, as it goes along.

Basic Terminology

- **plaintext** - the original message
- **ciphertext** - the coded message
- **cipher** - algorithm for transforming plaintext to cipher text
- **key** - info used in cipher known only to sender/receiver
- **encipher (encrypt)** - converting plaintext to cipher text
- **decipher (decrypt)** - recovering cipher text from plaintext
- **cryptography** - study of encryption principles/methods
- **cryptanalysis (code breaking)** - the study of principles/ methods of deciphering cipher text *without* knowing key
- **cryptology** - the field of both cryptography and cryptanalysis

Cryptosystem

Cryptosystem: is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system.**

Cryptographic Algorithms

- Often grouped into two broad categories, symmetric and asymmetric; today's popular cryptosystems use hybrid combination of symmetric and asymmetric algorithms
- Symmetric and asymmetric algorithms distinguished by types of keys used for encryption and decryption operations.

Symmetric Cryptographic Algorithm

- Symmetric encryption: uses same "secret key" to encipher and decipher message

- In symmetric key algorithms, the encryption and decryption keys are known both to sender and receiver. The encryption key is shared and the decryption key is easily calculated from it. In many cases, the encryption and decryption keys are the same.

Data Encryption Standards (DES) and Advanced Encryption Standards(AES) **Data Encryption Standards(DES):**

- The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST).
- DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only).

Advanced Encryption Standards (AES)

- The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.
- A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Operation of AES

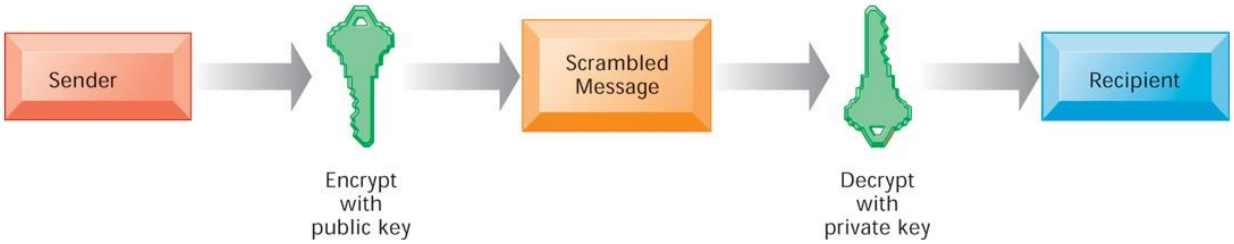
- AES is an iterative rather than Feistel cipher. It is based on ‘substitution–permutation network’. It comprises of a series of linked operations, some of which involve replacing inputs by specific outputs (substitutions) and others involve shuffling bits around (permutations).
- Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix
- Unlike DES, the number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

Asymmetric Cryptographic Algorithm

Asymmetric Encryption (public key encryption)

- Uses two different but related keys; either key can encrypt or decrypt message
- If Key A encrypts message, only Key B can decrypt
- Highest value when one key serves as private key and the other serves as public key

PUBLIC KEY ENCRYPTION:



ENCRYPTION TECHNIQUES

There are two basic building blocks of all encryption techniques:

substitution and transposition.

SUBSTITUTION TECHNIQUES

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

Caesar cipher (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar.

The Caesar cipher involves replacing each letter of the alphabet with the letter standing 3 places further down the alphabet. e.g., plain text : pay more money

Cipher text: SDB PRUH PRQHB

Note that the alphabet is wrapped around, so that letter following ‚z" is ‚a".

For each plaintext letter p, substitute the cipher text letter c such that $C = E(p) = (p+3) \bmod 26$

A shift may be any amount, so that general Caesar algorithm is

$C = E(p) = (p+k) \bmod 26$

Where k takes on a value in the range 1 to 25. The decryption algorithm is simply

$P = D(C) = (C-k) \bmod 26$

Playfair cipher

The best known multiple letter encryption cipher is the playfair, which treats digrams in the plaintext as single units and translates these units into cipher text digrams. The playfair algorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let the keyword be "monarchy" . The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetical order.

