Lecture 2

Threats in mobile and network environments

- **What is a threat in cybersecurity?**
- **Mobile Security Threats**
- **Network security threats**
- **Mobile Security Best Practices**

Threats in mobile and network environments

➢ What is a threat in cybersecurity?

In cybersecurity, a threat is any kind of action that has the potential to negatively impact an organization’s operations, procedures, systems, or data. Bad actors, such as hackers and scammers, exploit vulnerabilities within a digital security system to gain information, disrupt operations, and commit crimes like fraud and identity theft.

A- Mobile Security Threats

Users of mobile devices or so called mobile users are increasingly subject to malicious activity, mainly concerning pushing malware apps to smartphones, tablets, or other devices using a mobile OS. handheld devices, carried in our pockets, are used to store and protect sensitive information. Even though Google and Apple offer distribution environments that are closed and controlled, users are still exposed to different kinds of attacks.

Today's smartphones hold all the keys to our communications, finances, data, and social lives, which makes these ubiquitous devices lucrative targets for cybercriminals. To stay protected, we need to understand and recognize the most common threats.

1- Phishing :

The main platform for phishing attacks is spam emails, which are sent out in mass quantities by cybercriminals. Recently, we have witnessed a new form of phishing, which is using SMS text messaging(so-called “smishing”) to send a fraudulent link to a mobile device. Social media are also used by hackers to take advantage of mobile phone users.

Protection against this type of attack is common sense based and concerns mainly not responding to dubious messages, keeping applications up to date, etc.

2- Malware:

Smartphones are quickly approaching PC capabilities, and the same incentives exist for hackers: fraud, stealing personal and business information, and extortion—hackers are poised for the attack, with many different avenues available to spread malware

applications and the given OS should be kept up to date to maximize their protection, and running an antimalware app is also recommended.

3- Rooting/jailbreaking:

Rooting (Android) or jailbreaking (iOS) involves bypassing the manufacturer-imposed limitations on device functionality, which inherently compromises the device's security model. Some users deliberately do this to obtain root access and alter system files. However, this practice weakens device security, increasing its vulnerability to malware and unauthorized access.

4- Zero-day exploits:

Zero-day exploits represent a significant security risk, as they take advantage of vulnerabilities in software or apps that are unknown to the vendor. Attackers exploit these vulnerabilities before the vendor can release patches or updates, leading to a range of potential security issues.

5- Direct Hacker Attack and Intercepting Communication:

Contemporary users have access to sophisticated mobile devices which are part of their everyday lives, and this directly leads to an increase in the number of users. This rapid growth in users entices hackers to either intercept communication or directly attack mobile devices

Intercepting communication concerns a situation in which 2 mobile devices are communicating, usually via a public LAN—the users believe they are in direct communication. This interception of communication is called a man-in-the-middle attack (MITM); the perpetrator redirects the data route, either eavesdropping or impersonating one of the parties, to steal personal data. To prevent this type of attack, users should:

- avoid public Wi-Fi or non password-protected connections
- pay attention to notifications in their browser
- conduct sensitive transactions via secure connections

Taking into consideration the above rules, the user of a mobile device significantly reduces the likelihood of the interception of communication and the loss of sensitive data

6- Stolen and Lost Phones:

Mobile phones are considered to be personal devices on which users store lots of different types of data, either personal or business. Mobile device users, most frequently, simply lose their devices.Mobile device owners are themselves the greatest threat when it comes to losing sensitive data, yet, at the same time, their proper behavior can help protect such data. Implementing 2FA (two-factor authentication), avoiding automatic logins, and using password-lock applications can minimize the probability of losing sensitive data.

7- User Behavior:

Mobile device users often create vulnerabilities due to the blurred line dividing personal and business use. Some of the blameworthy behaviors include turning off all types of security apps, downloading apps from third-party application stores, and sharing confidential in-formation with unauthorized recipients. With smartphones, it becomes even easier to obtain sought-after information. Controlling user behavior is considered to be one of the greatest challenges in mobile device security .

8- Physical security:

Many of us forget an essential security measure: physically securing our mobile devices. If you don't use a PIN code, pattern, or biometric check such as a fingerprint or retina scan, your handset could be vulnerable to tampering. In addition, if you leave your phone unattended, it may be at risk of theft.

B-Network security threats

1- Internal security threats:

This can take the form of phishing attacks, careless decision-making, weak passwords, and more.

Insider actions that negatively impact your business's network and sensitive data can result in downtime, loss of revenue, and disgruntled customers.

2- Distributed denial-of-service (DDoS) attacks:

A DDoS attack causes websites to crash, malfunction, or experience slow loading times. In these cases, cybercriminals infect internet-connected devices (mobile phones, computers, etc.) and convert them into bots. Hackers send the bots to a victim's IP address.

This results in a high volume of internet traffic bombarding the website with requests and causing it to go offline. These attacks make it difficult to separate legitimate and compromised traffic.

3- Rogue security software:

Rogue security software tricks businesses into believing their IT infrastructure is not operational due to a virus. It usually appears as a warning message sent by a legitimate anti-malware solution.

