★ **What is Computer security ?**

Computer security refers to protecting and securing computers and their related data, networks, software, hardware from unauthorized access, misuse, theft, information loss, and other security issues.

Computer security is the protection of the assets of a computer system.

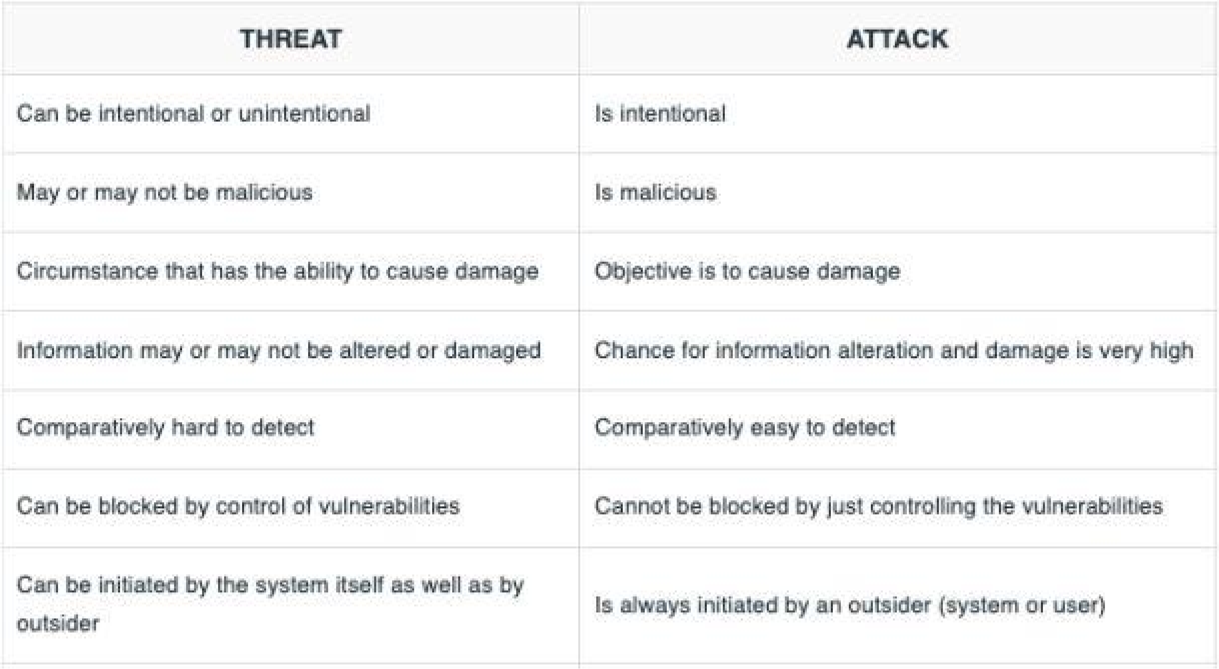
- Hardware
- Software
- Data

★ **Vulnerability** is a weakness in the security system
(i.e., in procedures, design, or implementation), that might be exploited to cause loss or harm.

★ **Threat** to a computing system is a set of circumstances that has the potential to cause loss or harm.

★ A human (criminal) who exploits a vulnerability perpetrates an **attack** on the system.

★ **The difference between threat and attack are:**



THREAT	ATTACK
Can be intentional or unintentional	Is intentional
May or may not be malicious	Is malicious
Circumstance that has the ability to cause damage	Objective is to cause damage
Information may or may not be altered or damaged	Chance for information alteration and damage is very high
Comparatively hard to detect	Comparatively easy to detect
Can be blocked by control of vulnerabilities	Cannot be blocked by just controlling the vulnerabilities
Can be initiated by the system itself as well as by outsider	Is always initiated by an outsider (system or user)

★ **Types of Threats**

1. Physical Threats
2. Non-physical threats

★ **Attacks**

1. Passive attack

Passive attack is a kind of attack in which the data that is sent from the sender to the receiver is read by the attacker in the middle of the transmission.

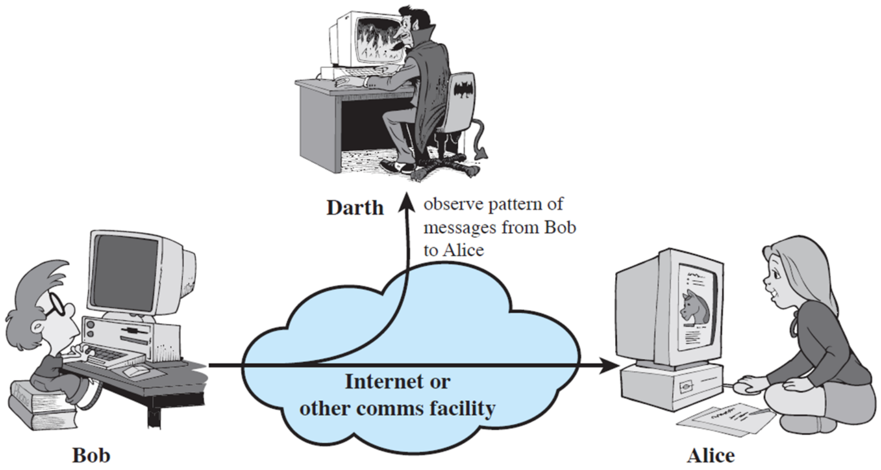
However, the main point to note here is that the passive attack is the attack in which the attacker does not modify or corrupt the data.

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

- Traffic Analysis

  As the name suggests, this attack focuses on the amount or volume of data sent between the sender and the receiver.

  The attacker can predict a lot of information about the sender and the receiver by knowing the amount of data sent.


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

- Eavesdropping

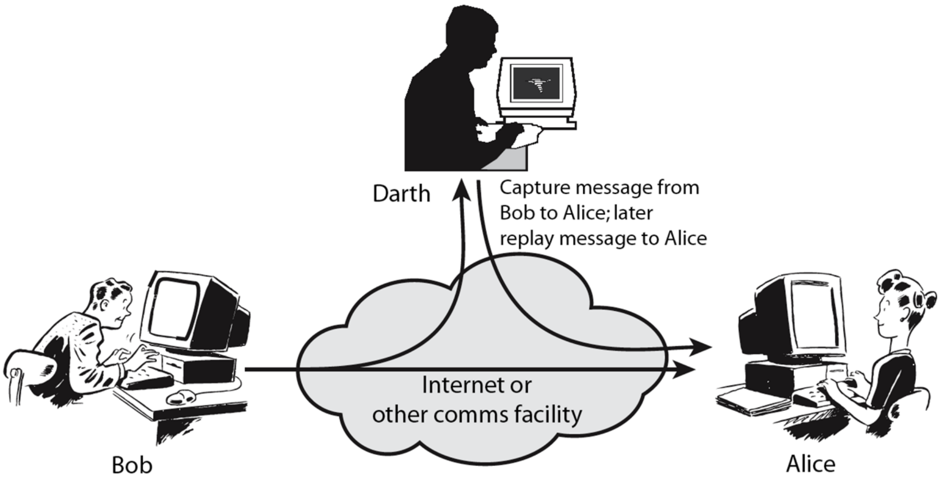
  In this kind of attack, the attacker reads the communication that happens between the sender and the receiver and then can use this information for many things.

2. Active attack

The focus of the attacker is to modify the data that is being exchanged between the sender and the receiver.

- Replay

  In a replay attack, the attacker acts as an authorized user and can use the details of the authorized user to log in to a system.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

This short note making resources are,google search engine,chat gpt and lecture slides

WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

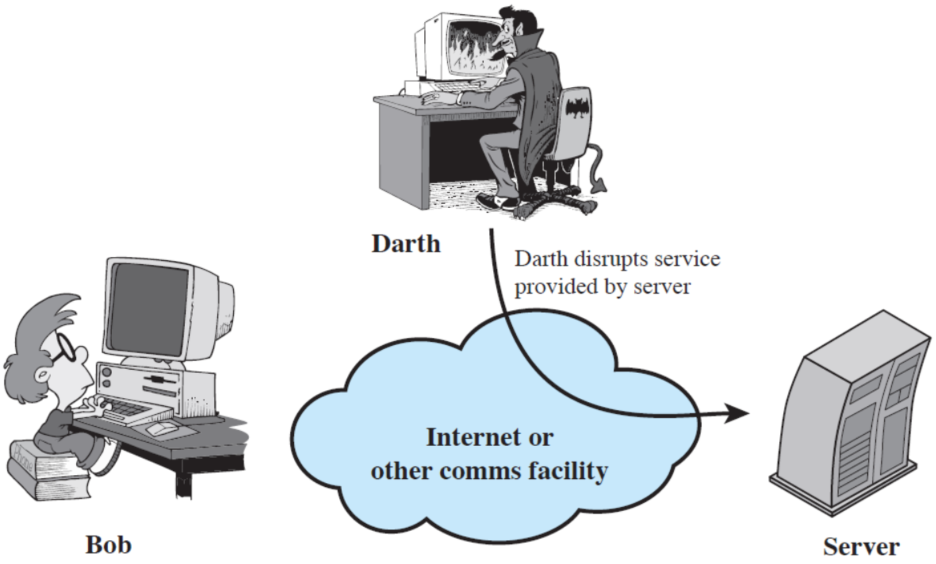
- Masquerade

  The attacker acts to be an authorized user. Now, this is not done by stealing the data packet. It is done by stealing the login details of the user somehow. So, no technical aspect of stealing the details is involved here.

- Denial of service (DoS)

  The denial-of-service attack is an attack in which a system is attacked by a lot of requests to the system at one time that it is not able to handle.

  The attacker sends multiple requests to the server at the same time and the server is not able to handle such requests.


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

★ How to make your system secure

- Always keep a backup of your data.
- Install firewall software and keep it updated every time.
- Install antivirus/ anti-spyware and keep it updated every time.
- Timely scan your complete system.
- Always keep your system updated.
- Make use of strong and difficult to crack passwords (having capital & small alphabets, numbers, and special characters).
- Before installing any program, check whether it is safe to install it (using Antivirus Software).
- Take extra caution when reading emails that contain attachments.

