[Type the company address]

8th Sem

Cyber laws and Ethics

by

Aishwarya Ghosh

OEC IT 802A

**UNIT – 2**

**Cybercrime Mobile & Wireless devices**

**Q: > Security challenges posted by mobile devices:--**

**Answer :>**

**Below are the most common examples of these threats,**

**1. Social Engineering**

Social engineering attacks are when bad actors send fake emails (phishing attacks) or text messages (smishing attacks) to your employees in an effort to trick them into handing over private information like their passwords or downloading malware onto their devices.

**2. Data Leakage via Malicious Apps**

As Dave Jevans, CEO and CTO of Marble Security, [explains](https://www.esecurityplanet.com/mobile-security/10-trickiest-mobile-security-threats.html), “Enterprises face a far greater threat from the millions of generally available apps on their employees’ devices than from mobile malware.”

How to Protect Against Data Leakage

The best way to protect your organization against data leakage through malicious or unsecured applications is by using mobile application management (MAM) tools. These tools allow IT admins to manage corporate apps (wipe or control access permissions) on their employees’ devices without disrupting employees’ personal apps or data.

**3. Unsecured Public WiFi**

Public Wi-Fi networks are generally [less secure](https://www.wired.com/story/public-wifi-safety-tips/) than private networks because there’s no way to know who set the network up, how (or if) it’s secured with encryption, or who is currently accessing it or monitoring it. And as more companies offer remote work options, the public Wi-Fi networks your employees use to access your servers (e.g., from coffee shops or cafes) could present a risk to your organization.

How to Reduce Risks Posed By Unsecured Public WiFi

The best way for you to protect your organization against threats over public WiFi networks is by requiring employees to use a VPN to access company systems or files. This will ensure that their session stays private and secure, even if they use a public network to access your systems.

**4. End-to-End Encryption Gaps**

An encryption gap is like a water pipe with a hole in it. While the point where the water enters (your users’ mobile devices) and the point where the water exits the pipe (your systems) might be secure, the hole in the middle lets bad actors access the water flow in between.

Solution: Ensure everything is Encrypted

For any sensitive work information, end-to-end encryption is a must. This includes ensuring any service providers you work with encrypt their services to prevent unauthorized access, as well as ensuring your users’ devices and your systems are encrypted as well.

**5. Internet of Things (IoT) Devices**

The types of mobile devices that access your organization’s systems are branching out from mobile phones and tablets to include wearable tech (like the Apple Watch) and physical devices (like Google Home or Alexa). And since many of the latest IoT mobile devices have IP addresses, it means bad actors can use them to gain access to your organizations’ network over the internet if those devices are connected to your systems.

**6. Spyware**

Spyware is used to survey or collect data and is most commonly installed on a mobile device when users click on a malicious advertisement (“malvertisement”) or through scams that trick users into downloading it unintentionally.

Whether your employees have an iOS or Android device, their devices are targets ripe for data mining with spyware—which could include your private corporate data if that device is connected to your systems.

How to Protect Against Spyware

Dedicated mobile security apps (like Google’s [Play Protect](https://developers.google.com/android/play-protect)) can help your employees detect and eliminate spyware that might be installed on their devices and be used to access company data. Ensuring your employees keep their device operating systems (and applications) up to date also helps ensure that their devices and your data are protected against the latest spyware threats.

**7. Poor Password Habits**

These bad password habits present a threat to organizations whose employees use their personal devices to access company systems. Since both personal and work accounts are accessible from the same device with the same password, it simplifies the work a bad actor has to do in order to breach your systems.

How to Reduce or Eliminate Mobile Password Threats

Password managers can simplify the work required for your employees to follow these guidelines.

Requiring your employees to use more than one authentication factor (multi-factor authentication or MFA) to access mobile company applications will also help reduce the risk that a bad actor could gain access to your systems since they’d need to verify their identity with additional authentication factors in order to log in.

**8. Lost or Stolen Mobile Devices**

Lost and stolen devices aren’t a new threat for organizations. But with more people [working remotely](https://www.businesswire.com/news/home/20201215005287/en/Upwork-Study-Finds-22-of-American-Workforce-Will-Be-Remote-by-2025) in public places like cafes or coffee shops and accessing your systems with a wider range of devices, lost and stolen devices pose a growing risk to your organization.

How to Protect Against Lost or Stolen Device Threats

First and foremost, you’ll want to ensure employees know what steps to take if they lose their device. Since most devices come with remote access to delete or transfer information, that should include asking employees to make sure those services are activated.

