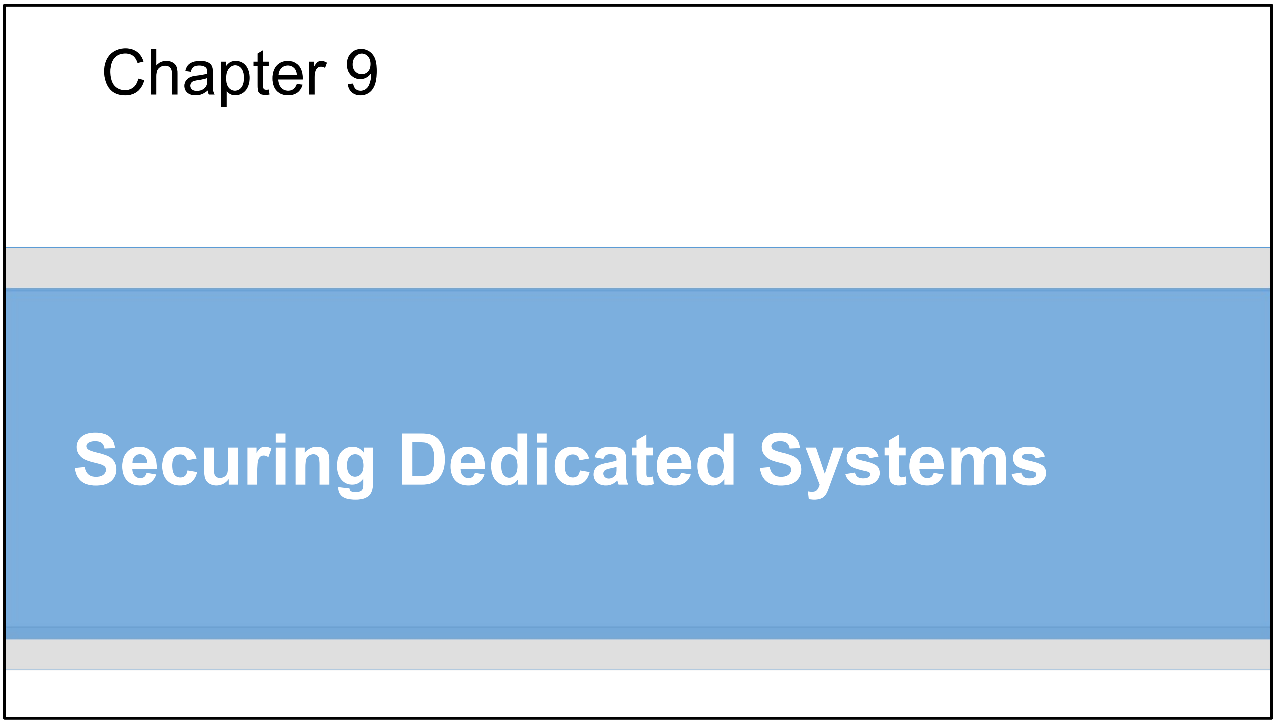
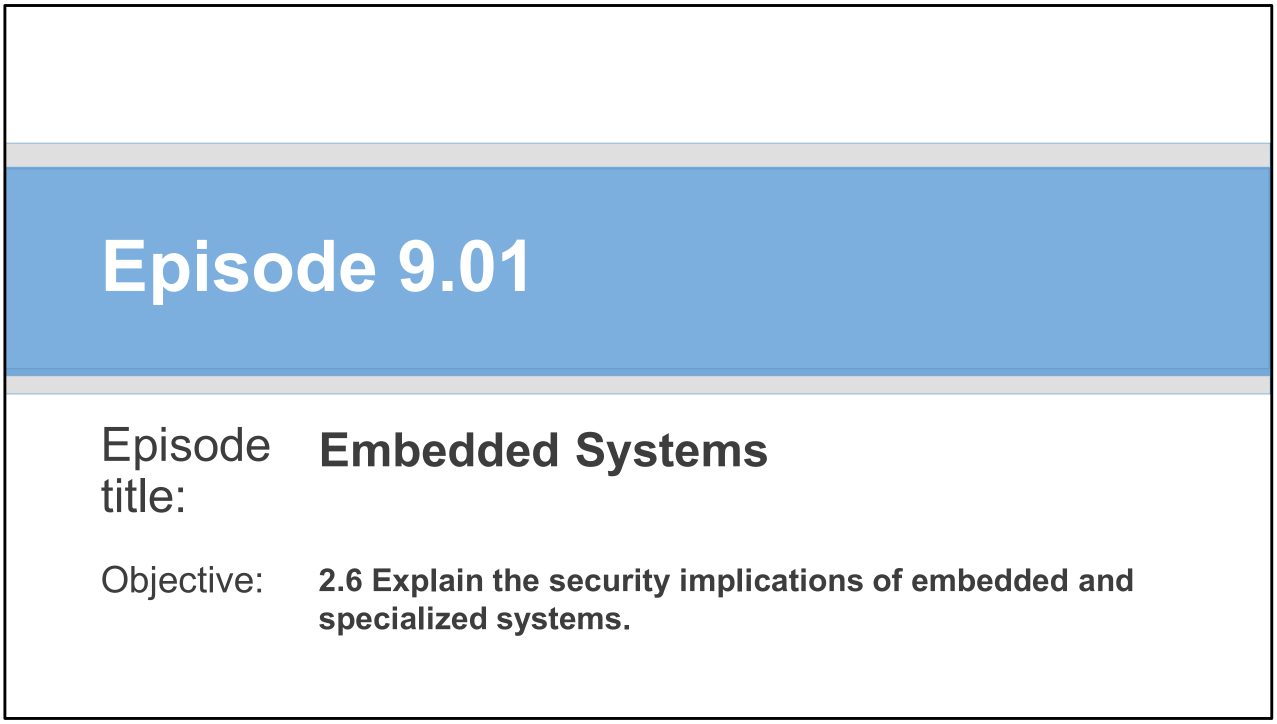


Chapter 9

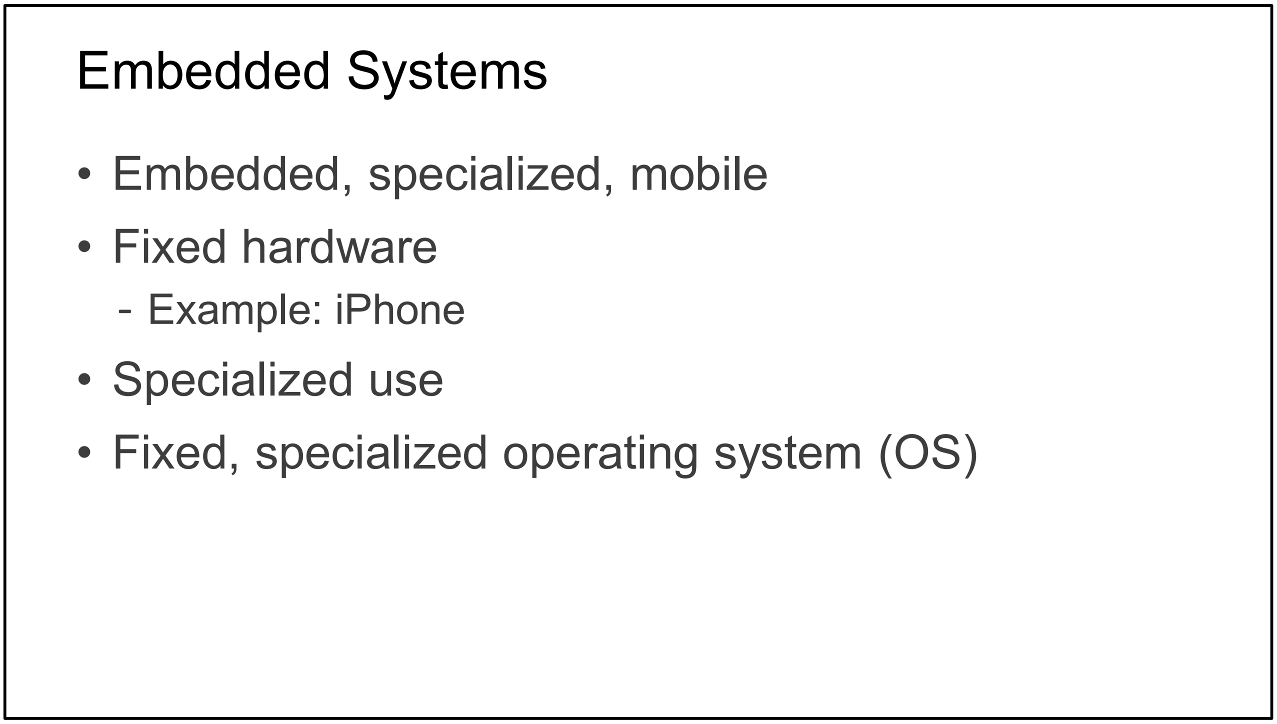
Securing Dedicated Systems



Episode 9.01

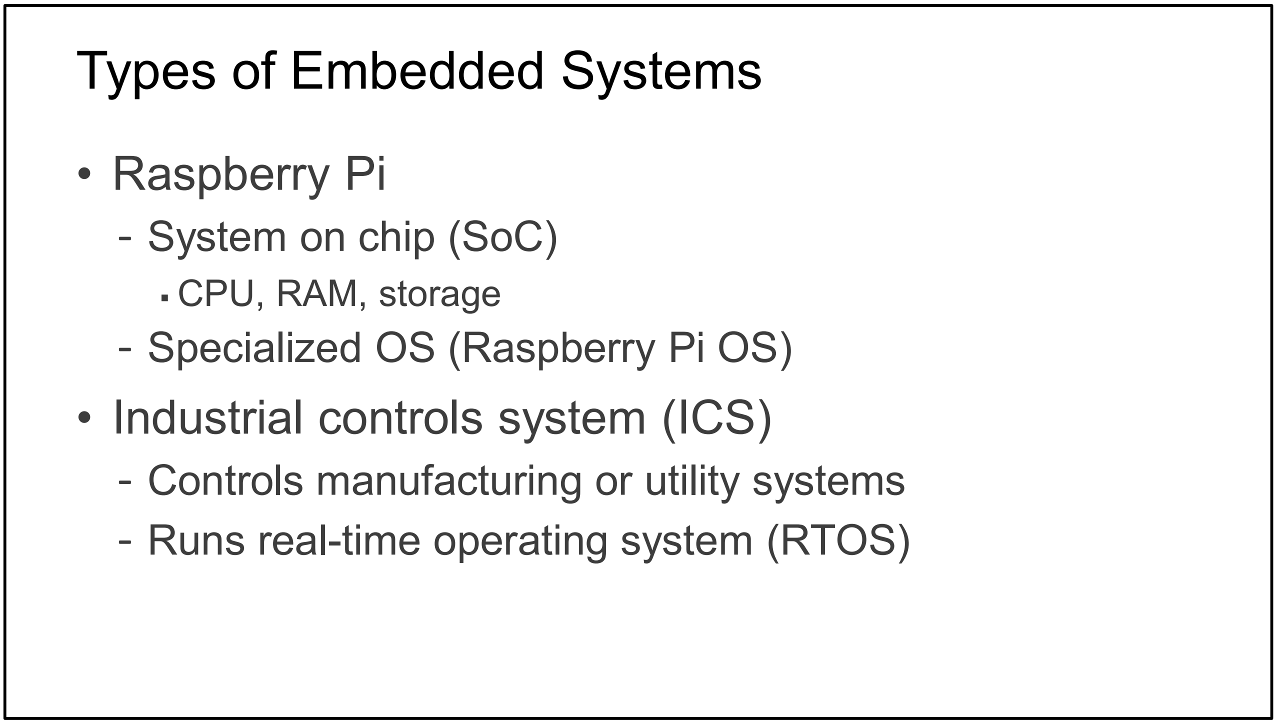
Episode title: **Embedded Systems**

Objective: **2.6 Explain the security implications of embedded and specialized systems.**