★ C-I-A Triad

1. Confidentiality - Prevent unauthorized read access to data
2. Integrity - Prevent unauthorized modification of information
3. Availability - You are able to access the data when you need it without any delays

★ Security Services

1. X.800

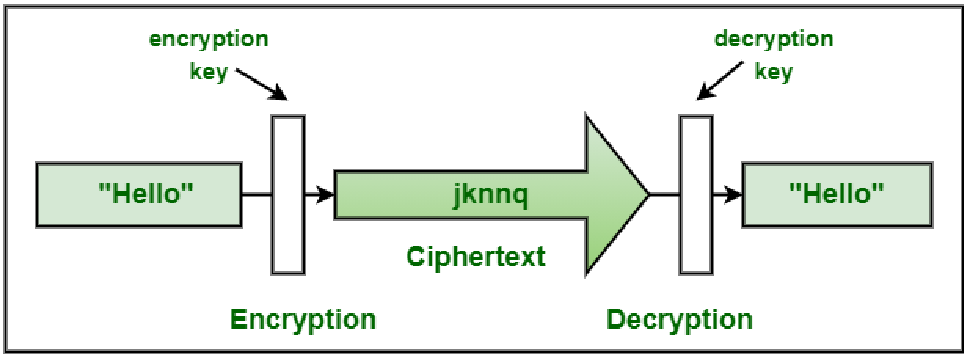
- Authentication - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- Access Control - prevention of the unauthorized use of a resource

- Data Confidentiality –protection of data from unauthorized disclosure
- Data Integrity - assurance that data received is as sent by an authorized entity
- Non-Repudiation - protection against denial by one of the parties in a communication
- Availability – resource accessible/usable

2. RFC 2828

★ **What is Cryptography?**

Cryptography is a technique of securing communication by converting plain text into unintelligible ciphertext.



Cryptography

Objectives of Information Security / Cryptography Principles

- Confidentiality (secrecy)
  Only the sender and intended receiver should be able to understand the contents of the transmitted message

- Authentication
  Both the sender and receiver need to confirm the identity of other party involved in the communication

- Data integrity
  The content of their communication is not altered, either maliciously or by accident, in transmission.

- Availability
  Timely accessibility of data to authorized entities.

- Non-repudiation
  An entity is prevented from denying its previous commitments or actions

- Access control
  An entity cannot access any entity that it is not authorized to.

- Anonymity
  The identity of an entity if protected from others.

This short note making resources are,google search engine,chat gpt and lecture slides

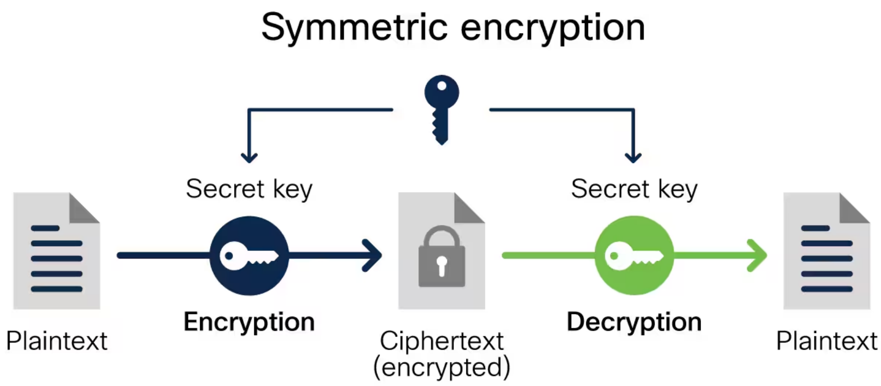
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

Types Of Cryptography / Types of Cryptographic Functions

1. Symmetric Key Cryptography / (private-key encryption)
2. Asymmetric Key Cryptography (public key encryption)
    - Digital Signature
3. Hash Functions

1. Symmetric Key Cryptography

uses the **same cryptographic keys** for both the **encryption of plaintext** and the **decryption of ciphertext.**



Both are classified as symmetric block ciphers.

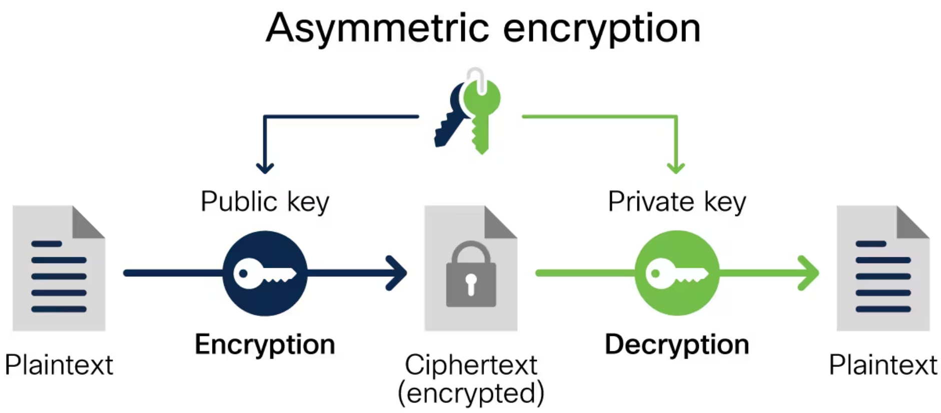
- Data Encryption System (DES)
- Advanced Encryption System (AES).

Difference between AES and DES ciphers

DES	AES
Key length 56 bits	Key length 128 / 192 / 256 bits
Block size 64 bits	Block size 128 bits
Fixed number of rounds 16	number of rounds depend on the key length
Comparatively slower	Comparatively faster

2. Asymmetric Key Cryptography

uses the different cryptographic keys for encryption and decryption. use the **public key** for **encryption of plaintext** and use the **private key** for **decryption of ciphertext.**

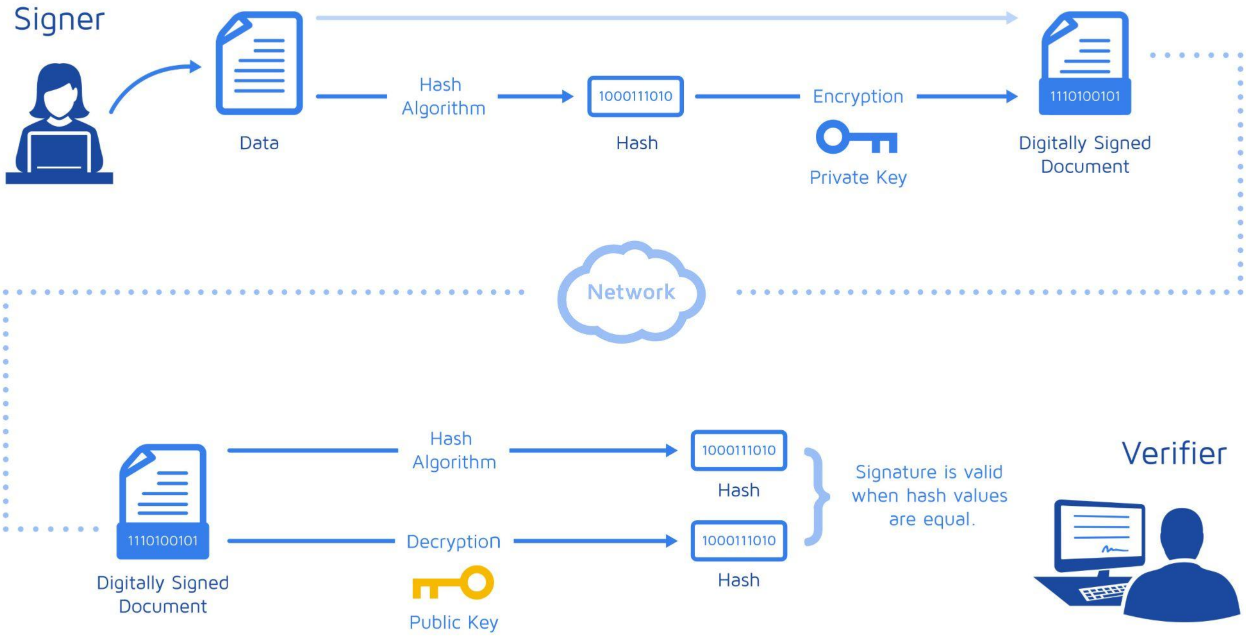


Digital Signature

Digital signatures are used to verify the identity of the sender and ensure that the received message or document has not been tampered with during transit.

The message is turned into a unique string of characters using a hash function.The **hash is encrypted** using the **sender's private key,** forming the digital signature.

The recipient uses the **sender's public key** to **decrypt the signature,** revealing the hash.The recipient hashes the received message.
If both hashes match, the message is verified as unchanged and sent by the rightful sender.



When the signature is generated by a Certification Authority (CA), the signature can be viewed as trusted.

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

Digital Signature Process

Step 1 - Hash (digest) the data using one of the supported Hashing algorithms, e.g., MD2, MD5, or SHA-1.

Step 2 - Encrypt the hashed data using the sender's private key.

Step 3 - Append the signature (and a copy of the sender's public key) to the end of the data that was signed.

Signature Verification Process

Step 1 - Hash the original data using the same hashing algorithm.

Step 2 - Decrypt the digital signature using the sender's public key. All digital signatures contain a copy of the signer's public key.

Step 3 - Compare the results of the hashing and the decryption. If the values match then the signature is verified. If the values do not match, then the data or signature was probably modified in transit.

Public key infrastructure or PKI

Public key infrastructure or PKI is the governing body behind issuing digital certificates.

It helps to protect confidential data and gives unique identities to users and systems. Thus, it ensures security in communications.

The public key infrastructure uses a pair of keys: the public key and the private key to achieve security.

