MODULE 1:

COMPUTER SECURITY

- The Computer Security can be defined as the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of Information system resources- NIST.

SECURITY ATTACK

- A THREAT is a potential for violation of security,which exits when there is a circumstance, capability,action or event that could breach security and cause harm.
- **An ATTACK** is an assault on system that derives from an intelligent threat that is an intelligent act that is a deliberate attempt to evade security and violate the security policy of a system.
- ATTACK is any action that compromises the security of information owned by an organization.
- Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems.
- Often threat & attack used to mean same thing. There is wide range of attacks & we can focus of generic types of attacks
- Passive Attacks
- Active Attacks

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.

Two types of passive attacks are the **release of message contents** and **traffic analysis.**

Passive attacks are very difficult to detect, because they do not involve any alteration of the data.

However, it is feasible to prevent the success of these attacks, usually by means of encryption.

Release of Message Content:

- The release of message contents is a type of attack that analyzes and read the message delivered between senders toreceiver.
- This attacker happens when confidential user data are released publicly over the network. Here,

Traffic Analysis: Under this the data transmission patterns are studied and trying to extract the original hidden data.

Active attack involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

- **A Masquerade** takes place when one entity pretends to be a different entity.Masquerade is a type of cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data. This can involve impersonating a legitimate user or system
- **Replay** involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.In this attack, the attacker can save a copy of the data

- **Modification** of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
- Denial of Service (DoS) is a type of cybersecurity attack that is designed to make a system or network unavailable to its intended users by overwhelming it with traffic or requests.
- In a DoS attack, an attacker floods a target system or network with traffic or requests in order to consume its resources, such as bandwidth, CPU cycles, or memory, and prevent legitimate users from accessing it.

SECURITY SERVICES

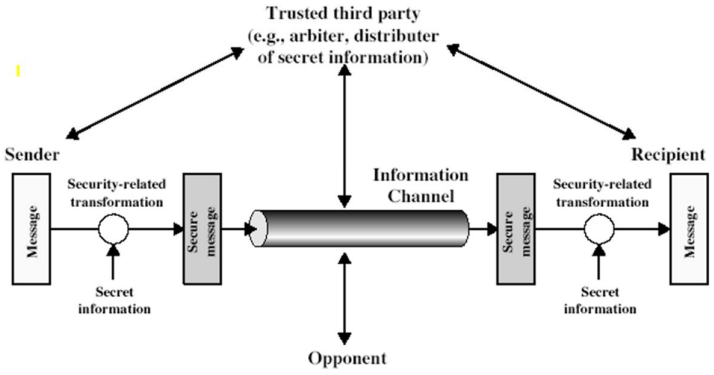
X.800:

"a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers"

RFC 2828:

"a processing or communication service provided by a system to give a specific kind of protection to system resources"

NETWORK SECURITY MODEL



SYMMETRIC ENCRYPTION	ASYMMETRIC ENCRYPTION
Method of using the same cryptographic keys for both encryptions of plaintext and decryption of ciphertext	Method of using a pair of keys: the public key, which is disseminated widely, and a private key, which is known only to the owner
Simple since only one key used in both operations	More complex as it uses separate keys for both operations
Has a faster execution speed	Comparatively slower
RC4, AES, DES, 3DES are some common algorithms	Diffie-Hellman and RSA algorithm are some common algorithms

CLASSICAL ENCRYPTION TECHNIQUES

The two basic building blocks of all encryption techniques are **Substitution** and **Transposition.**

- **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 ciphertext bit patterns.
- **A different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.**

CAESAR CIPHER

- The earliest known, and the simplest, use of a substitution cipher was by Julius Caesar.
- The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

==========

- The Playfair algorithm is based on the use of a 5 * 5 matrix of letters constructed using a keyword. Here is an example

VIGENERE CIPHER

- The best known, and one of the simplest, polyalphabetic ciphers is the Vigenère cipher.
- In this scheme, the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25.
- Thus, the first letter of the key is added to the first letter of the plaintext, mod 26, the second letters are added, and so on through the first m letters of the plaintext.
- For the next m letters of the plaintext, the key letters are repeated. This