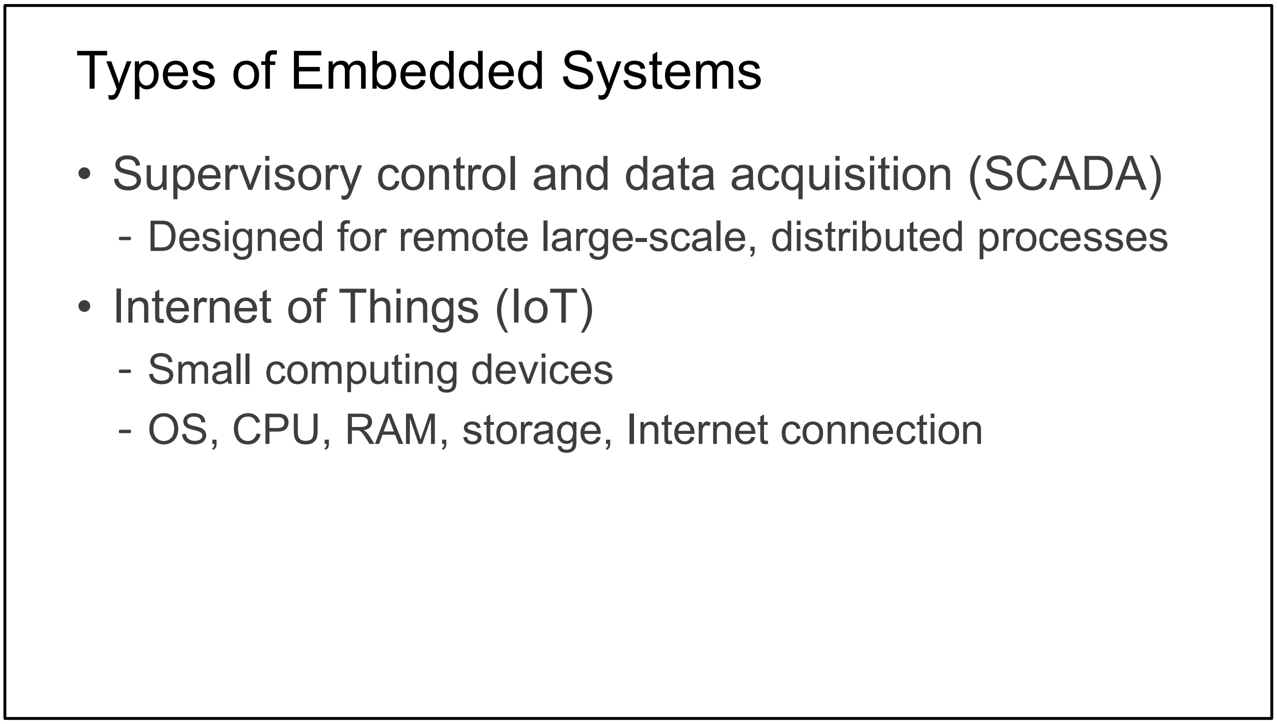
Embedded Systems

- Embedded, specialized, mobile
- Fixed hardware
  - Example: iPhone
- Specialized use
- Fixed, specialized operating system (OS)



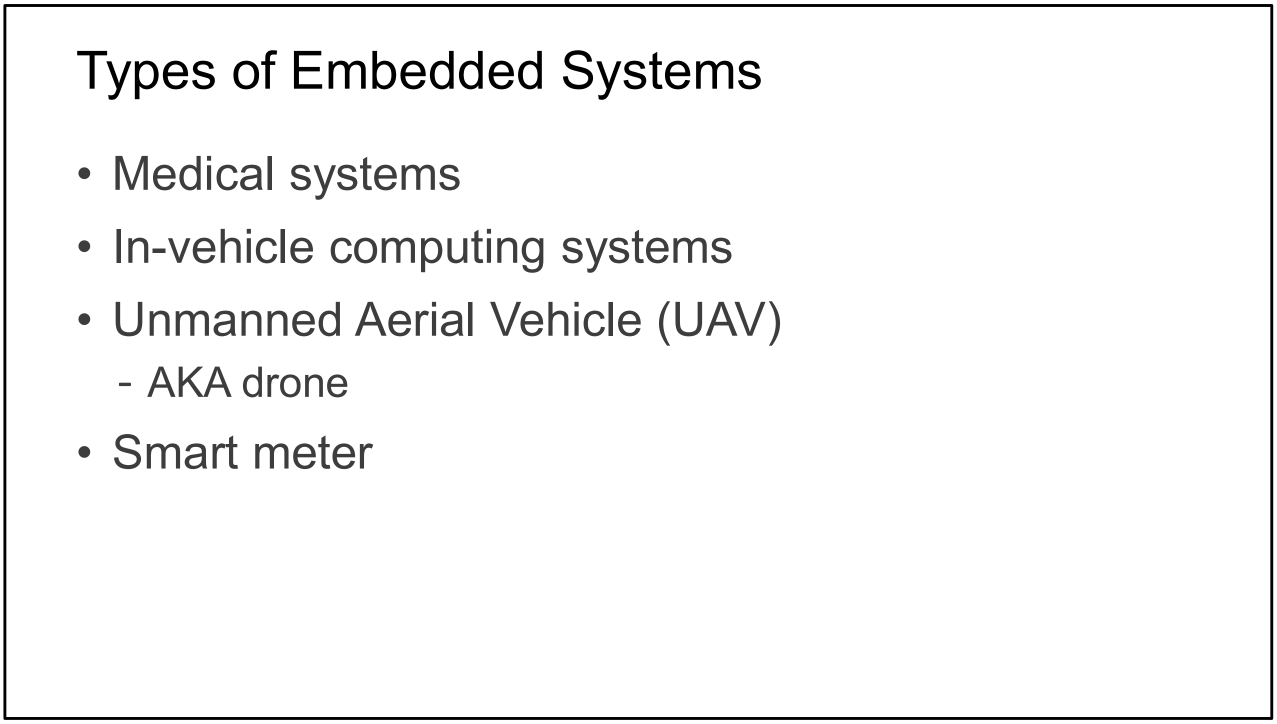
Types of Embedded Systems

- Raspberry Pi
  - System on chip (SoC)
    - CPU, RAM, storage
  - Specialized OS (Raspberry Pi OS)
- Industrial controls system (ICS)
  - Controls manufacturing or utility systems
  - Runs real-time operating system (RTOS)



Types of Embedded Systems

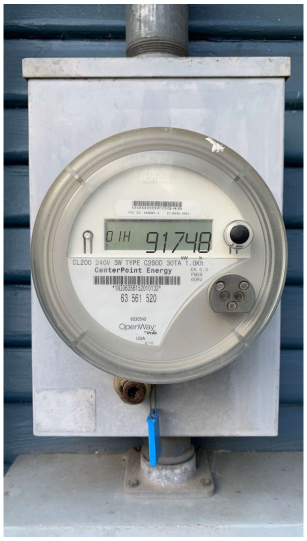
- Supervisory control and data acquisition (SCADA)
  - Designed for remote large-scale, distributed processes
- Internet of Things (IoT)
  - Small computing devices
  - OS, CPU, RAM, storage, Internet connection

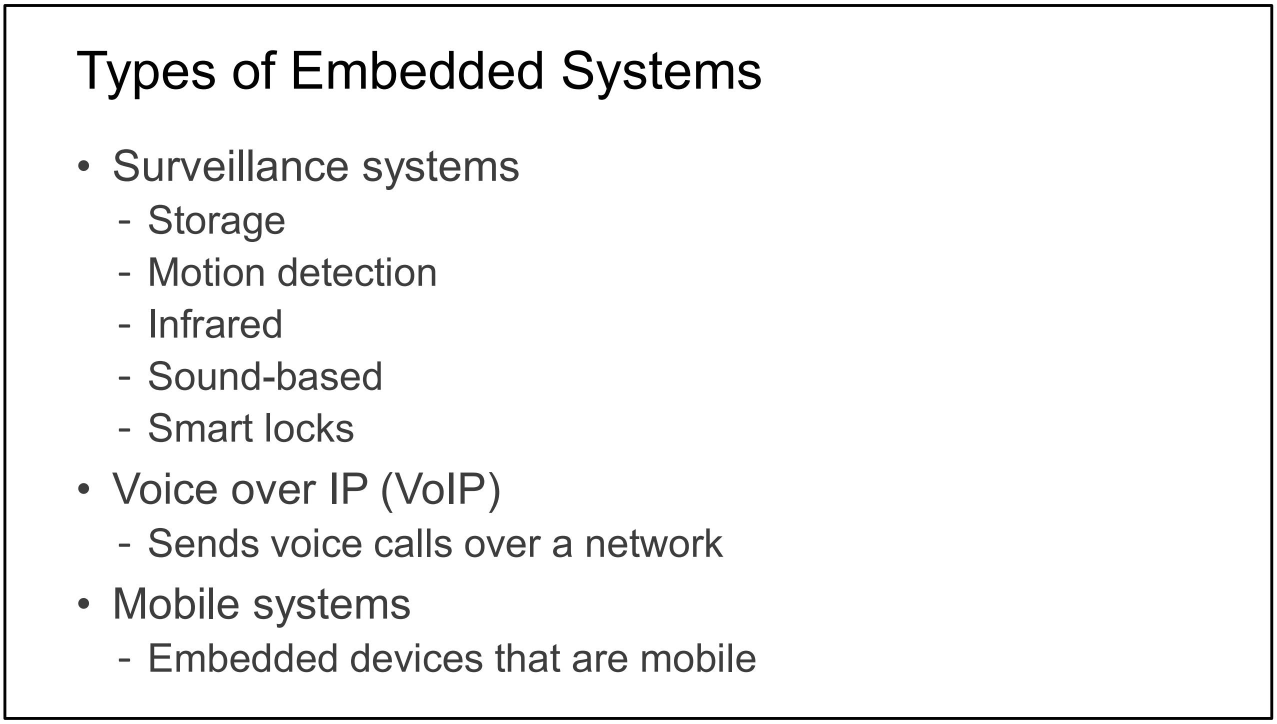


Types of Embedded Systems

- Medical systems
- In-vehicle computing systems
- Unmanned Aerial Vehicle (UAV)
  - AKA drone
- Smart meter

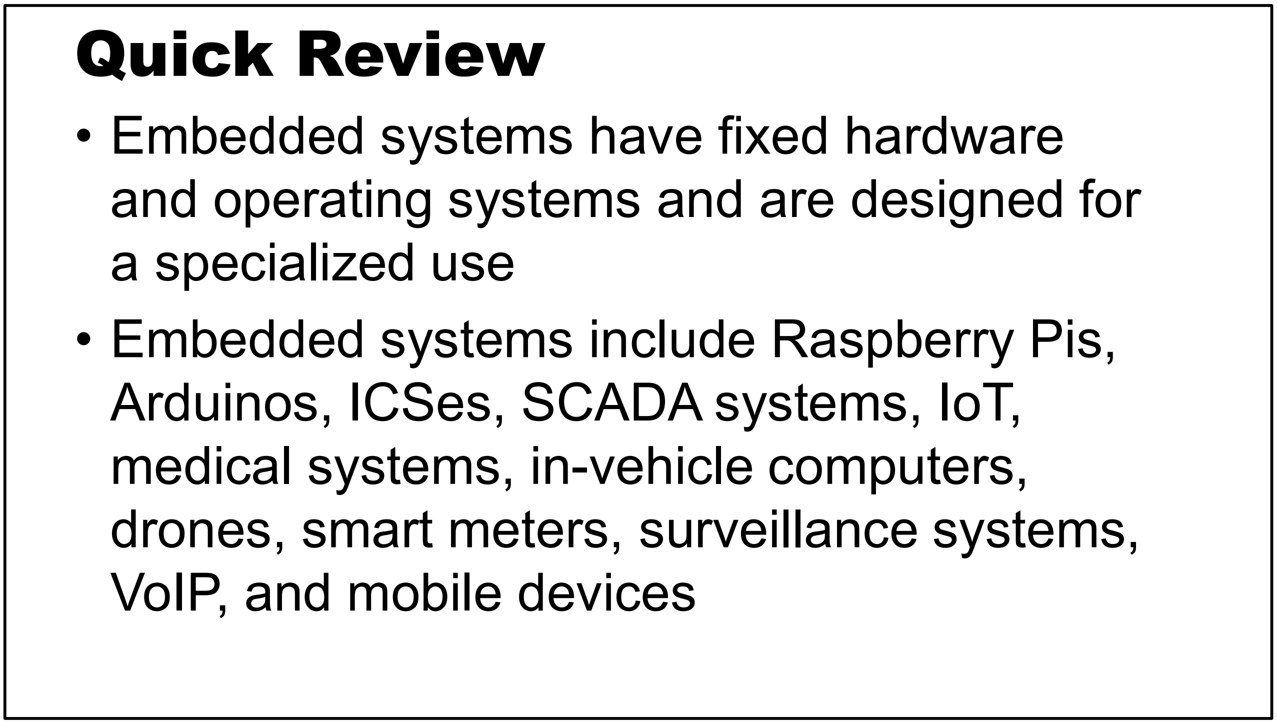
Smart Meter


CENTRON
00000F0349
FCC ID: SK9AMI-4 IC:864G-AMI4
01H 91748
kW h
CL200 240V 3W TYPE C2SOD 30TA 1.0Kh
CenterPoint Energy
CA 0.5
FM2S
60Hz
1NI06356152010132
63 561 520
9030549
OpenWay by Itron
USA
2/10



