MCA 205B: Cyber Security

UNIT - II

[Pick the date]

KMM INSTITUTE OF POST GRADUATE STUDIES

Prepared by S NOORTAJ

TYPES OF CYBER THREAT ACTORS

- In cybersecurity, this 'enemy' is called the threat actor. We can define a threat actor as person, group, or entity that creates all or part of an incident with the aim to impact an organization's security.
- However, knowing the types of threat actors isn't enough. To create an air-tight cybersecurity plan, you need to be aware of their motivations as well.
- Defending against a known attacker is much easier than an unknown one. Sun Tzu's famed quote from The Art of War comes to mind:

TYPES OF THREAT ACTORS

Cyber Terrorists

- Cyber Terrorists are a modern mutation of a widespread global problem that has plagued most countries for decades.
- These threat actors are usually focused on disrupting critical services and causing harm.

Chief Goal: Cause harm and destruction to further their cause.

Typical Targets: Cyber terrorists can target businesses, state machinery, and critical services that would cause the most harm, disruption, and destruction

Government-Sponsored/State-Sponsored Actors

- These threat actors are funded, directed, or sponsored by nations.
- They've been known to steal and exfiltrate intellectual property, sensitive information, and even funds to further their nation's espionage causes.

Chief Goal: Espionage, theft, or any other activity that furthers the interests of a particular nation/group of nations.

Typical Targets: Businesses and Government-run Organizations.

Organized Crime/Cybercriminals

- Crime is everywhere, and the internet is no different.
- Criminals who want to steal sensitive data, money, and personal information are out there. However, since they're after financial gain, the data they take does tend to show up on the black market or is sold to the highest bidder.
- These threat actors are also known to use ransomware to extort business owners directly.

Chief Goal: Financial Gain.

Typical Targets: Cash and/or Data-Rich Organizations and Businesses.

Hacktivists

- Hacktivists focus on bringing awareness.
- For example, almost all the information leaked by WikiLeaks was a result of hacktivists who wanted to expose the truth.
- They're usually motivated by ideological activism.

Chief Goal: Exposing secrets and disrupting services/organizations that are perceived as evil.

Typical Targets: Not limited to any specific type of organization or business.

Insiders

- Sometimes, you don't need to look far to find infiltrators.
- Some threat actors can go as far as infiltrating your workforce themselves or turning an insider towards their cause/goal.
- Insiders are a particularly nasty threat to any organization's cybersecurity because of the amount of access they'd have when working from within.

Chief Goal: Work from within an organization to get around its cybersecurity framework.

Typical Targets: Not limited to any specific type of organization.

Script Kiddies

- Some attackers aren't skilled/advanced enough to design penetration tools on their own.
- Script Kiddies use tools developed by other attackers to penetrate a network or system.

Chief Goal: Attack computer systems and networks, vandalize, and inflict as much damage as possible.

Typical Targets: Easy-to-penetrate systems, which are vulnerable to widely-known threats.

Internal User Errors

- Not all threat actors are malicious. But the damage they do cause can be quite extensive.
- Even simple user errors can end in catastrophe because of their elevated permissions within an organization's systems and networks.

Chief Goal: Not malicious, often inadvertent.

Typical Targets: Can affect any organization, however .

COMMON THREAT ACTOR MOTIVATIONS

- Political, Economic, Technical, and Military Agendas:
- Threat actors such as Hacktivists and Government-Backed Actors share such motivations.
- They are focused and have a set objective/target in mind when they start planning an attack.
- Moreover, this data is rarely seen available for sale on the black market.
- For example, the absence of data stolen from the Equifax Attack has many wondering whether the attack was orchestrated/sponsored by another country.

Profits/Financial Gain:

- The profit motivation is one of the most frequent motivations of cybercriminals.
- These threat actors won't usually care about penetrating a specific organization or business.
- Moreover, they won't care about the discoverability of the crime because they're only interested in stealing assets that they can convert into money as soon as possible.

Notoriety:

- Some threat actors are motivated by reputation and attention and will actively seek targets that will help them gain recognition.
- In fact, those agents that seek notoriety will often ignore chances to attack non-visible assets/targets that won't draw any attention.
- Getting back at someone is a pervasive human trait; it's also a common threat actor motivation.
- The threat actors who plan an attack for revenge are most likely to be either employees or ex-employees -- giving them intimate knowledge about an organization's systems, networks, and even defenses.

Overlap of Motivations:

- Of course, a threat actor may be motivated by more than one threat actor motivation.
- For example, they can have a revenge mindset along with a political agenda.

Types of Cyber Attacks

- A cyber-attack is an exploitation of computer systems and networks.
- It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.
- We are living in a digital era. Now a day, most of the people use computer and internet.
- Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:

Types of Cyber Attacks

Web-based attacks

These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

1. Injection attacks

- It is the attack in which some data will be injected into a web application to manipulate the application and fetch the required information.

Example- SQL Injection, code Injection, log Injection, XML Injection etc.

2. DNS Spoofing

- DNS Spoofing is a type of computer security hacking.
- Whereby a data is introduced into a DNS resolver's cache causing the name server to return an incorrect IP address, diverting traffic to the attackers computer or any other computer.
- The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

3. Session Hijacking

- It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions.
- By stealing the cookies, an attacker can have access to all of the user data.

4. Phishing

- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number.
- It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

5. Brute force

- It is a type of attack which uses a trial and error method
- This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number.
- This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

6. Denial of Service

- It is an attack which meant to make a server or network resource unavailable to the users.
- It accomplishes this by flooding the target with traffic or sending it information that triggers a crash.
- It uses the single system and single internet connection to attack a server.

It can be classified into the following-

Volume-based attacks-

- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.

Protocol attacks-

- It consumes actual server resources, and is measured in a packet.

Application layer attacks-

- Its goal is to crash the web server and is measured in request per second.

7. Dictionary attacks

- This type of attack stored the list of a commonly used password and validated them to get original password.

8. URL Interpretation

- It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

9. File Inclusion attacks

- It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

10. Man in the middle attacks

- It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them.
- Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

System-based attacks

- These are the attacks which are intended to compromise a computer or a computer network.
- Some of the important system-based attacks are as follows-

1. Virus

- It is a type of malicious software program that spread throughout the computer files without the knowledge of a user.
- It is a self-replicating malicious computer program that replicates by inserting copies of itself into other computer programs when executed.
- It can also execute instructions that cause harm to the system.

2. Worm

- It is a type of malware whose primary function is to replicate itself to spread to uninfected computers.
- It works same as the computer virus. Worms often originate from email attachments that appear to be from trusted senders.