RAIL FENCE CIPHER

- The simplest such cipher is the Rail Fence technique, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.
- It is also known as Keyless Transposition Cipher
- For example, to encipher the message “meet me after the toga party” with a rail fence of depth 2, we write the following:

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

- The encrypted message is MEMATRHTGPRYETEFETEOAAT

STEGANOGRAPHY

- A plaintext message may be hidden in one of two ways. The methods of steganography conceal the existence of the message, whereas the methods of cryptography render the message unintelligible to outsiders by various transformations of the text.
- A simple form of steganography, but one that is time-consuming to construct, is one in which an arrangement of words or letters within an apparently innocuous text spells out the real message.
- Various other techniques have been used historically; some examples are the following:

■ Character marking: Selected letters of printed or typewritten text are overwritten in pencil. The marks are ordinarily not visible unless the paper is held at an angle to bright light.

■ Invisible ink: A number of substances can be used for writing but leave no visible trace until heat or some chemical is applied to the paper.

■ Pin punctures: Small pin punctures on selected letters are ordinarily not visible unless the paper is held up in front of a light.

****

MODULE 2:

Stream Cipher	Block Cipher
Stream cipher operates on smaller Units of Plaintext	Block cipher operates on larger block of data
Faster than block cipher	Slower than Stream Cipher
Stream cipher processes the input element continuously producing output one element at a time	Block cipher processes the input one block of element at a time, producing an output block for each input block
Require less code	Requires more code
Only one time of key used.	Reuse of key is possible
Ex: One time pad	Ex: DES (Data Encryption Standard)
Application: SSL (secure connection on the web)	Application: Database, file encryption.
Stream cipher is more suitable for hardware implementation	Easier to implement in software.

DATA ENCRYPTION STANDARD

- The Data Encryption Standard (DES) was the most widely used encryption scheme. DES was issued in 1977 by the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard.
- It is a Symmetric Block Cipher.
- The algorithm is also referred to as the Data Encryption Algorithm (DEA).
- It was redundant after the invasion of Advanced Encryption Standard (AES) in 2001.
- For DES, data are encrypted in 64-bit blocks using a 56-bit key. The algorithm transforms 64-bit input in a series of steps into a 64-bit output. The same steps, with the same key, are used to reverse the encryption.

- The purpose of a digital signature is thus for an entity to **bind its identity to a message.**
- We use the term **signer** for an entity who creates a digital signature, and the term **verifier** for an entity who receives a signed message and attempts to check whether the digital signature is "correct" or not.

DES (Data Encryption Standard):

- DES is an older encryption algorithm that was developed in the 1970s.
- It uses a symmetric key, meaning the same key is used for both encryption and decryption.
- DES operates on 64-bit blocks of data and uses a 56-bit key.
- Over time, DES has been found to have security vulnerabilities due to its short key length, making it susceptible to brute force attacks. In the modern computing environment, it is not considered secure for most applications.
- Triple DES (3DES) is a variant of DES that applies the DES algorithm three times with different keys, making it more secure but still less secure than modern alternatives.

Working:

=Key Generation: DES uses a 56-bit key, but it actually starts with a 64-bit key

=Initial Permutation: rearranges the bits in a specific order.

=Fiestal Network:

- DES uses a Feistel network structure, which means that the data block is divided into two 32-bit halves (left and right). The left and right halves go through a series of rounds (16 rounds in the case of DES) in which they are subjected to a combination of bitwise operations, including expansion, substitution, permutation, and XOR.
- The right half is expanded to 48 bits and then combined with one of the 16 subkeys. This result is then passed through a substitution (S-box) operation, which provides non-linearity to the algorithm.
- After substitution, the 32-bit result is permuted.
- The output of each round is used as input to the next round.

=final permutation: After completing all 16 rounds, the left and right halves are swapped.

=Output: The final output of the Feistel network is the ciphertext, which is a 64-bit block.

=Decryption: The decryption process in DES is essentially the reverse of encryption.

