AKTU WALA

UNIT - 1

INTRODUCTION

(Computer System Security)

What is Computer Security and What to Learn ?

- **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.**

1. 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.
- *Computer Security* means securing a standalone machine by keeping it updated and patched
- *Network Security* is by securing both the software and hardware technologies

2. Cybersecurity is defined as protecting computer systems, which communicate over the computer networks

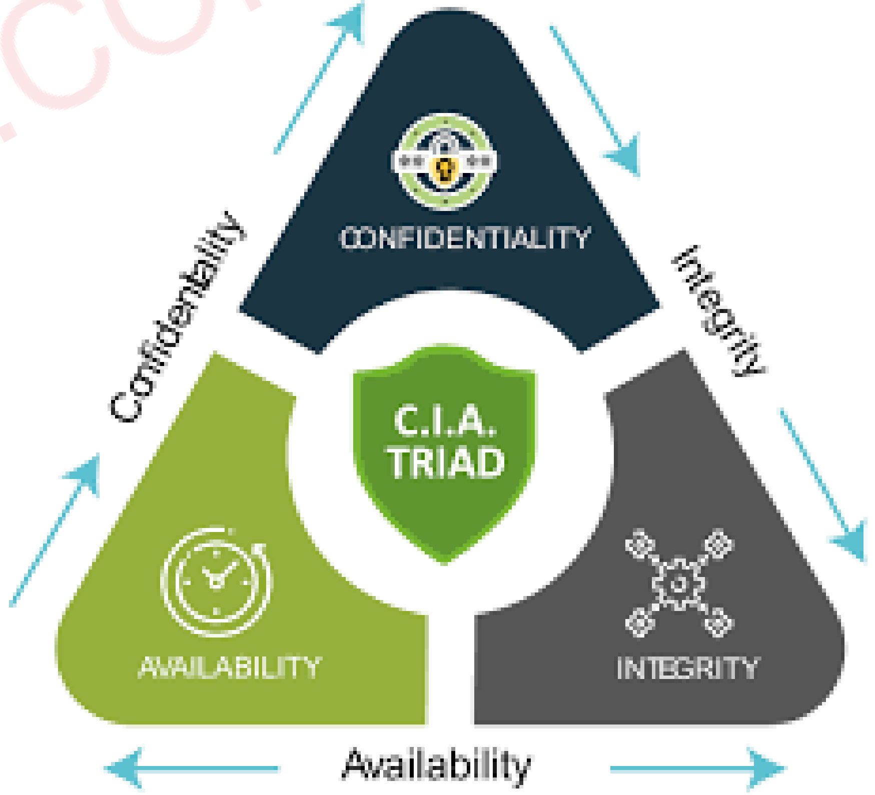
- It’s important to understand the distinction between these words, though there isn’t necessarily a clear consensus on the meanings and the degree to which they overlap or are interchangeable.

3. Computer security can be defined as controls that are put in place to provide confidentiality, integrity, and availability for all components of computer systems. Let’s elaborate the definition.

- **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** : Only authorized users can access the data resources and information .

- **Integrity** : Only authorized users should be able to modify the data when needed .

- **Availability** : Data should be available to user when needed .

- **Authentication** : Communication wiyh the authorized.

Computer Security threats

- A security threat is a threat that has the potential to harm computer systems and organizations. The cause could be physical, such as a computer containing sensitive information being stolen. It's also possible that the cause isn't physical, such as a viral attack.

Type

- **1. Physical Threats:** A physical danger to computer systems is a potential cause of an occurrence/event that could result in data loss or physical damage. It can be classified as:
- **Internal:** Short circuit, fire, non-stable supply of power, hardware failure due to excess humidity, etc. cause it.
- **External:** Disasters such as floods, earthquakes, landscapes, etc. cause it.
- **Human:** Destroying of infrastructure and/or hardware, thefts, disruption, and unintentional/intentional errors are among the threats.

- 2. Non-physical threats: A non-physical threat is a potential source of an incident that could result in:
- Hampering of the business operations that depend on computer systems.
- Sensitive – data or information loss
- Keeping track of other's computer system activities illegally.
- Hacking id & passwords of the users, etc.
- The non-physical threads can be commonly caused by:
- (i) Malware: Malware ("malicious software") is a type of computer program that infiltrates and damages systems without the users' knowledge. Malware tries to go unnoticed by either hiding or not letting the user know about its presence on the system. You may notice that your system is processing at a slower rate than usual.
- (ii) Virus: It is a program that replicates itself and infects your computer's files and programs, rendering them inoperable. It is a type of malware that spreads by inserting a copy of itself into and becoming part of another program. It spreads with the help of software or documents. They are embedded with software and documents and then transferred from one computer to another using the network, a disk, file sharing, or infected e-mail. They usually appear as an executable file.
- (iii) Spyware: Spyware is a type of computer program that tracks, records, and reports a user's activity (offline and online) without their permission for the purpose of profit or data theft. Spyware can be acquired from a variety of sources, including websites, instant chats, and emails. A user may also unwittingly obtain spyware by adopting a software program's End User License Agreement.
  Adware is a sort of spyware that is primarily utilized by advertising. When you go online, it keeps track of your web browsing patterns in order to compile data on the types of websites you visit.