3. Trojan horse

- It is a malicious program that occurs unexpected changes to computer setting and unusual activity, even when the computer should be idle.
- It misleads the user of its true intent.
- It appears to be a normal application but when opened/executed some malicious code will run in the background.

4. Backdoors

- It is a method that bypasses the normal authentication process.
- A developer may create a backdoor so that an application or operating system can be accessed for troubleshooting or other purposes.

5. Bots

- A bot (short for "robot") is an automated process that interacts with other network services.
- Some bots program run automatically, while others only execute.
- Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Define Security Attack

- ❖ The security attacks aim to compromise the five major security goals for network security (extended from CIA requirements):
- ❖ Confidentiality, Availability, Authentication, Integrity and Nonrepudiation.
- ❖ To serve these aims, a network attack is commonly composed of five stages

1. Preparation and reconnaissance phase including information gathering to discover and identify vulnerabilities/weaknesses to be exploited and tool configuration

2. Assessing vulnerabilities and potential exploits

3. Launching the attack

4. Core attack operations such as confidential data compromises or integrity damages

5. Post-attack operations such as getting rid of traces and removing/hiding evidence

Network Security Model

A Network Security Model exhibits how the security service has been designed over the network to prevent the opponent from causing a threat to the confidentiality or authenticity of the information that is being transmitted through the network.

In this section, we will be discussing the general 'network security model' where we will study how messages are shared between the sender and receiver securely over the network, And we will also discuss the 'network access security model' which is designed to secure your system from unwanted access through the network

- For a message to be sent or receive there must be a sender and a receiver. Both the sender and receiver must also be mutually agreeing to the sharing of the message.
- Now, the transmission of a message from sender to receiver needs a medium i.e. Information channel which is an Internet service.
- A logical route is defined through the network (Internet), from sender to the receiver and using the communication protocols both the sender and the receiver established communication.
- Well, we are concerned about the security of the message over the network when the message has some confidential or authentic information which has a threat from an opponent present at the information channel.

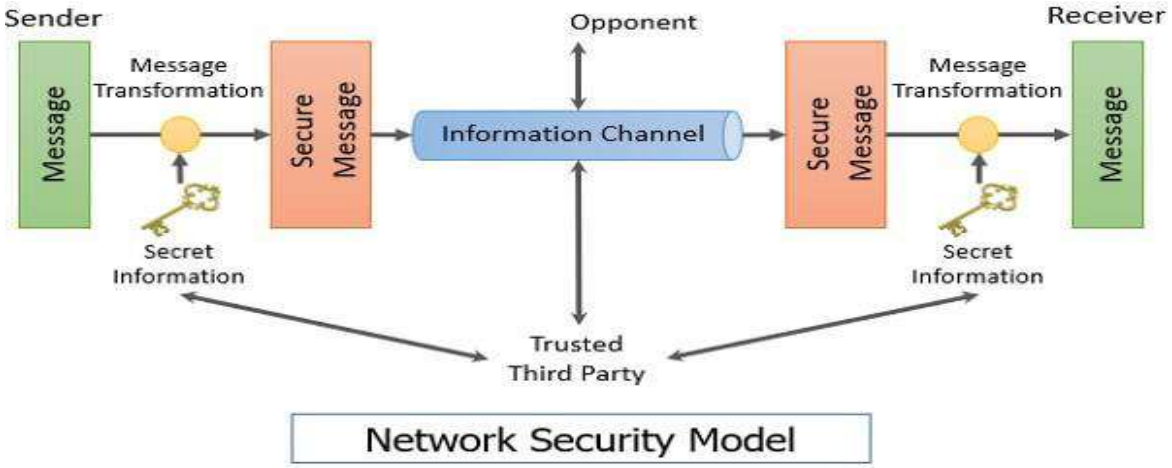
Any security service would have the three components discussed below:

1. Transformation of the information which has to be sent to the receiver. So, that any opponent present at the information channel is unable to read the message. This indicates the encryption of the message. It also includes the addition of code during the transformation of the information which will be used in verifying the identity of the authentic receiver.

2. Sharing of the secret information between sender and receiver of which the opponent must not any clue. Yes, we are talking of the encryption key which is used during the encryption of the message at the sender's end and also during the decryption of message at receiver's end.

3. There must be a trusted third party which should take the responsibility of distributing the secret information (key) to both the communicating parties and also prevent it from any opponent.

Now we will study a general network security model with the help of the figure given below:



Network Security Model

- The network security model presents the two communicating parties sender and receiver who mutually agrees to exchange the information. The sender has information to share with the receiver.
- But sender cannot send the message on the information cannel in the readable form as it will have a threat of being attacked by the opponent.
- So, before sending the message through the information channel, it should be transformed into an unreadable format.
- Secret information is used while transforming the message which will also be required when the message will be retransformed at the recipient side.
- That's why a trusted third party is required which would take the responsibility of distributing this secret information to both the parties involved in communication.

So, considering this general model of network security, one must consider the following three tasks while designing the security model.

1. To transform a readable message at the sender side into an unreadable format, an appropriate algorithm should be designed such that it should be difficult for an opponent to crack that security algorithm.

2. Next, the network security model designer is concerned about the generation of the secret information which is known as a key. This secret information is used in conjunction with the security algorithm in order to transform the message.

3. Now, the secret information is required at both the ends, sender's end and receiver's end.

- At sender's end, it is used to encrypt or transform the message into unreadable form and at the receiver's end, it is used to decrypt or retransform the message into readable form. So, there must be a trusted third party which will distribute the secret information to both sender and receiver.
- While designing the network security model designer must also concentrate on developing the methods to distribute the key to the sender and receiver.
- An appropriate methodology must be used to deliver the secret information to the communicating parties without the interference of the opponent.
- It is also takecare that the communication protocols that are used by the communicating parties should be supporting the security algorithm and the secret key in order to achieve the security service.

Till now we have discussed the security of the information or message over the network.

Network access security model

Now, we will discuss the network access security model which is designed to secure the information system which can be accessed by the attacker through the network. You are well aware of the attackers who attack your system that is accessible through the internet.

These attackers fall into two categories:

1. Hacker:

- The one who is only interested in penetrating into your system.
- They do not cause any harm to your system they only get satisfied by getting access to your system.