PKI Players

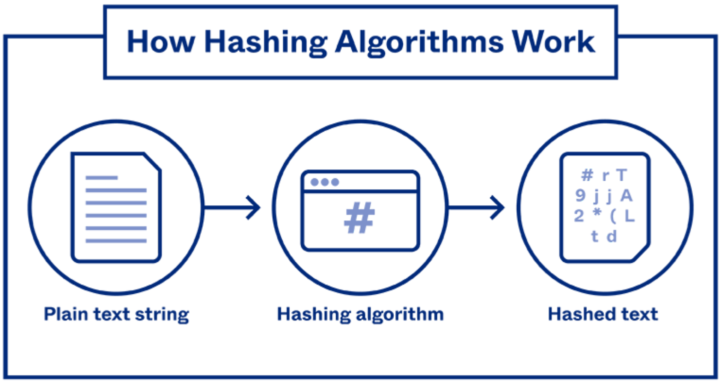
- Registration Authority (RA) to identity proof users
- Certification Authorities (CA) to issue certificates and CRL's
- Repositories (publicly available databases) to hold certificates and CRLs

3. Hash Functions

A Hash Function is a mathematical transformation that takes a message of arbitrary length and returns it to a fixed-length (short) number.

A Hash Function is a mathematical algorithm that converts a given numeric or alphanumeric key into a small practical integer value.

Commonly used hash functions, MD5 and SHA-256



:

★ **Differentiate between symmetric key encryption and asymmetric key encryption**

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher

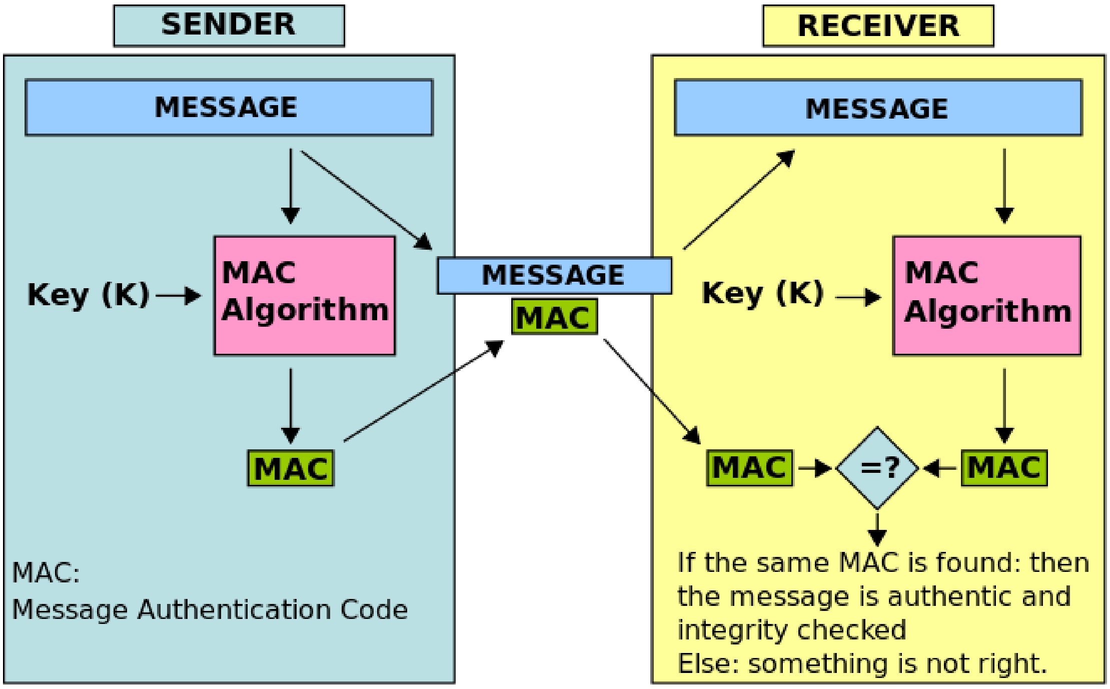
★ **Message Authentication Code (MAC)**

A Message Authentication Code (MAC) is a cryptographic tool that verifies a message's integrity and authenticity by using a secret key.

used for ensuring it hasn't been altered during transmission.

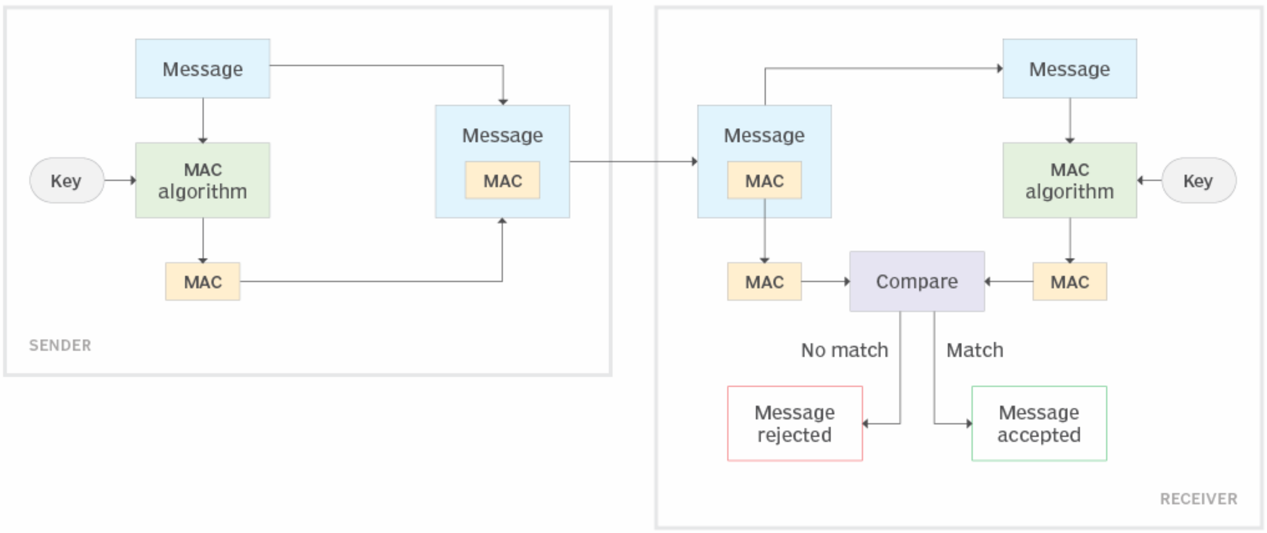
This short note making resources are,google search engine,chat gpt and lecture slides

WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj



MAC:
Message Authentication Code

If the same MAC is found: then the message is authentic and integrity checked
Else: something is not right.



★ **Authorization**

Authorization is the process of giving someone the ability to access a resource.

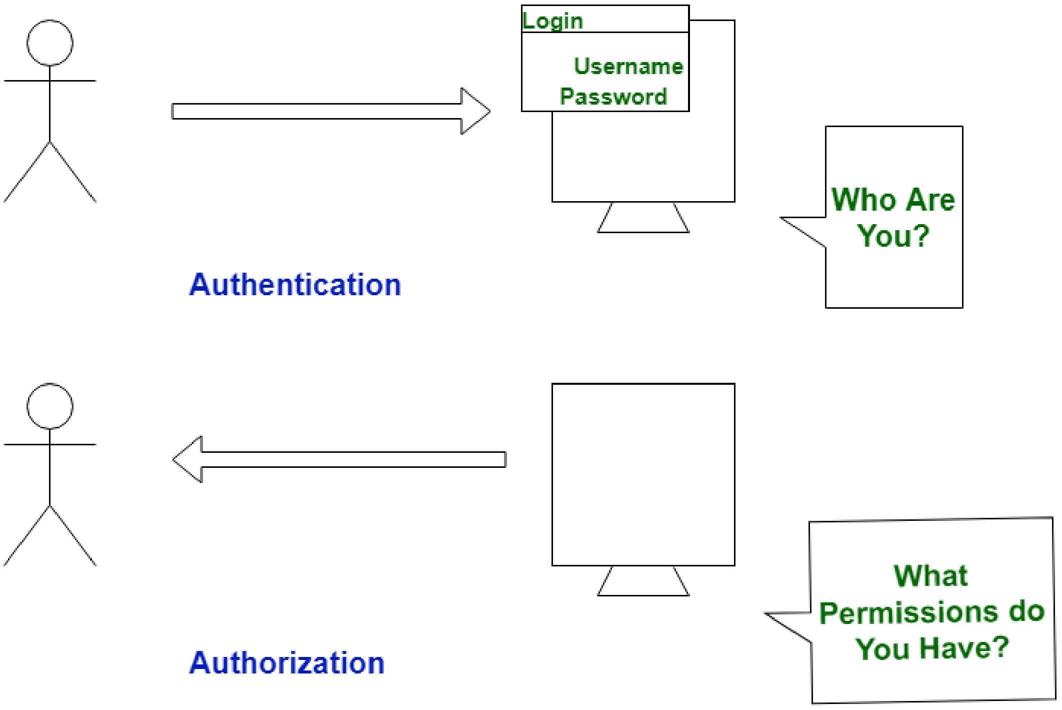
★ **Authentication**

Authentication is the process of validating the identity of a user or the integrity of a piece of data.

There are three technologies that provide authentication

1. Message Digests / Message Authentication Codes
2. Digital Signatures
3. Public Key Infrastructure

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj



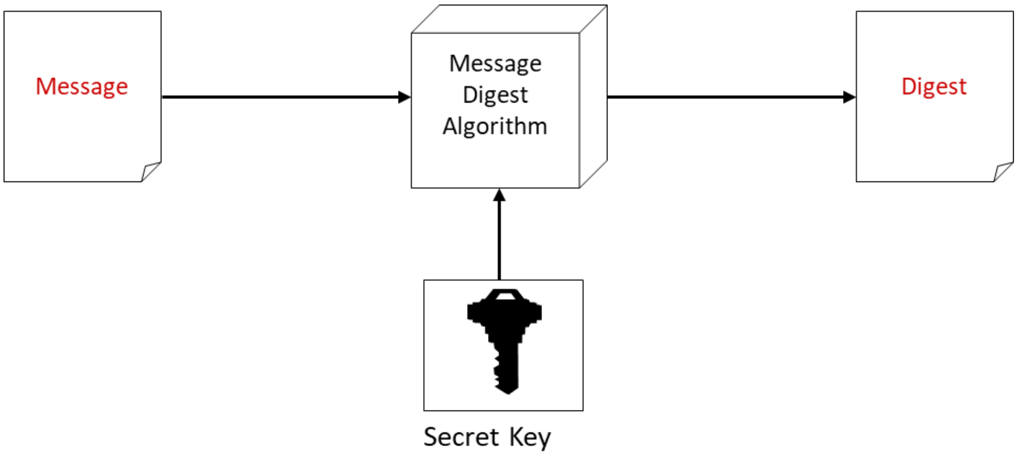
1. Message Digests / Message Authentication Codes

Message Digest is used to ensure the integrity of a message transmitted over an insecure channel (where the content of the message can be changed).

