Lesson 13

Implementing Secure Mobile Solutions

CompTIA®

Topic 13A

Implement Mobile Device Management

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Syllabus Objectives Covered

- 3.5 Given a scenario, implement secure mobile solutions

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Mobile Device Deployment Models

- Bring your own device (BYOD)
- Corporate owned, business only (COBO)
- Corporate owned, personally-enabled (COPE)
- Choose your own device (CYOD)
- Virtual desktop infrastructure (VDI)

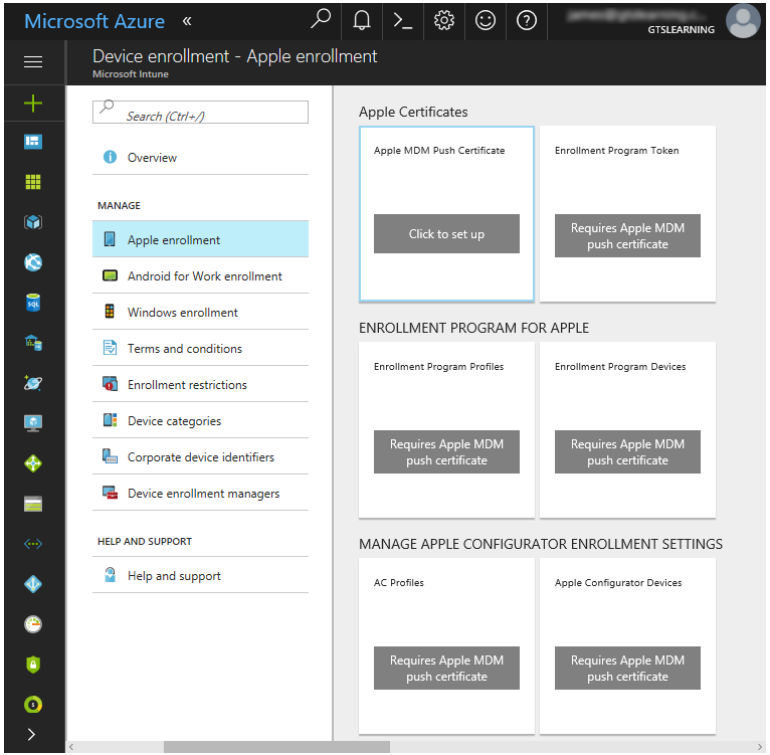
Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Enterprise Mobility Management

- Apply security policies to the use of mobile devices in the enterprise
- Visibility over use and configuration
- Enterprise mobility management (EMM)
- Mobile device management (MDM)
  - Network enrollment
  - Manage device functions
- Mobile application management (MAM)
  - Install and monitor corporate apps and data
- Unified endpoint management (UEM)

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

iOS in the Enterprise



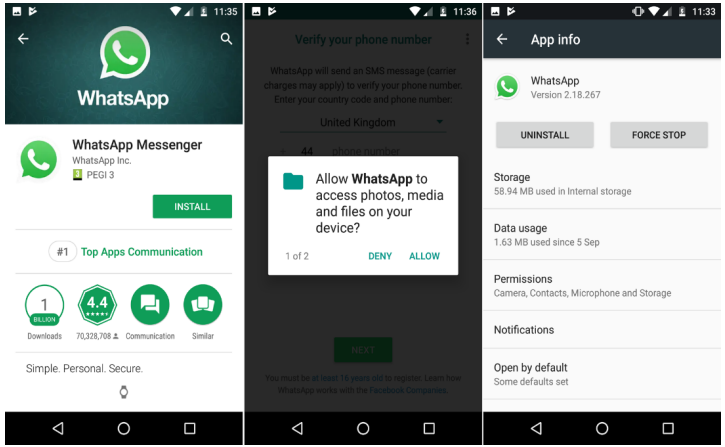
Screenshot used with permission from Microsoft.