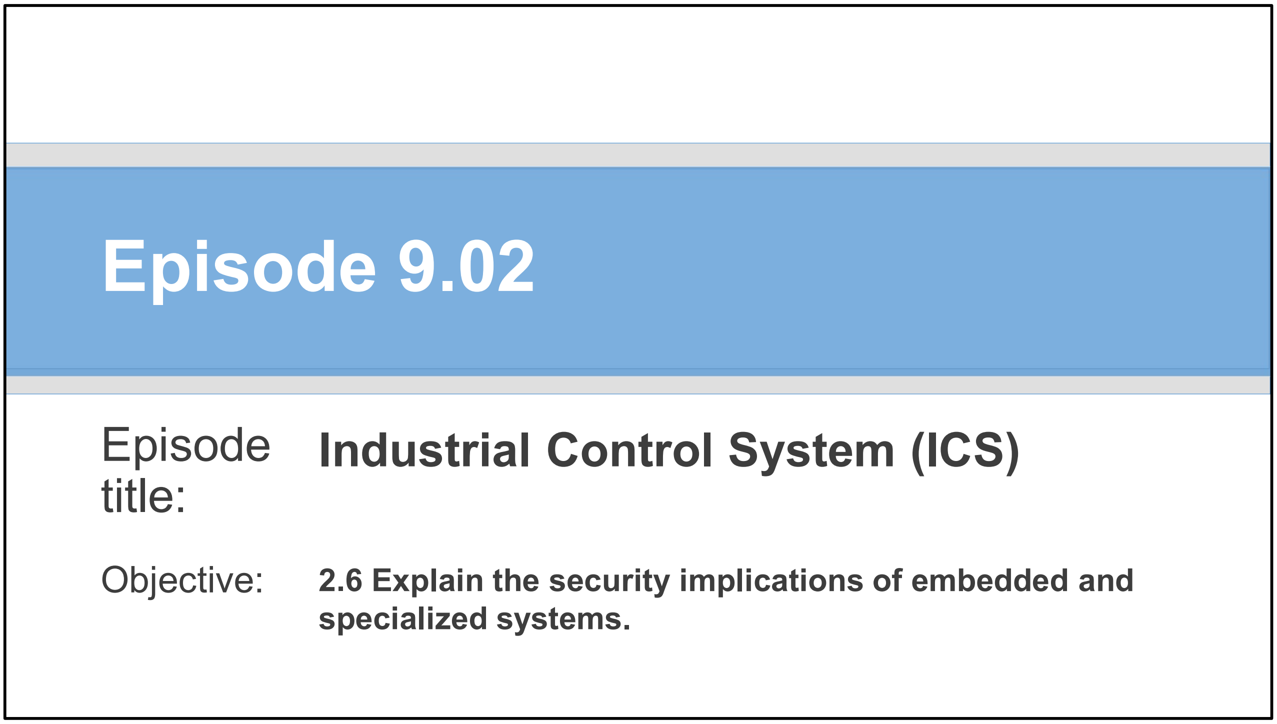
Types of Embedded Systems

- Surveillance systems
  - Storage
  - Motion detection
  - Infrared
  - Sound-based
  - Smart locks
- Voice over IP (VoIP)
  - Sends voice calls over a network
- Mobile systems
  - Embedded devices that are mobile



Quick Review

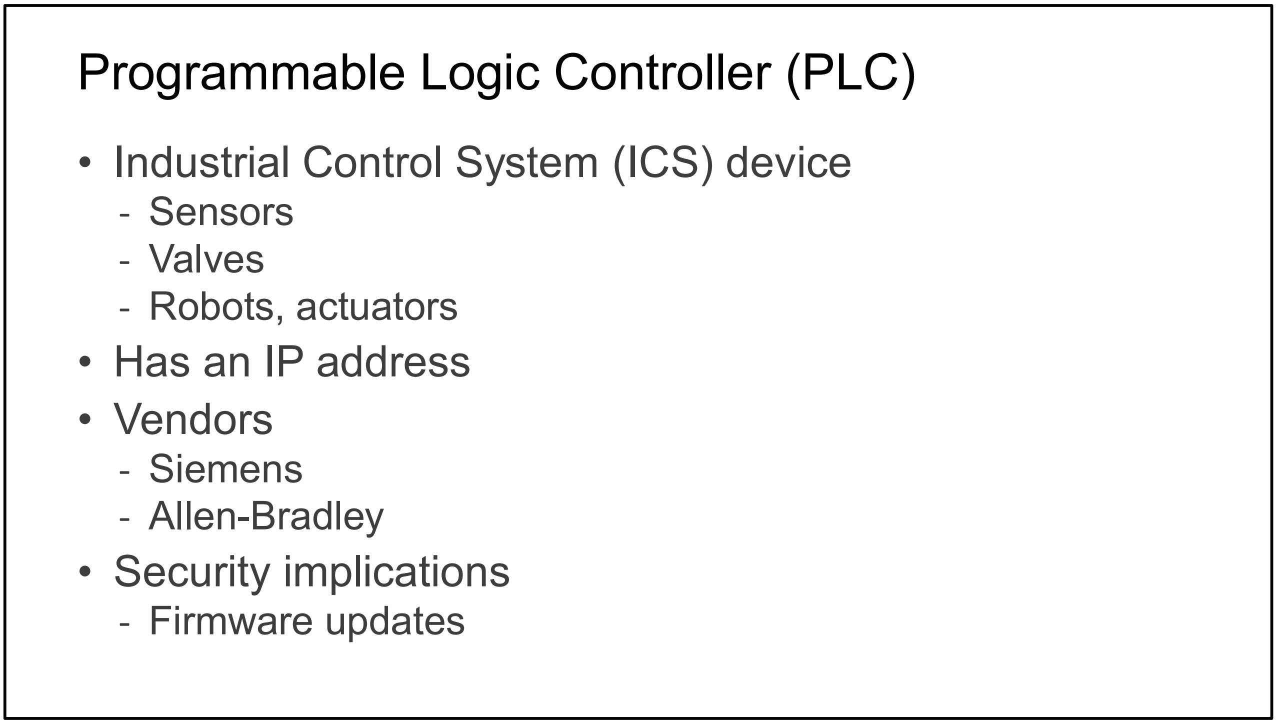
- Embedded systems have fixed hardware and operating systems and are designed for a specialized use
- Embedded systems include Raspberry Pis, Arduinos, ICSes, SCADA systems, IoT, medical systems, in-vehicle computers, drones, smart meters, surveillance systems, VoIP, and mobile devices



Episode 9.02

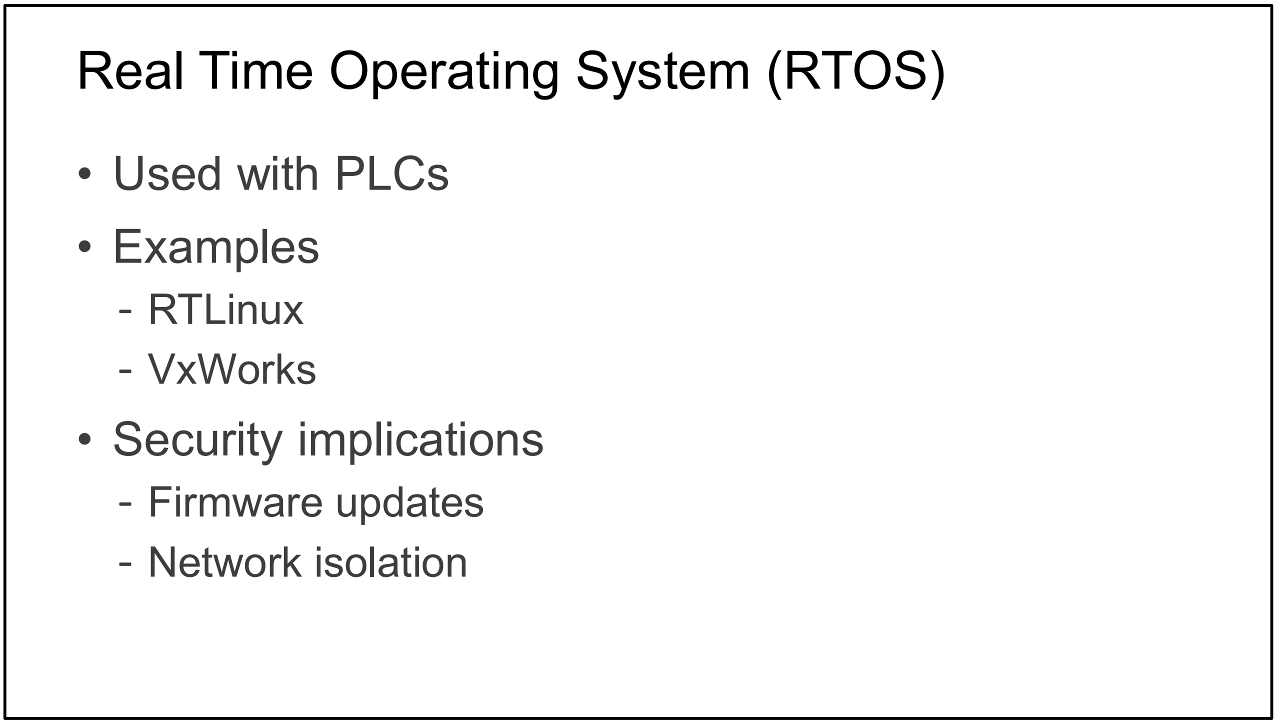
Episode title: **Industrial Control System (ICS)**

Objective: **2.6 Explain the security implications of embedded and specialized systems.**



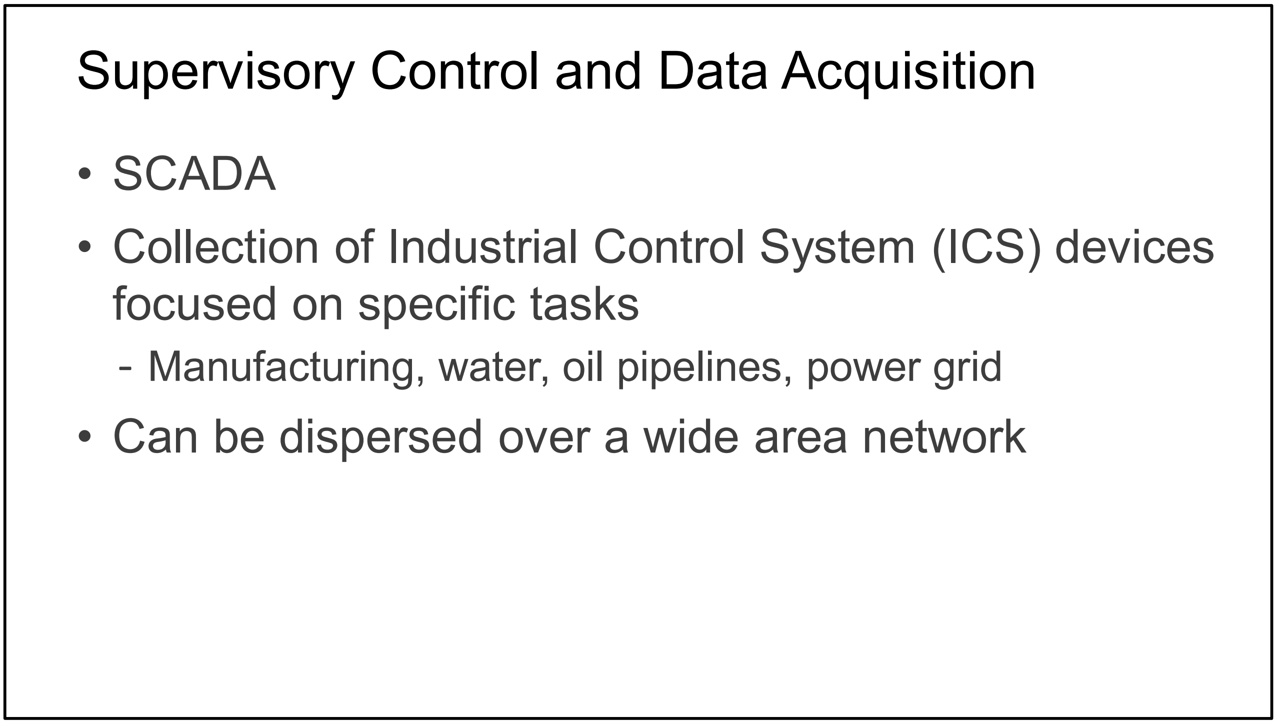
Programmable Logic Controller (PLC)