A message digest is a fingerprint for a document. Purpose of the message digest is to provide proof that data has not been altered. Process of generating a message digest from data is called hashing

Commonly used hash algorithms are,

- MD5 – 128 bit hashing algorithm by Ron Rivest of RSA
- SHA & SHA-1 – 162 bit hashing algorithm developed by NIST



Password Authentication

Message Digests commonly used for password authentication
Problems with password based authentication

- Attacker learns password by social engineering
- Attacker cracks password by brute-force and/or guesswork
- Eavesdrops password if it is communicated unprotected over the network
- Replays an encrypted password back to the authentication server

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only)   Credit - Kanishka viraj

Authentication Protocols

Kerberos

Kerberos is an authentication service that uses symmetric key encryption and a key distribution center.

Kerberos Authentication server contains symmetric keys of all users and also contains information on which user has access privilege to which services on the network

What are Kerberos 3 heads?

- authentication
- authorization
- accounting

Kerberos Limitations

- It doesn't work well in a timeshare environment
- Requires an always-on Kerberos server
- Stores all passwords are encrypted with a single key
- Each network service must be modified individually for use with Kerberos

Authentication

Personal Tokens

Personal Tokens are hardware devices that generate unique strings that are usually used in conjunction with passwords for authentication

Different types of tokens exist

- Storage Token - A secret value that is stored on a token and is available after the token has been unlocked using a PIN

- Synchronous one-time password generator - Generate a new password periodically (e.g. each minute) based on time and a secret code stored in the token

- Challenge-response - Token computes a number based on a challenge value sent by the server

- Digital Signature Token - Contains the digital signature private key and computes a computes a digital signature on a supplied data value

A variety of different physical forms of tokens exist
e.g. hand-held devices, Smart Cards, PCMCIA cards, USB tokens

Biometrics

Uses certain biological characteristics for authentication.

Different techniques exist

- Fingerprint Recognition
- Voice Recognition

- Handwriting Recognition
- Face Recognition
- Retinal Scan
- Hand Geometry Recognition

Iris Recognition

The scanning process takes advantage of the natural patterns in people's irises, digitizing them for identification purposes

Random Numbers

many uses of random numbers in cryptography

- nonces in authentication protocols to prevent replay
- session keys
- public key generation
- keystream for a one-time pad

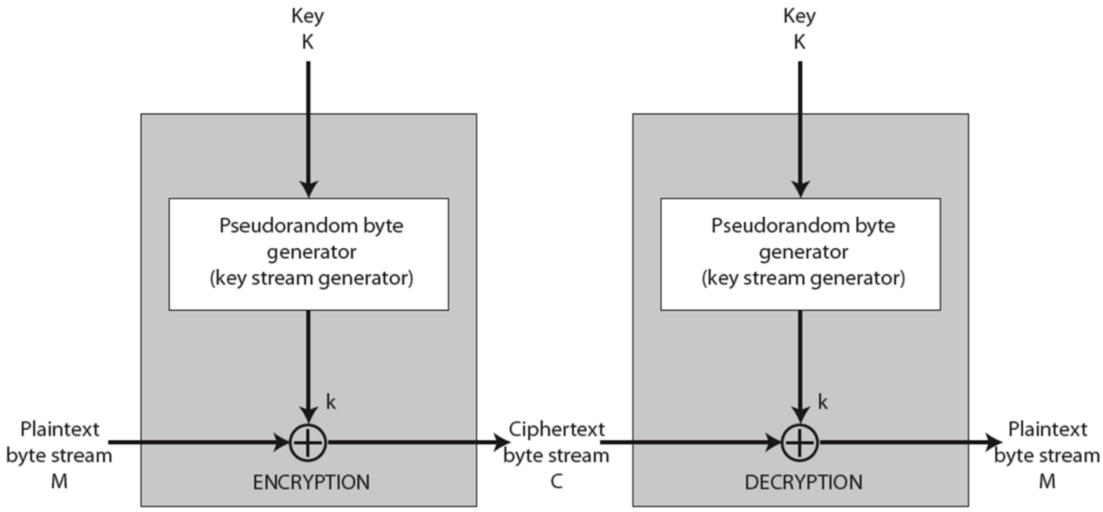
Pseudo Random Number Generator (PRNG)

Pseudo Random Number Generator(PRNG) refers to an algorithm that uses mathematical formulas to produce sequences of random numbers.

stream cipher

In stream cipher, one byte is encrypted at a time. combined (XOR) with plaintext bit by bit
while in block cipher ~128 bits are encrypted at a time.

Stream Cipher Structure

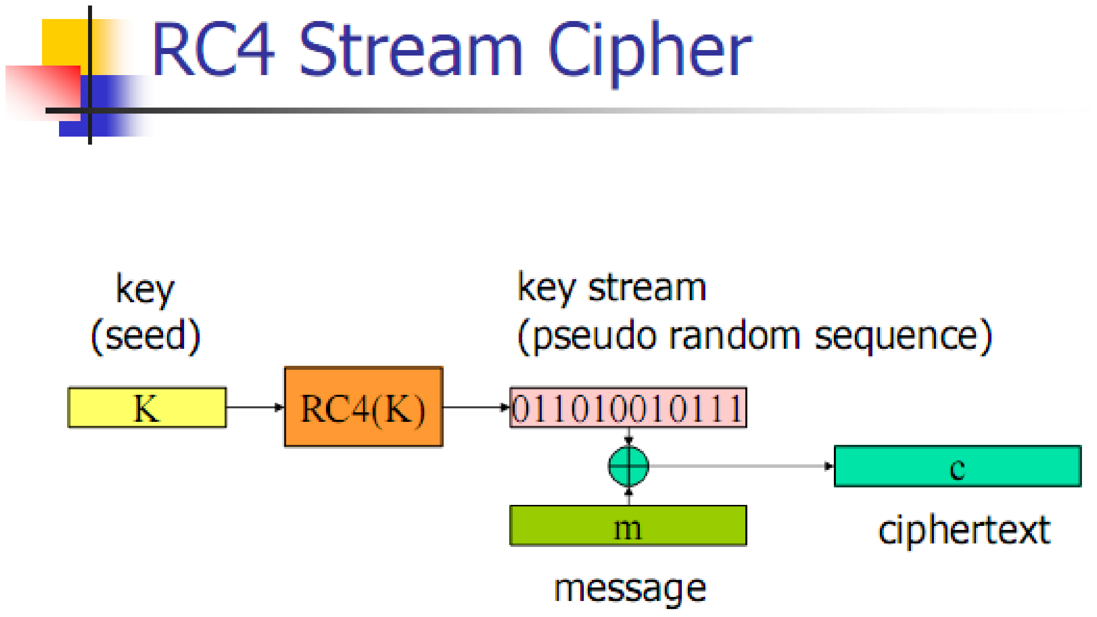

Key
K
Pseudorandom byte generator (key stream generator)
k
Plaintext byte stream M
ENCRYPTION
Ciphertext byte stream C
Key
K
Pseudorandom byte generator (key stream generator)
k
DECRYPTION
Plaintext byte stream M

RC4

RC4 is a stream cipher and variable-length key algorithm.
This algorithm encrypts one byte at a time (or larger units at a time). RC4 is a stream cipher, must never reuse a key

widely used (web SSL/TLS, wireless WEP/WPA)

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj



RC4 Stream Cipher

2. Public Key Infrastructure and Digital Signatures

Public Key Infrastructure (PKI) is that it uses a pair of keys to achieve the underlying security service. The key pair comprises private key and public key.

Public key infrastructure or PKI is the governing body behind issuing digital (certificates.Infrastructure = Certification Authorities)

Digital signatures are used to verify the identity of the sender and ensure that the received message or document has not been tampered with during transit.

Digital certificate contains (The authenticity)

- Name of certificate holder.
- Serial number which is used to uniquely identify a certificate,.
- Expiration dates.
- Copy of certificate holder’s public key.(used for decrypting messages and digital signatures)
- Digital Signature of the certificate issuing authority.

Ex - X.509 Certificates

Digital signature VS Digital certificate

Digital signature is used to verify authenticity, integrity, and non-repudiation . **Digital certificate** is used to verify the identity of the user, maybe sender or receiver.

Can Public Key Technology be used to perform Authentication and Access Control?

Sure Can, Using Digital Signatures and Digital Certificates

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

Secure Socket Layer (SSL) Protocol

Secure Socket Layer (SSL) is a Network Layer protocol used to secure data on TCP/IP networks.

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server.

Transport Layer Security (TLS) Protocol

Transport Layer Security (TLS) is designed to provide security at the transport layer. TLS ensures that no third party may eavesdrop or tamper with any message.

Authentication

Three Categories:

1. What you know

   - Password
   - Passphrase
   - PIN

2. What you have

   - Digital authentication
     - physical devices to aid authentication

     Common examples:
     - eToken

       On the client side, the token is accessed via password
       Successful client-side authentication with the password invokes the token to generate a stored or generated passcode, which is sent to the server-side for authentication.

       May store credentials such as passwords, digital signatures and certificates, and private keys

     - smart cards
     -

       Size of a credit card. Usually an embedded microprocessor with computational and storage capabilities.

       Programmable platforms:
       - C/C++
       - Visual Basic
       - Java
       - .Net (beta)

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

- RFID (Radio Frequency IDentification)
-

  Integrated circuit(s) with an antenna that can respond to an RF signal with identity information.No power supply necessary—IC uses the RF signal to power itself.13.56Mhz read/write support

  Examples:
  - Smart Tag, EZPass
  - Garage parking permits

3. Who you are

- Biometric authentication
  - Use of a biometric reading to confirm that a person is who he/she claims to be

    Ex - Fingerprint,Iris,DNA,Face Geometry

- Biometric reading
  - A recording of some physical or behavioral attribute of a person

Biometric Authentication Terms

- False Acceptance Rate (FAR)
- False Rejection Rate (FRR)
- Equal Error Rate

Authentication Token Formats

A security token (authentication token) is a representation of security-related data (not to be confused with an e-Token)

Examples:
- X.509 certificates (digital certificates)
- Kerberos tickets
- Custom security tokens

Remote authentication

Remote authentication allows users to authenticate to the system using credentials stored on an external authentication service.

