Cyber Security – UNIT III: Cybercrime on Mobile and Wireless Devices

3.1 Security Challenges Posed by Mobile Devices

Definition:

Mobile devices such as smsartphones, tablets, and smartwatches are compact computing platforms that store personal, professional, and financial data. Due to their portability, wireless connectivity, and diverse applications, they face **unique security challenges** that differ from traditional computers.

Key Challenges:

- **Device Loss/Theft:** Mobile devices are easily lost or stolen, making them physically vulnerable.
- **Unsecured Communication Channels:** Mobile devices frequently connect to public Wi-Fi, Bluetooth, and cellular networks, increasing the risk of interception.
- **Malicious Applications:** Users often download apps from untrusted sources, which may contain malware or spyware.
- **Operating System Fragmentation:** Android devices in particular may lack timely security updates due to manufacturer or carrier delays.
- **Insufficient User Awareness:** Many users fail to implement basic security practices such as screen locks, antivirus, and app permissions.

Features:

- Lightweight, portable, and multifunctional.
- Persistent connectivity to multiple networks.
- Store vast amounts of sensitive personal data.

Security Implications:

- Unauthorized access to emails, social media, banking apps, location data.

- Increased attack surface due to multiple interfaces (Wi-Fi, NFC, Bluetooth).
- Greater risk in BYOD (Bring Your Own Device) environments.

Examples:

- A lost phone with no screen lock can allow full access to social media and banking apps.
- A user connects to an open Wi-Fi network and their login credentials are stolen via packet sniffing.

3.2 Attacks on Wireless Networks

Definition:

Wireless networks are communication systems that transmit data over airwaves instead of cables. These include **Wi-Fi, Bluetooth, Zigbee, LTE, and 5G**, and they are inherently more vulnerable due to the **open nature** of wireless transmission.

Types of Wireless Network Attacks:

3.2.1 Eavesdropping:

- **Definition:** Intercepting and capturing data packets from an unencrypted or weakly encrypted wireless network.
- **Tools:** Wireshark, Kismet
- **Example:** An attacker listens to data transferred over an open Wi-Fi network and steals login credentials.

3.2.2 Man-in-the-Middle (MITM):

- **Definition:** The attacker positions themselves between two communicating parties and intercepts or alters data in transit.
- **Technique:** ARP spoofing, DNS spoofing
- **Example:** Attacker impersonates the Wi-Fi router and captures data being sent from the user to the server.

3.2.3 Rogue Access Point:

- **Definition:** A fake wireless access point set up by an attacker to trick users into connecting to it.
- **Effect:** Once connected, all user traffic can be intercepted or redirected.

3.2.4 Replay Attacks:

- **Definition:** A valid data transmission is captured and resent by the attacker to gain unauthorized access.
- **Example:** Replaying an authentication token sent over the network to gain access to a resource.

3.2.5 Jamming and DoS Attacks:

- **Definition:** Deliberate disruption of wireless communication by flooding the network with excessive signals or requests.
- **Effect:** Denial of service to legitimate users.

Importance of Securing Wireless Networks:

- Protects sensitive information transmitted over air.
- Prevents unauthorized access to internal resources.
- Essential for IoT devices connected over Wi-Fi/Bluetooth.

3.3 Credit Card Frauds in the Mobile and Wireless Era

Definition:

Credit card fraud refers to the **unauthorized use of credit/debit card information** for fraudulent transactions, often via mobile apps, wireless POS devices, or online platforms accessed from mobile devices.

Types of Credit Card Frauds:

3.3.1 Card-Not-Present (CNP) Fraud:

- Occurs when transactions are completed without the physical card being present.
- Common in mobile e-commerce transactions.
- Attackers use stolen card numbers from phishing or data breaches.

3.3.2 Skimming through Mobile POS:

- Fraudulent card readers installed in mobile Point-of-Sale devices capture magnetic stripe or chip data.

3.3.3 Mobile Wallet Exploitation:

- Exploiting flaws in services like Google Pay, Apple Pay, Paytm, etc.
- Attackers may clone NFC data or intercept app transactions.

3.3.4 Phishing via SMS/Apps:

- Fake messages/emails or malicious apps trick users into entering card details.

Process:

1. Attacker gathers card data through phishing/malware.
2. Uses data for unauthorized online transactions.
3. May use carding bots to validate stolen numbers before large transactions.

Prevention Strategies:

- Use only trusted apps for transactions.
- Enable 2FA (Two-Factor Authentication).
- Avoid storing card details in unprotected mobile apps.
- Monitor transaction alerts from banks.

3.4 Authentication Security Services

Definition:

Authentication is the process of verifying the identity of a user or device before granting access to resources. In mobile/wireless environments, secure authentication is critical due to the increased risk of remote exploitation.

Types of Authentication Factors:

1. **Knowledge-based (Something you know):** Passwords, PINs
2. **Possession-based (Something you have):** OTP tokens, smartphones, smartcards
3. **Inherence-based (Something you are):** Biometrics – fingerprint, iris scan, facial recognition

---

Authentication Models:

3.4.1 Single-Factor Authentication (SFA):

- Involves one credential (e.g., just a password).
- Less secure and more susceptible to breaches.

3.4.2 Two-Factor Authentication (2FA):

- Combines two factors like password + OTP or fingerprint + PIN.

3.4.3 Multi-Factor Authentication (MFA):

- Uses more than two factors for higher security.

Importance:

- Prevents unauthorized access to mobile services.
- Secures transactions, sensitive data, and device-level functions.

3.5 Attacks on Mobile Phones

3.5.1 Mobile Phone Theft

- **Definition:** Physical theft of mobile devices, which may contain sensitive information.
- **Risks:** Access to banking apps, emails, photos, contacts.
- **Mitigation:**
  - Enable screen lock (PIN, biometrics)
  - Enable remote tracking and wipe (Find My Device/iPhone)
  - Encrypt device storage

3.5.2 Mobile Virus

- **Definition:** Malicious programs targeting mobile operating systems, causing data theft, corruption, or unauthorized control.
- **Types:**
  - **Trojan:** Disguised as legitimate apps
  - **Worm:** Spreads via MMS, email
  - **Spyware:** Monitors user activity
- **Prevention:** Install apps only from trusted sources, update OS regularly.

3.5.3 Mishing

- **Definition:** SMS-based phishing attacks where users are tricked into clicking malicious links or sharing sensitive information.
- **Example:** SMS claiming your bank account is suspended with a fake link.
- **Prevention:** Don’t trust unknown SMS sources; banks never request OTPs or passwords over SMS.

3.5.4 Vishing

- **Definition:** Voice phishing – attackers call posing as authorities (e.g., bank officials) to extract personal/financial information.
- **Methods:** Caller ID spoofing, psychological manipulation.
- **Prevention:** Never share PINs or OTPs over phone; confirm identity via official channels.

3.5.5 Smishing

- **Definition:** A mix of SMS + phishing + social engineering.
- **Process:** Fake promotional messages → users click links → install malware or enter sensitive data.
- **Note:** Smishing and mishing are often used interchangeably but smishing emphasizes manipulation via marketing-like messages.

3.5.6 Hacking via Bluetooth

- **Definition:** Exploiting Bluetooth vulnerabilities to gain unauthorized access to devices.
- **Types of Attacks:**
  - **Bluesnarfing:** Access contacts, emails, messages without permission
  - **Bluebugging:** Gain control over device functions (e.g., calls, messages)
- **Prevention:**
  - Disable Bluetooth when not needed
  - Make device “non-discoverable”
  - Regularly update firmware and OS