- Industrial Control System (ICS) device
  - Sensors
  - Valves
  - Robots, actuators
- Has an IP address
- Vendors
  - Siemens
  - Allen-Bradley
- Security implications
  - Firmware updates



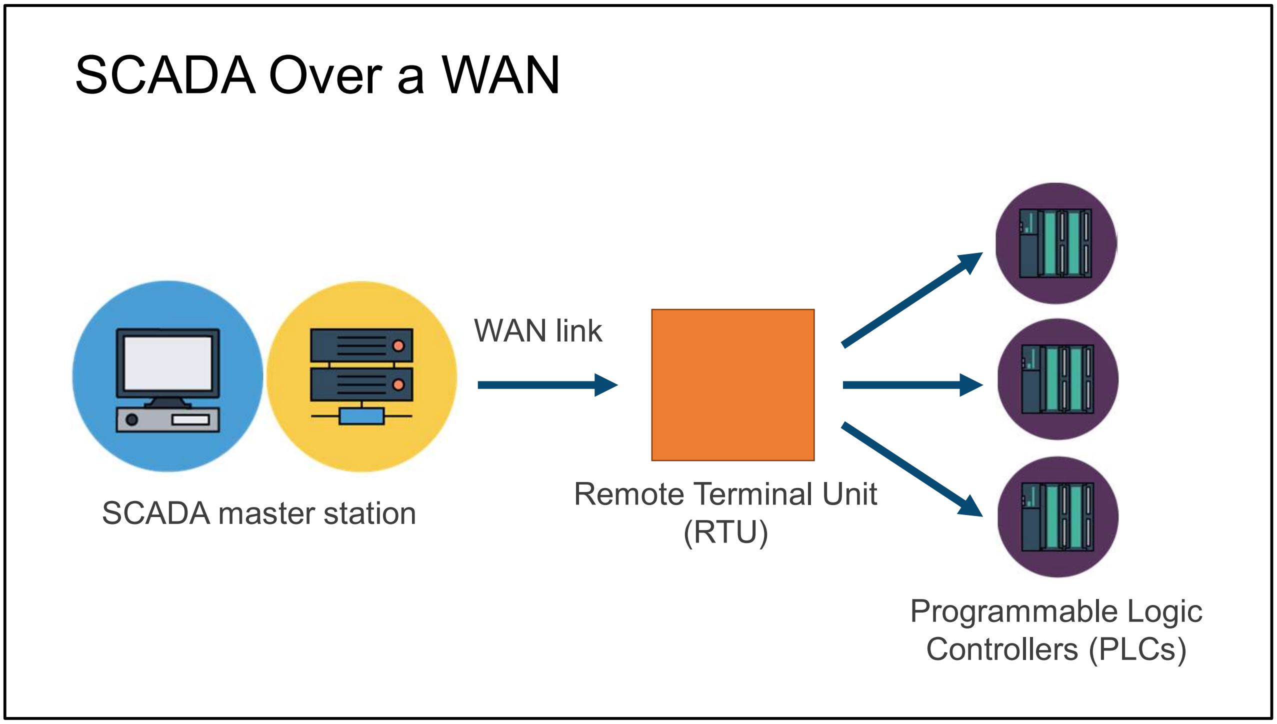
Real Time Operating System (RTOS)

- Used with PLCs
- Examples
  - RTLinux
  - VxWorks
- Security implications
  - Firmware updates
  - Network isolation



Supervisory Control and Data Acquisition

- SCADA
- Collection of Industrial Control System (ICS) devices focused on specific tasks
  - Manufacturing, water, oil pipelines, power grid
- Can be dispersed over a wide area network



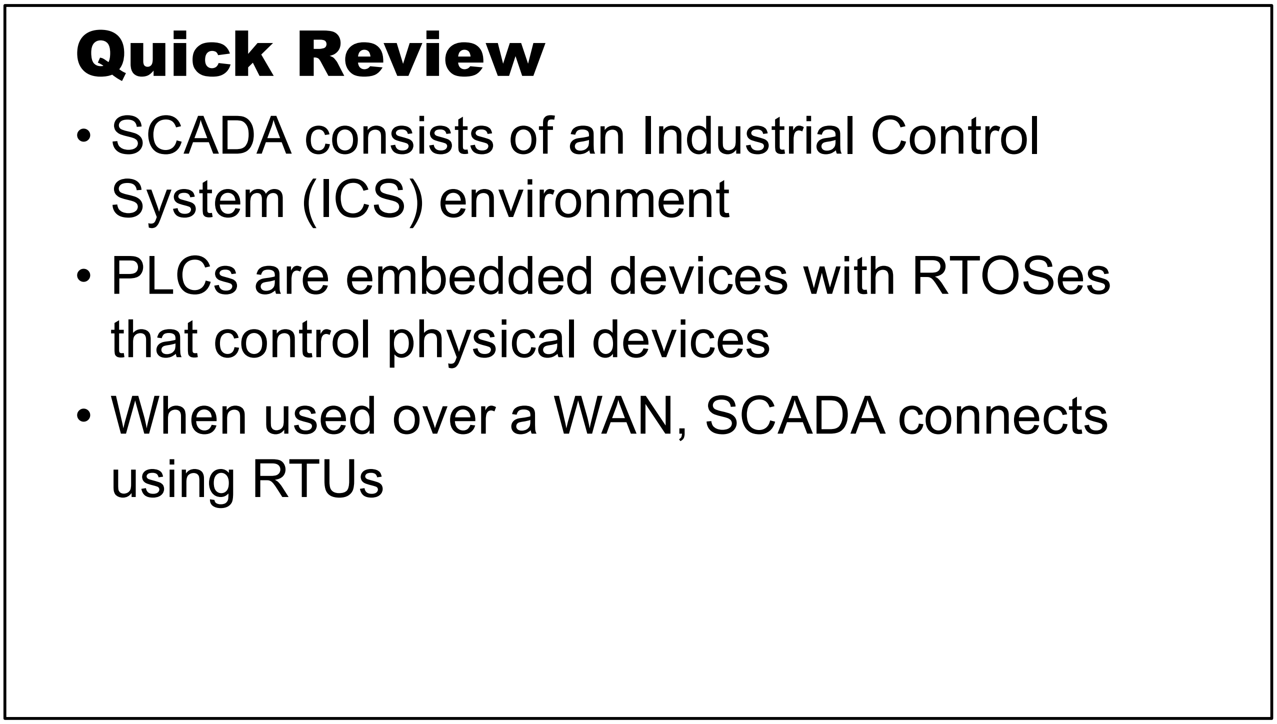
SCADA Over a WAN

SCADA master station

WAN link

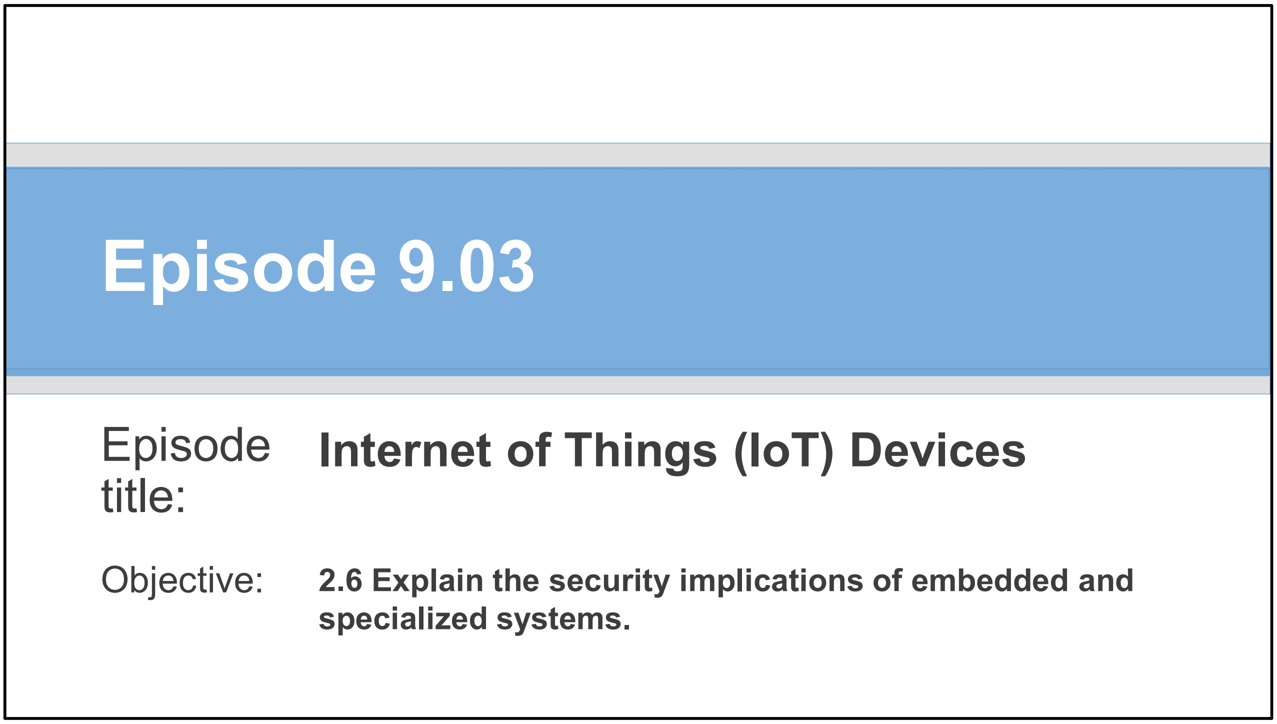
Remote Terminal Unit (RTU)

Programmable Logic Controllers (PLCs)



Quick Review

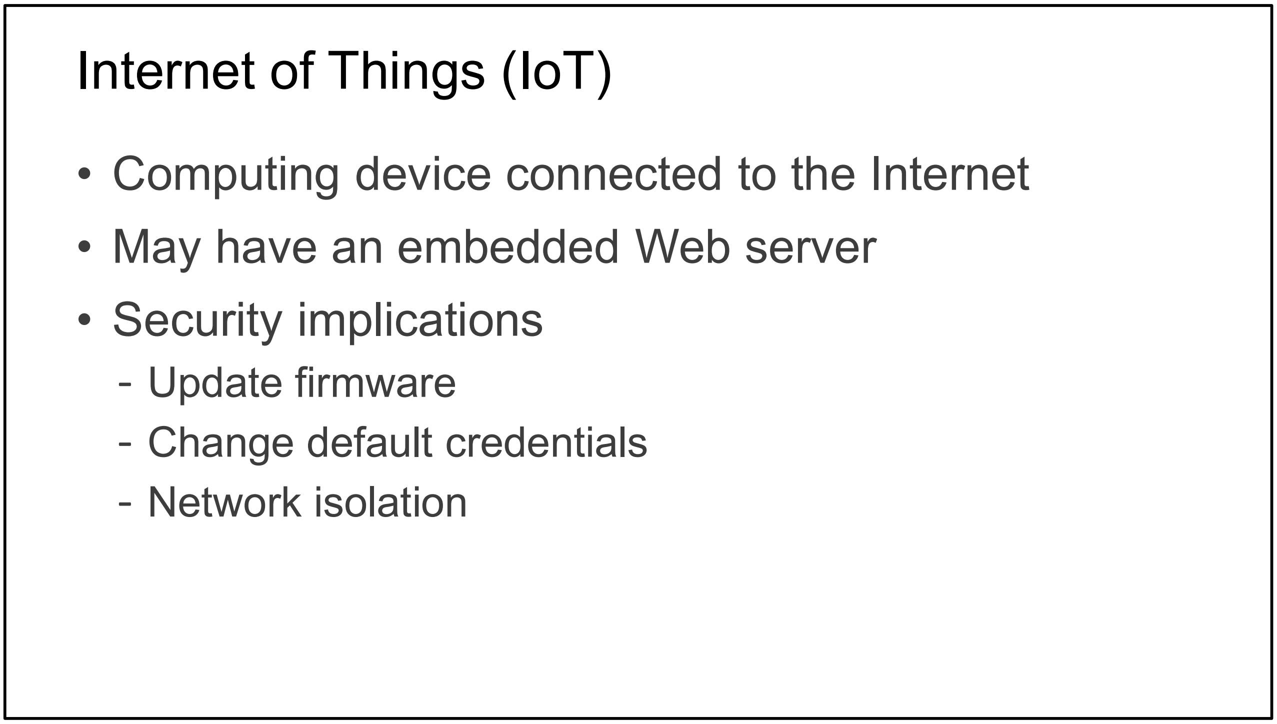
- SCADA consists of an Industrial Control System (ICS) environment
- PLCs are embedded devices with RTOSes that control physical devices
- When used over a WAN, SCADA connects using RTUs