**Q: > Cryptographic security for mobile devices:--**

**Answer :>**

* **Endpoint security**: As organizations embrace flexible and mobile workforces, they must deploy networks that allow remote access. [Endpoint security](https://www.cisco.com/c/en/us/solutions/small-business/security.html#endpoint-security) solutions protect corporations by monitoring the files and processes on every mobile device that accesses a network. By constantly scanning for malicious behaviour, endpoint security can identify threats early on. When they find malicious behaviour, endpoint solutions quickly alert security teams, so threats are removed before they can do any damage.
* **VPN:** A [virtual private network](https://www.cisco.com/site/us/en/products/security/secure-client/index.html), or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct remote work safely.
* **Secure web gateway:** Secure web gateways provide powerful, overarching cloud security. Because 70 percent of attacks are distinct to the organization, businesses need cloud security that identifies previously used attacks before they are launched. Cloud security can operate at the DNS and IP layers to defend against phishing, malware, and ransomware earlier. By integrating security with the cloud, you can identify an attack on one location and immediately prevent it at other branches.
* **Email security**: Email is both the most important business communication tool and the leading attack vector for security breaches. In fact, according to the [latest Cisco Midyear Cybersecurity Report](https://engage2demand.cisco.com/LP=16570), email is the primary tool for attackers spreading ransomware and other malware. Proper email security includes advanced threat protection capabilities that detect, block, and remediate threats faster; prevent data loss; and secure important information in transit with end-to-end encryption.
* **Cloud access security broker**: Your network must secure where and how your employees work, including in the cloud. You will need a cloud access security broker (CASB), a tool that functions as a gateway between on-premises infrastructure and cloud applications (Salesforce, Dropbox, etc.). A CASB identifies malicious cloud-based applications and protects against breaches with a cloud data loss prevention (DLP) engine.

**Q: > Attacks on mobile/cell phones:--**

**Answer :>**

**4 Different Types of Mobile Security Threats:-**

* **Mobile Application Security Threats**: Application-based threats happen when people download apps that look legitimate but actually skim data from their device. Examples are spyware and malware that steal personal and business information without people realizing it’s happening.
* **Web-Based Mobile Security Threats**: Web-based threats are subtle and tend to go unnoticed. They happen when people visit affected sites that seem fine on the front-end but, in reality, automatically download malicious content onto devices.
* **Mobile Network Security Threats**: Network-based threats are especially common and risky because cybercriminals can steal unencrypted data while people use public WiFi networks.
* **Mobile Device Security Threats:** Physical threats to mobile devices most commonly refer to the loss or theft of a device. Because hackers have direct access to the hardware where private data is stored, this threat is especially dangerous to enterprises.

**Q: > Theft, Virus, Hacking. Bluetooth:--**

**Answer :>**

**Cyber Crime – Identity Theft**

Identity Theft also called Identity Fraud is a crime that is being committed by a huge number nowadays. Identity theft happens when someone steals your personal information to commit fraud. This theft is committed in many ways by gathering personal information such as transactional information of another person to make transactions.

**Types of Identity theft:**

* Criminal Identity Theft – This is a type of theft in which the victim is charged guilty and has to bear the loss when the criminal or the thief backs up his position with the false documents of the victim such as ID or other verification documents and his bluff is successful.
* Senior Identity Theft – Seniors with age over 60 are often targets of identity thieves. They are sent information that looks to be actual and then their personal information is gathered for such use. Seniors must be aware of not being the victim.
* Driver’s license ID Identity Theft – Driver’s license identity theft is the most common form of ID theft. All the information on one’s driver’s license provides the name, address, and date of birth, as well as a State driver’s identity number. The thieves use this information to apply for loans or credit cards or try to open bank accounts to obtain checking accounts or buy cars, houses, vehicles, electronic equipment, jewelry, anything valuable and all are charged to the owner’s name.
* Medical Identity Theft – In this theft, the victim’s health-related information is gathered and then a fraud medical service need is created with fraud bills, which then results in the victim’s account for such services.
* Tax Identity Theft – In this type of attack attacker is interested in knowing your Employer Identification Number to appeal to get a tax refund. This is noticeable when you attempt to file your tax return or the Income Tax return department sends you a notice for this.
* Social Security Identity Theft – In this type of attack the thief intends to know your Social Security Number (SSN). With this number, they are also aware of all your personal information which is the biggest threat to an individual.
* Synthetic Identity Theft – This theft is uncommon to the other thefts, thief combines all the gathered information of people and they create a new identity. When this identity is being used than all the victims are affected.
* Financial Identity Theft – This type of attack is the most common type of attack. In this, the stolen credentials are used to attain a financial benefit. The victim is identified only when he checks his balances carefully as this is practiced in a very slow manner.

**Techniques of identity theft:**

* Pretext Calling – Thieves pretending to be an employee of a company over phone asking for financial information are an example of this theft. Pretending as legitimate employees they ask for personal data with some buttery returns.
* Mail Theft – This is a technique in which credit card information with transactional data is extracted from the public mailbox.
* Phishing – This is a technique in which emails pertaining to be from banks are sent to a victim with malware in it. When the victim responds to mail their information is mapped by the thieves.
* Internet – Internet is widely used by the world as attackers are aware of many techniques of making users get connected with public networks over Internet which is controlled by them and they add spyware with downloads.
* Dumpster Diving – This is a technique that has made much information out of the known institutions. As garbage collectors are aware of this they search for account related documents that contain social security numbers with all the personal documents if not shredded before disposing of.
* Card Verification Value (CVV) Code Requests – The Card Verification Value number is located at the back of your debit cards. This number is used to enhance transaction security but several attackers ask for this number while pretending as a bank official.

