❖ Security:

Security is defined as being free from danger, or feeling safe.

✓ **Common Goals:**

1) **Confidentiality:** Confidentiality is equivalent to privacy that avoids unauthorized access of information. It involves ensuring the data is accessible by those who are allowed to use it and blocking access to others. It prevents essential information from reaching the wrong people. Data encryption is an excellent example of ensuring confidentiality.
2) **Integrity:** Integrity refers to the trustworthiness of data or resources. Integrity includes data integrity (the content of the information) and origin integrity (the source of the data, often called authentication). This principle ensures that the data is authentic, accurate, and safeguarded from unauthorized modification by threat actors or accidental user modification. If any modifications occur, certain measures should be taken to protect the sensitive data from corruption or loss and speedily recover from such an event. In addition, it indicates to make the source of information genuine.
3) **Availability:** This principle makes the information to be available and useful for its authorized people always. It ensures that these accesses are not hindered by system malfunction or cyber-attacks.

❖ Threats:

A computer system threat is anything that leads to loss or corruption of data or physical damage to the hardware and infrastructure.

✓ **Security Threat:** Security threat is defined as a **risk** that which can potentially harm computer system.

→ **Physical damage:** It includes fire, water pollution etc.
→ **Natural Events:** It includes climate, Earthquake, volcanic activity etc.
→ **Loss of service:** It includes Electric power, air conditioning, telecom etc.
→ **Technical Failure:** It includes Problems in equipments, Software etc.
→ **Deliberate Type:** It includes Spying, illegal processing of data

✓ **Common threats:**

1. **Virus:** A computer virus is a illegal program designed to disrupt the normal functioning of computer without the permission of user.
2. **Worm:** Worm is a malicious, self- replicating software program which is affects he functions of software and hardware programs.
3. **Trojan horse:** It is hidden piece of code which is intended to leak your confidential information.
4. **Spyware:** It is a computer program that monitors user's online activities or install programs with user's consent for profit or theft of personal information.
5. **Hackers:** Hackers are programmers who put others on threats for their personal gain by breaking into computer system with purpose to steal, change or destroy information.
6. **Phishing Threat:** It is illegal activity through which phishers attempt to steal sensitive financial or personal data by means of fraudent email or instant messages.

❖ Computer Security:

Computer security refers to the protection of a computer's hardware and the data that it holds.
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.

Computer security can be implemented using passwords, encryption, and firewalls, and denying physical access to a computer's location.

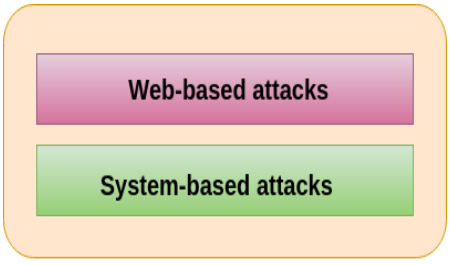
✓ **Types of Computer Security**

1. **Application Security:** Application security is the types of cyber security which developing application by adding security features within applications to prevent from cyber attacks. The attacks can be SQL injection, denial of service (DoS) attacks, data breaches or other cyber-attacks. There are some application security tools and techniques such as firewalls, antivirus software, encryption, and web application firewall which can help to prevent from cyber-attacks.
2. **Information security:** Information security is a type of computer security which refers to the process and methodology to protect the confidentiality, integrity and availability of computer system from unauthorized access, use, modification and destruction. Information security focuses on the CIA triad model, which ensures confidentiality, integrity, and availability of data, without affecting organization productivity.
3. **Network Security:** Network security is another type of computer security which process of preventing and protecting against unauthorized intrusion into computer networks. It is a set of rules and configurations which designed to protect the confidentiality, integrity and accessibility of computer networks system and information using both software and hardware technologies. Network Security is by securing both the software and hardware technologies.
4. **Endpoint Security:** Human error is a major weak point which is easily exploited by cyber criminals. End users are becoming the largest security risk in any organizations. However, end user has no fault of their own, and mostly due to a lack of awareness and ICT policy. They can unintentional open the virtual gates to cyber attackers.
5. **Internet Security:** Internet security is the important types of computer security which has defined as a process to create set of rules and actions to protect computer systems that are connected to the Internet. It is a branch of computer security that deals specifically with internet-based threats such as: Hacking, Computer Viruses, Denial-of-Service Attacks, Malware etc.

❖ Sample Attacks:

A cyber-attack is an exploitation of computer systems and networks.

1. **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-
   a) **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.
   b) Example- SQL Injection, code Injection, log Injection, XML Injection etc.
   c) **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.
   d) **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.
   e) **Phishing:** Phishing is a type of attack which attempts to steal sensitive information like user login credentials and credit card number.



Classification of Cyber attacks

f) **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.

g) **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.

h) **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.

i) **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.