The letter „i" and „j" count as one letter. Plaintext is encrypted two letters at a time according to the following rules:

- Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x".
- Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last.
- Plaintext letters that fall in the same column are replaced by the letter beneath, with the top element of the column following the last.
- Otherwise, each plaintext letter is replaced by the letter that lies in its own row And the column occupied by the other plaintext letter.

Playfair cipher Example with keyword "monarchy"

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

- Plaintext = meet me at the school house
- Splitting two letters as a unit => me et me at th es ch ox ol ho us ex
- Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

Vigenère cipher

In a Caesar cipher, each letter of the alphabet is shifted along some number of places; for example, in a Caesar cipher of shift 3, A would become D, B would become E, Y would become B and so on. The Vigenère cipher consists of several Caesar ciphers in sequence with different shift values. To encrypt, a table of alphabets can be used, termed a tabula recta, Vigenère square, or Vigenère table. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers. At different points in the encryption process, the cipher uses a different alphabet from one of the rows. The alphabet used at each point depends on a repeating keyword.

The Vigenère square or Vigenère table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

The Vigenère square or Vigenère table, also known as the *tabula recta*, can be used for encryption and decryption.

For example, suppose that the plaintext to be encrypted is:

ATTACKATDAWN

The person sending the message chooses a keyword and repeats it until it matches the length of the plaintext, for example, the keyword "LEMON":

LEMONLEMONLE

Each row starts with a key letter. The remainder of the row holds the letters A to Z (in shifted order). Although there are 26 key rows shown, you will only use as many keys (different alphabets) as there are unique letters in the key string, here just 5 keys, {L, E, M, O, N}. For successive letters of the message, we are going to take successive letters of the key string, and encipher each message letter using its corresponding key row. Choose the next letter of the key, go along that row to find the column heading that matches the message character; the letter at the intersection of [key-row, msg-col] is the enciphered letter.

For example, the first letter of the plaintext, A, is paired with L, the first letter of the key. So use row L and column A of the Vigenère square, namely L. Similarly, for the second letter of the plaintext, the second letter of the key is used; the letter at row E and column T is X. The rest of the plaintext is enciphered in a similar fashion:

- Plaintext: ATTACKATDAWN
- Key: LEMONLEMONLE
- Ciphertext: LXFOPVEFRNHR

Decryption is performed by going to the row in the table corresponding to the key, finding the position of the ciphertext letter in this row, and then using the column's label as the plaintext. For example, in row L (from LEMON), the ciphertext L appears in column A, which is the first plaintext letter. Next we go to row E (from LEMON), locate the ciphertext X which is found in column T, thus T is the second plaintext letter.

Vigenère Algebraic description

Vigenère can also be viewed algebraically. If the letters A–Z are taken to be the numbers 0–25, and addition is performed modulo 26, then Vigenère encryption using the key can be written,

$Ci=Ek(Mi)=(Mi+Ki) \mod 26$ and decryption using the key ,

$Mi=Dk(Ci)=(Ci-Ki) \mod 26$

Whereas M= M0..Mn is the message, C=C0...Cn is the cipher text and K=K0…Km is the used key. Thus using the previous example, to encrypt A=0 with key letter l=11 the calculation would result in 11=L

11=(0+11)mod 26=11

Therefore to decrypt R=17 with key letter E=4 the calculation would result in 13=N

13=(17-4(mod26

TRANSPOSITION TECHNIQUES

Transposition technique is achieved by performing some kind of permutation on the plaintext letters. It is very simple to realize this kind of cipher. We can do it by the example. If the plaintext is “meet me after the party”, we can rearrange it by this way:

m e m a t r h p r y e t e f e t e a t

So we get the plaintext and the ciphertext like this:

plaintext: meet me after the party ciphertext: mematrhpryetefeteat

Columnar transposition

Another simple transposition cipher is called Columnar transposition. If the plaintext is “data encryption”, we will compose the sentence into a 3*5 matrix. For example: key: 4 1 2 3 5 plaintext : d a t a

e n c r y

p t i o n

ciphertext: anttciarodep yn

Of course, the transposition cipher can be made more secure by performing more than one stage of transposition. For example, doing the Columnar transposition 2 or 3 times and it will efficiently to increase the security of this cipher.