- App development
  - Software Development Kit (macOS only)
  - App Store
  - Device Enrollment Program
  - Volume Purchase Program
  - Developer Enterprise Program
- iOS vulnerabilities and patch management

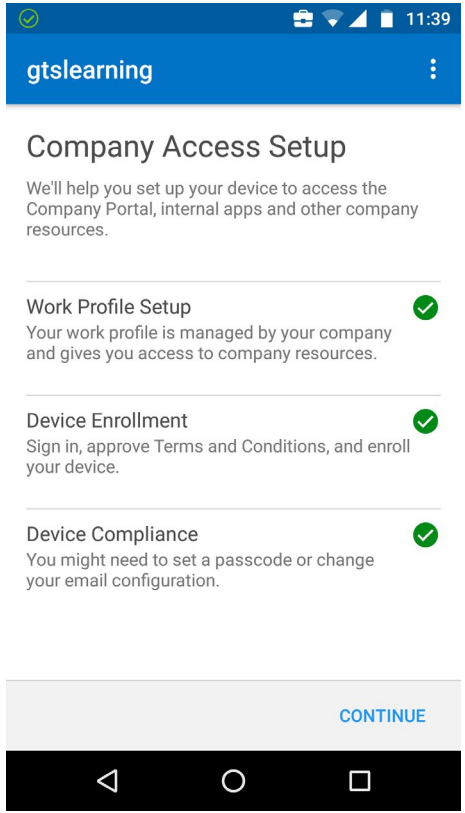
Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Android in the Enterprise

- App stores and developer programs
- Android vulnerabilities and patch management
- Security Enhanced Android (SEAndroid)
  - App permissions



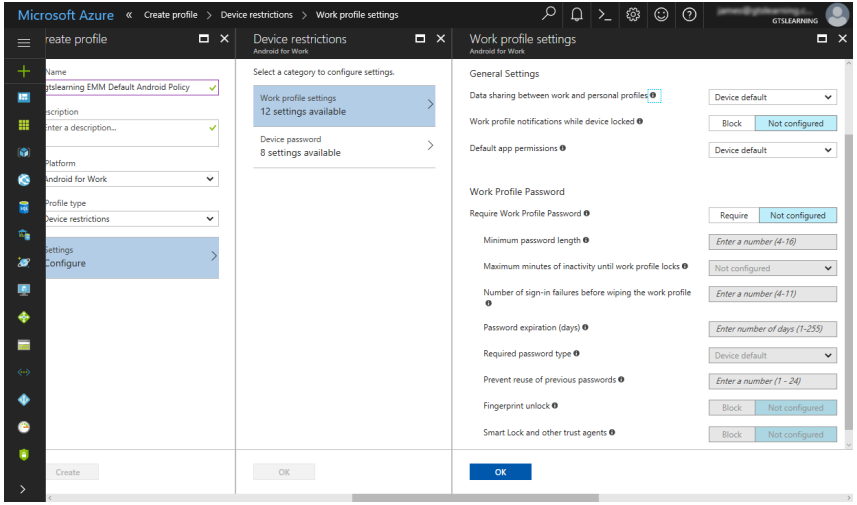
Android is a trademark of Google LLC.



Android is a trademark of Google LLC.