2. **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-

a) **Virus**

b) **Worm**

c) **Trojan horse**

These three definition is above (in Threat Topic)

d) **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.

e) **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. Vulnerabilities are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities. The aim is to significantly replace trial and error with a robust understanding of markets, markets habitually governed by social virtues.

1. Hardware Vulnerability: Hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely.

For examples: Old version of systems or devices, unprotected storage, Unencrypted devices, etc.

2. Software Vulnerability: Software vulnerability is a defect in software that could allow an attacker to gain control of a system. For examples: Lack of input validation, Unverified uploads, Unencrypted data, etc.

3. Network Vulnerability: A weakness happen in network which can be hardware or software.

For examples: Unprotected communication, Malware or malicious software (e.g.: Viruses, Keyloggers, Worms, etc), Social engineering attacks, Misconfigured firewalls etc.

4. Procedural Vulnerability: A weakness happen in an organization operational methods.

For examples: Password procedure – Password should follow the standard password policy.

Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

❖ Error 404 Hacking digital India part 1 chase

- 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.
- 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.
- 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.
- 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.

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

A) Web Application attacks :

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

B.) Network Security attacks:

- Network Security attacks are unauthorized actions against private , corporate or governmental IT assets in order to destroy them modify them or steal sensitive data.
- 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:

- Mobile security, or mobile device security, has become increasingly important in mobile computing.
- The security of personal and business information now stored on smartphones
- More and more users and businesses use smartphones to communicate, but also to plan and organize their users' work and also private life.
- Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks.
- Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must can be controlled to protect the privacy of the user and the intellectual property of the company.

❖ Hijacking

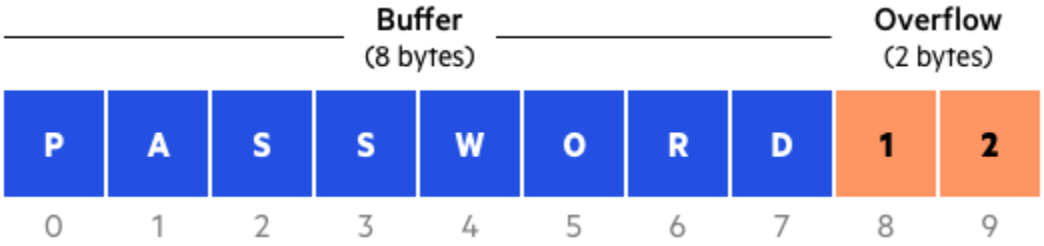
Cyber hijacking, or computer hijacking, is a type of network security attack in which the attacker takes control of computer systems, software programs and/or network communications. Ex: browser hijacking, session hijacking, domain hijacking, clipboard hijacking, domain name system (DNS) hijacking, Internet Protocol (IP) hijacking, page hijacking.

✓ Control Hijacking

1) Buffer overflows attacks:

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.

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, the program may write the excess data past the buffer boundary.



Buffer overflow attack, Attackers exploit buffer overflow issues by overwriting the memory of an application. If attackers know the memory layout of a program, they can intentionally feed input that the buffer cannot store, and overwrite areas that hold executable code, replacing it with their own code. For example, an attacker can overwrite a pointer (an object that points to another area in memory) and point it to an exploit payload, to gain control over the program.

C and C++ are two languages that are highly susceptible to buffer overflow attacks, as they don't have built-in safeguards against overwriting or accessing data in their memory.

✓ **Types of Buffer Overflow Attacks**

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

ii. **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.

✓ **How to Prevent Buffer Overflows**

a) **Address space randomization (ASLR)—**randomly moves around the address space locations of data regions.

b) **Data execution prevention—**flags certain areas of memory as non-executable or executable, which stops an attack from running code in a non-executable region.

c) **Structured exception handler overwrite protection (SEHOP)—**helps stop malicious code from attacking Structured Exception Handling (SEH), a built-in system for managing hardware and software exceptions. It thus prevents an attacker from being able to make use of the SEH overwrite exploitation technique. At a functional level, an SEH overwrite is achieved using a stack-based buffer overflow to overwrite an exception registration record, stored on a thread's stack.

2) Integer overflow attack: Integer overflow, also known as wraparound. An integer overflow is a type of an arithmetic overflow error when the result of an integer operation does not fit within the allocated memory space. Instead of an error in the program, it usually causes the result to be unexpected. Integer overflows have been listed as the number 8 most dangerous software error in the most recent CWE 2019 list.

For example, we have a 16-bit integer value which may store an unsigned integer ranging from 0 to 65535, or signed integer ranging from -32768 to 32767. So, during an arithmetic operation, if the results require more than the allocated space (like 65535+1), the compiler may:

- completely ignore the error caused, or
- Abort the program.

Most compilers will ignore the overflow and store unexpected output or error. This will result in various attacks such buffer overflow which is the most common attack and leads to executing malicious programs or privilege escalation.