Periodic The transposition

The transposition cipher is also called permutation ciphers, rearrange the plaintext message symbols in different order. Often the permutation of the characters will be done over a fixed period of d symbols.

M=m1,m2,…,md,md+1,md+2,…,m2d,m2d+1, …

$C=E_K(M)$

C=mf(1),mf(2(,…,mf(d),mf(d+1),mf(d+2),…,mf(2d),mf(2d+1), …

C=mf(1),mf(2),…,mf(d),md+f(1),md+f(2),…,md+f(d),m2d+f(1), …

There the function f(i) is the permutation of the ith input symbol index

Example

permutation function f(i)

be: i= 1, 2, 3, 4, 5, 6 f(i)=3,

1, 6, 5, 2 ,4

Then if the original message M is “mobile channel ”

M= m o b i l e c h a n n e l …

m_1 m_2 m_3 m_4 m_5 m_6 m_7 m_8 m_9 m_{10} m_{11} m_{12} m_{13} …

the periodic permutation cipher is C is obtained by the following permutation,(period=6):

$C=m_{f(1)}$ $m_{f(2)}$ $m_{f(3)}$ $m_{f(4)}$ $m_{f(5)}$ $m_{f(6)}$ $m_{f(7)}$ $m_{f(8)}$ $m_{f(9)}$ …

$= m_{f(1)}$ $m_{f(2)}$ $m_{f(3)}$ $m_{f(4)}$ $m_{f(5)}$ $m_{f(6)}$ $m_{6+f(1)}$ $m_{6+f(2)}$ $m_{6+f(3)}$ …

$= m_3$ m_1 m_6 m_5 m_2 m_4 m_{6+3} m_{6+1} m_{6+6} …

$= m_3$ m_1 m_6 m_5 m_2 m_4 m_9 m_7 m_{12} …

C= B M E L O I A C E …

That is C is “BMELOIACENHN” after the transposition transformation

digital signature

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document. The digital equivalent of a handwritten signature or stamped seal, a digital signature offers far more inherent security, and it is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide the added assurances of evidence of origin, identity and status of an electronic document, transaction or message and can acknowledge informed consent by the signer.

In many countries, including the United States, digital signatures are considered legally binding in the same way as traditional document signatures.

- Encrypted messages that can be mathematically proven to be authentic

- Created in response to rising need to verify information transferred using electronic systems
- Asymmetric encryption processes used to create digital signatures

Digital Certificates

- Electronic document containing key value and identifying information about entity that controls key
- Digital signature attached to certificate's container file to certify file is from entity it claims to be from

Access control

- Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization.
- There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

To secure a facility, organizations use electronic access control systems that rely on user credentials, access card readers, auditing and reports to track employee access to restricted business locations and proprietary areas, such as data centers. Some of these systems incorporate access control panels to restrict entry to rooms and buildings as well as alarms and lockdown capabilities to prevent unauthorized access or operations.

Access control systems perform authentication and authorization of users and entities by evaluating required login credentials that can include passwords, personal identification numbers (PINs), biometric scans, security tokens or other authentication factors.

Types of access control

• **Mandatory access control (MAC):** A security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system or security kernel, grants or denies access to those resource objects based on the information security

clearance of the user or device.

• **Discretionary access control (DAC):** An access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. A common criticism of DAC systems is a lack of centralized control.

