ITMC411
Security in mobile computing

LECTURE 4
Mobile Device Vulnerabilities

COMMON MOBILE SECURITY THREATS

- There are different security threats in different parts of the mobility landscape:
  - **Web-based** mobile threats.
  - **App-based** threats.
  - **Network** threats.
  - **Physical** threats.

What are the most common mobile threats and what are the **EMM** best practices to **prevent** or **mitigate** them?

Note: **Enterprise mobility management (EMM)** is the set of people, processes and technology focused on managing mobile devices, wireless networks, and other mobile computing services in a business context.

COMMON MOBILE SECURITY THREATS

1. LOST OR STOLEN DEVICES

- The most basic threat to physical device security is also the most common, **loss or theft**.
- **Biometrics** and **kill-switches** are reducing the incidence of mobile device theft.

LOST OR STOLEN DEVICES
PREVENTION / MITIGATION

Strong Password Policies	Enforce **complex device passwords** to prevent unauthorized parties from using **manual/brute-force** techniques to guess the password and gain access to the device.
Enforce Encryption	**Encrypt data** to prevent extraction from the device.
Disable USB (applicable for Android and Windows devices)	**Disable USB** to prevent access to sensitive information via **USB debugging**, prevent side loading of malicious files/programs and prevent download of information from the device's storage.
Real-time Location Services (RTLS)	Configure **geographic boundaries** for company-owned devices. If the device **leaves the approved area**, a**n EMM solution can automatically lock it down**, **wipe** sensitive/confidential information and/or notify appropriate personnel.
Kiosk/Lockdown	**Lockdown the user interface** of the device to prevent access to **apps** and **settings** that may compromise the functionality of the device, or the **data** on the device and to improve the user experience.

2. JAILBREAKING / ROOTING

	What does it mean?	Why do device users do this?
Jailbreak	Remove software restrictions put into place by **Apple**™ on devices that run the **iOS** operating system.	• Customize user experience and expand functionalities. • Gain access to a greater variety of unofficial apps. • Unlock SIM cards in order to use the device with another carrier
Root	Remove software restrictions put into place by **Google**™ to gain the ability to replace the entire operating system.	• Carry features over from one device to another. • Remove system apps that typically cannot be uninstalled. • Unlock SIM cards in order to use the device with another carrier.

JAILBREAKING / ROOTING
PREVENTION / MITIGATION

Jailbreak/Root Detection	An **EMM agent** will **block enrollment** and notifies the IT manager if a device is **Jailbroken/Rooted**.
Wipe Content	An EMM solution's secure document manager and secure browser will **block access to content and wipe downloaded content** if the device is **jailbroken/rooted**.
OS Patching/Updating	Identify and segregate devices running **old/vulnerable OSs** and **limit** the settings and apps pushed to the devices **until they receive suitable OS updates.**
Integration with Device Attestation Services	An EMM solution integrates with **device attestation services** to verify the integrity of the hardware, firmware and OS.

3. MAN IN THE MIDDLE ATTACK

- **A man-in-the-middle (MITM)** attack can **listen** in, or even **alter** the traffic going to and from a mobile device. The most common way for this to happen is over **public, unsecured WiFi** networks.

MAN IN THE MIDDLE ATTACK
PREVENTION / MITIGATION

Whitelist WiFi Access Points	**Pre-configure** devices with approved **WiFi** access points and restrict the device user from creating new **WiFi** connections or modifying existing **WiFi** connections, effectively creating a **white list/safe** list of **WiFi** access points to which the device can connect.
Disable Bluetooth Pairing	Mitigate Bluetooth vulnerabilities by temporarily **disabling Bluetooth communications**
Disable Access to Websites with Invalid SSL/TLS Certificates	Prevent MITM attacks by **using secure browser** to avoid connecting to sites with certificates that are untrusted.
Configure and Enforce VPN/ per-app VPN	To **secure communication** even over **insecure/ compromised** networks.

4. MALWARE

Malware is the catch-all term for dozens different types of potentially harmful applications (**PHA**).

The most common are:

- **Trojans**; opening a backdoor, rooting/ jailbreaking, keylogging/spying, and spreading botnets for **DDoS** attacks.
- **Ransomware**; An external user takes over and **locks down something you need**, whether it's important data or a critical system. You are then required to **pay money**.
- **Adware / Clickware**; is a potentially unwanted program that displays **pop-up ads** and **unwanted advertisements** on web pages that you visit or may track your online activity.

MALWARE
PREVENTION / MITIGATION

Antivirus Protection	An integrated antivirus solution can offer **scanning**, **quarantining** and **deleting** of infected files or apps.
Whitelist/Blacklist apps	Define a **list of apps** that **can/ cannot be installed** and run on devices,
Prevent Installation of Untrusted Apps	**Create approved enterprise app catalogs** that device users can use to install pre-approved public app store and in-house apps. **Prevent** end-user side **loading of apps (via USB)** or installation of app from unauthorized app stores.