**Steps Of Prevention From Identity Theft:**

1. Use Strong Passwords and do not share your PIN with anyone on or off the phone.
2. Use two-factor notification for emails.
3. Secure all your devices with a password.
4. Don’t install random software from the internet.
5. Don’t post sensitive information over social media.
6. While entering passwords at payment gateway ensure its authenticity.
7. Limit the personal information to be carried with out.
8. Keep a practice of changing your PIN and password regularly.
9. Do not disclose your information over phone.
10. While traveling do not disclose personal information with strangers.
11. Never share your Aadhar/PAN number (In India) with anyone whom you do not know/trust.

**Bluetooth:-**

Bluetooth hacking is a type of cyber-attack carried out through vulnerabilities present in Bluetooth’s hardware and software. Hackers purposefully look for exploitable weaknesses in the security of Bluetooth; once one has been found, they use it to access devices and information that they should not have access to.

**How is Bluetooth Hacking Carried Out?**

**Bluejacking:**

Through this vulnerability, any malicious hacker within range of your Bluetooth-activated device will be able to send unsolicited messages to you. Generally, this form of hack does not go beyond that, hence making it comparable to prank calls and other minor inconveniences.

The main risk posed by Bluejacking is emotional, given the fact that the messages being sent by the hackers may be threatening or otherwise disturbing to the receiver.

**Bluesnarfing**

A much more serious type of Bluetooth cyberattack is Bluesnarfing. The mechanism behind this type of attack is complex; however, broadly speaking, Bluesnarfing involves hackers connecting to your phone through Bluetooth without your consent or realization.

Once connected, these hackers will have access to a plethora of data present within your phone.

**Bluebugging**

This is arguably the most dangerous type of Bluetooth attack that you can encounter. Fortunately, however, it is also very rare because only extremely skilled hackers can perform it.

Bluebugging takes place when a hacker manages to place a backdoor in your device. A backdoor, in this context, is a piece of software that allows them access to your device whenever they want. Through this, they can connect to it without your knowledge or permission.

Moreover, they will be able to view what you are doing and listen in on your phone calls in real-time.

Perhaps the worst thing about Bluebugging is that the victim is not even aware that their cybersecurity has been compromised. The hacker will simply be able to use your device on your behalf without alerting you indefinitely.

**How to Protect Yourself From Bluetooth Hacking:**

* Turning Bluetooth Off When It Is Not In Use
* Updating Drivers
* Avoid Pairing in Public
* Watch Who You Pair With
* Do Not Share Sensitive Information
* Use a Virtual Private Network(VPN)

**Q: > Different viruses on laptop:--**

**Answer :>**

A computer virus is a program or piece of code designed to damage your computer by corrupting system files, wasting resources, destroying data or otherwise being a nuisance.

[Viruses](https://www.avg.com/en/signal/topic/viruses) are unique from other forms of malware in that they are self-replicating — capable of copying themselves across files or other computers without a user's consent.

Basically, they are really contagious.

**File Virus:**

This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a Parasitic virus because it leaves no file intact but also leaves the host functional.

**Boot sector Virus:**

It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as memory viruses as they do not infect the file systems.

**Macro Virus:**

Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spread-sheet files.

**Source code Virus**:

It looks for source code and modifies it to include virus and to help spread it.

**Polymorphic Virus**:

A virus signature is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of the virus remains the same but its signature is changed.

**Encrypted Virus:**  
In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.

**Stealth Virus:**   
It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of viruses becomes very difficult. For example, it can change the read system call such that whenever the user asks to read a code modified by a virus, the original form of code is shown rather than infected code.

**Tunnelling Virus:**  
This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunnelling virus. Similar viruses install themselves in device drivers.

**Multipartite Virus:**  
This type of virus is able to infect multiple parts of a system including the boot sector, memory, and files. This makes it difficult to detect and contain.

**Armoured Virus:**  
An armoured virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

**Browser Hijacker:**   
As the name suggests this virus is coded to target the user’s browser and can alter the browser settings. It is also called the browser redirect virus because it redirects your browser to other malicious sites that can harm your computer system.

**UNIT – 3**

**Tools and Methods used in Cyber crime**

**Q: > Proxy servers:--**

**Answer :>**

A proxy server is a system or router that provides a gateway between users and the internet. Therefore, it helps prevent cyber attackers from entering a private network. It is a server, referred to as an “intermediary” because it goes between end-users and the web pages they visit online.

When a computer connects to the internet, it uses an IP address. This is similar to your home’s street address, telling incoming data where to go and marking outgoing data with a return address for other devices to authenticate. A proxy server is essentially a computer on the internet that has an IP address of its own.

**Benefits of a Proxy Server**

Proxies come with several benefits that can give your business an advantage:

1. **Enhanced security**: Can act like a firewall between your systems and the internet. Without them, hackers have easy access to your IP address, which they can use to infiltrate your computer or network.
2. **Private browsing, watching, listening, and shopping**: Use different proxies to help you avoid getting inundated with unwanted ads or the collection of IP-specific data. With a proxy, site browsing is well-protected and impossible to track.
3. **Access to location-specific content**: You can designate a proxy server with an address associated with another country. You can, in effect, make it look like you are in that country and gain full access to all the content computers in that country are allowed to interact with. For example, the technology can allow you to open location-restricted websites by using local IP addresses of the location you want to appear to be in.
4. **Prevent employees from browsing inappropriate or distracting sites**: You can use it to block access to websites that run contrary to your organization’s principles. Also, you can block sites that typically end up distracting employees from important tasks. Some organizations block social media sites like Facebook and others to remove time-wasting temptations.