Episode 9.03

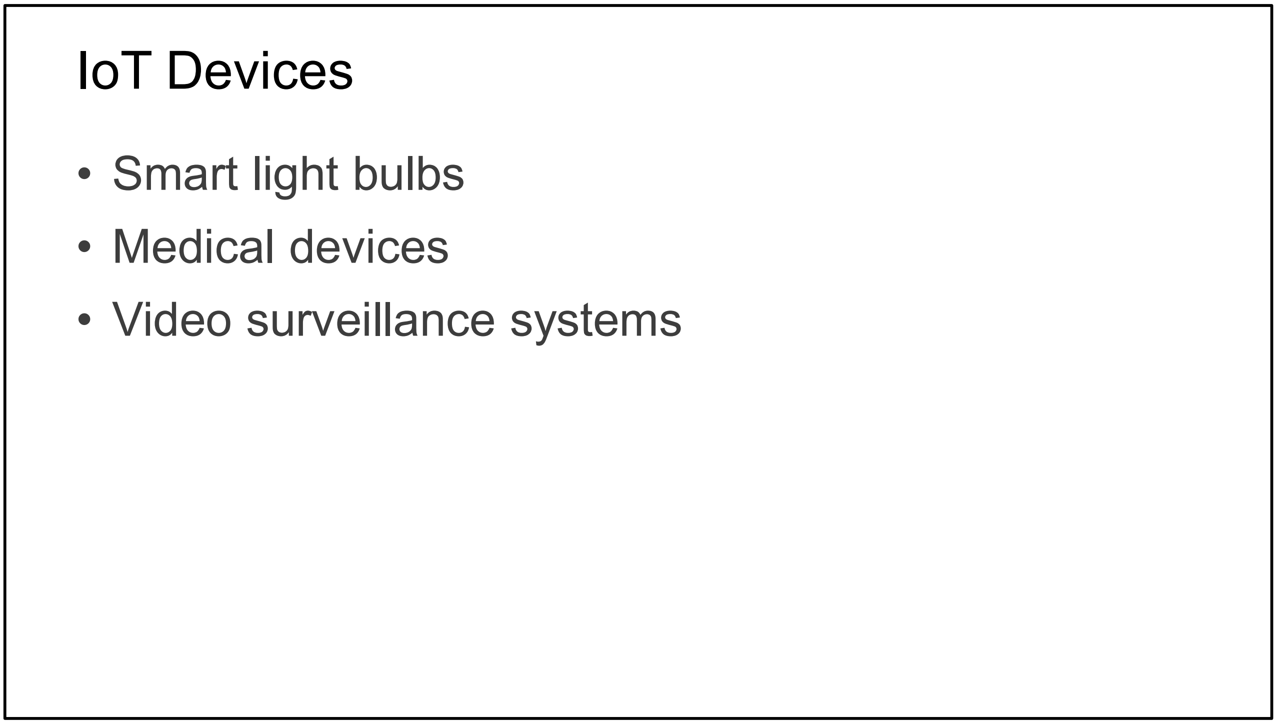
Episode title: **Internet of Things (IoT) Devices**

Objective: **2.6 Explain the security implications of embedded and specialized systems.**



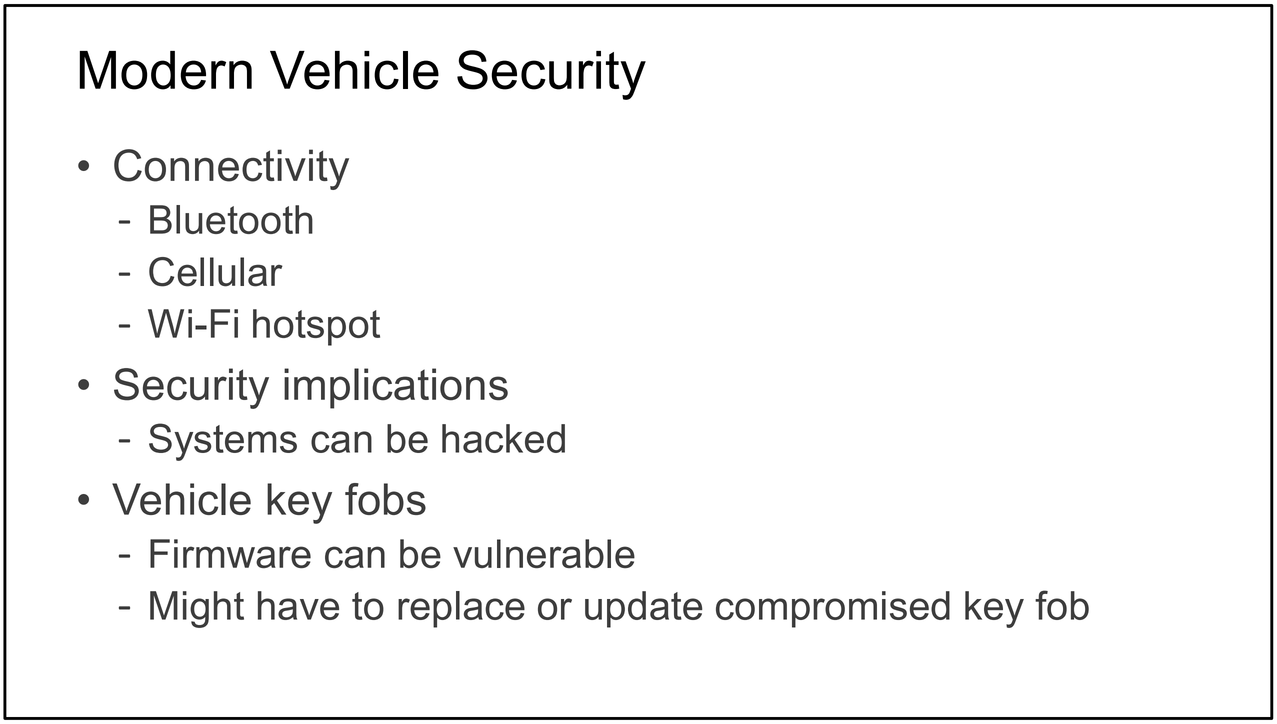
Internet of Things (IoT)

- Computing device connected to the Internet
- May have an embedded Web server
- Security implications
  - Update firmware
  - Change default credentials
  - Network isolation



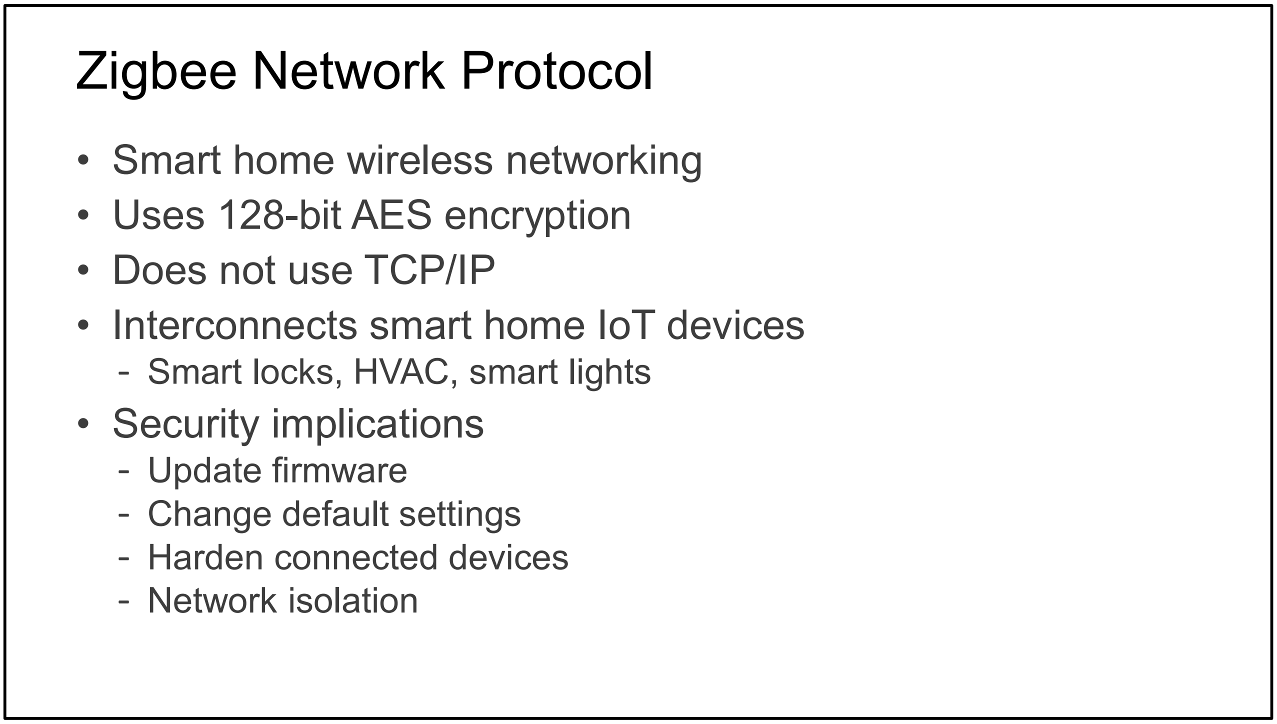
IoT Devices

- Smart light bulbs
- Medical devices
- Video surveillance systems



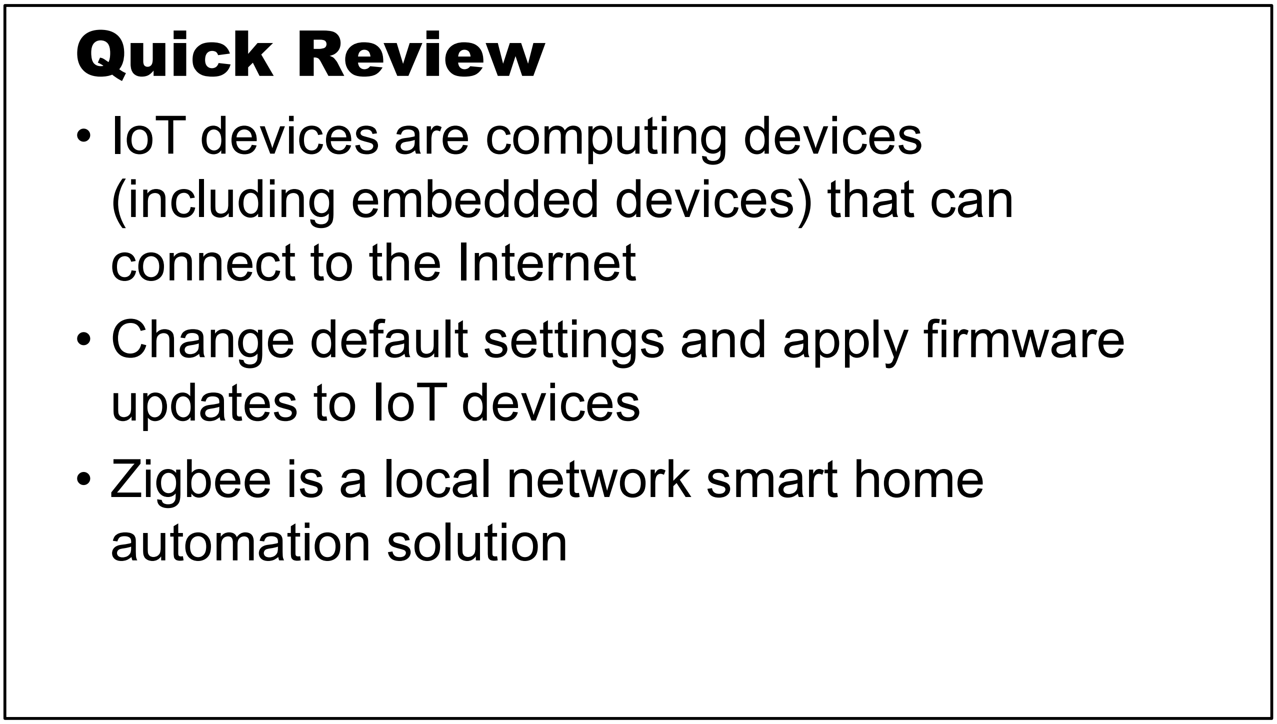
Modern Vehicle Security

- Connectivity
  - Bluetooth
  - Cellular
  - Wi-Fi hotspot
- Security implications
  - Systems can be hacked
- Vehicle key fobs
  - Firmware can be vulnerable
  - Might have to replace or update compromised key fob



