What is computer security?

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

There are various types of computer security which is widely used to protect the valuable information of an organization.

What is Computer Security and its types?

One way to ascertain the similarities and differences among Computer Security is by asking what is being secured. For example,

- *Information security* is securing information from unauthorized access, modification & deletion
- *Application Security* is securing an application by building security features to prevent from Cyber Threats such as SQL injection, DoS attacks, data breaches and etc.
- C*omputer Security* means securing a standalone machine by keeping it updated and patched
- *Network Security* is by securing both the software and hardware technologies
- *Cybersecurity* is defined as protecting computer systems, which communicate over the computer networks

Components of computer system

The components of a computer system that needs to be protected are:

- *Hardware,* the physical part of the computer, like the system memory and disk drive
- *Firmware,* permanent software that is etched into a hardware device's nonvolatile memory and is mostly invisible to the user
- *Software,* the programming that offers services, like operating system, word processor, internet browser to the user

The CIA Triad

Computer security is mainly concerned with three main areas:

- Confidentiality is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories.
- Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality).

- Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information.

Sample Attacks/ 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 in two categories:

1. Web-based attacks
2. System-based 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 attacker?s 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.

3. **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.

4. **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.

5. 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. It is also known as fabrication attack

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 commands when they receive specific input. Common examples of bots program are the crawler, chatroom bots, and malicious bots.

Active Attack	Passive Attack
In an active attack, Modification in information takes place.	While in passive attack, Modification in the information does not take place.
Active Attack is a danger to Integrity as well as availability.	Passive Attack is a danger to Confidentiality.
In an active attack, attention is on prevention.	While in passive attack attention is on detection.
Due to active attacks, the execution system is always damaged.	While due to passive attack, there is no harm to the system.
In an active attack, Victim gets informed about the attack.	While in a passive attack, Victim does not get informed about the attack.

In an active attack, System resources can be changed.	While in passive attack, System resources are not changing.
Active attack influences the services of the system.	While in passive attack, information and messages in the system or network are acquired.
In an active attack, information collected through passive attacks are used during executing.	While passive attacks are performed by collecting information such as passwords, and messages by themselves.
Active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibited in comparison to active attack.
Can be easily detected.	Very difficult to detect.

The Marketplace for vulnerabilities

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack, or allow an attacker to manipulate the system in some way. Vulnerable consumers fail to understand their preferences and/or lack the knowledge, skills, or freedom to act on them. The aim is to significantly replace trial and error with a robust understanding of markets. This is why Google(with the help of certified and Google Awarded cyber security experts) have a marketplace for everyone to choose cyber security solutions to ease their life.

Vulnerability Types

Computer security vulnerabilities can be divided into:

Network Vulnerabilities: These are issues with a network's hardware or software that expose it to possible intrusion by an outside party. Examples include insecure Wi-Fi access points and poorly-configured firewalls.

Operating System Vulnerabilities: These are vulnerabilities within a particular operating system. Examples include default super user accounts that may exist in some OS installs and hidden backdoor programs.

Error 404 Hacking Digital India Part 1 Chase

1. In error 404 hacking digital India part 1 chase, the cyber crime and cyber attacks hack the information of users like bank detail and personal information.

2. It is real time incident. In this, attacker or hacker creates an attractive video so that victim gets attracted and plays that video into system.

3. When we clicked on video to play then at the time of buffering, hacker can know our current location and GPS history but also have complete access to our contacts, text messages, Facebook, Whatsapp and most importantly our bank details, including our CVV number.

4. Hackers are creating a kind Trojan file, and android apk files. The apk files are distributed all over the internet. Those who download this file will be hacked easily.

5. Potential cyber attacks that is most common in error 404 hacking :

A).Web Application attacks :

i.) A web application is a client - server computer program which uses web browsers and web technology to allow its visitors to store and retrieve data to / from the database over the internet

ii). If there is flaw in the web application , it allows the attacker to manipulate data using SQL injection attack .

B). Network security attacks:

i).Network security attacks are unauthorized actions against private , corporate or governmental IT assets in order to destroy them modify them or steal sensitive data .

ii). As more enterprises invite employees to access data from mobile devices , networks become vulnerable to data theft or total destruction of the data or network .

C). Mobile security attacks:

I). Mobile security, or mobile device security, has become increasingly important in mobile computing.

ii)The security of personal and business information now stored on smartphones.

iii) More and more users and businesses use smartphones to communicate, but also to plan and organize their users work and also private life.

iv). Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks .

Hijacking and Defense:

Control Hijacking:

1. Hijacking is a type of network security attack in which the attacker takes control of a communication.

2. In hijacking (also known as a man in the middle attack), the attacker takes control of an established connection while it is in progress.

3. The attacker intercepts messages in a public key exchange and then retransmits them , substituting their own public key for the requested one , so that the two original parties still appear to be communicating with each other directly .

4. The attacker uses a program that appears to be the server to the client and appears to be the client to the server.

5. This attack may be used simply to gain access to the messages, or to enable the attacker to modify them before retransmitting them.

6. There are three types of control hijacking in computer security:

1. Buffer overflow attacks, 2. Integer overflow attacks, 3. Format string vulnerabilities

Buffer overflow

A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory buffer. As a result, the program attempting to write the data to the buffer overwrites adjacent memory locations. Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes. Types of Buffer Overflow Attacks.

Stack-based buffer overflows are more common, and leverage stack memory that only exists during the execution time of a function.

Heap-based attacks are harder to carry out and involve flooding the memory space allocated for a program beyond memory used for current runtime operations.

Integer overflow

It is also known as wraparound, occurs when an arithmetic operation outputs a numeric value that falls outside allocated memory space or overflows the range of the given value of the integer. Mostly in all programming languages, integers values are allocated limited bits of storage.

Format String Vulnerabilities

Format strings are used in many programming languages to insert values into a text string. In some cases, this mechanism can be abused to perform buffer overflow attacks, extract information or execute arbitrary code. Let’s take a closer look at format string vulnerabilities and see why they exist.

Defense against Control Hijacking:

Run-time Defenses

In order to prevent data loss, prevent data theft,minimize employee downtime, and maximize IT productivity, businesses need an additional line of preventative defense that can block attacks that antivirus doesn’t – before any harm is done. Runtime defense is the set of features that provide predictive protection for containers and threat based active protection for running containers, hosts and serverless functions. Threat based protection includes capabilities like detecting when malware is added to a workload or when a workload connects to a botnet. An emerging category of software known as Runtime Malware Defense offers a promising solution that works by detecting and blocking malware and exploits at runtime.

Advanced Control Hijacking attacks

A control hijack attack is carried out by overwriting part of the data structures of a victim program, causing it to lose control of its control flow and, as a result, the program's and perhaps the underlying system's control. These types of attacks eventually lead to the corruption or overwriting of the data they were holding. A control hijacking attack subverts a program's intended control flow by exploiting a program fault, typically a memory corruption vulnerability, at runtime. A variety of defensive mechanisms have been proposed to mitigate control-flow hijacking attacks. As previously mentioned, complete memory safety, code pointer integrity, and control flow integrity are promising defenses.