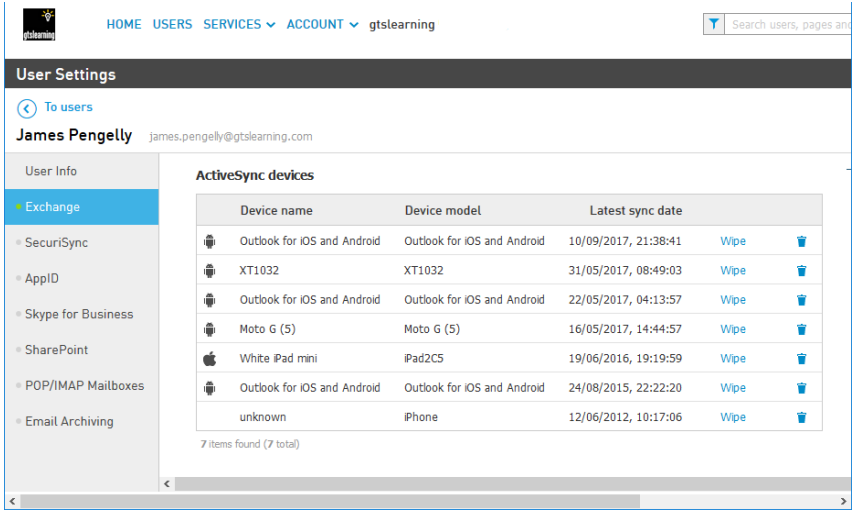
Mobile Access Control Systems

- Smartphone authentication
  - Password
  - PIN
  - Swipe pattern
  - Biometric
- Screen lock
- Context-aware authentication



Screenshot used with permission from Microsoft.

Remote Wipe



Screenshot used with permission from Intermedia.

- "Kill switch"
- Sets device to factory defaults or clears storage (or storage segment)
- Initiated from enterprise management software
- Thief might be able to keep device from receiving the wipe command

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

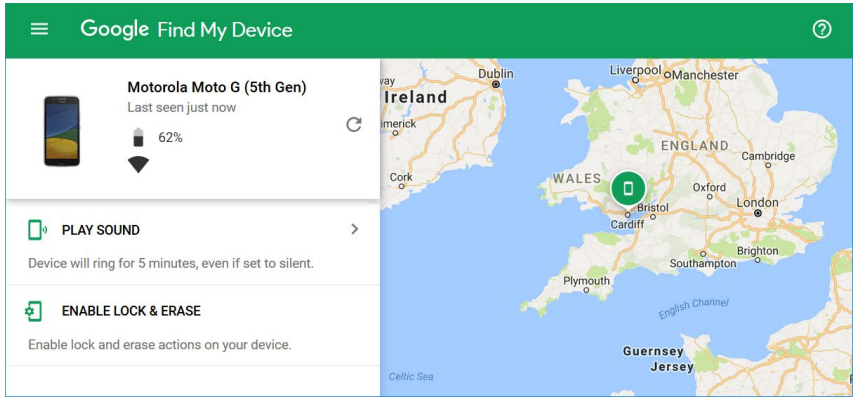
Full Device Encryption and External Media

- iOS device encryption
  - Secure erase encryption
  - Data protection
- Android device encryption
  - From version 10, only uses file-level encryption of user data
- External media
- MicroSD HSM

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

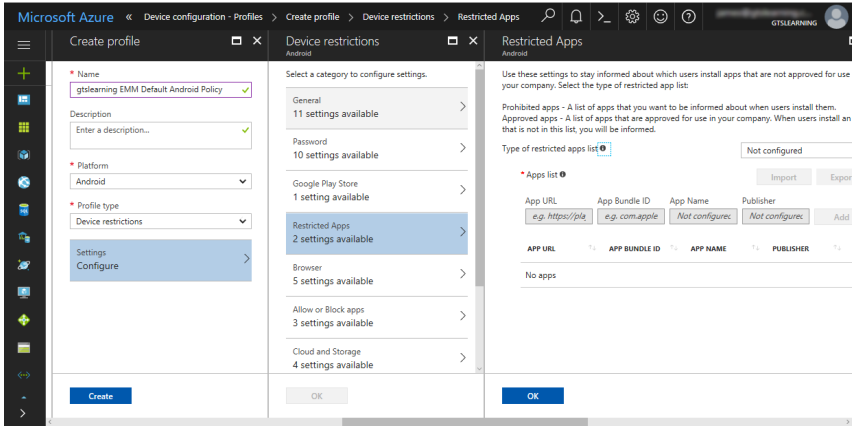
Location Services

- Geolocation
- Location Services
  - Global Positioning System (GPS)
  - Indoor Positioning Systems (IPS)
- Geofencing to apply location-based policies automatically
  - Disable on-board camera/video through MDM/EMM controls
- GPS tagging
  - Risks to personal information
  - Track movements (assist social engineering)



Android is a trademark of Google LLC.