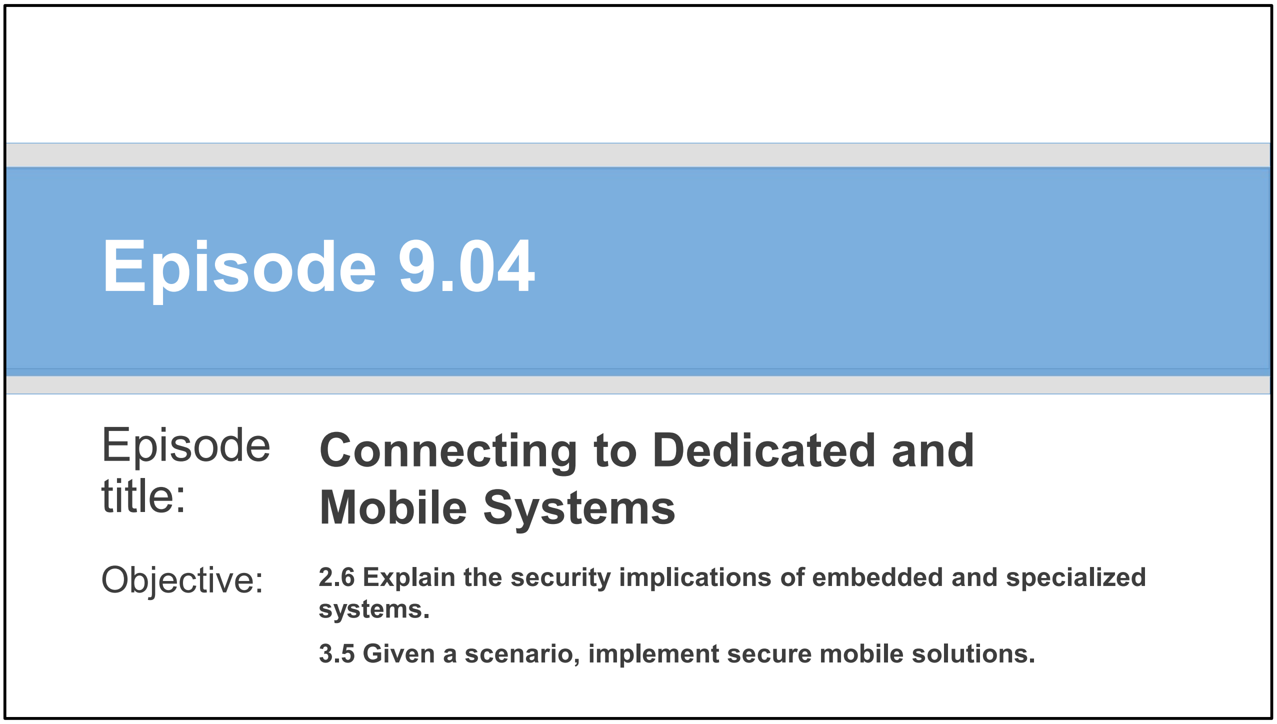
Zigbee Network Protocol

- Smart home wireless networking
- Uses 128-bit AES encryption
- Does not use TCP/IP
- Interconnects smart home IoT devices
  - Smart locks, HVAC, smart lights
- Security implications
  - Update firmware
  - Change default settings
  - Harden connected devices
  - Network isolation



Quick Review

- IoT devices are computing devices (including embedded devices) that can connect to the Internet
- Change default settings and apply firmware updates to IoT devices
- Zigbee is a local network smart home automation solution

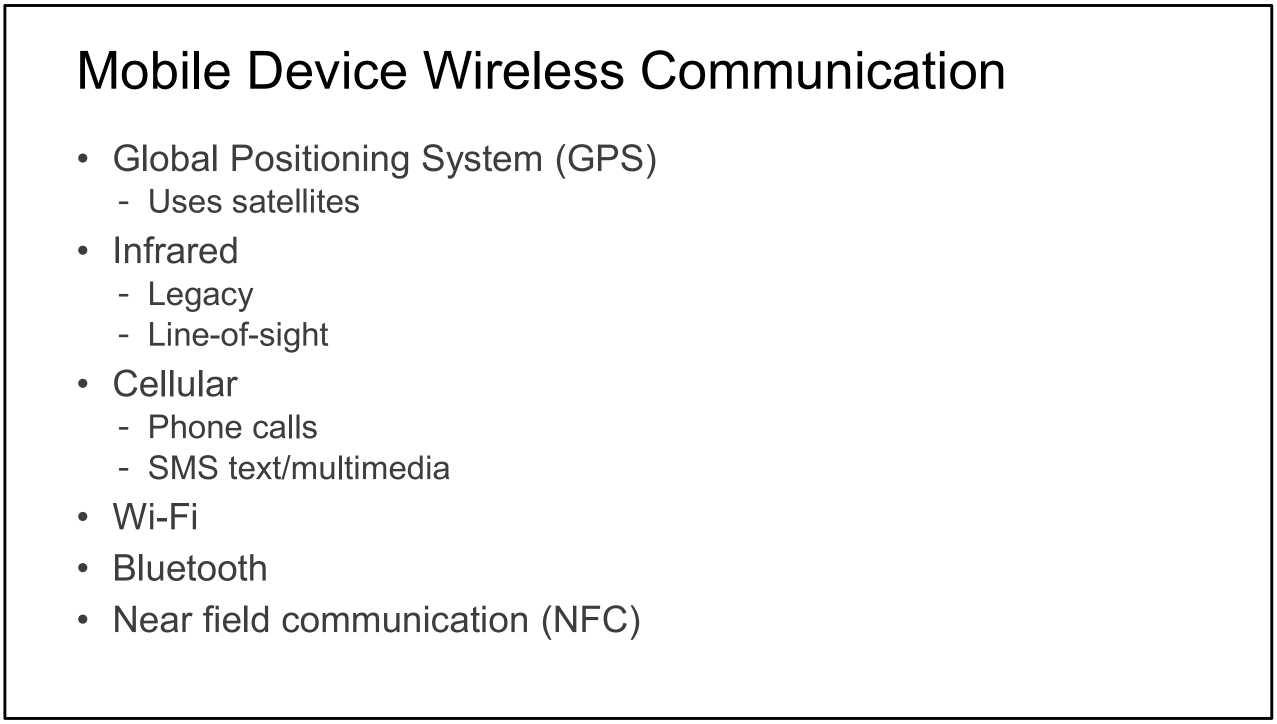


Episode 9.04

Episode title: **Connecting to Dedicated and Mobile Systems**

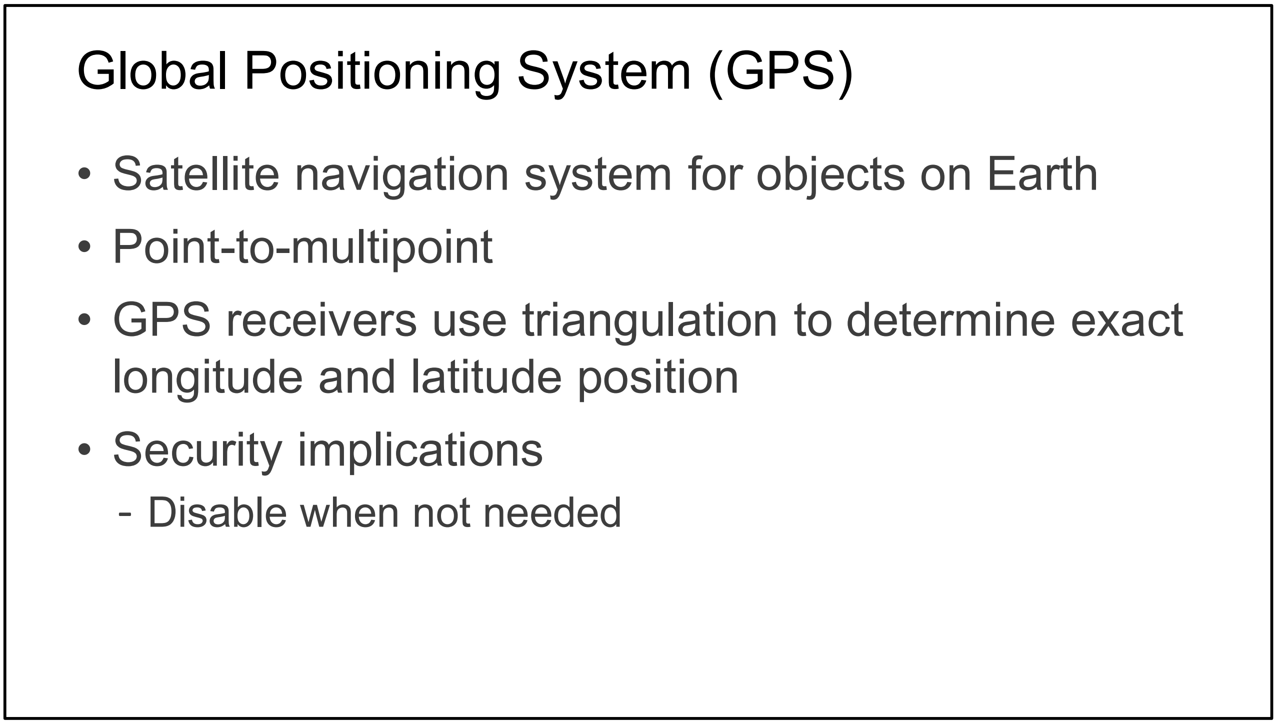
Objective: **2.6 Explain the security implications of embedded and specialized systems.**

3.5 Given a scenario, implement secure mobile solutions.



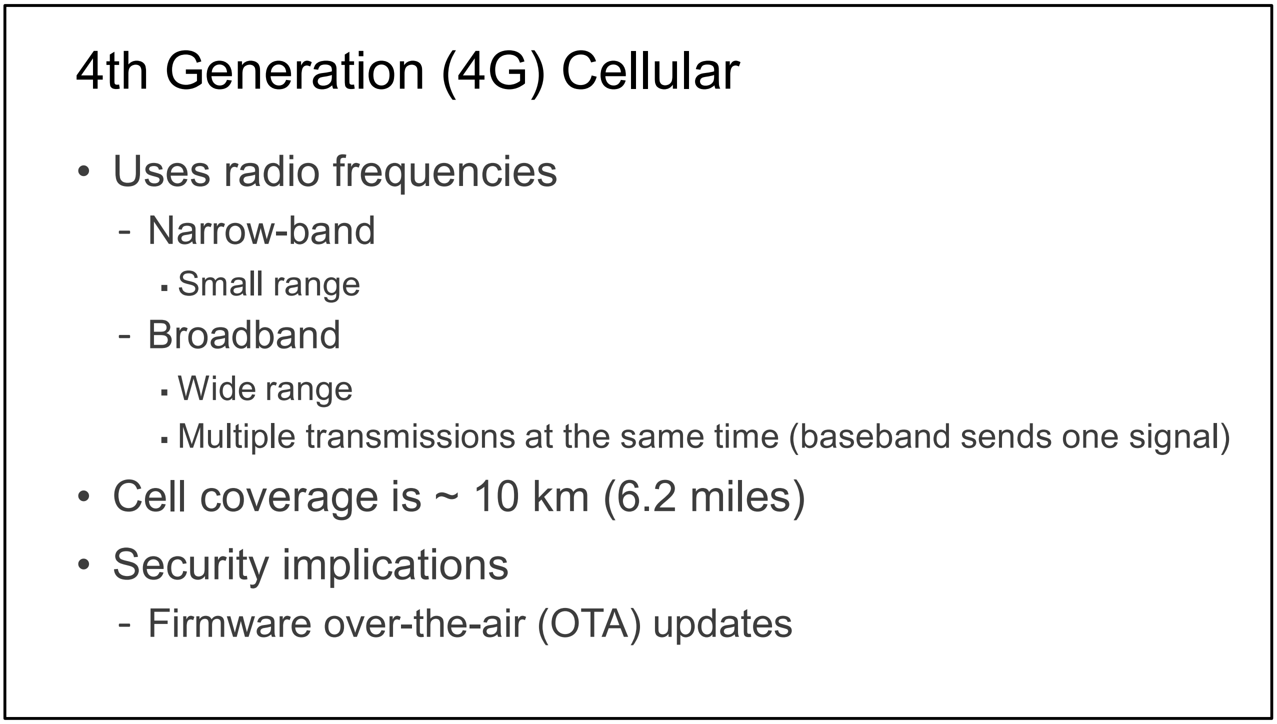
Mobile Device Wireless Communication

- Global Positioning System (GPS)
  - Uses satellites
- Infrared
  - Legacy
  - Line-of-sight
- Cellular
  - Phone calls
  - SMS text/multimedia
- Wi-Fi
- Bluetooth
- Near field communication (NFC)