2. Intruders:

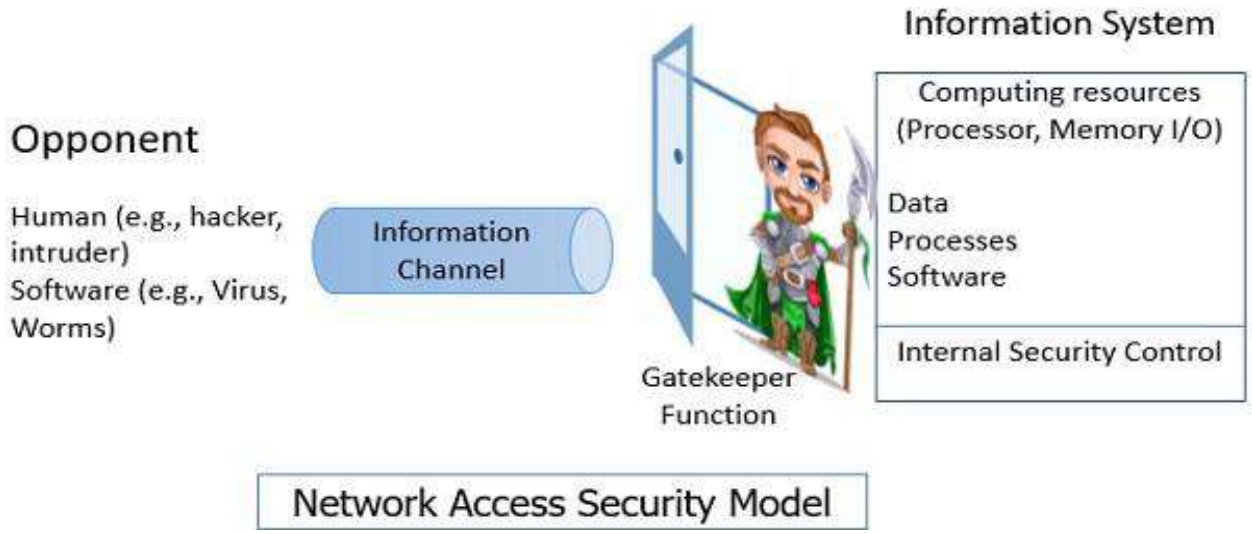
- These attackers intend to do damage to your system or try to obtain the information from the system which can be used to attain financial gain.
- The attacker can place a logical program on your system through the network which can affect the software on your system. This leads to two kinds of risks:

a. Information threat:

- This kind of threats modifies data on the user's behalf to which actually user should not access. Like enabling some crucial permission in the system.

b. Service threat:

- This kind of threat disables the user from accessing data on the system.
- Well, these kinds of threats can be introduced by launching worms and viruses and may more like this on your system.
- Attack with worms and viruses are the software attack that can be introduced to your system through the internet.
- The network security model to secure your system is shown in the figure below:



There are two ways to secure your system from attacker :

- Gatekeeper function.
- Antivirus

Gatekeeper function.

- Introducing gatekeeper function means introducing login-id and passwords which would keep away the unwanted access.
- In case the unwanted user gets access to the system the second way to secure your system is introducing internal control which would
- detect the unwanted user trying to access the system by analyzing system activities.

Antivirus

- This second method we call as antivirus which we install on our system to prevent the unwanted user from accessing your computer system through the internet.

So, this is all about the network security model. We have discussed two network security model.

- One, securing your information over the network during information transmission.
- Second, securing your information system which can be accessed by the hacker through the network or internet.

Types of Security Threats to Organizations

different types of security threats to organizations, which are as follows:

1. Computer Viruses

- A virus is a software program that can spread from one computer to another computer or one network to another network without the user's knowledge and performs malicious attacks.
- It has capability to corrupt or damage organization's sensitive data, destroy files, and format hard drives.

How does a virus attack?

There are different ways that a virus can be spread or attack, such as:

- Clicking on an malicious executable file
- Installing free software and apps
- Visiting an infected and unsecured website
- Clicking on advertisement
- Using of infected removable storage devices, such USB drives
- Opening spam email or clicking on URL link .
- Downloading free games, toolbars, media players and other software.
- Computer Viruses are types of security threats to organizations

2. Trojans Horse

- Trojan horse is a malicious code or program that developed by hackers to disguise as legitimate software to gain access to organization's systems.
- It has designed to delete, modify, damage, block, or some other harmful action on your data or network.

How does Trojans horse attack?

- The victim receives an email with an attachment file which is looking as an original official email.
- The attachment file may contain malicious code that is executed as soon as when the victim clicks on the attachment file.
- In that case, the victim does not suspect or understand that the attachment is actually a Trojan horse.

3. Adware

- Adware is a software program that contains commercial and marketing related advertisements such as display advertisements through pop-up windows or bars, banner ads, video on your computer screen.
- Its main purpose is to generate revenue for its developer (Adware) by serving different types advertisements to an internet user.

How does adware attack?

- When you click on that type of advertisements then it redirect you to an advertising websites and collect information from to you.
- It can be also used to steal all your sensitive information and login credentials by monitoring your online activities and selling that information to the third party.
- Adware is types of security threats to organizations

4. Spyware

- Spyware is unwanted types of security threats to organizations which installed in user's computer and collects sensitive information such as personal or organization's business information, login credentials and credit card details without user knowledge.
- This type of threats monitor your internet activity, tracking your login credentials, and spying on your sensitive information.
- So, every organization or individual should take an action to prevent from spyware by using anti-virus, firewall and download software only from trusted sources.

How does Spyware install?

- It can be automatically installs itself on your computer or hidden component of software packages or can be install as traditional malware such as deceptive ads, email and instant messages.

5. Worm

- Computer worm is a type of malicious software or program that spreads within its connected network and copies itself from one computer to another computer of an organization.

How does worm spreads?

- It can spread without any human assistance and exploit the security holes of the software and trying to access in order to stealing

- sensitive information, corrupting files and installing a back door for remote access to the system.

6. Denial-of-Service (DoS) Attacks

- Denial-of-Service is an attack that shut down a machine or network or making it inaccessible to the users.
- It typically flooding a targeted system with requests until normal traffic is unable to be processed, resulting in denial-of-service to users.

How does DoS attack?

- It occurs when an attacker prevents legitimate users from accessing specific computer systems, devices or other resources.
- The attacker sends too much traffic to the target server
- Overloading it with traffic and the server is overwhelmed, which causes to down websites, email servers and other services which connect to the Internet.

7. Phishing

- Phishing is a type of social engineering attack that attempt to gain confidential information such as usernames, passwords, credit card information, login credentials, and so more.

How does Phishing attack?

- In a phishing email attack, an attacker sends phishing emails to victim's email that looks like it came from your bank and they are asked to provide your personal information.
- The message contains a link, which redirects you to another vulnerable website to steal your information.
- So, it is better to avoid or don't click or don't open such type of email and don't provide your sensitive information.
- Phishing is a type of social engineering attack

8. SQL Injection

- SQL injection is type of an injection attack and one of the most common web hacking techniques that allows attacker to control the back end database to change or delete data.