**Types of Proxy Servers:-**

**Forward Proxy**

A forward proxy sits in front of clients and is used to get data to groups of users within an internal network. When a request is sent, the proxy server examines it to decide whether it should proceed with making a connection.

**Transparent Proxy**

A transparent proxy can give users an experience identical to what they would have if they were using their home computer. In that way, it is “transparent.” They can also be “forced” on users, meaning they are connected without knowing it.

**Anonymous Proxy**

An anonymous proxy focuses on making internet activity untraceable. It works by accessing the internet on behalf of the user while hiding their identity and computer information.

A anonymous proxy is best suited for users who want to have full anonymity while accessing the internet. While anonymous proxies provide some of the best identity protection possible, they are not without drawbacks. Many view the use of anonymous proxies as underhanded, and users sometimes face pushback or discrimination as a result.

**High Anonymity Proxy**

A high anonymity proxy is an anonymous proxy that takes anonymity one step further. It works by erasing your information before the proxy attempts to connect to the target site.

The server is best suited for users for whom anonymity is an absolute necessity, such as employees who do not want their activity traced back to the organization. On the downside, some of them, particularly the free ones, are decoys set up to trap users in order to access their personal information or data.

**Distorting Proxy**

A distorting proxy identifies itself as a proxy to a website but hides its own identity. It does this by changing its IP address to an incorrect one.

**Residential Proxy**

A residential proxy gives you an IP address that belongs to a specific, physical device. All requests are then channeled through that device.

**Public Proxy**

A public proxy is accessible by anyone free of charge. It works by giving users access to its IP address, hiding their identity as they visit sites.

**Shared Proxy**

Shared proxies are used by more than one user at once. They give you access to an IP address that may be shared by other people, and then you can surf the internet while appearing to browse from a location of your choice.

**Q: > Pan word checking, Random checking:--**

**Answer:>**

* **Pan word checking:-**

Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system’s defences which attackers could take advantage of.

**What are the types of pen tests?**

* **Open-box pen test** - In an open-box test, the hacker will be provided with some information ahead of time regarding the target company’s security info.
* **Closed-box pen test** - Also known as a ‘single-blind’ test, this is one where the hacker is given no background information besides the name of the target company.
* **Covert pen test** - Also known as a ‘double-blind’ pen test, this is a situation where almost no one in the company is aware that the pen test is happening, including the IT and security professionals who will be responding to the attack. For covert tests, it is especially important for the hacker to have the scope and other details of the test in writing beforehand to avoid any problems with law enforcement.
* **External pen test** - In an external test, the ethical hacker goes up against the company’s external-facing technology, such as their website and external network servers. In some cases, the hacker may not even be allowed to enter the company’s building. This can mean conducting the attack from a remote location or carrying out the test from a truck or van parked nearby.
* **Internal pen test** - In an internal test, the ethical hacker performs the test from the company’s internal network. This kind of test is useful in determining how much damage a disgruntled employee can cause from behind the company’s firewall.
* **Random checking:-**

Random numbers play an important role in the use of encryption for various network security applications. In this section, we provide a brief overview of the use of random numbers in network security and then look at some approaches to generating random numbers.

**The Use of Random Numbers:-**

**Randomness**

Traditionally, the concern in the generation of a sequence of allegedly random numbers has been that the sequence of numbers be random in some well-defined statistical sense. The following two criteria are used to validate that a sequence of numbers is random:

* Uniform distribution: The distribution of numbers in the sequence should be uniform; that is, the frequency of occurrence of each of the numbers should be approximately the same.
* Independence: No one value in the sequence can be inferred from the others.

**Unpredictability**

In applications such as reciprocal authentication and session key generation, the requirement is not so much that the sequence of numbers be statistically random but that the successive members of the sequence are unpredictable. With "true" random sequences, each number is statistically independent of other numbers in the sequence and therefore unpredictable.

**Q: > Trojan Horses and backdoors:--**

**Answer:>**

* **Trojan Horses:-**

The name of the Trojan Horse is taken from a classical story of the Trojan War.  It is a code that is malicious in nature and has the capacity to take control of the computer. It is designed to steal, damage, or do some harmful actions on the computer. It tries to deceive the user to load and execute the files on the device. After it executes, this allows cybercriminals to perform many actions on the user’s computer like deleting data from files, modifying data from files, and more.

**Some features of the Trojan horse are as follows :**

* It steals information like a password and more.
* It can be used to allow remote access to a computer.
* It can be used to delete data and more on the user’s computers.

**How Trojans are used?**

1. **Spy**–   
   Some Trojans act as spyware. It is designed to take the data from the victim like social networking (username and passwords), credit card details, and more.
2. **Creating backdoors –**  
   The Trojan makes some changes in the system or the device of the victim, So this is done to let other malware or any cyber criminals get into your device or the system.
3. **Zombie –**  
   There are many times that the hacker is not at all interested in the victim’s computer, but they want to use it under their control.

**Advantage of the Trojan Horse:**

* It can be sent as an attachment in an email.
* It can be in some pop-up ads that we find on the web page.

**Disadvantages of the Trojan Horse:**

* It can’t manifest by itself. It requires the implementation of the .exe files.
* It remains undetected and starts its execution when the user is doing any online transaction activity.