Firewall

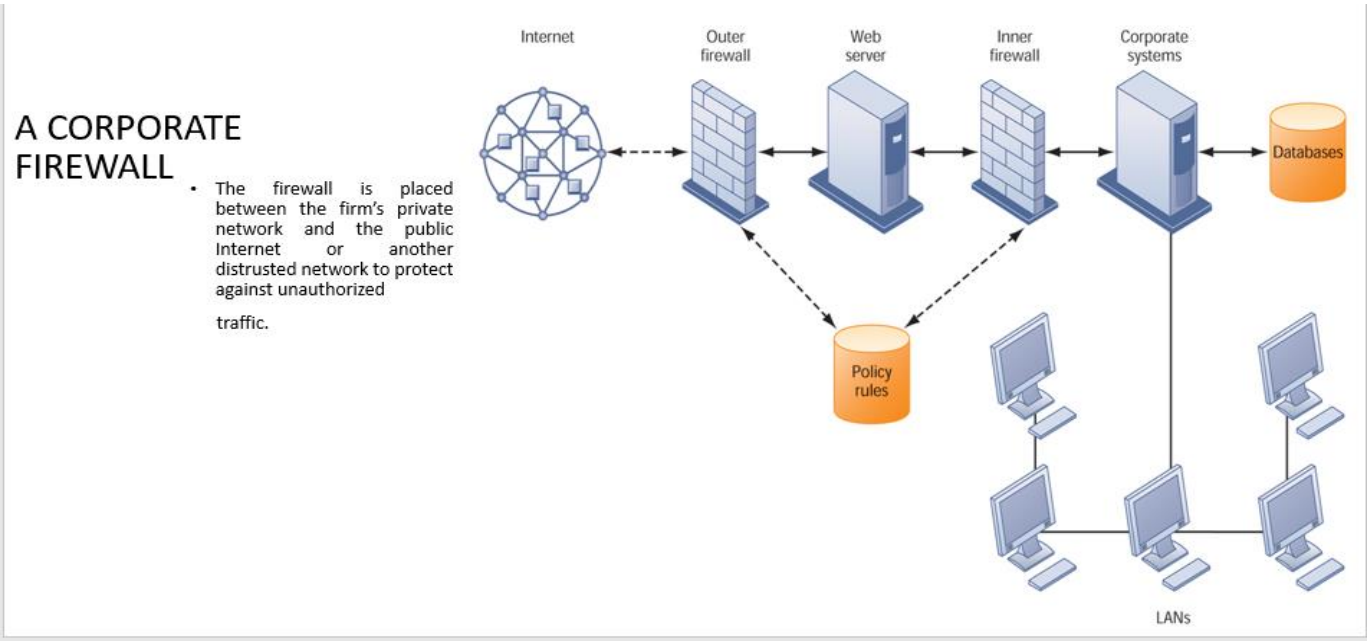
Firewall: Combination of hardware and software that prevents unauthorized users from accessing private networks.

Technologies include:

- Static packet filtering
- Network address translation (NAT)
- Application proxy filtering

How Firewalls work?

Firewall examine all the data packets passing through them to see if they meet the rules defined by the ACL (Access Control List) made by the administrator of the network. Only, If the Data Packets are allowed as per ACL, they will be Transmitted over the Connection.



Classification of Firewalls

- A packet filter is a firewall that lives at the network layer.
- A stateful packet filter is a firewall that operates at the transport layer.
- An application proxy is, as the name suggests, a firewall that operates at the application layer where it functions as a proxy.

Intrusion detection systems

• Intrusion detection is the process of monitoring the events occurring in your network and analyzing them for signs of possible incidents, violations, or imminent threats to your security policies. Intrusion prevention is the process of performing intrusion detection and then stopping the detected incidents. These security measures are available as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which become part of your network to detect and stop potential incidents.

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While anomaly detection and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.

Different types of intrusion detection systems

Intrusion detection systems come in different flavors and detect suspicious activities using different methods, including the following:

- A network intrusion detection system (NIDS) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.
- Snort, one of the most widely used intrusion detection systems is an open source, freely available and lightweight NIDS that is used to detect emerging threats. Snort can be compiled on most Unix or Linux operating systems, and a version is available for Windows as well.