How does SQL injection attack?

- It is an application security weakness and when an application fails to properly sanitize the SQL statements then attacker can include their own malicious SQL commands to access the organization database.
- Attacker includes the malicious code in SQL statements, via web page input.

9. Rootkit

- Rootkit is a malicious program that installs and executes malicious code on a system without user consent in order gain administrator-level access to a computer or network system.
- There are different types of Rootkit virus such as Bootkits, Firmware Rootkits, Kernel-Level Rootkits and application Rootkits.

How does Rootkit install?

- It can be infected in a computer either by sharing infected disks or drives.
- It is typically installed through a stolen password or installed through by exploiting system vulnerabilities, social engineering tactics, and phishing techniques without the victim's knowledge.

10. Malware

- Malware is software that typically consists of program or code and which is developed by cyber attackers.
- It is types of cyber security threats to organizations which are designed to extensive damage to systems or to gain unauthorized access to a computer.

How does malware attack?

- There are different ways that a malware can infect a device such as it can be delivered in the form of a link or file over email and it requires the user to click on that link or open the file to execute the malware.
- This type of attack includes computer viruses, worms, Trojan horses and spyware.
- Malware is a software that consists of program or codes

11. Ransomware

- Ransomware is type of security threats that blocks to access computer system and demands for bitcoin in order to access the system.
- The most dangerous ransomware attacks are WannaCry, Petya, Cerber, Locky and Crypto Locker etc.

How does Ransomware install?

All types of threats typically installed in a computer system through the following ways:

- When download and open a malicious email attachment
- Install an infected software or apps
- When user visit a malicious or vulnerable website
- Click on untrusted web link or images

12. Data breach

- A data breach is a security threat that exposes confidential or protected information and the information is accessed from a system without authorization of the system's owner.
- The information may involve sensitive, proprietary, or confidential such as credit card numbers, customer data, trade secrets etc.

13. Zero day attack

- Zero day attack is the application based cyber security threats which is unknown security vulnerability in a computer software or application. When an organization going to launch an application, they don't what types of vulnerability is there?

How does Zero day attack?

- When the patch has not been released or the software developers were unaware of or did not have sufficient time to fix the vulnerability of the application.
- If the vulnerability is not solved by the developer then it can affect on computer programs, data, or a network.

14. Careless Employees of organization

- Employees are the greatest security risk for any organization, because they know everything of the organizations such as where the sensitive information is stored and how to access it.
- In addition to malicious attacks, careless employees are other types of cyber security threats to organizations**.**

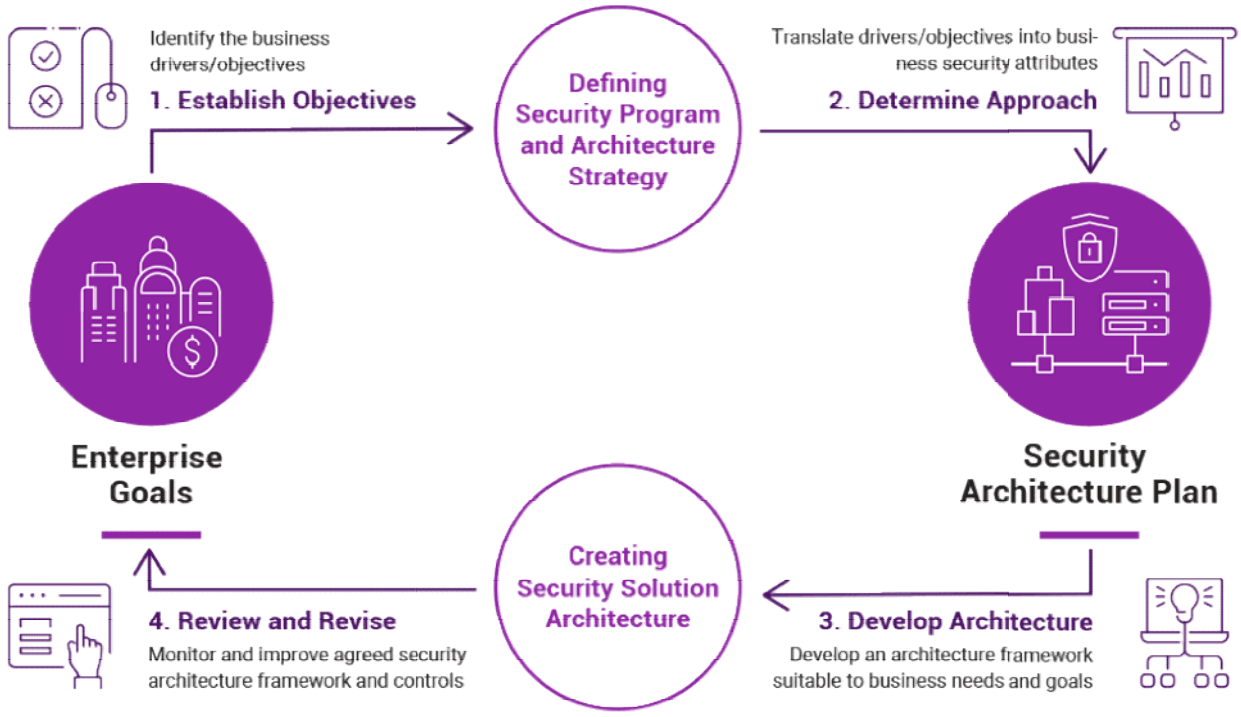
How does attack?

- They use very simple password to remember their mind and also share passwords.
- Another common problem is that employees opening suspicious email attachments, clicking on the link or visit malicious websites, which can introduce malware into the system.

SECURITY ARCHITECTURE?

- Security architecture is a means to reduce the risk of cyber breaches and protect your assets from digital harm.

ELEMENTS OF SECURITY ARCHITECTURE



Purpose

- Security architectures typically share the same purpose - protect the organization from cyber harm.
- In order to achieve this, architects will often try to install themselves in your business for a period of time while they learn what makes you, and your people, different.
- They will talk to your leaders and employees, seeking to understand your individual business goals, the requirements of your systems, the needs of your customers and other critical factors.

Examples of common security architecture frameworks

TOGAF:

- The Open Group Architecture Framework, or TOGAF, helps determine what problems a business wants to solve with security architecture.
- It focuses on the preliminary phases of security architecture, an organization's scope and goal, setting out the problems a business intends to solve with this process.
- However, it does not give specific guidance on how to address security issues.

SABSA:

- Sherwood Applied Business Security Architecture, or SABSA, is a quite policy driven framework that helps define key questions that must be answered by security architecture: who, what, when and why.
- Its aim is to ensure that security services are designed, delivered and supported as an integral part of the enterprise's IT management.
- However, while often described as a 'security architecture method', it does not go into specifics regarding technical implementation.