Application Management



Screenshot used with permission from Microsoft.

- MDM/EMM application use policies
- Corporate workspaces
- Restricting third-party app stores
- Enterprise app development and fulfillment
  - Sideloading

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Content Management

- Privately owned but corporate use issues
  - Data ownership
  - Privacy
- Containerization sets up a corporate workspace segmented from the employee's private apps and data
- Storage segmentation ensures separation of data
- Enforcing content management/DLP policies

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Rooting and Jailbreaking

- Rooting
  - Principally Android
  - Custom firmware/ROM
- Jailbreaking
  - Principally iOS
  - Patched kernel
  - Tethered jailbreak
- Carrier unlocking
- Risks to enterprise management

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Topic 13B

Implement Secure Mobile Device Connections

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

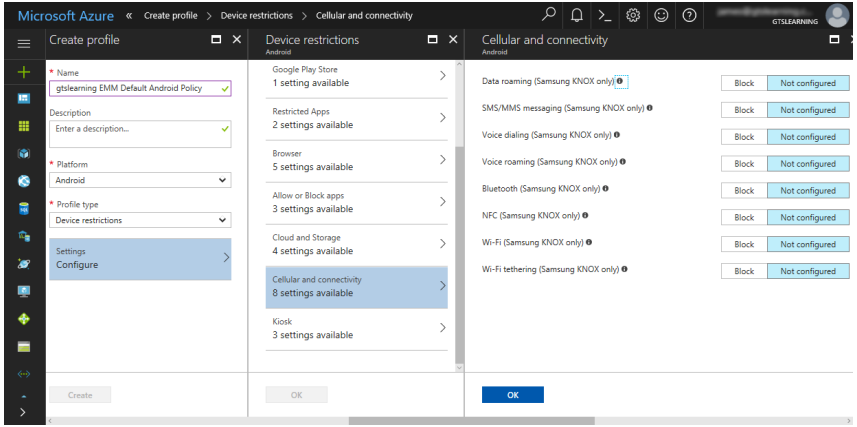
Syllabus Objectives Covered

- 1.4 Given a scenario, analyze potential indicators associated with network attacks
- 3.5 Given a scenario, implement secure mobile solutions

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Cellular and GPS Connection Methods

- Disable cellular data if unmonitored or unfiltered
- Prevent use for data exfiltration
- Attacks on cellular connections
- Global Positioning System (GPS)



Screenshot used with permission from Microsoft.