Once a device is infected with a rogue program, the malware spams the victim with messages, forcing them to pay for a non-existent security solution, which is often malware. Rogue security software can also corrupt your pre-existing cyber security programs to prolong their attack.

4- Malware:

Malware are malicious software programs used to gather information about victims through compromised devices. After successful deployments, hackers can mine devices for classified information (email addresses, bank accounts, passwords, etc.) and use them to commit identity theft, blackmail, or other business-damaging actions.

Malware includes:

- **Trojans:** This malware, also called a Trojan horse virus, impersonates a legitimate application so that you download it without realizing its true intent.

- **Adware:** Adware displays or downloads advertising materials onto a computer or mobile device. While some adware is used for legitimate marketing purposes, bad actors use it for more malicious purposes, like spying or stealing data.

- **Spyware:** This malware installs itself onto mobile devices to monitor your online behavior and gain sensitive information.

- **Ransomware:** This malware encrypts files on a device, effectively making it unusable without decryption. Bad actors then demand a ransom to decrypt the device.

5- Phishing attacks:

Phishing attacks are scams where hackers disguise themselves as a trusted entity and attempt to gain access to networks and steal personal information, such as credit card details. Phishing scams take the form of emails, text messages, or phone calls.

Similar to rogue security software, phishing attacks are designed to appear legitimate. This encourages victims to click on malicious links or download malware-laden attachments.

6- Man-in-the-middle (MitM):

Man-in-the-middle (MitM) attacks occur when a malicious actor inserts themselves between two parties who believe they're communicating with one another but are actually communicating with the attacker.

Also called "machine-in-the-middle" and "on path" attacks, man-in-the-middle attacks usually involve a cybercriminal first detecting insecure traffic and then sending network users to spoof websites, which they use to collect log-in credentials. Afterward, attackers use the acquired credentials to log in to the actual website, stealing further sensitive data or committing financial crimes like theft.

7- Insecure Wi-Fi networks:

Insecure Wi-Fi networks are susceptible to exploitation, allowing attackers to intercept data transmissions and gain unauthorized access. Cybercriminals use techniques like eavesdropping or setting up rogue Wi-Fi hotspots to illegally access systems, launch MITM attacks, or intercept transmission of sensitive data.

8- Data leakage:

Data leakage refers to the unauthorized transmission of sensitive data from an organization to an external recipient. This typically happens because of unencrypted connections or when apps have excessive permissions that let them access and share user data without consent. Data leakage exposes personal or corporate information, leading to privacy breaches.

On the network level, data leakage can occur when unwanted individuals access private information being transmitted over the network due to weak network security protocols or compromised network devices.

Data leakage in devices happens when confidential data stored on the device is accessed by attackers through malware, physical theft of the device, or weak mobile security settings.

9- Sql injection:

Attackers inject malicious SQL queries into web applications to access databases.

➢ Mobile Security Best Practices :

Mobile security best practices are recommended guidelines and safeguards for protecting mobile devices and users' data.

some best practices for mobile devices and applications as follow :

1- **Make user authentication the highest priority:** most mobile devices can be locked with a screen lock and unlocked with a password, biometric (e.g., finger-print and face recognition) or personal identification number (PIN).

2- **Update mobile operating systems and on-board applications with security patches:** keeping the operating system (Android and iOS) and the in-stalled applications up to date is a must. Both Google and Apple provide regular updates to users, which resolve recent vulnerabilities or other threats, as well as sharing additional performance and security features .

3- **Back up user data on a regular basis:** backing up is a basic method of preventing data loss or deletion. A backup schedule should be adapted to an increase in data over time. Examples of user data include individual user files (documents and spreadsheets),media files (e.g., pictures and videos), contacts, and other sensitive data. In case of mobile devices, the obvious choice is a remote backup, which means copying and storing files in a private or public cloud.

4- **Utilize encryption:** data encryption translates data into another form, or code, so that only authorized parties can decrypt and read these data. Thee encryption feature is used for data stored on the mobile device as well as for data transmission over the network. Nevertheless, by default, encryption requires a password to encrypt and decrypt data files. If one forgets the password, the data recovery is usually problematic and not always successful.

5- **Enable remote data wipe:** in case a user has their device with sensitive data stolen and there is little chance of retrieving them in a relatively short period of time, one should consider turning on the device capability which allows a factory reset message to be remotely executed . Further more, remote data wipe is imperative in case of termination of employment or contracting a mal-ware infection which cannot be uninstalled or deleted.

6- **Disable Bluetooth and Wi-Fi when not needed:** minimizing both Bluetooth and Wi-Fi usage reduces exposure to having vulnerabilities exploited.

7- **Be aware of social engineering techniques**: social engineering is a term that encompasses a broad spectrum of malicious activity such as phishing, pretexting, baiting, quid pro quo, and tailgating(“piggybacking”). With this human-centric focus in mind, it is up to a user to be aware of malicious “actors” who engage in social engineering attacks hunting.

8- **Install mobile security and antivirus applications:** since there is no additional protection by default, mobile security and antivirus real-time scanners safeguard against malicious applications and viruses, as well as identify theft, ransomware, and cryptominers. Moreover, some tools can also scan URLs and block dangerous sites, monitor links in text messages, and provide parental control .