Approaches
- Direct Dial-in
- Referer URL Authentication
- Authenticated Proxy-server

  Most often used to speed up Internet access and reduce bandwidth by caching frequently used pages

  Advantages
  - Can place database links anywhere
  - A single URL from the database vendor
  - Proxy servers scale better

Disadvantages

- Problems with auto-configuration proxy
- Problems with multiple proxy servers
- Problems with firewalls
- All traffic goes through proxy server (single point of failure)
- User has to manually configure and un-configure settings

★ Access Control

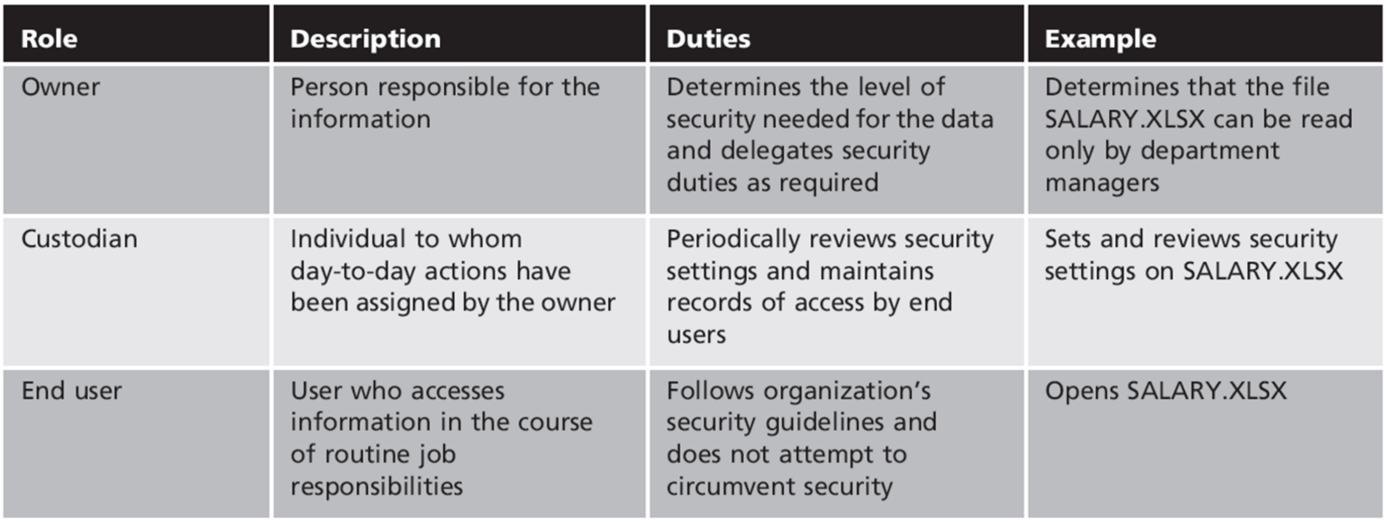
Access Control is a Granting or denying approval to use specific resources

Access Control Terminology

- Identification
  - Presenting credentials
  - Example: delivery driver presenting employee badge , user enter username

- Authentication
  - Checking the credentials
  - Example: examining the delivery driver’s badge, user provide password

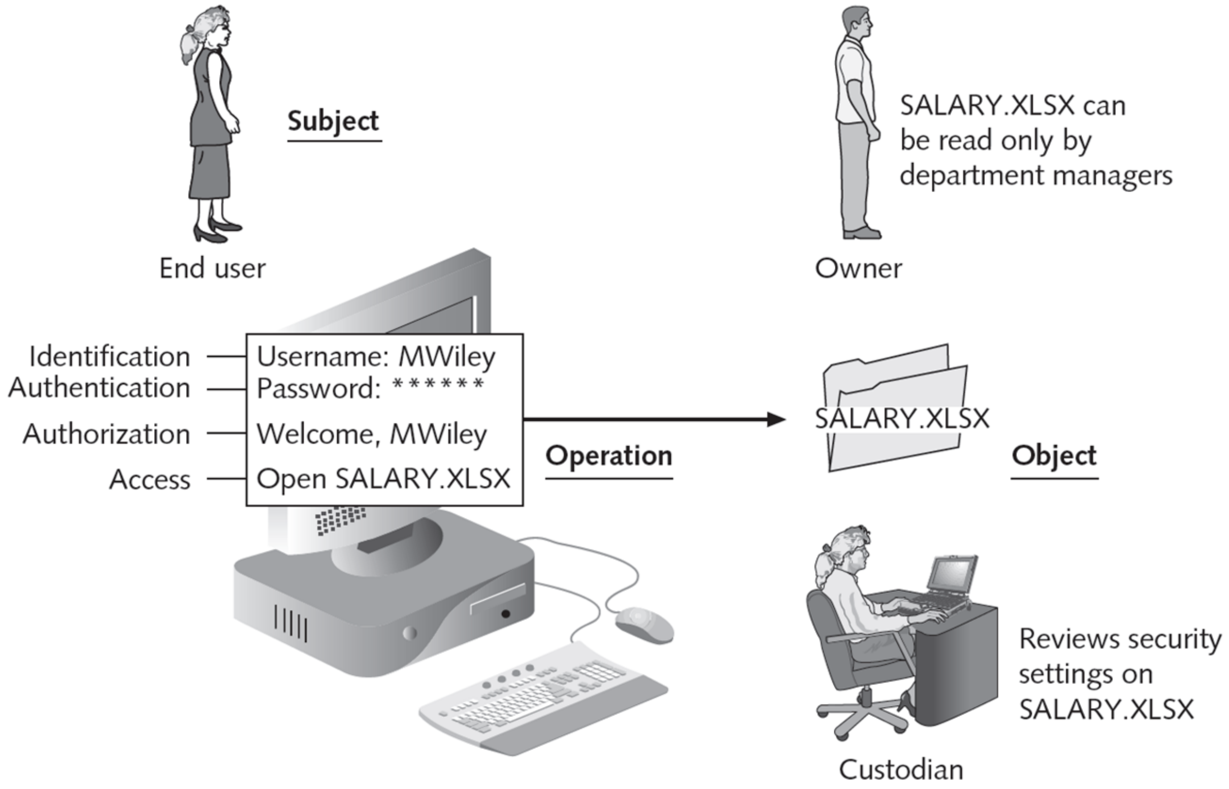
- Authorization
  - Granting permission to take action
  - Example: allowing delivery driver to pick up package, user authorized to the login



Role	Description	Duties	Example
Owner	Person responsible for the information	Determines the level of security needed for the data and delegates security duties as required	Determines that the file SALARY.XLSX can be read only by department managers
Custodian	Individual to whom day-to-day actions have been assigned by the owner	Periodically reviews security settings and maintains records of access by end users	Sets and reviews security settings on SALARY.XLSX
End user	User who accesses information in the course of routine job responsibilities	Follows organization’s security guidelines and does not attempt to circumvent security	Opens SALARY.XLSX

Access control process and terminology

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj



Access Control Models

Used to implement access control in a device or application
Custodians can configure security based on owner's requirements

Four major access control models,

1. Mandatory Access Control (MAC)
2. Discretionary Access Control (DAC)
3. Role Based Access Control (RBAC)
4. Rule Based Access Control (RBAC)

1. Mandatory Access Control (MAC)

Most restrictive access control model
Typically found in military settings

Two major implementations of MAC

- Lattice model
- Bell-LaPadula model

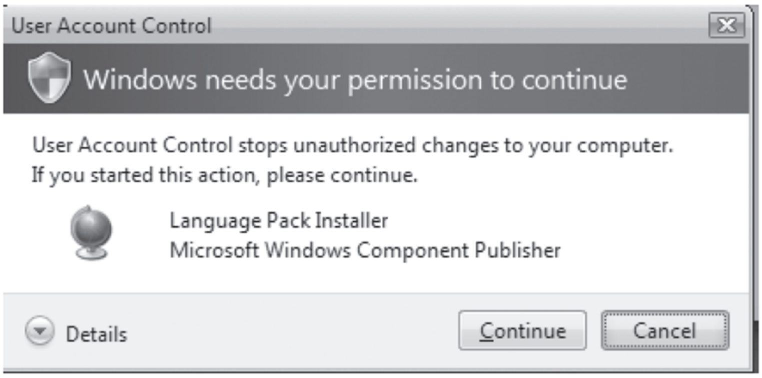
Example -

Windows 7/Vista has four security levels
Specific actions by a subject with lower classification require administrator approval

2. Discretionary Access Control (DAC)

Least restrictive model.
Every object has an owner.
Owners have total control over their objects.
Owners can give permissions to other subjects over their objects.

Example - Used on operating systems such as most types of UNIX and Microsoft Windows



User Account Control

Windows needs your permission to continue

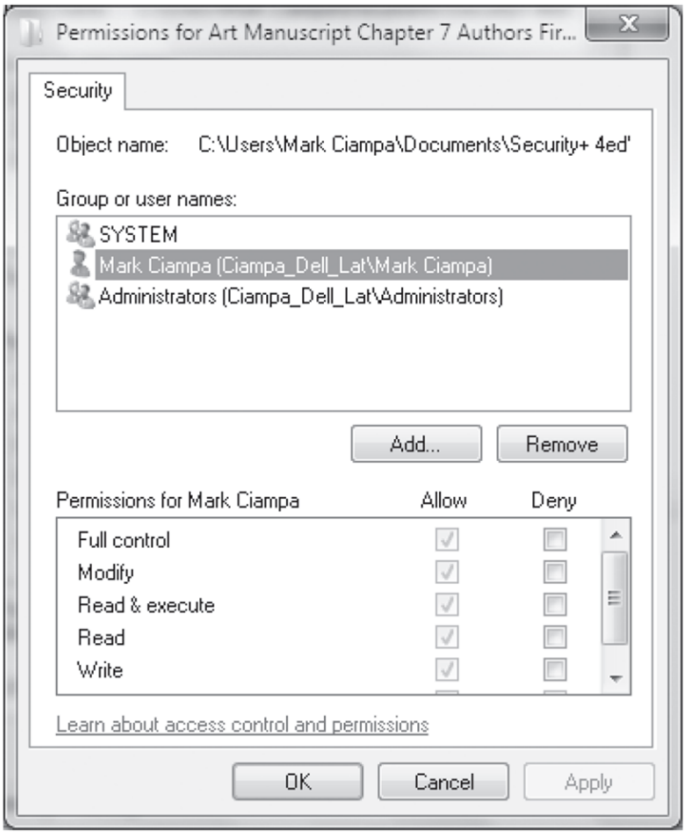
User Account Control stops unauthorized changes to your computer.
If you started this action, please continue.