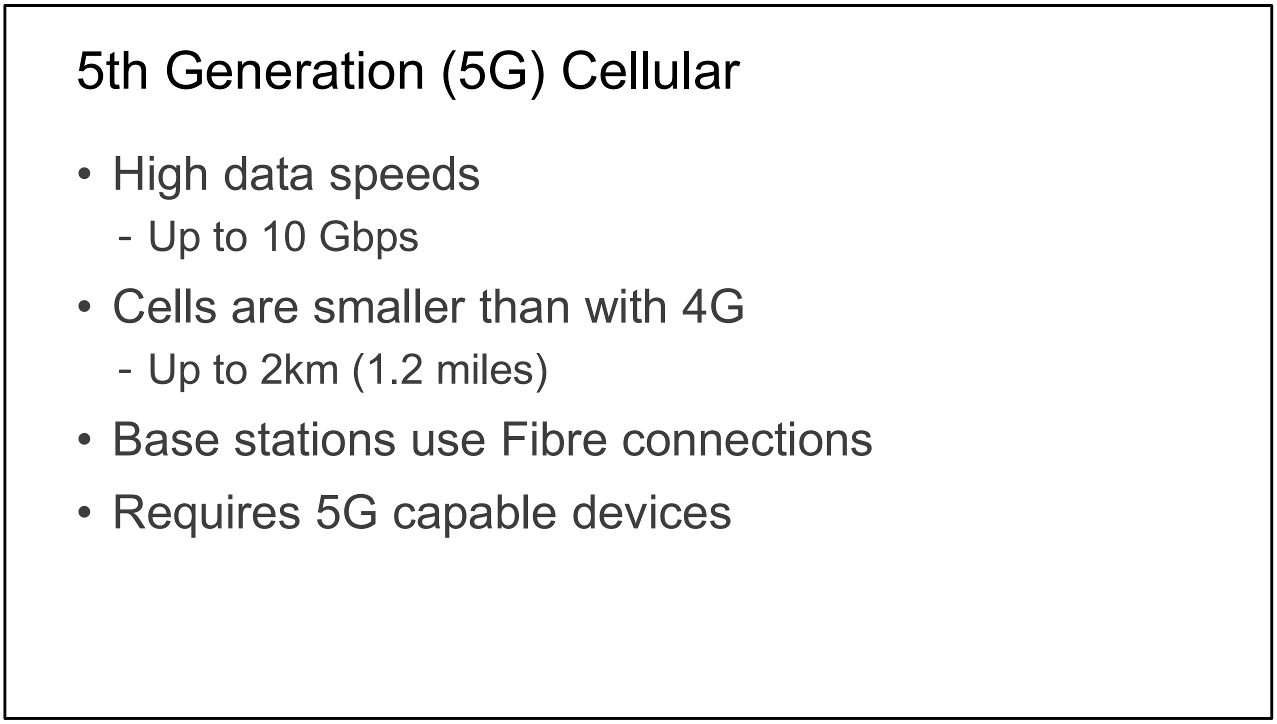
Global Positioning System (GPS)

- Satellite navigation system for objects on Earth
- Point-to-multipoint
- GPS receivers use triangulation to determine exact longitude and latitude position
- Security implications
  - Disable when not needed



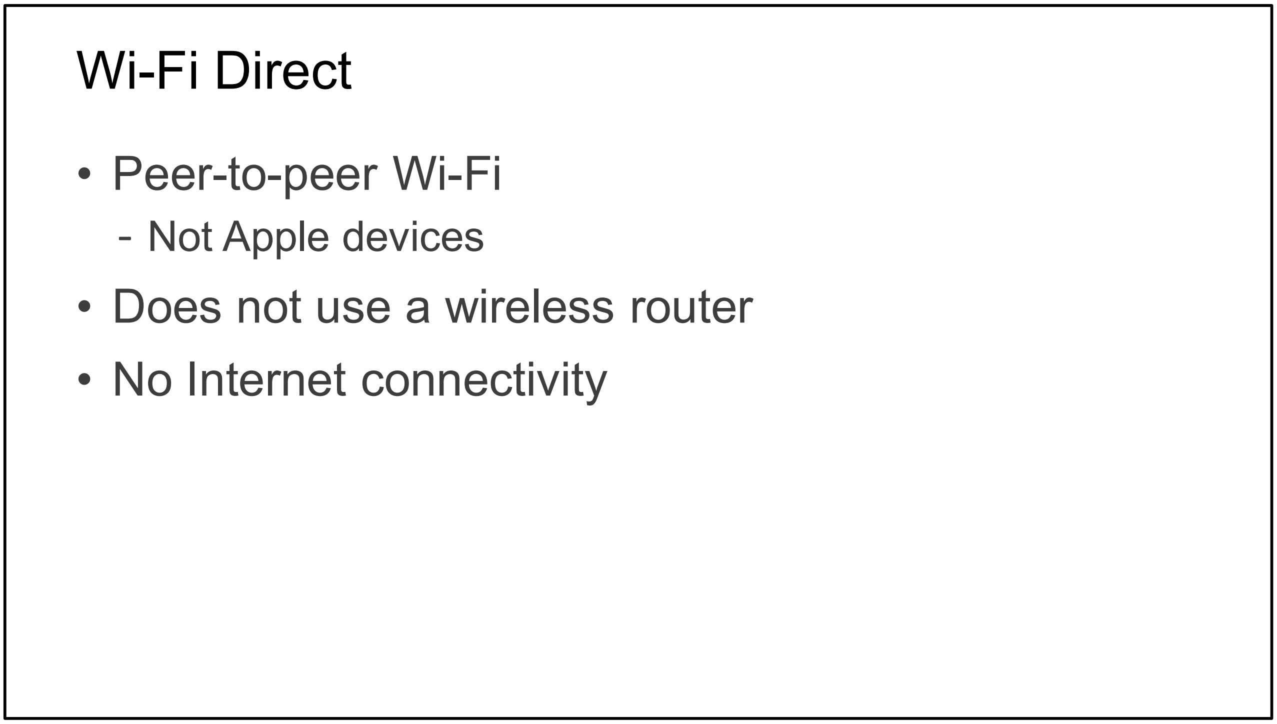
4th Generation (4G) Cellular

- Uses radio frequencies
  - Narrow-band
    - Small range
  - Broadband
    - Wide range
    - Multiple transmissions at the same time (baseband sends one signal)
- Cell coverage is ~ 10 km (6.2 miles)
- Security implications
  - Firmware over-the-air (OTA) updates



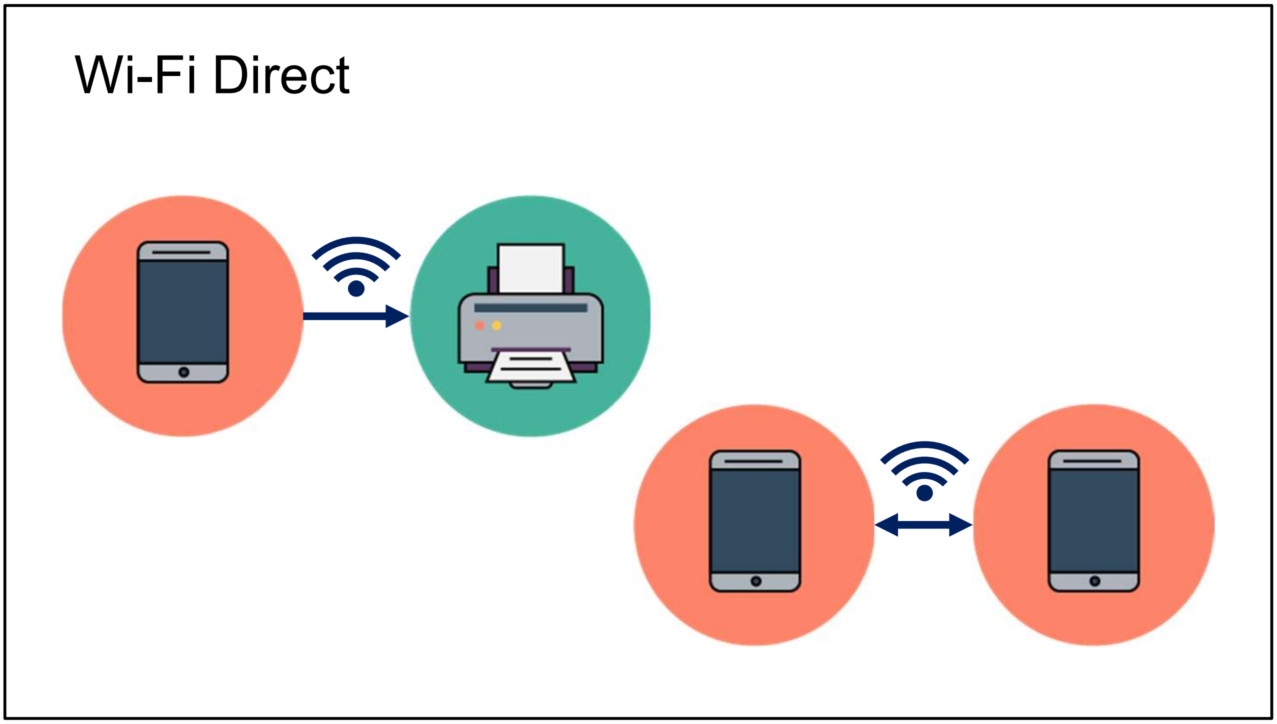
5th Generation (5G) Cellular

- High data speeds
  - Up to 10 Gbps
- Cells are smaller than with 4G
  - Up to 2km (1.2 miles)
- Base stations use Fibre connections
- Requires 5G capable devices

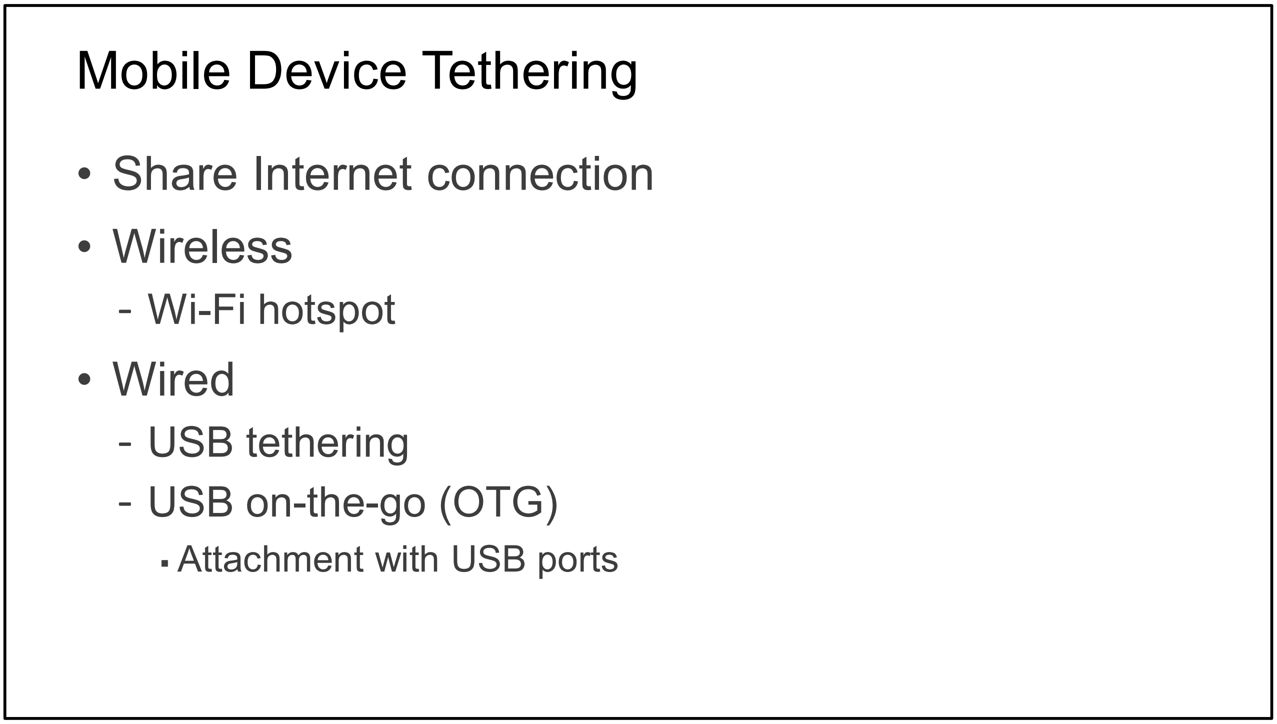


Wi-Fi Direct

- Peer-to-peer Wi-Fi
  - Not Apple devices
- Does not use a wireless router
- No Internet connectivity