5. PHISHING / SOCIAL ENGINEERING

- **Social engineering** is a manipulation technique that **exploits human error to gain private information**, access, or valuables ‹ Attacks can happen **online**, in-person, and via other **interactions**.

PREVENTION / MITIGATION

Web Filtering	**Use secure browser and whitelisted / blacklisted domains** or categories of sites to minimize the chances of a user accessing a malicious or compromised site.
Disable Access to Websites with Invalid SSL/TLS Certificates	**secure browser** will block access to sites with invalid certificates.

6. DATA LEAKAGE

- **Data leakage :** is the **unauthorized transmission of data** from within an organization to an external destination or recipient.

DATA LEAKAGE
PREVENTION / MITIGATION

Multi-factor Authentication	Use **multiple modes of authentication** (passcode, biometrics, ID services) to confirm the end user's identity before enrolling the device and deploying settings and software.
Certificate-based Authentication	**Mutual certificate-based authentication** establishes trust between managed devices and the EMM server. Provision devices with identity certificates to secure access to company resources, such as **WiFi** and **VPN**.
Secure Email Gateway	**Use an EMM email gateway to secure on-premise MS Exchange email** and ensure email can only be accessed from managed and compliant devices.
Content Management Apps	Use an EMM solution's secure document manager and secure web browser to prevent sharing of sensitive information within corporate files and websites. **Encrypt corporate files and web content on the device**, and wipe downloaded content when a device is retired, rooted or jailbroken.
Enforce Separation of Work and Personal Data and Apps	**Prevent sharing of data from company apps and emails accounts to personal apps** and emails accounts on the device.

7. BYOD

BYOD (Bring Your Own Device): is the increasing trend toward **employee-owned devices within a business**. Smartphones are the most common example but employees also take their own tablets, laptops and USB drives into the workplace.

PREVENTION / MITIGATION

Formal BYOD Policy	Around 60% of companies have formal **BYOD policies**. Even in the absence of EMM, a BYOD policy can reduce many security risks.

MOBILE SECURITY CHECKLIST

Hardware/OS	✓ Enforce **complex password** policies ✓ Enforce **encryption** of internal storage and removable SD card(s) ✓ **Disable USB access** on dedicated purpose devices ✓ **Update/patch OS** (if supported by the device)
Apps	✓ Apply a **company-branded kiosk** on dedicated purpose devices to limit access to settings and apps Update/patch apps ✓ **Disable side loading** of apps or installation of apps from **3rd** party apps stores ✓ **Blacklist unapproved apps** on BYOD or company-owned personally enabled (COPE) devices
Content	✓ Use **an EMM email gateway** for Exchange email ✓ Enforce **app sharing restrictions** to prevent data leakage from business apps and email accounts ✓ Use of an **EMM secure document manager** and secure web browser to grant secure access to corporate files and websites
Communication	✓ **Disable Bluetooth pairing** if not required for the device, or if unpatched Bluetooth vulnerabilities are identified ✓ Configure and enforce **VPN/per-app VPN** ✓ **Whitelist WiFi access points** on dedicated purpose devices
Cyber threats	✓ Use **an EMM secure browser and block access to unapproved categories of websites** (e.g. gambling websites) or websites with invalid certificates ✓ Enable/Configure antivirus protection

Steps to Protect Your Mobile Phone

- **When choosing a mobile phone, consider its security features.**
  - Ask the service provider if the device **offers file encryption**.
  - The ability for the **provider to find and wipe the device** remotely.
  - The ability to **delete known malicious apps remotely**.
  - Authentication features such as **device access passwords**.
  - look for an option to **encrypt the backup**.
  - If you plan to use the device for VPN access, ask the provider if the device **supports certificate-based authentication**.
- **Configure the device to be more secure**.
  - Enable **PIN and password feature** that locks the device.
  - Enable **encryption**,
  - remote **wipe capabilities**,
  - **antivirus software** if available.

Steps to Protect Your Mobile Phone

- **Configure web accounts to use secure connections.**
  - Accounts for certain websites can be configured to use secure, encrypted connections (look for "**HTTPS**" or "**SSL**" in account options pages).
- **Do not follow links sent in suspicious email or text messages.** Such links may lead to malicious websites.
- **Limit exposure of your mobile phone number.**
  - Think carefully before posting your mobile phone number to a public website. Attackers can use software to collect mobile phone numbers from the web and then use those numbers to target attacks.

Steps to Protect Your Mobile Phone

- **Be choosy when selecting and installing apps.**
  - Do a **little research** on apps before installing them.
  - Check what **permissions** the app requires.
- Do not "**root**" or "**jailbreak**" the device**.**
- **Disable** interfaces that are not currently in use, **Bluetooth**, infrared, or **Wi-Fi**.
- Set **Bluetooth**-enabled devices to **non-discoverable**.
- **Avoid** joining **unknown Wi-Fi** networks and using **public Wi-Fi** hotspots.
- **Carefully consider** what **information** you want stored on the device.