OSA

- Open Security Architecture, or OSA, is a framework related to functionality and technical security controls.
- It offers a comprehensive overview of key security issues, principles, components and concepts underlying architectural decisions that are involved when designing effective security architectures.
- That said, it can typically only be used once the security architecture is already designed.

BENEFIT OF SECURITY ARCHITECTURE

- Strong Security Architecture Leads To Fewer Security Breaches
- Proactive Security Measures Save Money
- It May Help Mitigate Disciplinary Measures In The Event Of A Breach

Steps in Building a Healthy Security Architecture

1. Limit Access

- Part of every security architect's task is to assess the so-called "network topology."
- That refers to the network's layout. It defines how different nodes or systems are connected to and communicate with each other.
- Security architects need to know where and how users can access the resources they require to perform tasks while making sure that security policies and measures are in place.

- Security architects should segregate the network—splitting it into zones to control who can access what.

2. Use VLANs

- Virtual local area networks (VLANs) allow for easy user segregation within a network.
- A VLAN is an isolated broadcast domain in a computer network.
- It is easier for any organization to implement security policies and measures if it does so by zone.
- Security architects can group users based on their access rights and assign each to a particular VLAN.
- That way, they can tighten or loosen security in individual network parts, depending on the confidentiality of data stored in a VLAN.
- User segregation also makes responding to incidents easier as threats can be contained in affected zones.

3. Enable System Lockdown

- Once security architects fully understand the business requirements, who the users are, and what systems are required, they can then begin to determine what security solutions, policies, and protocols to put in place.
- Apart from using username-password combinations to access systems, for instance, they can require multi-factor authentication (MFA) for computers or servers that contain privileged-access data.
- MFA requires the use of an additional device (typically a mobile phone) to grant access. All devices should also be capable of being locked down by administrators should these be compromised.
- That would prevent an entire network shutdown in case of a breach.
- A network's security architecture must evolve with the changing times.
- A sound security architecture is one that can successfully address threats, whether known or unknown.

What Is Internet Security

- Internet security consists of a range of security tactics for protecting activities and transactions conducted online over the internet.
- These tactics are meant to safeguard users from threats such as hacking into computer systems, email addresses, or websites; malicious software that can infect and inherently

damage systems; and identity theft by hackers who steal personal data such as bank account information and credit card numbers.

- Internet security is a specific aspect of broader concepts such as cybersecurity and computer security, being focused on the specific threats and vulnerabilities of online access and use of the internet.
- In today's digital landscape, many of our daily activities rely on the internet. Various forms of communication, entertainment, and financial and work-related tasks are accomplished online.
- This means that tons of data and sensitive information are constantly being shared over the internet.
- The internet is mostly private and secure, but it can also be an insecure channel for exchanging information.
- With a high risk of intrusion by hackers and cybercriminals, internet security is a top priority for individuals and businesses alike.

Types of internet security threats

- **Malware:** Short for "malicious software," malware comes in several forms, including computer viruses, worms, Trojans, and dishonest spyware.
  icon-ransomware
- **Computer worm:** A computer worm is a software program that copies itself from one computer to the next. It does not require human interaction to create these copies and can spread rapidly and in great volume.
- **Spam:** Spam refers to unwanted messages in your email inbox. In some cases, spam can simply include junk mail that advertises goods or services you aren't interested in. These are usually considered harmless, but some can include links that will install malicious software on your computer if they're clicked on.
- **Phishing:** Phishing scams are created by cybercriminals attempting to solicit private or sensitive information. They can pose as your bank or web service and lure you into clicking links to verify details like account information or passwords.
- **Botnet:** A botnet is a network of private computers that have been compromised. Infected with malicious software, these computers are controlled by a single user and are often prompted to engage in nefarious activities, such as sending spam messages or denial-of-service (DoS) attacks.

Sniffing attack

Sniffing attacks refer to data thefts caused by capturing network traffic through packet sniffers that can unlawfully access and read the data which is not encrypted. The data packets are captured when they flow through a computer network.

Sniffing attack or a sniffer attack is the context of network security, corresponds to theft or interception of data by capturing the network traffic using a sniffer.

Sniffing Motives:

- Getting username a passwords
- Stealing bank-related/transaction-related information
- Spying on email and chat messages
- Identity theft

Types of Sniffing

- There are two types of sniffing- active and passive. As the name suggests, active involves some activity or interaction by the attacker in order to gain information.
- In passive the attacker is just hiding dormant and getting the information. Let's discuss passive sniffing first.

Passive Sniffing:

- This kind of sniffing occurs at the hub. A hub is a device that received the traffic on one port and then retransmits that traffic on all other ports.
- It does not take into account that the traffic is not meant for other destinations. In this case, if a sniffer device is placed at the hub then all the network traffic can be directly captured by the sniffer.
- The sniffer can sit there undetected for a long time and spy on the network. Since hubs are not used these days much, this kind of attack will be an old-school trick to perform.
- Hubs are being replaced by switches and that is where active sniffing comes into the picture.

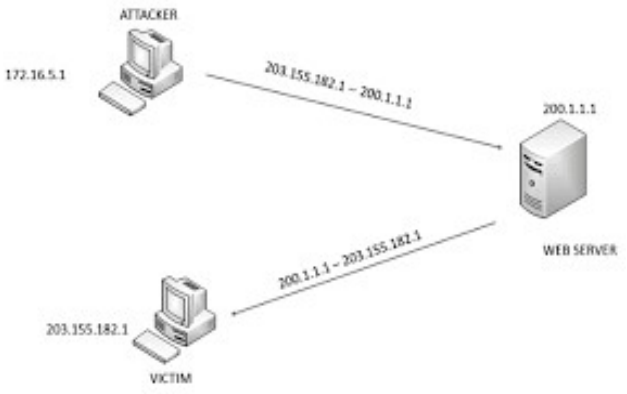
Active Sniffing:

- In a nutshell, a switch learns a CAM table that has the mac addresses of the destinations.
- Basis this table the switch is able to decide what network packet is to be sent where.
- Inactive sniffing, the sniffer will flood the switch with bogus requests so that the CAM table gets full.
- Once the CAM is full the switch will act as a switch and send the network traffic to all ports.

- Now, this is legitimate traffic that gets distributed to all the ports. This way the attacker can sniff the traffic from the switch.