**How to prevent this virus:**

1. Do not download anything like the images, and audios from an unsecured website.
2. Do not click on the ads that pop up on the page with advertisements for online games.
3. Do not open any attachment that has been sent from an unknown use.

* **Backdoors:-**

A [backdoor](https://www.safetydetectives.com/blog/what-is-a-backdoor-and-how-to-protect-against-it/#Backdoor) is any method that can allow another user to access your device without your knowledge or consent (and usually without the device’s knowledge, either). A backdoor can be installed by software and hardware developers, or it can be installed by cybercriminals in order to gain unauthorized access to a device, install malware, steal user data, or sabotage a network.

In cyber security, a backdoor is anything that can allow an outside user into your device without your knowledge or permission. Backdoors can be installed in two different parts of your system:

* **Hardware/firmware.**Physical alterations that provide remote access to your device.
* **Software.**Malware files that hide their tracks so your operating system doesn’t know that another user is accessing your device.

A backdoor can be installed by software and hardware developers for remote tech support purposes, but in most cases, backdoors are installed either by cybercriminals or intrusive governments to help them gain access to a device, a network, or a software application.

**Best Ways to Prevent Backdoor Attacks:-**

* Use an Antivirus
* Download with Care
* Use a Firewall
* Use a Password Manager
* Stay on Top of Security Updates/Patches

**Q: > DOS & DDOS attacks:--**

**Answer:>**

* **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.

**DoS attacks typically fall in 2 categories:**

**1.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.

**2.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.

* **Distributed denial-of-service (DDoS) attack:-**

A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as [IoT devices](https://www.cloudflare.com/learning/ddos/glossary/internet-of-things-iot/).

**Types of DDoS Attacks:-**

**1. Volume-Based or Volumetric Attacks**

This type of attack aims to control all available bandwidth between the victim and the larger internet. Domain name system (DNS) amplification is an example of a volume-based attack. In this scenario, the attacker spoofs the target's address, then sends a DNS name lookup request to an open DNS server with the spoofed address.

2. **Protocol Attacks**

A SYN flood is an example of a protocol attack, in which the attacker sends the target an overwhelming number of [transmission control protocol (TCP)](https://www.fortinet.com/resources/cyberglossary/tcp-ip) handshake requests with spoofed source [Internet Protocol (IP) addresses](https://www.fortinet.com/resources/cyberglossary/what-is-ip-address). The targeted servers attempt to respond to each connection request, but the final handshake never occurs, overwhelming the target in the process.

**3. Application-Layer Attacks**

A server runs database queries to generate a web page. In this form of attack, the attacker forces the victim's server to handle more than it normally does. An HTTP flood is a type of application-layer attack and is similar to constantly refreshing a web browser on different computers all at once. In this manner, the excessive number of HTTP requests overwhelms the server, resulting in a DDoS.

**Difference between DOS and DDOS:**

| **DOS** | **DDOS** |
| --- | --- |
| DOS Stands for Denial of service attack. | DDOS Stands for Distributed Denial of service attack. |
| In Dos attack single system targets the victim system. | In DDoS multiple systems attacks the victims system.. |
| Victim PC is loaded from the packet of data sent from a single location. | Victim PC is loaded from the packet of data sent from Multiple location. |
| Dos attack is slower as compared to DDoS. | DDoS attack is faster than Dos Attack. |
| Can be blocked easily as only one system is used. | It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations. |
| In DOS Attack only single device is used with DOS Attack tools. | In DDoS attack,The volumeBots are used to attack at the same time. |
| DOS Attacks are Easy to trace. | DDOS Attacks are Difficult to trace. |
| Volume of traffic in the Dos attack is less as compared to DDos. | DDoS attacks allow the attacker to send massive volumes of traffic to the victim network. |
| Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack | Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack. |

**Q: > SQL injection:--**

**Answer:>**

SQL injection (SQLi) is a cyberattack that injects malicious SQL code into an application, allowing the attacker to view or modify a database. According to the Open Web Application Security Project, injection attacks, which include SQL injections, were the third most serious web application security risk in 2021. In the applications they tested, there were 274,000 occurrences of injection.

**3 Types of SQL Injection**

**1. In-band SQL Injection**

In-band SQL injection is the most common type of attack. With this type of SQL injection attack, a malicious user uses the same communication channel for the attack and to gather results. The following techniques are the most common types of in-band SQL injection attacks:

* **Error-based SQL injection**: With this technique, attackers gain information about the database structure when they use a SQL command to generate an error message from the database server. Error messages are useful when developing a web application or web page, but they can be a vulnerability later because they expose information about the database. To prevent this vulnerability, you can disable error messages after a website or application is live.
* **Union-based SQL injection**: With this technique, attackers use the UNION SQL operator to combine multiple select statements and return a single HTTP response. An attacker can use this technique to extract information from the database. This technique is the most common type of SQL injection and requires more security measures to combat than error-based SQL injection.