AES (Advanced Encryption Standard):

- AES is a more modern and secure encryption algorithm.
- It was established as the standard encryption algorithm by the U.S. National Institute of Standards and Technology (NIST) in 2001.
- AES also uses a symmetric key, but it supports key lengths of 128, 192, or 256 bits, providing a higher level of security.
- AES operates on 128-bit blocks of data and can use one of the three key lengths mentioned above, with longer keys providing stronger security.
- AES is widely used in various applications, including secure communications, data encryption, and encryption of data at rest. It is considered very secure and is not vulnerable to brute force attacks when used with a sufficient key length.

Working

=Key Expansion: AES starts with a secret key that can be 128, 192, or 256 bits in length.

=Initial Round: AES begins with an initial round of transformations. The plaintext is divided into a 4x4 matrix (a 2D array of bytes).

=Rounds:

In each round, the following operations are performed on the 4x4 matrix:

SubBytes: Each byte is replaced with a corresponding byte from an S-box lookup table. This step adds non-linearity to the encryption.

ShiftRows: Bytes within each row of the matrix are shifted by different offsets.

MixColumns: Columns of the matrix are mixed using a mathematical transformation.

AddRoundKey: The round key for the current round is XORed with the matrix.

=Output:

After the final round, the 4x4 matrix represents the ciphertext.

=Decryption:

The ciphertext is subjected to a series of transformations in reverse order, using the same round keys but in reverse order.

RSA ALGORITHM:

Key generation:

- generates a pair of keys: a public key and a private key.
- The public key is used for encryption and is shared openly, while the private key is kept secret and is used for decryption or signing.

Encryption:

- To encrypt a message (plaintext), the sender uses the recipient's public key.
- The sender converts the plaintext into a numerical value M.
- The sender calculates the ciphertext C as C ≡ M^e (mod n)

Decryption:

- To decrypt the ciphertext, the recipient uses their private key.
- The recipient calculates the original numerical value M as M ≡ C^d (mod n).

p q =>prime numbers

e=>public key :(e,n)

d=>private key :(d,n)

n=p*q

Ø(n)=(p-1)*(q-1)

de=1

de=1+k(Ø(n)

put values of k to get an integer not a decimal

encryption: c=m^e mod n

decryption: m=c^d mod n

RSA Digital Signature Scheme

It is the most popular asymmetric cryptographic algorithm. It is primarily used for encrypting messages but can also be used for performing digital signature over a message. Let us

KERBEROS

- Kerberos is a protocol for authenticating service requests between trusted hosts across an untrusted network, such as the internet. Kerberos support is built in to all major computer operating systems, including Microsoft Windows, Apple macOS, FreeBSD and Linux.
- Since Windows 2000, Microsoft has used the Kerberos protocol as the default authentication method in Windows, and it is an integral part of the Windows Active Directory (AD) service. Broadband service providers also use the protocol to authenticate cable modems and set-top boxes accessing their networks.
- Kerberos was developed for Project Athena at the Massachusetts Institute of Technology (MIT). The name was taken from Greek mythology; Kerberos (Cerberus) was a three-headed dog who guarded the gates of Hades. The three heads of the Kerberos protocol represent the following:\

1. the client or principal;
2. the network resource, which is the application server that provides access to the network resource;
3. a key distribution center (KDC), which acts as Kerberos' trusted third-party authentication service

	HMAC	CMAC
Fullform	Hash-based msg authentication code	Cipher-based msg authentication code
Functionality	for creating a MAC (Message Authentication Code	creating a MAC, similar to HMAC, but it operates in combination with a block cipher instead of a cryptographic hash function.
Components	Cryptographic hash function (such as SHA-256, SHA-3, or MD5)	a block cipher algorithm (such as AES)
Use case	used in various security protocols, including TLS (Transport Layer Security)	such as disk encryption

MODULE 3:

Malicious Software

- Malware is short form for malicious software.
- It is a software used or created to disrupt computer operation, gather sensitive information, or gain access to private computer systems.
- It can appear in the form of code, scripts, active content, and other software.
- Malware' is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software.
- Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others. Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general. However, malware is often used against individuals to gain personal information such as social security numbers, bank or credit card numbers, and so on.

Terminology related to Malware

- Installation: How the malware reaches the system eg: attachments
- Detection and Removal: How the malware's presence can be detected rf: Antivirus, Antimalware.
- Payload: Actual function that the malware performs eg: Deletion of files.
- Trigger: Event that invokes the malware eg: clicking a file.
- Replication: Capability of the malware to further replicate or copy itself and infect other systems.
- Eradication: The malware might remove itself after delivering payload.