- **(iv) Worms:** Computer worms are similar to viruses in that they replicate themselves and can inflict similar damage. Unlike viruses, which spread by infecting a host file, worms are freestanding programs that do not require a host program or human assistance to proliferate. Worms don't change programs; instead, they replicate themselves over and over. They just eat resources to make the system down.
- **(v) Trojan:** A Trojan horse is malicious software that is disguised as a useful host program. When the host program is run, the Trojan performs a harmful/unwanted action. A Trojan horse, often known as a Trojan, is malicious malware or software that appears to be legal yet has the ability to take control of your computer. A Trojan is a computer program that is designed to disrupt, steal, or otherwise harm your data or network.
- **(vi) Denial Of Service Attacks:** A Denial of Service attack is one in which an attacker tries to prohibit legitimate users from obtaining information or services. An attacker tries to make a system or network resource unavailable to its intended users in this attack. The web servers of large organizations such as banking, commerce, trading organizations, etc. are the victims.
- **(vii) Phishing:** Phishing is a type of attack that is frequently used to obtain sensitive information from users, such as login credentials and credit card details. They deceive users into giving critical information, such as bank and credit card information, or access to personal accounts, by sending spam, malicious Web sites, email messages, and instant chats.
- **(viii) Key-Loggers**: Keyloggers can monitor a user's computer activity in real-time. Keylogger is a program that runs in the background and records every keystroke made by a user, then sends the data to a hacker with the intent of stealing passwords and financial information.

Sample Attacks

- A cyber attack is **any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage**. Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.

1. Web Based attacks.
2. System Based attacks.

1. Web Based attacks.

- Web-based attacks are **an attractive method by which threat actors can delude victims using web systems and services as the threat vector**.

- **Cross-site scripting (XSS).** That involves an attacker uploading a piece of malicious script code onto your website that can then be used to steal data or perform other kinds of mischief. Although this strategy is relatively unsophisticated, it remains quite common and can do significant damage.
- **SQL Injection (SQLI).** This happens when a hacker submits destructive code into an input form. If your systems fail to clean this information, it can be submitted into the database, changing, deleting, or revealing data to the attacker.
- **Path traversal.** Also resulting from improper protection of data that has been inputted, these webserver attacks involve injecting patterns into the webserver hierarchy that allow bad actors to obtain user credentials, databases, configuration files, and other information stored on hard drives.
- **Local File Inclusion.** This relatively uncommon attack technique involves forcing the web application to execute a file located elsewhere on the system.
- **Distributed Denial of Service (DDoS) attacks.** Such destructive events happen when an attacker bombards the server with requests. In many cases, hackers use a network of compromised computers or bots to mount this offensive. Such actions paralyze your server and prevent legitimate visitors from gaining access to your services.

2. System Based attacks.

- 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.

- **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.

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.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, markets habitually governed by social virtues.

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 that will be 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 .

Control Hijacking

- Control-flow hijacking attacks **allow an attacker to subvert a value that is loaded into the program counter of a running program, typically redirecting execution to his own injected code**.

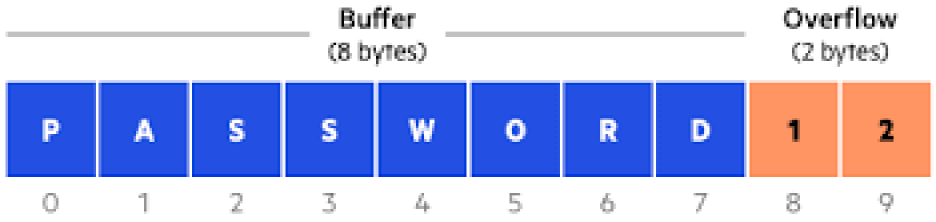
- Buffer overflow attacks.
- Integer overflow attacks.
- Format string attacks.

• What is Buffer Overflow

- Buffers are memory storage regions that temporarily hold data while it is being transferred from one location to another. 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.
- For example, a buffer for log-in credentials may be designed to expect username and password inputs of 8 bytes, so if a transaction involves an input of 10 bytes (that is, 2 bytes more than expected), the program may write the excess data past the buffer boundary.

• Buffer overflow attacks.

- Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information. For example, an attacker may introduce extra code, sending new instructions to the application to gain access to IT systems.



Buffer (8 bytes)								Overflow (2 bytes)	
P	A	S	S	W	O	R	D	1	2
0	1	2	3	4	5	6	7	8	9

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 attacks.

- **If a program performs a calculation and the true answer is larger than the available space**, it may result in an integer overflow. These integer overflows can cause the program to use incorrect numbers and respond in unintended ways, which can then be exploited by attackers.
- For example, if an integer data type allows integers up to two bytes or 16 bits in length (or an unsigned number up to decimal 65,535), and two integers are to be added together that will exceed the value of 65,535, the result will be integer overflow.

- How can integer overflows be avoided?

- Avoidance. By **allocating variables with data types that are large enough to contain all values that may possibly be computed and stored in them**, it is always possible to avoid overflow.

- Format string attacks.

- The Format String exploit occurs when the submitted data of an input string is evaluated as a command by the application. In this way, the attacker could execute code, read the stack, or cause a segmentation fault in the running application, causing new behaviors that could compromise the security or the stability of the system.

• Format string Vulnerability.

A format string vulnerability is a bug where user input is passed as the format argument to `printf`, `scanf`, or another function in that family.

The format argument has many different specifies which could allow an attacker to leak data if they control the format argument to `printf`. Since `printf` and similar are *variadic* functions, they will continue popping data off of the stack according to the format.

For example, if we can make the format argument "%x.%x.%x.%x", `printf` will pop off four stack values and print them in hexadecimal, potentially leaking sensitive information.

Defense Against Controle Hijacking Platform - Runtime Defense

- **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.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**

Important Question

- Explain briefly computer security and components of computer system.
- Explain CIA traits.
- Explain problems related to computer security.
- Discuss various attacks in computer security.
- Discuss error 404 hacking in India part one chase.
- Explain control hijacking.
- Briefly describe buffer overflow attack.
- What is sample attack. Explain SQL injection attack and its prevention.
- Discuss session fixation attack.
- Discuss denial of service attack.

Thankyou

Made By – AKTU WALA (Satyam Sahu)

AKTU WALA

YouTube