**2. Inferential SQL Injection**

Inferential SQL injection is also called blind SQL injection because the website database doesn’t transfer data to the attacker like with in-band SQL injection. Instead, a malicious user can learn about the structure of the server by sending data payloads and observing the response. Inferential SQL injection attacks are less common than in-band SQL injection attacks because they can take longer to complete. The two types of inferential SQL injection attacks use the following techniques:

* Boolean injection: With this technique, attackers send a SQL query to the database and observe the result. Attackers can infer if a result is true or false based on whether the information in the HTTP response was modified.
* Time-based injection: With this technique, attackers send a SQL query to the database, making the database wait a specific number of seconds before responding. Attackers can determine if the result is true or false based on the number of seconds that elapses before a response. For example, a hacker could use a SQL query that commands a delay if the first letter of the first database’s name is A. Then, if the response is delayed, the attacker knows the query is true.

**3. Out-of-Band SQL Injection**

Out-of-band SQL injection is the least common type of attack. With this type of SQL injection attack, malicious users use a different communication channel for the attack than they use to gather results. Attackers use this method if a server is too slow or unstable to use inferential SQL injection or in-band SQL injection.

## 9 Best Practices to Protect Your Database from SQL Injection

1. Install the latest software and security patches from vendors when available.
2. Give accounts that connect to the SQL database only the minimum privileges needed.
3. Don’t share database accounts across different websites and applications.
4. Use validation for all types of user-supplied input, including drop-down menus.
5. Configure error reporting instead of sending error messages to the client web browser.
6. Use prepared statements with parameterized queries that define all the SQL code and pass in each parameter so attackers can’t change the intent of a query later.
7. Use stored procedures to build SQL statements with parameters that are stored in the database and called from the application.
8. Use allowlist input validation to prevent unvalidated user input from being added to query.
9. Escape all user-supplied input before putting it in a query so that the input isn’t confused with SQL code from the developer.

**Q: > Buffer over flow:--**

**Answer:>**

Buffer overflow is a software coding error or vulnerability that can be exploited by hackers to gain unauthorized access to corporate systems. It is one of the best-known software security vulnerabilities yet remains fairly common. This is partly because buffer overflows can occur in various ways and the techniques used to prevent them are often error-prone.

The software error focuses on buffers, which are sequential sections of computing memory that hold data temporarily as it is transferred between locations. Also known as a buffer overrun, buffer overflow occurs when the amount of data in the buffer exceeds its storage capacity. That extra data overflows into adjacent memory locations and corrupts or overwrites the data in those locations.

**Types of Buffer Overflow Attacks**

1. Stack-based buffer overflows: This is the most common form of buffer overflow attack. The stack-based approach occurs when an attacker sends data containing malicious code to an application, which stores the data in a stack buffer. This overwrites the data on the stack, including its return pointer, which hands control of transfers to the attacker.
2. Heap-based buffer overflows: A heap-based attack is more difficult to carry out than the stack-based approach. It involves the attack flooding a program’s memory space beyond the memory it uses for current runtime operations.
3. Format string attack: A format string exploit takes place when an application processes input data as a command or does not validate input data effectively. This enables the attacker to execute code, read data in the stack, or cause segmentation faults in the application. This could trigger new actions that threaten the security and stability of the system.

**How to Prevent Buffer Overflows**

Application developers can prevent buffer overflows by building security measures into their development code, using programming languages that include built-in protection, and regularly testing code to detect and fix errors.

1. Address space layout randomization (ASLR): Buffer overflow attacks typically need to know where executable code is located. ASLR moves at random around locations of data regions to randomize address spaces, which makes overflow attacks almost impossible.
2. Data execution prevention: This method prevents an attack from being able to run code in non-executable regions by flagging areas of memory as executable or non-executable.
3. Structured exception handling overwrite protection (SEHOP): Attackers may look to overwrite the structured exception handling (SEH), which is a built-in system that manages hardware and software exceptions. They do this through a stack-based overflow attack to overwrite the exception registration record, which is stored on the program’s stack. SEHOP prevents attackers’ malicious code from being able to attack the SEH and use its overwrite exploitation technique.

**UNIT – 4A**

**Phishing & Identity Theft**

**Q: > Phishing methods:--**

**Answer** :> Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim’s machine. Phishing is a common type of cyber-attack that everyone should learn about in order to protect themselves.

**Types of phishing attacks:**

**1. Spear phishing:** Spear phishing targets specific individuals instead of a wide group of people. Spear phishing is often the first step used to penetrate a company’s defenses and carry out a targeted attack.

**2. Whaling:** These attackers often spend considerable time profiling the target to find the opportune moment and means of stealing login credentials. Whaling is of particular concern because high-level executives are able to access a great deal of company information.

**3. Pharming**: Similar to phishing, pharming sends users to a fraudulent website that appears to be legitimate. However, in this case, victims do not even have to click a malicious link to be taken to the bogus site. Attackers can infect either the user’s computer or the website’s DNS server and redirect the user to a fake site even if the correct URL is typed in.

**Spear phishing: Going after specific targets**

**Whaling: Going after the big one**

**Clone phishing: When copies are just as effective**

**Vishing: Phishing over the phone**

**Smishing: Phishing via text message**

**Snowshoeing: Spreading poisonous messages**

**Q: > ID Theft:--**

**Answer :>** Identity Theft also called Identity Fraud is a crime that is being committed by a huge number nowadays. Identity theft happens when someone steals your personal information to commit fraud. This theft is committed in many ways by gathering personal information such as transactional information of another person to make transactions.