Language Pack Installer
Microsoft Windows Component Publisher

DAC weaknesses

- Relies on decisions by end user to set proper security level
  - Incorrect permissions may be granted
- Subject's permissions will be "inherited" by any programs the subject executes
- Trojans are a particular problem with DAC

Discretionary Access Control (DAC)



Permissions for Art Manuscript Chapter 7 Authors Fir...

Security

Object name: C:\Users\Mark Ciampa\Documents\Security+ 4ed'

Group or user names:

SYSTEM
Mark Ciampa (Ciampa_Dell_Lat\Mark Ciampa)
Administrators (Ciampa_Dell_Lat\Administrators)

Permissions for Mark Ciampa	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
Read	☑	□
Write	☑	□

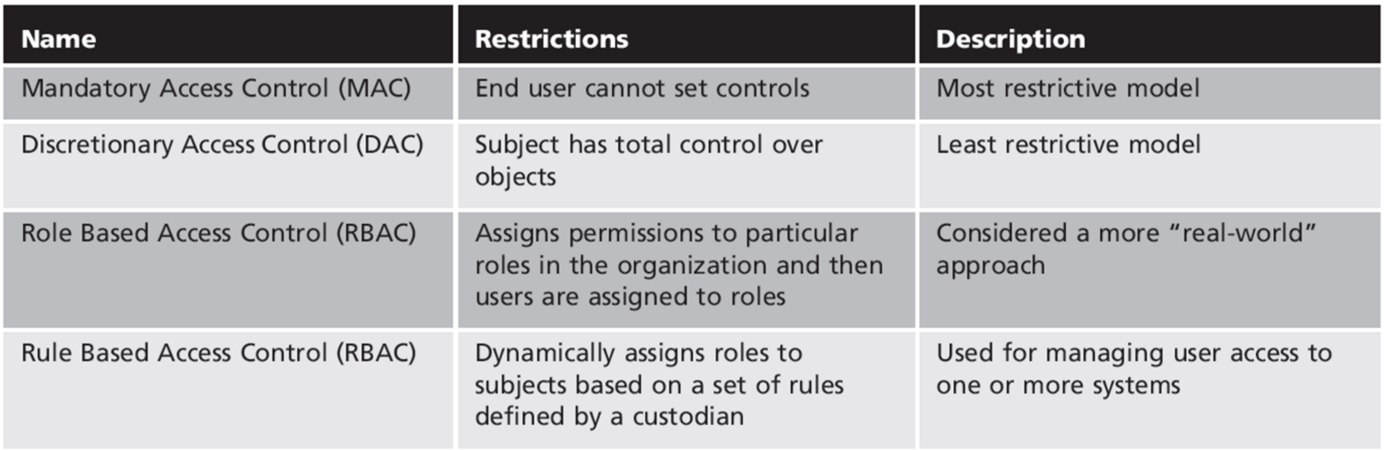
3. Role Based Access Control (RBAC)

Also called Non-discretionary Access Control
Access permissions are based on user's job function
RBAC assigns permissions to particular roles in an organization

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

4. Rule Based Access Control (RBAC)

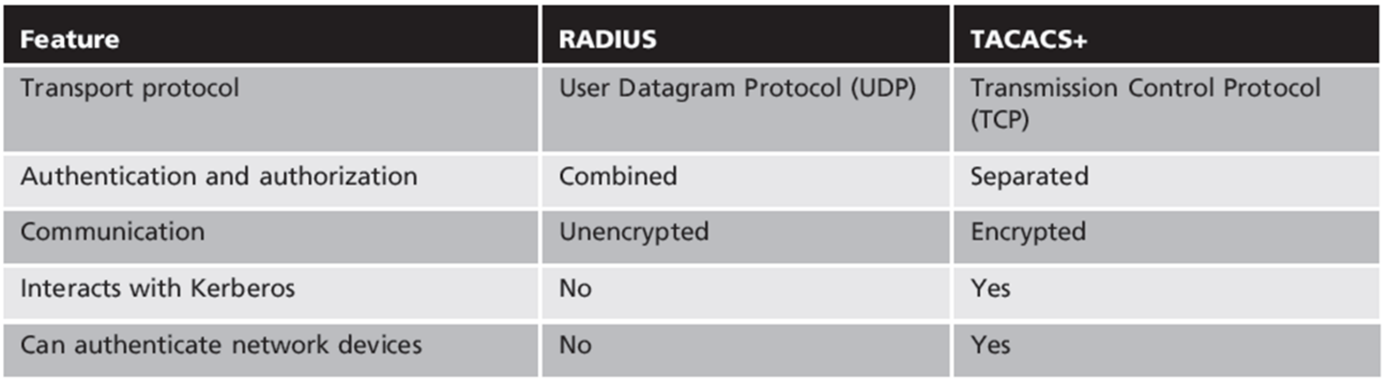
- Dynamically assigns roles to subjects based on a set of rules defined by a custodian
- Each resource object contains access properties based on the rules
- When user attempts access, system checks object's rules to determine access permission
- Often used for managing user access to one or more systems



Name	Restrictions	Description
Mandatory Access Control (MAC)	End user cannot set controls	Most restrictive model
Discretionary Access Control (DAC)	Subject has total control over objects	Least restrictive model
Role Based Access Control (RBAC)	Assigns permissions to particular roles in the organization and then users are assigned to roles	Considered a more "real-world" approach
Rule Based Access Control (RBAC)	Dynamically assigns roles to subjects based on a set of rules defined by a custodian	Used for managing user access to one or more systems

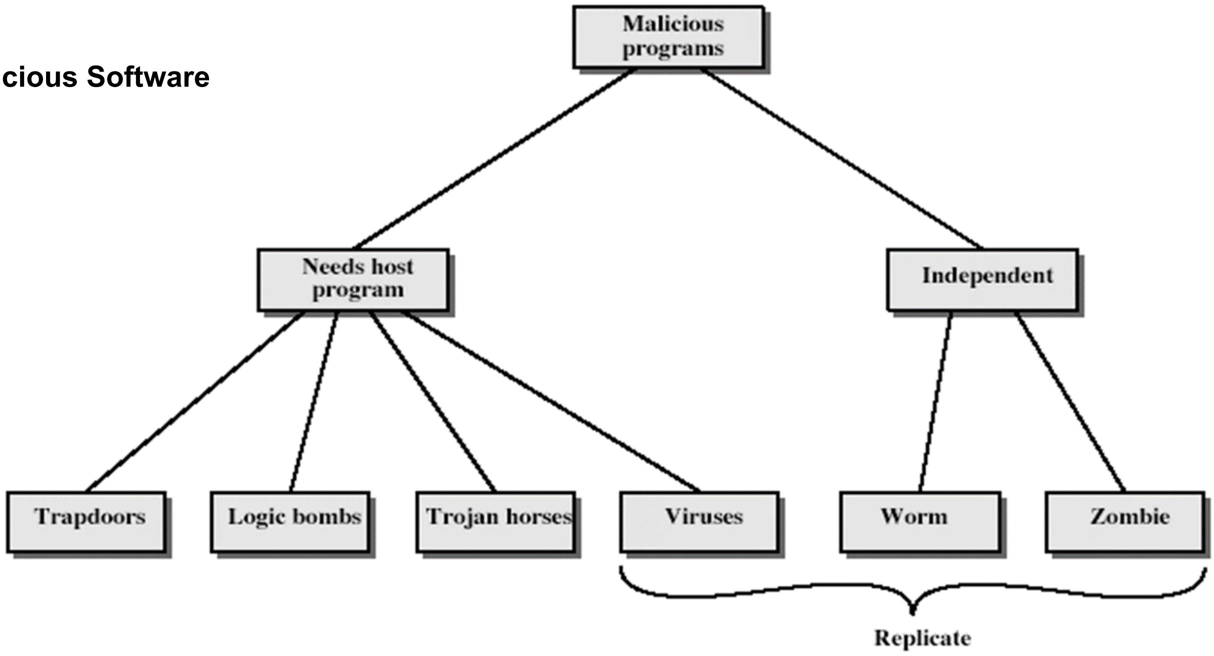
Common types of authentication and AAA servers

Kerberos, RADIUS, TACACS, LDAP



Feature	RADIUS	TACACS+
Transport protocol	User Datagram Protocol (UDP)	Transmission Control Protocol (TCP)
Authentication and authorization	Combined	Separated
Communication	Unencrypted	Encrypted
Interacts with Kerberos	No	Yes
Can authenticate network devices	No	Yes

