13- Implementing Secure Mobile Solutions

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

13.1- Implement Mobile Device Management

MOBILE DEVICE DEPLOYMENT MODELS

- Mobile devices have replaced computers for many email and diary management tasks and are integral to accessing many other business processes and cloud-based applications.
- A **mobile device deployment** model describes the way employees are provided with mobile devices and applications.
- Bring your own device (BYOD)
  - ✓ The mobile device is owned by the employee.
  - ✓ The mobile will have to meet whatever profile is required by the company (in terms of OS version and functionality) and the employee will have to agree on the installation of corporate apps and to some level of oversight and auditing.
  - ✓ This model is usually the most popular with employees but poses the most difficulties for security and network managers.

MOBILE DEVICE DEPLOYMENT MODELS (cont.)

- Corporate owned, business only (COBO)
  - ✓ The device is the property of the company and may only be used for company business.
- Corporate owned, personally-enabled (COPE)
  - ✓ The device is chosen and supplied by the company and remains its property.
  - ✓ The employee may use it to access personal email and social media accounts and for personal web browsing (subject to whatever acceptable use policies are in force).
- Choose your own device (CYOD)
  - ✓ Much the same as COPE but the employee is given a choice of device from a list.

ENTERPRISE MOBILITY MANAGEMENT

- Enterprise mobility management (EMM) is a class of management software designed to apply security policies to the use of mobile devices and apps in the enterprise.
- There are two main functions of an EMM product suite:
  - ✓ Mobile Device Management (MDM)—sets device policies for authentication, feature use (camera and microphone), and connectivity, MDM can also allow device resets and remote wipes.
  - ✓ Mobile Application Management (MAM)—sets policies for apps that can process corporate data, and prevents data transfer to personal apps, This type of solution configures an enterprise-managed container or workspace.

MOBILE ACCESS CONTROL SYSTEMS

- If a threat actor is able to gain access to a smartphone or tablet, they can obtain a huge amount of information and the tools with which to launch further attacks.

- Smartphone Authentication
  - ✓ The majority of smartphones and tablets are single-user devices.
  - ✓ Access control can be implemented by configuring a screen lock that can only be bypassed using the correct password, PIN, or swipe pattern.
  - ✓ Many devices now support biometric authentication, usually as a fingerprint reader but sometimes using facial or voice recognition.

MOBILE ACCESS CONTROL SYSTEMS (cont.)

- Screen Lock
  - ✓ The screen lock can also be configured with a lockout policy.
  - ✓ This means that if an incorrect passcode is entered, the device locks for a set period.
  - ✓ This could be configured to escalate (so the first incorrect attempt locks the device for 30 seconds while the third locks it for 10 minutes, for instance).
  - ✓ This deters attempts to guess the passcode.

REMOTE WIPE

- A remote wipe or kill switch means that if the handset is stolen it can be set to the factory defaults or cleared of any personal data (sanitization).
- Some utilities may also be able to wipe any plug-in memory cards too.
- The remote wipe could be triggered by several incorrect passcode attempts or by enterprise management software.
- Other features include backing up data from the phone to a server first and displaying a "Lost/stolen phone—return to XX" message on the handset.
- *In theory, a thief can prevent a remote wipe by ensuring the phone cannot connect to the network, then hacking the phone and disabling the security.*

FULL DEVICE ENCRYPTION AND EXTERNAL MEDIA

- All but the early versions of mobile device OSes for smartphones and tablets provide full device encryption.
- In iOS, there are various levels of encryption.
  - ✓ All user data on the device is always encrypted but the key is stored on the device, This is primarily used as a means of wiping the device, The OS just needs to delete the key to make the data inaccessible rather than wiping each storage location.
  - ✓ Email data and any apps using the "Data Protection" option are subject to a second round of encryption using a key derived from and protected by the user's credential, This provides security for data in the event that the device is stolen, Not all user data is encrypted using the "Data Protection" option; contacts, SMS messages, and pictures are not, for example.

LOCATION SERVICES

- Geolocation is the use of network attributes to identify (or estimate) the physical position of a device.
- The device uses location services to determine its current position.
- Location services can make use of two systems:
  - ✓ Global Positioning System (GPS)—a means of determining the device's latitude and longitude based on information received from satellites via a GPS sensor.
  - ✓ Indoor Positioning System (IPS)—works out a device's location by triangulating its proximity to other radio sources, such as cell towers, Wi-Fi access points, and Bluetooth/RFID beacons.
- Location services is available to any app where the user has granted the app permission to use it.

ROOTING AND JAILBREAKING

- Like Windows and Linux, the account used to install the OS and run kernel-level processes is not the one used by the device owner.
- Users who want to avoid the restrictions that some OS vendors, handset OEMs, and telecom providers (carriers) put on the devices must use some type of privilege escalation:

  ✓ Rooting—this term is associated with Android devices, Some vendors provide authorized mechanisms for users to access the root account on their device, For some devices it is necessary to exploit a vulnerability or use custom firmware, Custom firmware is essentially a new Android OS image applied to the device, This can also be referred to as a custom ROM, after the term for the read only memory chips that used to hold firmware.

ROOTING AND JAILBREAKING (cont.)

- ✓ Jailbreaking—iOS is more restrictive than Android so the term "jailbreaking" became popular for exploits that enabled the user to obtain root privileges, sideload apps, change or add carriers, and customize the interface, iOS jailbreaking is accomplished by booting the device with a patched kernel, For most exploits, this can only be done when the device is attached to a computer when it boots (tethered jailbreak).

- ✓ Carrier unlocking—for either iOS or Android, this means removing the restrictions that lock a device to a single carrier.