What is IP spoofing

- IP spoofing is the creation of Internet Protocol (IP) packets which have a modified source address in order to either hide the identity of the sender, to impersonate another computer system, or both.
- It is a technique often used by bad actors to invoke DDoS attacks against a target device or the surrounding infrastructure.
- Sending and receiving IP packets is a primary way in which networked computers and other devices communicate, and constitutes the basis of the modern internet.
- All IP packets contain a header which precedes the body of the packet and contains important routing information, including the source address. In a normal packet, the source IP address is the address of the sender of the packet. If the packet has been spoofed, the source address will be forged.



- IP Spoofing is analogous to an attacker sending a package to someone with the wrong return address listed.
- If the person receiving the package wants to stop the sender from sending packages, blocking all packages from the bogus address will do little good, as the return address is easily changed. Relatedly, if the receiver wants to respond to the return address, their response package will go somewhere other than to the real sender.
- The ability to spoof the addresses of packets is a core vulnerability exploited by many DDoS attacks.

- DDoS attacks will often utilize spoofing with a goal of overwhelming a target with traffic while masking the identity of the malicious source, preventing mitigation efforts.
- If the source IP address is falsified and continuously randomized, blocking malicious requests becomes difficult. IP spoofing also makes.
- it tough for law enforcement and cyber security teams to track down the perpetrator of the attack.
- Spoofing is also used to masquerade as another device so that responses are sent to that targeted device instead.
- Volumetric attacks such as NTP Amplification and DNS amplification make use of this vulnerability.
- The ability to modify the source IP is inherent to the design of TCP/IP, making it an ongoing security concern.
- Tangential to DDoS attacks, spoofing can also be done with the aim of masquerading as another device in order to sidestep authentication and gain access to or "hijack" a user's session.

How to protect against IP spoofing (packet filtering)

- While IP spoofing can't be prevented, measures can be taken to stop spoofed packets from infiltrating a network.
- A very common defense against spoofing is ingress filtering, outlined in BCPD (a Best Common Practice document).
- Ingress filtering is a form of packet filtering usually implemented on a network edge device which examines incoming IP packets and looks at their source headers.
- If the source headers on those packets don't match their origin or they otherwise look fishy, the packets are rejected.
- Some networks will also implement egress filtering, which looks at IP packets exiting the network, ensuring that those packets have legitimate source headers to prevent someone within the network from launching an outbound malicious attack using IP spoofing.

What is a denial-of-service (DoS) attack?

- A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.
- DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users.

- A DoS attack is characterized by using a single computer to launch the attack.
- A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.

How does a DoS attack work?

• The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. The multiple attack vectors of DoS attacks can be grouped by their similarities.

DoS attacks typically fall in 2 categories:

Buffer overflow attacks

- An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of service.

Flood attacks

- By saturating a targeted server with an overwhelming amount of packets, a malicious actor is able to oversaturate server capacity, resulting in denial-of-service.
- In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

What are some historically significant DoS attacks?

- Historically, DoS attacks typically exploited security vulnerabilities present in network, software and hardware design.
- These attacks have become less prevalent as DDoS attacks have a greater disruptive capability and are relatively easy to create given the available tools. In reality, most DoS attacks can also be turned into DDoS attacks.

A few common historic DoS attacks include:

- **Smurf attack** - a previously exploited DoS attack in which a malicious actor utilizes the broadcast address of vulnerable network by sending spoofed packets, resulting in the flooding of a targeted IP address.
- **Ping flood** - this simple denial-of-service attack is based on overwhelming a target with ICMP (ping) packets. By inundating a target with more pings than it is able to respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack.

- **Ping of Death** - often conflated with a ping flood attack, a ping of death attack involves sending a malformed packet to a targeted machine, resulting in deleterious behavior such as system crashes.

How can you tell if a computer is experiencing a DoS attack?

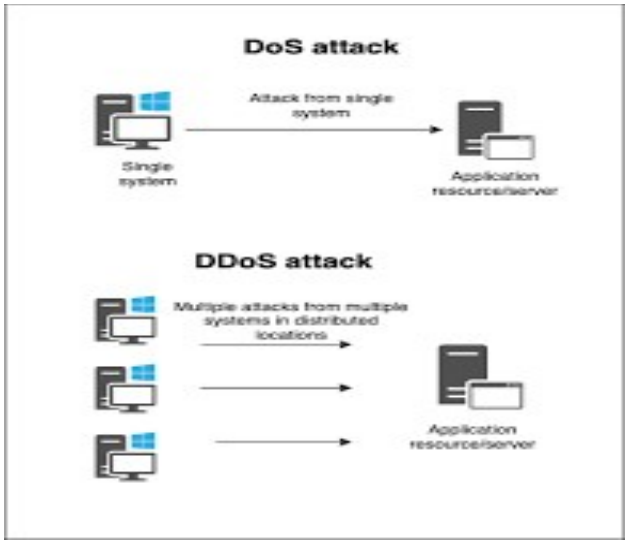
While it can be difficult to separate an attack from other network connectivity errors or heavy bandwidth consumption, some characteristics may indicate an attack is underway.

Indicators of a DoS attack include:

- Atypically slow network performance such as long load times for files or websites
- The inability to load a particular website such as your web property
- A sudden loss of connectivity across devices on the same network

What is the difference between a DDoS attack and a DOS attack?

- The distinguishing difference between DDoS and DoS is the number of connections utilized in the attack.
- Some DoS attacks, such as "low and slow" attacks like Slow Loris, derive their power in the simplicity and minimal requirements needed to them be effective.



- DoS utilizes a single connection, while a DDoS attack utilizes many sources of attack traffic, often in the form of a botnet.
- Generally speaking, many of the attacks are fundamentally similar and can be attempted using one more many sources of malicious traffic.
- Learn how Cloudflare's DDoS protection stops denial-of-service attacks.

What is Social Engineering

- Social engineering is the art of manipulating people so they give up confidential information.
- The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.
- Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software.
- For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).

Generally, social engineering attackers have one of two goals:

Sabotage: Disrupting or corrupting data to cause harm or inconvenience.

Theft: Obtaining valuables like information, access, or money.

How Does Social Engineering Work?

- Most social engineering attacks rely on actual communication between attackers and victims.
- The attacker tends to motivate the user into compromising themselves, rather than using brute force methods to breach your data.
- The attack cycle gives these criminals a reliable process for deceiving you.
- Steps for the social engineering attack cycle are usually as follows:
- Prepare by gathering background information on you or a larger group you are a part of.
- Infiltrate by establishing a relationship or initiating an interaction, started by building trust.
- Exploit the victim once trust and a weakness are established to advance the attack.
- Disengage once the user has taken the desired action.
- This process can take place in a single email or over months in a series of social media chats.
- It could even be a face-to-face interaction. But it ultimately concludes with an action you take, like sharing your information or exposing yourself to malware.
- It's important to beware of social engineering as a means of confusion. Many employees and consumers don't realize that just a few pieces of information can give hackers access to multiple networks and accounts.