★ Malicious Software



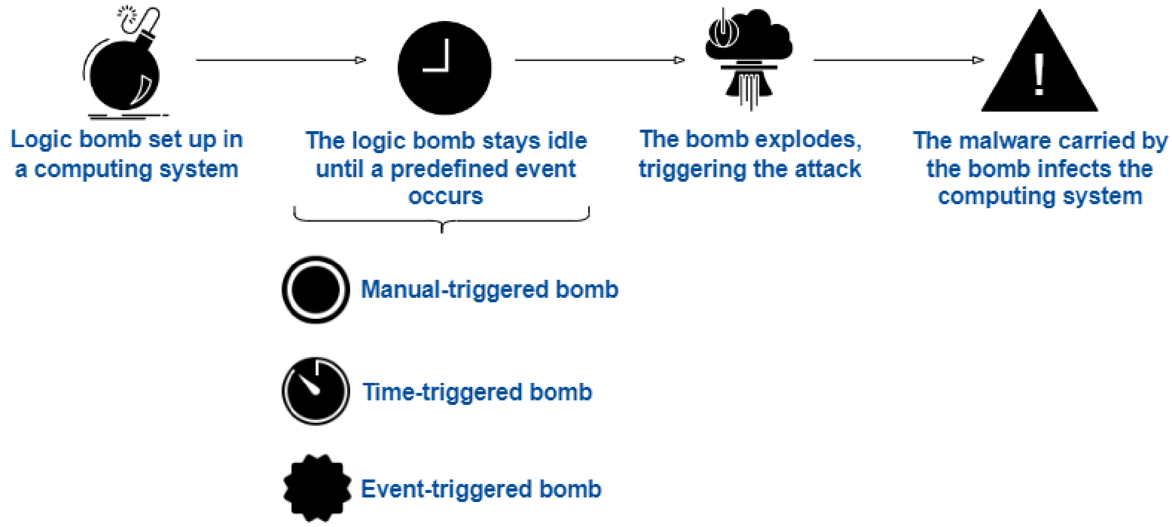
This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only)   Credit - Kanishka viraj

1. Trapdoors

- secret entry point into a program
- allows those who know access bypassing usual security procedures
- have been commonly used by developers
- a threat when left in production programs allowing exploited by attackers
- very hard to block in O/S
- requires good software development & update

2. Logic Bomb

- one of oldest types of malicious software
- code embedded in legitimate program
- activated when specified conditions met
    - eg presence/absence of some file
    - particular date/time
    - particular user
- when triggered typically damage system
- modify/delete files/disks


Logic bomb set up in a computing system
The logic bomb stays idle until a predefined event occurs
The bomb explodes, triggering the attack
The malware carried by the bomb infects the computing system
Manual-triggered bomb
Time-triggered bomb
Event-triggered bomb

3. Trojan Horse

- program with hidden side-effects
- which is usually superficially attractive
    - eg game, s/w upgrade etc
- when run performs some additional tasks
    - allows attacker to indirectly gain access they do not have directly
- often used to propagate a virus/worm or install a backdoor or simply to destroy data

4. Zombie

- program which secretly takes over another networked computer
- then uses it to indirectly launch attacks
- often used to launch distributed denial of service (DDoS) attacks
- exploits known flaws in network systems

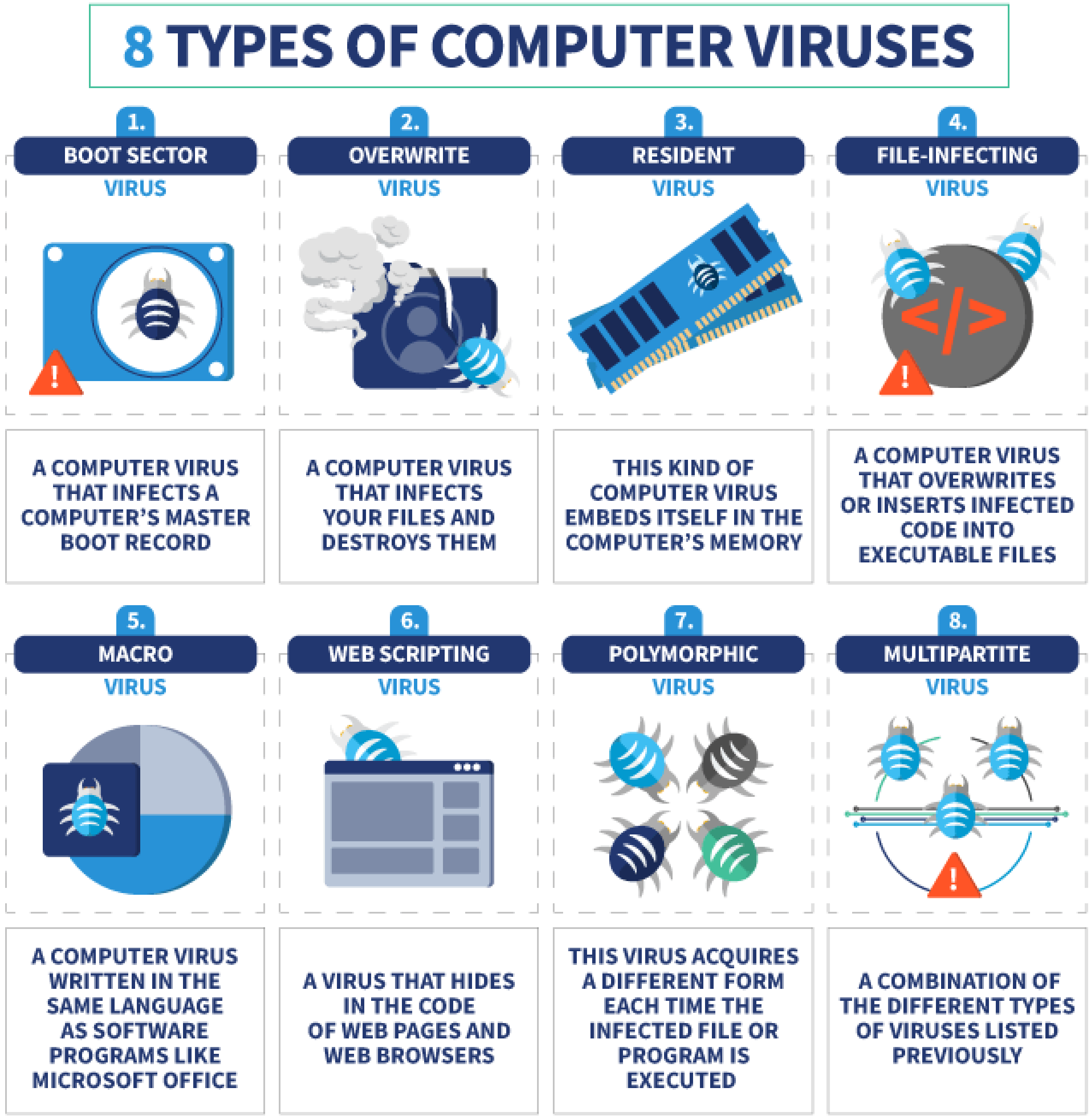
This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

5. Viruses

- a piece of self-replicating code attached to some other code
  - cf biological virus
- both propagates itself & carries a payload
  - carries code to make copies of itself.
  - as well as code to perform some covert task

Types of Viruses

can classify on basis of how they attack



8 TYPES OF COMPUTER VIRUSES

1. BOOT SECTOR VIRUS
A COMPUTER VIRUS THAT INFECTS A COMPUTER'S MASTER BOOT RECORD

2. OVERWRITE VIRUS
A COMPUTER VIRUS THAT INFECTS YOUR FILES AND DESTROYS THEM

3. RESIDENT VIRUS
THIS KIND OF COMPUTER VIRUS EMBEDS ITSELF IN THE COMPUTER'S MEMORY

4. FILE-INFECTING VIRUS
A COMPUTER VIRUS THAT OVERWRITES OR INSERTS INFECTED CODE INTO EXECUTABLE FILES

5. MACRO VIRUS
A COMPUTER VIRUS WRITTEN IN THE SAME LANGUAGE AS SOFTWARE PROGRAMS LIKE MICROSOFT OFFICE

6. WEB SCRIPTING VIRUS
A VIRUS THAT HIDES IN THE CODE OF WEB PAGES AND WEB BROWSERS

7. POLYMORPHIC VIRUS
THIS VIRUS ACQUIRES A DIFFERENT FORM EACH TIME THE INFECTED FILE OR PROGRAM IS EXECUTED

8. MULTIPARTITE VIRUS
A COMBINATION OF THE DIFFERENT TYPES OF VIRUSES LISTED PREVIOUSLY

1. parasitic virus - A Parasitic Virus (also referred to as a file virus) is a type of virus that spreads by attaching itself to another program

2. memory-resident virus - A Memory-Resident Virus is a virus that is located in the memory of a computer, even after the 'host' application or program has stopped running (been terminated).

This short note making resources are,google search engine,chat gpt and lecture slides
WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj

3. boot sector virus - A boot sector virus is a type of virus that infects the boot sector of floppy disks or the primary boot record of hard disks (some infect the boot sector of the hard disk instead of the primary boot record).

4. stealth - A stealth virus is a computer virus that uses various mechanisms to avoid detection by antivirus software.

5. Polymorphic virus - A polymorphic virus, sometimes referred to as a metamorphic virus, is a type of malware that is programmed to repeatedly mutate its appearance or signature files through new decryption routines.

6. Macro Virus

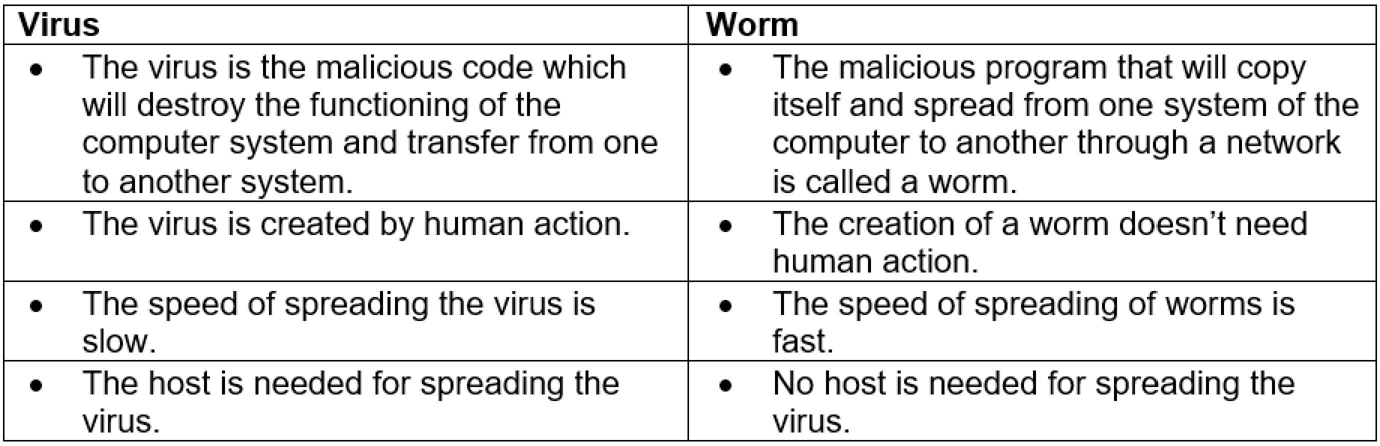
- macro code attached to some data file
- interpreted by program using file
    - eg Word/Excel macros
    - esp. using auto command & command macros
- code is now platform independent
- is a major source of new viral infections
- blurs distinction between data and program files making task of detection much harder

7. Email Virus

- spread using email with attachment containing a macro virus
    - cf Melissa
- triggered when user opens attachment or worse even when mail viewed by using scripting features in mail agent
- usually targeted at Microsoft Outlook mail agent & Word/Excel documents

6. Worms

- replicating but not infecting program
- typically spreads over a network
- using users distributed privileges or by exploiting system vulnerabilities
- widely used by hackers to create zombie PC's, subsequently used for further attacks, esp DoS
- major issue is lack of security of permanently connected systems, esp PC's



Virus	Worm
• The virus is the malicious code which will destroy the functioning of the computer system and transfer from one to another system.	• The malicious program that will copy itself and spread from one system of the computer to another through a network is called a worm.
• The virus is created by human action.	• The creation of a worm doesn't need human action.
• The speed of spreading the virus is slow.	• The speed of spreading of worms is fast.
• The host is needed for spreading the virus.	• No host is needed for spreading the virus.