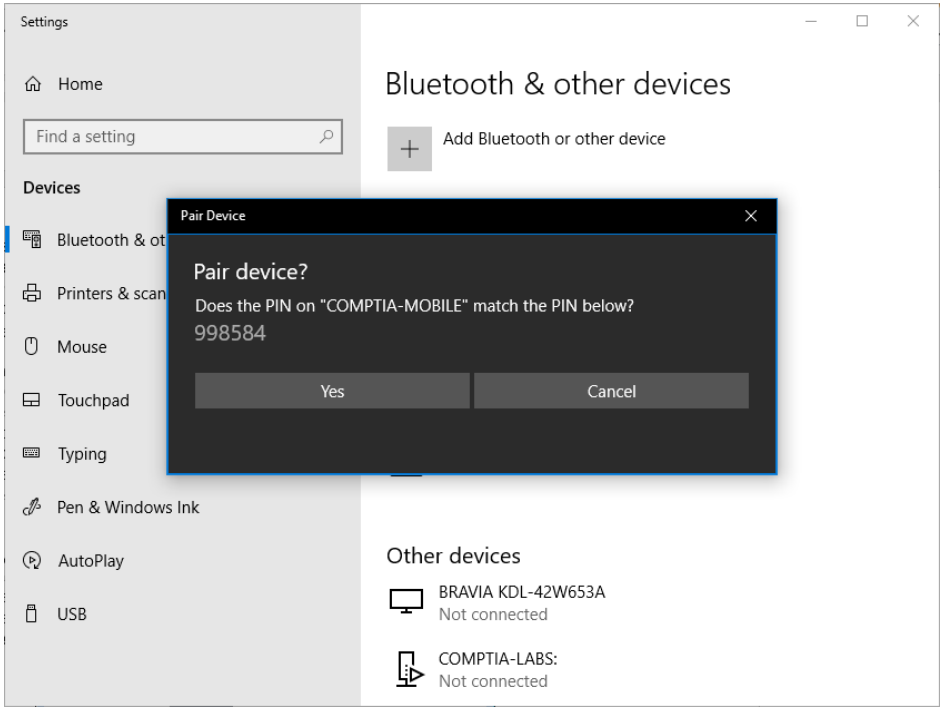
Wi-Fi and Tethering Connection Methods

- Risks from Wi-Fi
  - Legacy security methods
  - Open access points
  - Rogue access points
- Personal Area Network (PAN) technologies
- Wi-Fi Direct
  - Ad hoc networks
  - Soft access point
  - Wireless mesh networking
- Tethering and hotspots

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Bluetooth Connection Methods

- Device discovery
- Authentication and authorization
  - Pairing mechanism
- Malware and exploits
  - Bluebourne
  - Bluejacking
  - Bluesnarfing
  - Rogue firmware peripheral devices



Screenshot used with permission from Microsoft.

Infrared and RFID Connection Methods

- Infrared
  - IR blaster
  - IR sensor
- Radio Frequency ID (RFID)
  - (Usually) unpowered tags
  - Transmit when in range of reader
  - Skimming attack
  - Encrypt sensitive information

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Near Field Communications and Mobile Payment Services

- Near Field Communications (NFC)
- Connection configuration/bump
- Mobile wallet apps
- Eavesdropping/skimming
- Denial of service

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

USB Connection Methods

- USB OTG allows a port to function as a device or hub
- USB with malicious firmware might be able to perform an exploit
  - Spread malware between computers using the device as a vector
  - Install or run malware to try to compromise the smartphone itself
- Juice jacking

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

SMS/MMS/RCS and Push Notifications

- Short message service (SMS)
  - Exploits against 2-step verification
- Multimedia message service (MMS)
- Rich communication services (RCS)
  - Exploits against handling of attachments or rich formatting
- Push notifications
  - Potential vector for spam, phishing, or hoaxing
  - Make sure developer account credentials are kept secure

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Firmware Over-the-Air Updates

- Baseband updates and radio firmware
- Over the Air (OTA) update delivery
- Risks from rooted/jailbroken devices
- Risks from highly targeted attacks

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

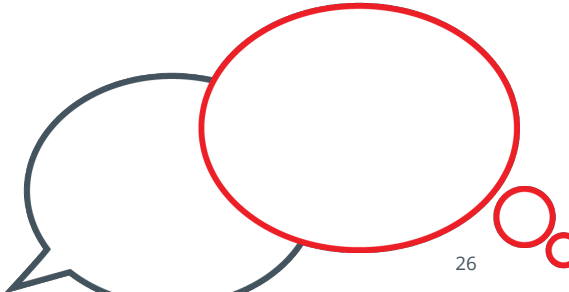
Microwave Radio Connection Methods

- Backhaul link from cell tower to provider network
- Private links between premises
- Point-to-point (P2P) microwave
  - High gain directional antenna
- Point-to-multipoint (P2M) microwave
  - Smaller sectoral antennas
  - Links multiple sites/mobile subscribers to a single hub
- Other types of multipoint

Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.

Lesson 13

Summary



Copyright © 2020 CompTIA Properties, LLC. All Rights Reserved.