✓ **Preventing Integer Overflow Attacks**

a) **Requirement Phase:** We need to ensure that all rules and protocols are defined strictly for all out-of-bound operations.

b) **Architecture & Design:** It is recommended to use libraries and frameworks that are used in secure coding, and best practices in order to avoid undefined or erroneous behavior while handling numbers.

c) **Implementation Phase:** As pointed out earlier, make sure to provide input validation for numbers that are entered by the user.

3) Format string vulnerabilities: A Format String attack can occur when an input string's submitted data is evaluated as a command by the application. Taking advantage of a Format String vulnerability, an attacker can execute code, read the Stack, or cause a segmentation fault in the running application – causing new behaviors that compromise the security or the stability of the system.

Safe Code

The line printf("%s", argv[1]); in the example is safe, if you compile the program and run it:
./example "Hello World %s%s%s%s%s%s"

The printf in the first line will not interpret the "%s%s%s%s%s%s" in the input string, and the output will be: "Hello World %s%s%s%s%s%s".

Vulnerable Code

The line printf(argv[1]); in the example is vulnerable, if you compile the program and run it:
./example "Hello World %s%s%s%s%s%s"

The printf in the second line will interpret the %s%s%s%s%s%s in the input string as a reference to string pointers, so it will try to interpret every %s as a pointer to a string, starting from the location of the buffer (probably on the Stack). At some point, it will get to an invalid address, and attempting to access it will cause the program to crash.

✓ **Preventing Format String Vulnerabilities**

a) Always specify a format string as part of program, not as an input. Most format string vulnerabilities are solved by specifying "%s" as format string and not using the data string as format string

b) If possible, make the format string a constant. Extract all the variable parts as other arguments to the call. Difficult to do with some internationalization libraries.

c) If the above two practices are not possible, use defenses such as Format_Guard . Rare at design time. Perhaps a way to keep using a legacy application and keep costs down. Increase trust that a third-party application will be safe.

❖ Defense against Control Hijacking - Platform Defenses

Same as How to Prevent Buffer Overflows (this topic is above in this unit)

❖ Defense against Control Hijacking - Run-time Defenses

1) **StackGuard:** StackGuard is a compiler extension that enhances the executable code produced by the compiler so that it detects and thwarts buffer-overflow attacks against the stack. StackGuard basically works by inserting a small value known as a canary between the stack variables (buffers) and

the function return address. When a stack-buffer overflows into the function return address, the canary is overwritten.

✓ **Canary Types**

i. **Random canary:** A random canary is chosen at random at the time the program execution. With this method, the attacker could not learn the canary value prior to the program start by searching the executable image.

ii. **Terminator canaries:** Most buffer overflow attacks are based on certain string operations which end at string terminators. A terminator canary contains NULL(0x00), CR (0x0d), LF (0x0a), and EOF (0xff), four characters that should terminate most string operations. This prevents attacks using strcpy() and other methods that return upon copying a null character while the undesirable result is that the canary is known.

2) **Libsafe:** Libsafe is an implementation of vulnerable copy functions in C library such as strcpy().Libsafe is implemented as a shared library that is preloaded to intercept C library function calls. Programs are protected without recompilation unless they are statically linked with the C library. Libsafe protects only those C library functions whereas StackGuard and StackShield protect all functions.

3) **StackShield:** StackShield is also a GNU C compiler extension that protects the return address. When a function is called StackShield copies away the return address to a non-overflowable area, and restores the return address upon returning from a function. Even if the return address on the stack is altered, it has no effect since the original return address is remembered. As with StackGuard, programs needs to be recompiled.

4) **Control-flow integrity:** Control-flow integrity is a general term for computer security techniques that prevent a wide variety of malware attacks from redirecting the flow of execution of a program.

❖ Advanced Control Hijacking attacks

Heap spraying: Heap spraying is a technique used to aid the exploitation of vulnerabilities in computer systems. It is called "spraying the heap" because it involves writing a series of bytes at various places in the heap. The heap is a large pool of memory that is allocated for use by programs. The basic idea is similar to spray painting a wall to make it all the same color. Like a wall, the heap is "sprayed" so that its "color" (the bytes it contains) is uniformly distributed over its entire memory "surface."

✓ **Procedure For The Attack**

i. In the attack, the attacker first uses the exploits in the web browsers and other applications or languages such as Actionscript or Javascript in the Adobe Reader to put the malicious code in the memory heap at some predetermined location.

ii. The attacker further exploits the vulnerability by using the scripting support. For this, he makes the Extended Instruction Pointer (EIP) to directly point the predetermined location.

iii. The attacker thus can further run the malicious code and perform the malicious activity.

✓ **Mitigations For The Attack**

Running the web browsers with the least privileges makes it much harder for the hackers to gain the admin access, which helps in mitigating this attack. Also, update the web browsers regularly to patch up the known bugs.