Types of Social Engineering Attacks

Here are some common methods used by social engineering attackers:

Phishing Attacks

Phishing attackers pretend to be a trusted institution or individual in an attempt to persuade you to expose personal data and other valuables. Attacks using phishing are targeted in one of two ways: Spam phishing, or mass phishing, is a widespread attack aimed at many users.

- These attacks are non-personalized and try to catch any unsuspecting person.
- Spear phishing and by extension, whaling , use personalized info to target particular users.
- Whaling attacks specifically aim at high-value targets like celebrities, upper management, and high government officials.
- Whether it's a direct communication or via a fake website form, anything you share goes directly into a scammer's pocket.
- You may even be fooled into a malware download containing the next stage of the phishing attack.
- Methods used in phishing each have unique modes of delivery, including but not limited to: **Voice phishing (vishing)** phone calls may be automated message systems recording all your inputs. Sometimes, a live person might speak with you to increase trust and urgency.

SMS phishing (smishing) texts or mobile app messages might include a web link or a prompt to follow-up via a fraudulent email or phone number.

Email phishing is the most traditional means of phishing, using an email urging you to reply or follow-up by other means. Web links, phone numbers, or malware attachments can be used. **Angler phishing** takes place on social media, where an attacker imitates a trusted company's customer service team. They intercept your communications with a brand to hijack and divert your conversation into private messages, where they then advance the attack.

Search engine phishing attempt to place links to fake websites at the top of search results. These may be paid ads or use legitimate optimization methods to manipulate search rankings. **URL phishing links** tempt you to travel to phishing websites. These links are commonly delivered in emails, texts, social media messages, and online ads. Attacks hide links in hyperlinked text or buttons, using link-shortening tools, or deceptively spelled URLs. In-session phishing appears as an interruption to your normal web browsing. For example, you may see such as fake login pop-ups for pages you're currently visiting.

Baiting Attacks Baiting abuses your natural curiosity to coax you into exposing yourself to an attacker. Typically, potential for something free or exclusive is the manipulation used to exploit you. The attack usually involves infecting you with malware.

Popular methods of baiting can include:

USB drives left in public spaces, like libraries and parking lots.

Email attachments including details on a free offer, or fraudulent free software.

Physical Breach Attacks

- Physical breaches involve attackers appearing in-person, posing as someone legitimate to gain access to otherwise unauthorized areas or information.
- Attacks of this nature are most common in enterprise environments, such as governments, businesses, or other organizations.
- Attackers may pretend to be a representative of a known, trusted vendor for the company.
- attackers may even be recently fired employees with a vendetta against their former employer.
- They make their identity obscure but believable enough to avoid questions.
- This requires a bit of research on the attacker's part and involves high-risk. So, if someone is attempting this method, they've identified clear potential for a highly valuable reward if successful.

Pretexting Attacks

- Pretexting uses a deceptive identity as the "pretext" for establishing trust, such as directly impersonating a vendor or a facility employee.
- This approach requires the attacker to interact with you more proactively.
- The exploit follows once they've convinced you they are legitimate.

Access Tailgating Attacks

- Tailgating , or piggybacking, is the act of trailing an authorized staff member into a restricted-access area.
- Attackers may play on social courtesy to get you to hold the door for them or convince you that they are also authorized to be in the area. Pretexting can play a role here too.

Quid Pro Quo Attacks

- Quid pro quo is a term roughly meaning "a favor for a favor," which in the context of phishing means an exchange of your personal info for some reward or other compensation.
- Giveaways or offers to take part in research studies might expose you to this type of attack.
- The exploit comes from getting you excited for something valuable that comes with a low investment on your end.
- However, the attacker simply takes your data with no reward for you.

DNS Spoofing and Cache Poisoning Attacks

- DNS spoofing manipulates your browser and web servers to travel to malicious websites when you enter a legitimate URL.
- Once infected with this exploit, the redirect will continue unless the inaccurate routing data is cleared from the systems involved.
- DNS cache poisoning attacks specifically infect your device with routing instructions for the legitimate URL or multiple URLs to connect to fraudulent websites.

Scareware Attacks

- Scareware is a form of malware used to frighten you into taking an action. This deceptive malware uses alarming warnings that report fake malware infections or claim one of your accounts has been compromised.
- As a result, scareware pushes you to buy fraudulent cybersecurity software, or divulge private details like your account credentials.

Watering Hole Attacks

- Watering hole attacks infect popular webpages with malware to impact many users at a time. • It requires careful planning on the attacker's part to find weaknesses in specific sites. They look for existing vulnerabilities that are not known and patched — such weaknesses are deemed zero-day exploits
- Other times, they may find that a site has not updated their infrastructure to patch out known issues.
- Website owners may choose delay software updates to keep software versions they know are stable.
- They'll switch once the newer version has a proven track record of system stability. Hackers abuse this behavior to target recently patched vulnerabilities.

Unusual Social Engineering Methods

In some cases, cybercriminals have used complex methods to complete their cyberattacks, including:

Fax-based phishing:

When one bank's customers received a fake email that claimed to be from the bank — asking the customer to confirm their access codes – the method of confirmation was not via the usual email / Internet routes. Instead, the customer was asked to print out the form in the email, then fill in their details and fax the form to the cybercriminal's telephone number.

Traditional mail malware distribution:

- In Japan, cybercriminals used a home-delivery service to distribute CDs that were infected with Trojan spyware.
- he disks were delivered to the clients of a Japanese bank. The clients' addresses had previously been stolen from the bank's database.
- When malware creators use social engineering techniques, they can lure an unwary user into launching an infected file or opening a link to an infected website.
- Many email worms and other types of malware use these methods. Without a comprehensive security software suite for your mobile and desktop devices, you're likely exposing yourself to an infection.

Worm Attacks

- The cybercriminal will aim to attract the user's attention to the link or infected file – and then get the user to click on it.

Examples of this type of attack include:

- The LoveLetter worm that overloaded many companies' email servers in 2000. Victims received an email that invited them to open the attached love letter. When they opened the attached file, the worm copied itself to all of the contacts in the victim's address book. This worm is still regarded as one of the most devastating, in terms of the financial damage that it inflicted.

The Mydoom email worm — which appeared on the Internet in January 2004 — used texts that imitated technical messages issued by the mail server.

- The Swen worm passed itself off as a message that had been sent from Microsoft.
- It claimed that the attachment was a patch that would remove Windows vulnerabilities.

- It's hardly surprising that many people took the claim seriously and tried to install the bogus security patch — even though it was really a worm.