★ Antivirus software

Antivirus software (antivirus program) is a security program designed to prevent, detect, search and remove viruses and other types of malware from computers.

★ Network Security

What Is “DoS Attack”

Denial-Of-Service Attack = DOS Attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to its customers.

DoS = when a single host attacks
DDoS = when multiple hosts attack simultaneously

Types of DoS Attacks

1. Penetration
2. Eavesdropping
3. Man-In-The-Middle
4. Flooding

1. Penetration

Attacker gets inside your machine
Can take over machine and do whatever he wants
Achieves entry via software flaw(s), stolen passwords or insider access

2. Eavesdropping

Attackers gain access to the same network.
Listen to traffic going in and out of your machine.

3. Man-in-the-Middle

Attacker listens to output and controls output
Can substitute messages in both directions

4. Flooding

- Attacker sends an overwhelming number of messages at your machine; great congestion
- The congestion may occur in the path before your machine
- Messages from legitimate users are crowded out
- Usually called a Denial of Service (DoS) attack, because that’s the effect.
- Usually involves a large number of machines, hence Distributed Denial of Service (DDoS) attack

Firewall

A firewall is a network security device that prevents unauthorized access to a network.
Two Types,

1. Packet Filters
2. Proxies

1. **Packet Filters**

Packet filter selectively passes packets from one network interface to another
Usually done within a router between external and internal networks

- screening router

Example filters

Block all packets from outside except for SMTP servers
Block all traffic to a list of domains
Block all connections from a specified domain

2. **Proxies**

A proxy server is a system or router that provides a gateway between users and the internet.

Advantages

Better policy enforcement
Better logging
Fail closed

Disadvantages

Doesn't perform as well
One proxy for each application
Client modification

Traffic to the legitimate hosts/services can have attacks, any Solution?

1. Intrusion Detection Systems
2. Monitor data and behavior
3. Report when identify attacks

1. **Intrusion Detection Systems**
A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed.

It is software that checks a network or system for malicious activities or policy violations.
Types of IDS

1. Signature-based
2. Anomaly-based
3. Host-based
4. Network-based

1. **Signature-based**

   Uses known pattern matching to signify attack

   Advantages
   - Widely available
   - Fairly fast
   - Easy to implement
   - Easy to update

   Disadvantages
   - Cannot detect attacks for which it has no signature

2. **Anomaly-based**

   Uses statistical model or machine learning engine to characterize normal usage behaviors

   Recognizes departures from normal as potential intrusions

   Advantages
   - Can detect attempts to exploit new and unforeseen vulnerabilities
   - Can recognize authorized usage that falls outside the normal pattern

   Disadvantages
   - Generally slower, more resource intensive compared to signature-based IDS
   - Greater complexity, difficult to configure
   - Higher percentages of false alerts

3. **Network-based**

   NIDS examine raw packets in the network passively and triggers alerts

   Advantages
   - Easy deployment
   - Unobtrusive
   - Difficult to evade if done at low level of network operation

   Disadvantages
   - Fail Open
   - Different hosts process packets differently
   - NIDS needs to create traffic seen at the end host
   - Need to have the complete network topology and complete host behavior

IP fragmentation attacks

IP fragmentation attacks is a type of cyber attack that exploits how IP packets are fragmented and reassembled to evade security controls and launch attacks.

Attackers manipulate fragmented packet parameters like offsets and sizes to trigger vulnerabilities or bypass firewall rules.

IP fragmentation occurs when an IP packet exceeds the Maximum Transmission Unit (MTU) size for a network path. Routers must split the large packet into smaller fragments to be transmitted.

TCP / IP attacks

TCP/IP attacks are malicious attempts to disrupt, hijack, or damage network communications that use the TCP/IP protocol suite.

IP Spoofing

IP address spoofing involves maliciously creating TCP/IP packets using other IP address as source address with the aim to either conceal own identity or impersonate the identity of the owner of the IP address used

Connection Hijacking

Connection hijacking is a cyber attack where someone intercepts and takes control of an ongoing communication between two parties.

★ Web Security

Web application security is the practice of protecting websites, applications, and APIs from attacks.

1. Cross-site scripting (XSS)

Cross-site scripting (XSS) is an exploit where the attacker attaches code onto a legitimate website that will execute when the victim loads the website.

2. SQL injection

SQL Injection is a code-based vulnerability that allows an attacker to read and access sensitive data from the database.

3. Denial-of-Service (DoS)

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

Buffer overflow is an anomaly that occurs when software writing data to a defined space in memory known as a buffer.

Overflowing the buffer’s capacity results in adjacent memory locations being overwritten with data.

This behavior can be exploited to inject malicious code into memory,

4. Buffer overflow

- Buffer overflow is an anomaly that occurs when software writes data to a defined space in memory known as a buffer.

- Overflowing the buffer’s capacity results in adjacent memory locations being overwritten with data.

- This behavior can be exploited to inject malicious code into memory,

5. Virtual Private Network (VPN)

VPNs are private data networks over public networks – usually the Internet.

A Virtual Private Network (VPN) is a tool that creates a secure, encrypted connection over the internet, allowing users to browse privately, access restricted content, and enhance online security.

6. XML encryption

XML encryption is a security mechanism that assures the data confidentiality of transmitted messages

★ Electronic Mail Security

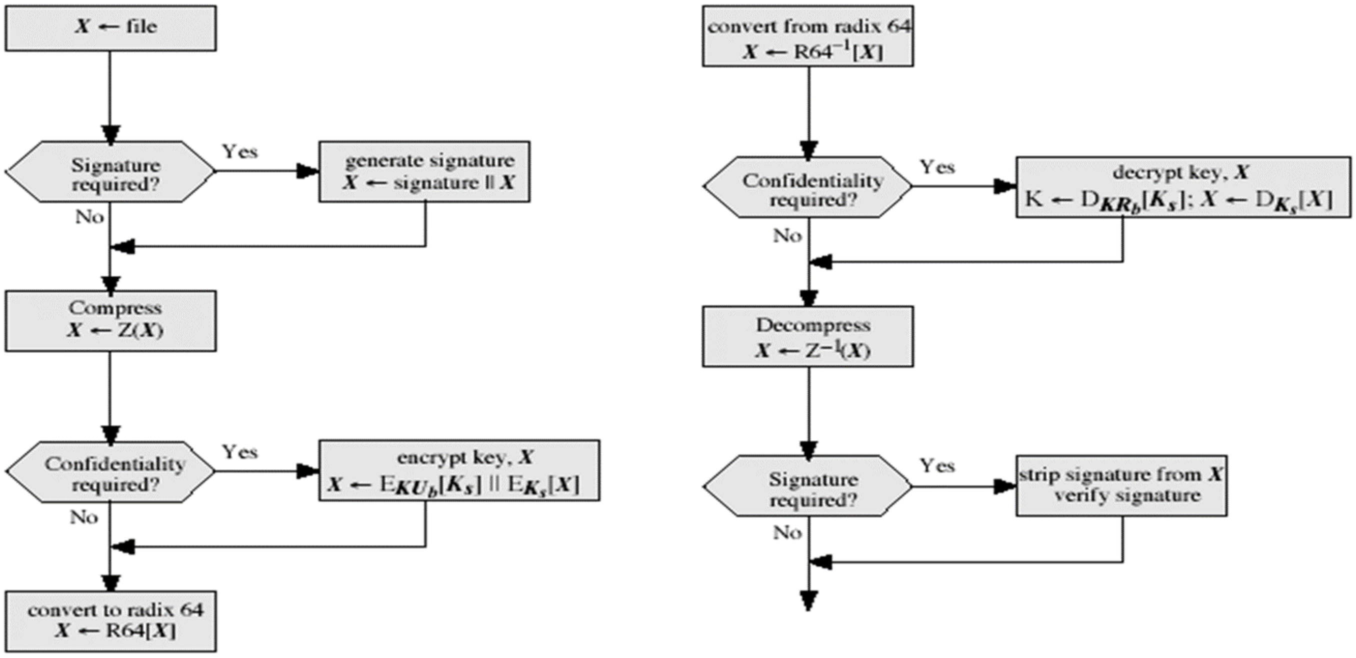
Pretty Good Privacy (PGP)

widely used de facto secure email
selected best available crypto algos to use
integrated into a single program

- available on Unix, PC, Macintosh and Amiga systems

PGP Operation – Authentication

1. sender creates a message
2. SHA-1 used to generate 160-bit hash code of message
3. hash code is encrypted with RSA using the sender's private key, and result is attached to message
4. receiver uses RSA or DSS with sender's public key to decrypt and recover hash code
5. receiver generates new hash code for message and compares with decrypted hash code, if match, message is accepted as authentic



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

This short note making resources are,google search engine,chat gpt and lecture slides

WhatsApp group (click on this/new syllabus notes only) Credit - Kanishka viraj