VIRUSES

- A computer virus is a type of malicious software, or malware, that spreads between computers and causes damage to data and software.
- Computer viruses aim to disrupt systems, cause major operational issues, and result in data loss and leakage.
- A key thing to know about computer viruses is that they are designed to spread across programs and systems.
- Computer viruses typically attach to an executable host file, which results in their viral codes executing when a file is opened.

SYMPTOMS OF INFECTION

Given below are such signs which may help you identify computer viruses:

- **Speed of the System –** In case a virus is completely executed into your device, the time taken to open applications may become longer and the entire system processing may start working slowly
- **Pop-up Windows –** One may start getting too many pop up windows on their screen which may be virus affected and harm the device even more
- **Self Execution of Programs –** Files or applications may start opening in the background of the system by themselves and you may not even know about them
- **Log out from Accounts –** In case of a virus attack, the probability of accounts getting hacked increase and password protected sites may also get hacked and you might get logged out from all of them
- **Crashing of the Device –** In most cases, if the virus spreads in maximum files and programs, there are chances that the entire device may crash and stop working

TYPES OF VIRUSES

Nw, Browser, File, Macro

Resident Virus: Viruses propagate the
resident virus achieves this by infecting
virus is capable of infecting executable fil

Multipartite Virus: A multipartite vir
computers. It will typically remain in the
through and infect more drives by alteri
lag and application memory running l
attachments from untrusted sources anc

Direct Action: A direct action virus acce

WORM

- A worm refers to a malicious program that replicates itself, automatically spreading through a network. In this definition of computer worms, the worm exploits vulnerabilities in your security software to steal sensitive information, install backdoors that can be used to access the system, corrupt files, and do other kinds of harm.
- Worms consume large volumes of memory, as well as bandwidth. This results in servers, individual systems, and networks getting overloaded and malfunctioning. A worm is different from a virus, however, because a worm can operate on its own while a virus needs a host computer.
- It works on law of exponential growth.
- To get a worm in a computer, the worm is often transmitted through vulnerabilities in software. They could also be sent through email attachments or within instant messages or spam emails. After a file is opened, it may link the user to a malicious website or it could download the worm to the user's device automatically.

Steps for Worm Mitigation

Step 1: Containment: The first step in mitigating a worm attack is to move swiftly to contain the spread of the worm and determine which machines are infected, and whether these devices are patched or unpatched. Infected machines must be isolated from machines that are not yet infected.

Step 2: Inoculation: Once it is clear which parts of the network the worm has infected, and those parts have been contained, other vulnerable systems must be scanned and patched. Patching the vulnerabilities the worm is using to spread will help contain the attack.

Step 3: Quarantine: In this third step of worm mitigation, infected machines are isolated and then disconnected and removed from the network. If removal is not possible, then the infected machines need to be blocked from connecting to and accessing the network.

Step 4: Treat: This last step in the worm mitigation process involves remediating from the attack as well as addressing any other necessary patching of machines and systems. Depending on the severity of the attack, infected systems may need to be reinstalled entirely to ensure a thorough cleanup from the event.

Types of Worm

Email-Worm: An email-worr
to email messages.

IM-Worm: An Instant Messe
an IM-worm is operating, it
copy of itself to all of the per

Net-Worm: A net-worm ref
network. This is done using
(LAN).

P2P-Worm: A P2P-worm is s
copies of itself to users.

SPAM

- Spam email is unsolicited and unwanted junk email sent out in bulk to an indiscriminate recipient list. Typically, spam is sent for commercial purposes. It can be sent in massive volume by botnets, networks of infected computers.
- The classic definition of spam is unsolicited bulk messages, that is, messages sent to multiple recipients who did not ask for them.
- Often, spam email is sent for commercial purposes. While some people view it as unethical, many businesses still use spam. The cost per email is incredibly low, and businesses can send out mass quantities consistently. Spam email can also be a malicious attempt to gain access to your computer.
- The original impetus for spam was advertising. Some spam also does non-commercial advertising. There has always been a modest amount of religious spam, and surges of political spam before elections.
- The other major use of spam is phishing, impersonating a trusted party to steal the victim's credentials. Phish spam often pretends to be from banks, ISPs, or mail providers, telling victims to confirm or update their accounts