- Anomaly-based intrusion detection systems monitor network traffic and compare it against an established baseline, to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type of IDS alerts administrators to potentially malicious activity.

- Historically, intrusion detection systems were categorized as passive or active; a passive IDS that detected malicious activity would generate alert or log entries, but would take no actions. An active IDS, sometimes called an intrusion detection and prevention system, would generate alerts and log entries, but could also be configured to take actions, like blocking IP addresses or shutting down access to restricted resources.

- Host intrusion detection systems (HIDS) run on all computers or devices in the network with direct access to both the internet and the enterprise internal network. HIDS have an advantage over NIDS in that they may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. HIDS may also be able to identify malicious traffic that originates from the host itself, as when the host has been infected with malware and is attempting to spread to other systems.

- Signature-based intrusion detection systems monitor all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software.

Authentication

The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization , which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authentication is the process of determining whether someone or something is, in fact, who or what it declares itself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials in a database of authorized users or in a data authentication server.

Users are usually identified with a user ID, and authentication is accomplished when the user provides a credential, for example a password, that matches with that user ID. Most users are most familiar with using a password, which, as a piece of information that should be known only to the user, is called a knowledge authentication factor.

Authentication begins when a user tries to access information. First, the user must prove his access rights and identity. When logging into a computer, users commonly enter usernames and passwords for authentication purposes. This login combination, which must be assigned to each user, authenticates access. However, this type of authentication can be circumvented by hackers.

- A better form of authentication, biometrics, depends on the user's presence and biological makeup (i.e.,fingerprints). This technology makes it more difficult for hackers to break into computer systems.
- The Public Key Infrastructure (PKI) authentication method uses digital certificates to prove a user's identity. There are other authentication tools, too, such as key cards and USB tokens. One of the greatest authentication threats occurs with email, where authenticity is often difficult to verify. For example, unsecured emails often appear legitimate.

Chapter 5:
Security at Different Layers

PHYSICAL SECURITY

Physical security exists in order to deter persons from entering a physical facility. Historical examples of physical security city walls. The key factor is the technology used for physical security has changed over time. While in past eras, there was no passive infrared (PIR) based technology, electronic access control systems, or video surveillance system (VSS) cameras, the essential methodology of physical security has not altered over time.

Physical security has three important components: access control, surveillance and testing.

- The first hardening measures include fencing, locks, access control cards, biometric access control systems and fire suppression systems.
- Second, physical locations should be monitored using surveillance cameras and notification systems, such as intrusion detection sensors, heat sensors and smoke detectors.
- Third, disaster recovery policies and procedures should be tested on a regular basis to ensure safety and to reduce the time it takes to recover from disruptive man-made or natural disasters.

There are at least five layers of physical security:

- Environmental design
- Mechanical, electronic and procedural access control
- Intrusion detection
- Video monitoring
- Personnel Identification

The goal is to convince potential attackers that the likely costs of attack exceed the value of making the attack.

The initial layer of security for a campus, building, office, or physical space uses crime prevention through environmental design to deter threats. Some of the most common examples are also the most basic - barbed wire, warning signs and fencing, concrete bollards, metal barriers, vehicle height-restrictors, site lighting and trenches.

Application Security

- Average sized organization has hundreds of in-house and externally developed applications.
- Business process are continually moving towards web services
- However, data and critical business services are being exposed:
    - Lack of testing
    - Insecure applications
    - Human error
- Security must be an integral part of application lifecycle:
    - from initial concept to final disposal
- A golden rule of application security:
    - You cannot test in security! It must be designed into the application and verified each step of the lifecycle.

Network Security

Network protocols are not secure.

- Port scan/direct attack

- Malicious Web Sites
- Social Engineering
- Phishing/Pharming
- Denial of Service attacks
- Viruses/Worms
- Others