* **Criminal Identity Theft –**This is a type of theft in which the victim is charged guilty and has to bear the loss when the criminal or the thief backs up his position with the false documents of the victim such as ID or other verification documents and his bluff is successful.
* **Senior Identity Theft –**Seniors with age over 60 are often targets of identity thieves. They are sent information that looks to be actual and then their personal information is gathered for such use. Seniors must be aware of not being the victim.
* **Driver’s license ID Identity Theft –**Driver’s license identity theft is the most common form of ID theft. All the information on one’s driver’s license provides the name, address, and date of birth, as well as a State driver’s identity number. The thieves use this information to apply for loans or credit cards or try to open bank accounts to obtain checking accounts or buy cars, houses, vehicles, electronic equipment, jewellery, anything valuable and all are charged to the owner’s name.
* **Medical Identity Theft –**In this theft, the victim’s health-related information is gathered and then a fraud medical service need is created with fraud bills, which then results in the victim’s account for such services.
* **Tax Identity Theft** – In this type of attack attacker is interested in knowing your Employer Identification Number to appeal to get a tax refund. This is noticeable when you attempt to file your tax return or the Income Tax return department sends you a notice for this.
* **Social Security Identity Theft** – In this type of attack the thief intends to know your Social Security Number (SSN). With this number, they are also aware of all your personal information which is the biggest threat to an individual.
* **Synthetic Identity Theft** – This theft is uncommon to the other thefts, thief combines all the gathered information of people and they create a new identity. When this identity is being used than all the victims are affected.
* **Financial Identity Theft** – This type of attack is the most common type of attack. In this, the stolen credentials are used to attain a financial benefit. The victim is identified only when he checks his balances carefully as this is practiced in a very slow manner.

**Steps Of Prevention From Identity Theft:**

Following are some methods by which you can enhance your security for identity thefts :

1. Use Strong Passwords and do not share your PIN with anyone on or off the phone.
2. Use two-factor notification for emails.
3. Secure all your devices with a password.
4. Don’t install random software from the internet.
5. Don’t post sensitive information over social media.
6. While entering passwords at payment gateway ensure its authenticity.
7. Limit the personal information to be carried with out.
8. Keep a practice of changing your PIN and password regularly.
9. Do not disclose your information over phone.
10. While traveling do not disclose personal information with strangers.

**Q: > Online identity method:--**

**Answer :>**

**Here are the top 10 ways you can protect yourself online:**

**1. Use Strong Passwords**

**2. Look for Encryption**

**3. Install Security Suites**

**4. Turn on Web Browser Blacklisting**

**5. Avoid Phishing Scams**

**6. Get Private Data Protection**

**7. Password-Protect Your Wireless Router**

**8. Hide Your Personal Information**

**9. Enable Cookies on Your Web Browser Only When Required**

**10. Protect Your Credit Card Info**

**11. Enable Only Vital Browser Cookies**

**12. Delete Existing Cookies**

**13. Avoid Using Public Wi-Fi**

**14. Don't Overshare Online**

**15. Limit Credit Card for Online Shopping**

**UNIT – 4B**

**Cybercrime & Cyber security**

**Q: > Legal aspects:--**

**Answer :>**

The legal aspects of cybercrime and security vary depending on the jurisdiction, but there are several common elements and legal frameworks that address these issues globally. Here are some key legal aspects related to cybercrime and security:

1. Legislation: Countries around the world have enacted legislation to address cybercrime and ensure cybersecurity. These laws define various cyber offenses, prescribe penalties for committing them, and outline procedures for investigation, prosecution, and punishment. Examples include the Computer Fraud and Abuse Act (CFAA) in the United States, the Computer Misuse Act (CMA) in the United Kingdom, and the Cybercrime Prevention Act in the Philippines.
2. Jurisdiction: Determining jurisdiction in cyberspace can be challenging due to the global nature of the internet. Legal frameworks define rules regarding jurisdiction for investigating and prosecuting cybercrimes. International cooperation and mutual legal assistance treaties facilitate cooperation between countries to combat cybercrime effectively.
3. Data Protection and Privacy Laws: Laws related to data protection and privacy play a crucial role in ensuring cybersecurity. They regulate the collection, storage, processing, and sharing of personal and sensitive data, imposing obligations on organizations to protect the privacy of individuals. Examples include the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States.
4. Intellectual Property Rights: Cybercrime often involves intellectual property (IP) violations such as copyright infringement, trademark violations, and trade secret theft. Laws related to IP protection address these issues and provide legal remedies for the owners of intellectual property.
5. International Cooperation: Cybercrime is a global issue that requires international cooperation among law enforcement agencies. International agreements, such as the Budapest Convention on Cybercrime, facilitate cooperation in investigating and prosecuting cybercrimes across borders.
6. Cybersecurity Standards and Regulations: Governments and industry bodies may establish cybersecurity standards and regulations to protect critical infrastructure and sensitive systems. Compliance with these standards may be mandatory in certain sectors to ensure adequate security measures are implemented.
7. Digital Forensics: Digital forensics plays a vital role in cybercrime investigations and legal proceedings. Laws and procedures govern the collection, preservation, and admissibility of digital evidence in court.
8. Penalties and Sentencing: Legal frameworks establish penalties for cybercrimes, including fines and imprisonment. The severity of the punishment depends on the nature and severity of the offense committed.