TYPES OF SPAMS

- **Commercial advertisements:** States it's subject to the guideli often subscribe you to their ne out an online form, look for a c most are harmless, and by law continue to receive spam, upda inbox.
- **Antivirus warnings:** Ironically, computer virus infection and o the bait and clicking the link ca you suspect that your compute cybersecurity software solutior
- **Sweepstakes winners:** Spamr They urge you to respond quicl information. If you don't recog or reply with any personal deta

TYPES OF SPAMS

- **Money scams:** Unfortunatel emails asking for help in dire emergency or a tragic life eve you just send your bank acc personal information or send
- **Email spoofing:** Why are phi legitimate corporate messag victims will trust, such as a b you reply or click anything, c

A simple way to answer the question "what is Trojan" is it is a type of malware that typically gets hidden as an attachment in an email or a free-to-download file, then transfers onto the user's device. Once downloaded, the malicious code will execute the task the attacker designed it for, such as gain backdoor access to corporate systems, spy on users' online activity, or steal sensitive data. Indications of a Trojan being active on a device include unusual activity such as computer settings being changed unexpectedly.

TYPES OF TROJANS

- **Backdoor Trojan**: A backdoor Trojan enables control of it using a backdoor. This enables the r deleting files, rebooting the computer, stealing used to create a botnet through a network of zo
- **Banker Trojan**: A banker Trojan is designed t attempts to steal account data for credit and del
- **Distributed denial-of-service (DDoS) Trojan** network with traffic. It will send multiple reque target web address and cause a denial of service
- **Downloader Trojan**: A downloader Trojan targe downloads and installs more malicious progra malware like adware.
- **Mailfinder Trojan**: A mailfinder Trojan aims to computer.
- **Ransom Trojan**: Ransom Trojans seek to impair the user can no longer access or use it. The att pay a ransom fee to undo the device damage or

LOGIC BOMBS

- A logic bomb is a malicious piece of code that's secretly inserted into a computer network, operating system, or software application. It lies dormant until a specific condition occurs.
- When this condition is met, the logic bomb is triggered.

Characteristics of a logic bomb virus

- **It lies dormant for a specific amount of time**
- **Its payload is unknown until it triggers**
- **It's triggered by a certain condition**

PHISHING

- Phishing is an attack in which the threat actor poses as a trusted person or organization to trick potential victims into sharing sensitive information or sending them money.
- As with real fishing, there's more than one way to reel in a victim: Email phishing, smishing, and vishing are three common types.

How the attack works:

- The phisher begins by **determining who their targeted victims will be** (whether at an organization or individual level) and creates strategies to collect data they can use to attack.
- Next, the phisher will create **methods like fake emails or phony web pages to send messages** that lure data from their victims.
- Phishers then send messages that appear **trustworthy** to the victims and begin the attack.
- Once the attack has been deployed, phishers will **monitor and collect the data** that victims provide on the fake web pages.
- Finally, phishers use the collected data to make illegal purchases or **commit fraudulent acts**..

TYPES OF PHISHING

- **Email phishing**
  The most common form of phishin
  recipients into sharing their persor
  provider like Microsoft or Google, c
- **Spear phishing**
  Where most phishing attacks cast a
  information gathered through rese
  customized, making them particula
- **Smishing**
  A combination of the words "SMS"
  trustworthy communications from
  SMS scams, as text messages are d
- **Vishing**
  In vishing campaigns, attackers in f
  information over the phone. In ma
  installing malware onto their devic
- **Whaling**

Zombies

- In computing, a zombie is a computer connected to a network that has been compromised by a hacker, a virus or a Trojan. It can be used remotely for malicious tasks.
- Most owners of zombie computers do not realize that their system is being used in this way, hence the comparison with the living dead.
- Zombies are frequently used in denial-of-service attacks (DDoS), which refers to the saturation of websites with a multitude of computers accessing at the same time. As so many users are making requests at the same time to the server hosting the Web page, the server crashes, denying access to genuine users.