Malware Link Delivery Channels

- Links to infected sites can be sent via email, ICQ and other IM systems — or even via IRC Internet chat rooms.
- Mobile viruses are often delivered by SMS message.
- Whichever delivery method is used, the message will usually contain eye-catching or intriguing words that encourage the unsuspecting user to click on the link.
- This method of penetrating a system can allow the malware to bypass the mail server's antivirus filters.

Peer-to-Peer (P2P) Network Attacks

- P2P networks are also used to distribute malware. A worm or a Trojan virus will appear on the P2P network but will be named in a way that's likely to attract attention and get users to download and launch the file.
- In some cases, the malware creators and distributors take steps that reduce the likelihood of victims reporting an infection:
- Victims may respond to a fake offer of a free utility or a guide that promises illegal benefits like:
- Free Internet or mobile communications access.
- The chance to download a credit card number generator. • A method to increase the victim's online account balance.
- In these cases, when the download turns out to be a Trojan virus, the victim will be keen to avoid disclosing their own illegal intentions.
- Hence, the victim will probably not report the infection to any law enforcement agencies.
- As an example of this technique, a Trojan virus was once sent to email addresses that were taken from a recruitment website. People that had registered on the site received fake job offers, but the offers included a Trojan virus. The attack mainly targeted corporate email addresses. The cybercriminals knew that the staff that received the Trojan would not want to tell their employers that they had been infected while they were looking for alternative employment.

How to Spot Social Engineering Attacks

- Defending against social engineering requires you to practice selfawareness.

- Always slow down and think before doing anything or responding.
- Attackers expect you to take action before considering the risks, which means you should do the opposite. How to Prevent Social Engineering Attacks
- Beyond spotting an attack, you can also be proactive about your privacy and security.
- Knowing how to prevent social engineering attacks is incredibly important for all mobile and computer users.

Here are some important ways to protect against all types of cyberattacks:

- Safe Communication and Account Management Habits
- Online communication is where you're especially vulnerable. Social media, email, text messages are common targets, but you'll also want to account for in-person interactions as well.
- Never click on links in any emails or messages .
- You'll want to always manually type a URL into your address bar, regardless of the sender.
- However, take the extra step of investigating to find an official version of the URL in question.
- Never engage with any URL you have not verified as official or legitimate.
- Use multi-factor authentication.
- Online accounts are much safer when using more than just a password to protect them.
- Multi-factor authentication adds extra layers to verify your identity upon account login.
- These "factors" can include biometrics like fingerprint or facial recognition, or temporary passcodes sent via text message.
- Use strong passwords (and a password manager).
- Each of your passwords should be unique and complex.
- Aim to use diverse character types, including uppercase, numbers, and symbols. Also, you will probably want to opt for longer passwords when possible.
- To help you manage all your custom passwords, you might want to use a password manager to safely store and remember them.
- Avoid sharing names of your schools, pets, place of birth, or other personal details.
- You could be unknowingly exposing answers to your security questions or parts of your password.
- If you set up your security questions to be memorable but inaccurate, you'll make it harder for a criminal to crack your account.
- If your first car was a "Toyota," writing a lie like "clown car" instead could completely throw off any prying hackers.
- Be very cautious of building online-only friendships.

- While the internet can be a great way to connect with people worldwide, this is a common method for social engineering attacks.
- Watch for tells and red flags that indicate manipulation or a clear abuse of trust. phishing attack
- Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number.
- It occurs when an attacker is masquerading as a trustworthy entity in electronic communication.

WHAT IS VISHING?

- Vishing is a cybercrime that uses the phone to steal personal confidential information from victims.
- Often referred to as voice phishing, cybercriminals use savvy social engineering tactics to convince victims to act, giving up private information and access to bank accounts.
- Similar to phishing or smishing, vishing relies on convincing victims that they are doing the right thing by responding to the caller.
- Often the caller will pretend to be calling from the government, tax department, police, or the victim's bank.
- Using threats and convincing language cybercriminals make victims feel as though they have no other option than to provide the information being asked of them.
- Some cybercriminals use strong and forceful language and others suggest they are helping the victim to avoid criminal charges.
- A second and common tactic is to leave threatening voicemails that tell the recipient to call back immediately or they risk being arrested, having bank accounts shut down, or worse.
- below are a few steps that you can implement to prevent yourself from becoming victimized by a vishing attack
- Use mobile apps to block caller
- Don't pick up the phone
- Hang up immediately if the caller sounds suspicious
- Verify the caller's identity – obtain name and organization web address
- Establish strict security policies for wiring money or updating payment information
- E.g. require offline confirmation before sending money requests
- Conduct regular vishing exercises Follow-up with security awareness training for staff
- Enroll in an Identity Theft Protection service

Cyberwarfare

Cyberwarfare is the use of cyber attacks against a nation-state, causing it significant harm, up to and including physical warfare, disruption of vital computer systems and loss of life.

What kinds of cyber weapons are used in warfare?

Examples of acts that might qualify as cyberwarfare include the following:

- viruses, phishing, computer worms and malware that can take down critical infrastructure;
- distributed denial-of-service (DDoS) attacks that prevent legitimate users from accessing targeted computer networks or devices;
- hacking and theft of critical data from institutions, governments and businesses;
- spyware or cyber espionage that results in the theft of information that compromises national security and stability
- ransomware that holds control systems or data hostage; and propaganda or disinformation campaigns used to cause serious disruption or chaos.

Types of cyberwarfare attacks?

Destabilization

- In recent years, cybercriminals have been attacking governments through critical infrastructure, including such entities as transportation systems, banking systems, power grids, water supplies, dams and hospitals.
- The adoption of the internet of things makes the manufacturing industry increasingly susceptible to outside threats.
- From a national security perspective, destabilizing critical digital infrastructure inflicts damage on vital modern services or processes.
- For example, an attack on the energy grid could have massive consequences for the industrial, commercial and private sectors.

Sabotage

- Cyber attacks that sabotage government computer systems can be used to support conventional warfare efforts.
- Such attacks can block official government communications, contaminate digital systems, enable the theft of vital intelligence and threaten national security.
- State-sponsored or military-sponsored attacks, for example, may target military databases to get information on troop locations, weapons and equipment being used.

Data theft

- Cybercriminals hack computer systems to steal data that can be used for intelligence, held for ransom, sold, used to incite scandals and chaos, or even destroyed.
- The Center for Strategic and International Studies (CSIS) maintains a timeline record of cyber attacks on government agencies and defense and high-tech companies, as well as economic crimes with losses of more than $1 million.
- In CSIS timelines dating back to 2006, many of the recorded cyber incidents involve hacking and data theft from nation-states.