**Q: > Indian laws, IT act:--**

**Answer :>**

The Information Technology (IT) Act of 2000 is an Indian legislation that deals with various aspects of cybercrime, electronic commerce, and digital signatures. It was enacted to provide legal recognition for electronic transactions, promote e-governance, and establish mechanisms for addressing cybersecurity concerns. Here are some key highlights of the IT Act pertaining to cybercrime and security:

1. Definition of Cybercrime: The IT Act defines various cybercrimes, including unauthorized access to computer systems, hacking, identity theft, phishing, data theft, cyber stalking, distributing obscene materials, and cyber terrorism.
2. Offenses and Penalties: The Act outlines offenses related to cybercrime and prescribes corresponding penalties. For example, unauthorized access to a computer system, downloading, or tampering with data without permission is punishable with imprisonment and/or fines. The severity of penalties depends on the nature and impact of the offense.
3. Cyber Security and Data Protection: The IT Act emphasizes the importance of maintaining cybersecurity and protecting sensitive data. It mandates organizations to implement reasonable security practices to safeguard electronic data and personal information. Failure to comply with data protection requirements can result in legal consequences.
4. Digital Signatures: The Act recognizes digital signatures as legally valid and provides a framework for their use in electronic transactions. It establishes the Controller of Certifying Authorities (CCA) to regulate and license Certifying Authorities (CAs) responsible for issuing digital signatures.
5. Cyber Appellate Tribunal: The Act established the Cyber Appellate Tribunal (CAT) to handle appeals against orders issued by the Adjudicating Officer under the Act. CAT has the authority to hear and dispose of appeals related to cybercrimes and other offenses.
6. Blocking of Websites and Intermediaries: The Act grants the government the power to block websites or take down content that violates the law. It also defines the obligations and liabilities of intermediaries, such as internet service providers and social media platforms, for hosting or transmitting unlawful content.
7. Preservation and Retention of Data: The Act requires service providers to retain and preserve user data for a specified period to assist law enforcement agencies in investigating cybercrimes.

It is important to note that the IT Act has undergone amendments over the years to address emerging challenges and align with international standards. Additionally, the Act works in conjunction with other relevant laws, such as the Indian Penal Code (IPC) and the Indian Evidence Act, to ensure comprehensive legal provisions for combating cybercrime and ensuring cybersecurity in India.

**Q: > Public key certificate:--**

**Answer :>**

A public key certificate is a digitally signed document that serves to validate the sender's authorization and name. It uses a cryptographic structure that binds a public key to an entity, such as a user or organization. The digital document is generated and issued by a trusted third party called a *certification authority*.

Public key certificates, which are also known as [digital certificates](https://www.techtarget.com/searchsecurity/definition/digital-certificate), include the [public key](https://www.techtarget.com/searchsecurity/definition/public-key), identity information about the owner and the name of the issuing [certificate authority](https://www.techtarget.com/searchsecurity/definition/certificate-authority) (CA).

**How does a public key certificate work?**

There are different types of public key certificates for different functions, such as authorization for a specific type of action. The following are common fields found in digital certificates:

* **Serial number.**This number distinguishes the certificate from other certificates.
* **Algorithm information.**The issuer uses this algorithm to sign the certificate.
* **Issuer.**This is the name of the CA that issued the certificate.
* **Validity period of the certificate.**These are the start and end dates that define when the certificate is valid.
* **Subject distinguished name.**This is the name of the identity to which the certificate is issued.
* **Subject public key information.**This is the public key that is associated with the identity.

**What are the different types of certificates?**

* **Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates:-** These certificates are the core of transport layer security (TLS) protocol, which is an updated version of SSL. These digital files contain a public encryption key that is used to validate server identity and a digital signature to ensure the integrity and the source of data and other information transmitted online.
* **Email certificate.**Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard for sending encrypted email. [RSA Security](https://www.techtarget.com/whatis/definition/RSA-Security) created it to resolve the problem of sending encrypted email without the need to exchange a public key. It is commonly used within an organization that has its own CA.
* **EMV certificate.**[EMV](https://www.techtarget.com/whatis/definition/EMV-card) payment cards have an embedded microchip containing a card issuer certificate. The embedded microchip enables the EMV payment card to generate a unique code for each transaction. EMV stands for Europay, MasterCard and Visa, the organizations that constitute the certificate authority.
* **Code-signing certificate.**Code-signing certificates are used in software development and IT operations to digitally sign the software or firmware of an application or device. This provides recipients with assurance about who created the code and the integrity of the code
* **Root certificate.**A root certificate is a digital certificate that is used to sign other digital certificates. It is sometimes referred to as a trust anchor because it is at the top of a hierarchy of digital certificates that are used to verify other digital certificates.
* **Leaf certificate.**A leaf certificate, or an end entity, is the endpoint for the signing and encrypting of data and cannot be used to sign other certificates. These include TLS/SSL, email and code-signing certificates.
* **Self-signed certificate.**A self-signed certificate is a certificate that is signed by the same entity to whom it is assigned. Most certificates can be self-signed and are verified by their own public key. They are not signed by a CA, which means they might be perceived as less trustworthy.