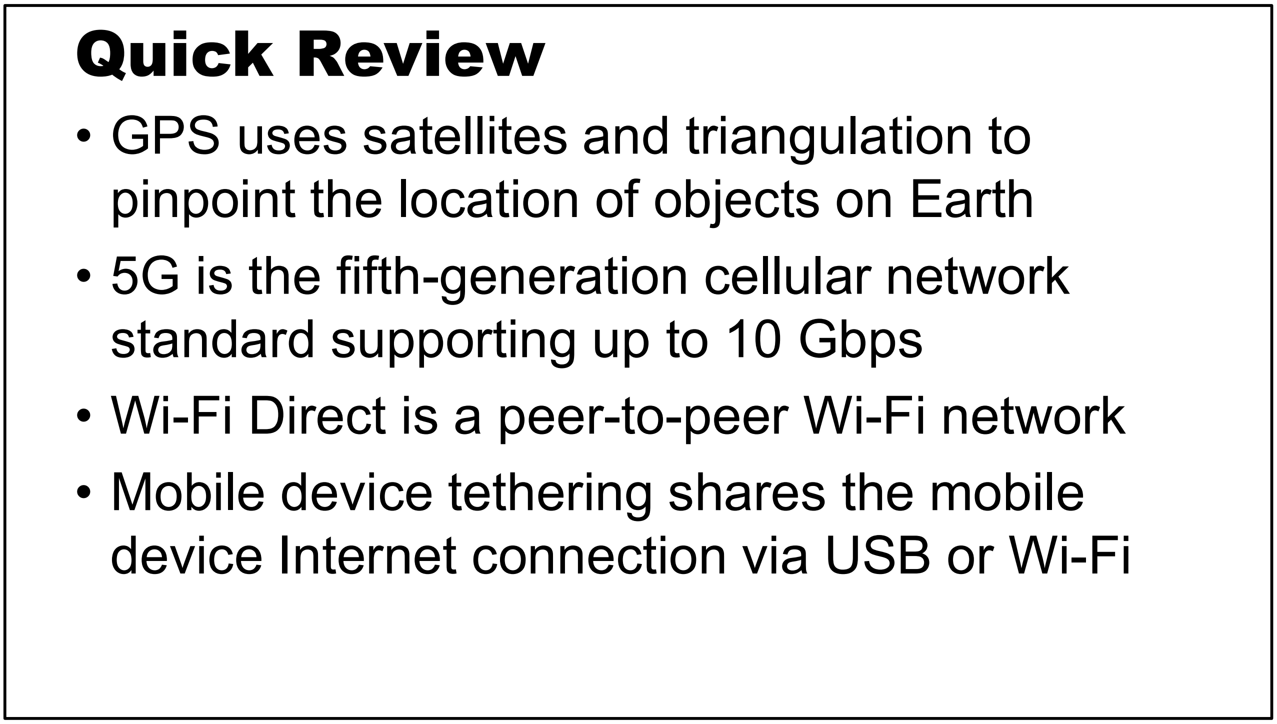


Wi-Fi Direct



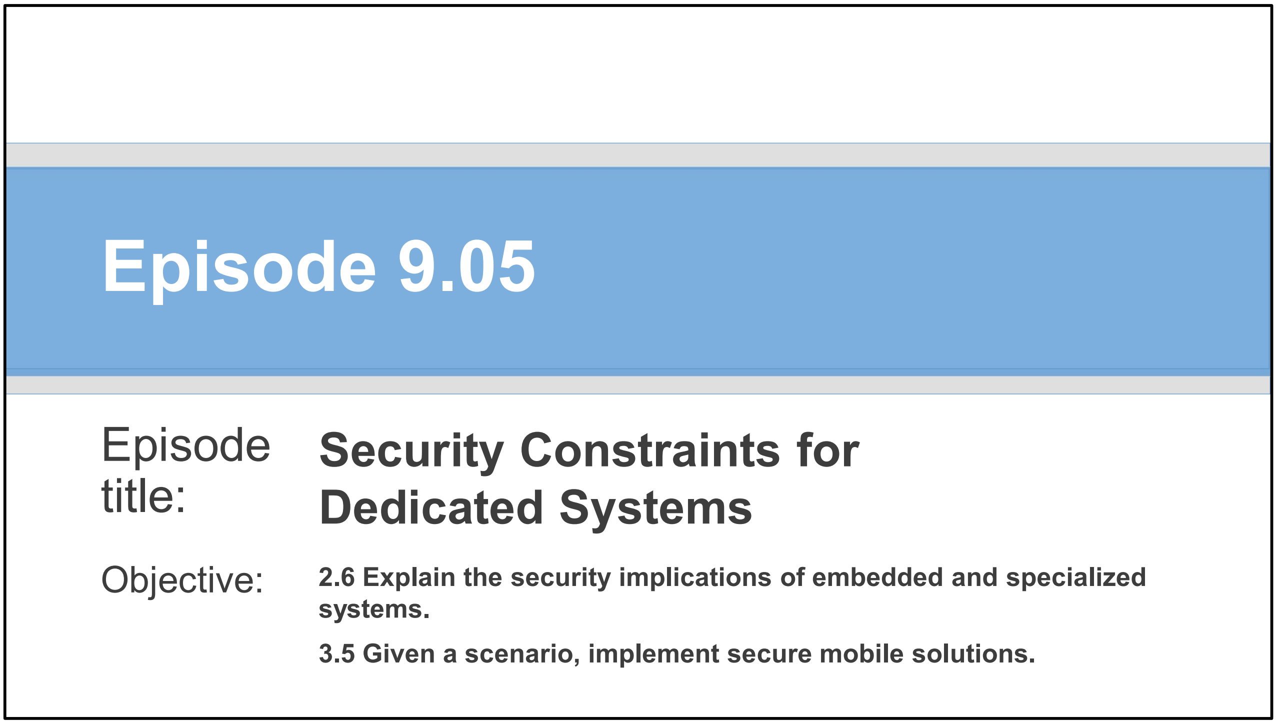
Mobile Device Tethering

- Share Internet connection
- Wireless
  - Wi-Fi hotspot
- Wired
  - USB tethering
  - USB on-the-go (OTG)
    - Attachment with USB ports



Quick Review

- GPS uses satellites and triangulation to pinpoint the location of objects on Earth
- 5G is the fifth-generation cellular network standard supporting up to 10 Gbps
- Wi-Fi Direct is a peer-to-peer Wi-Fi network
- Mobile device tethering shares the mobile device Internet connection via USB or Wi-Fi

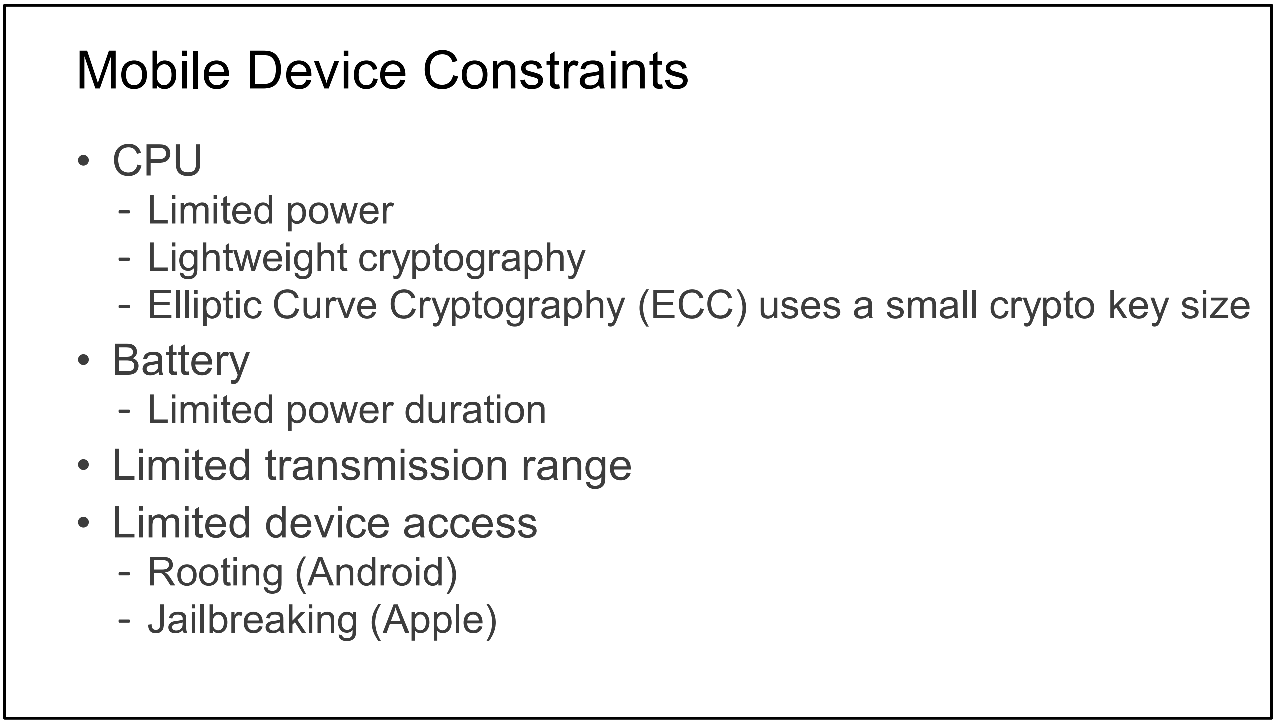


Episode 9.05

Episode title: **Security Constraints for Dedicated Systems**

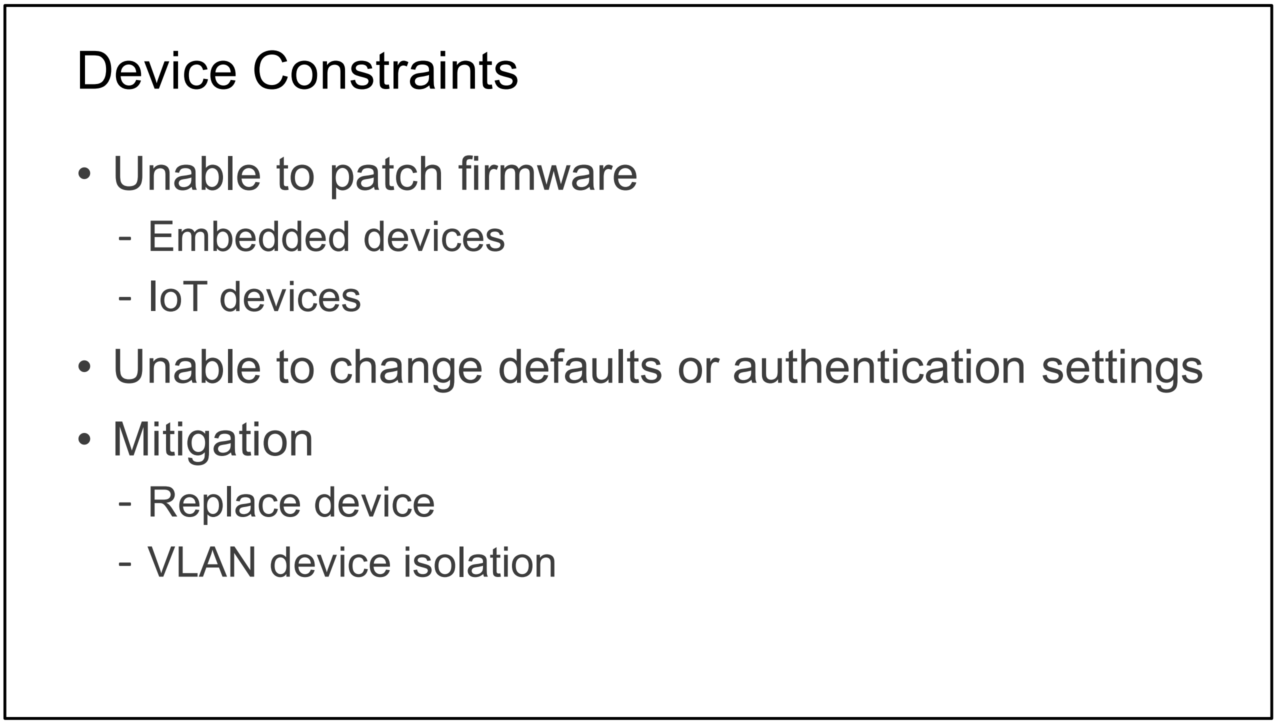
Objective: **2.6 Explain the security implications of embedded and specialized systems.**

3.5 Given a scenario, implement secure mobile solutions.



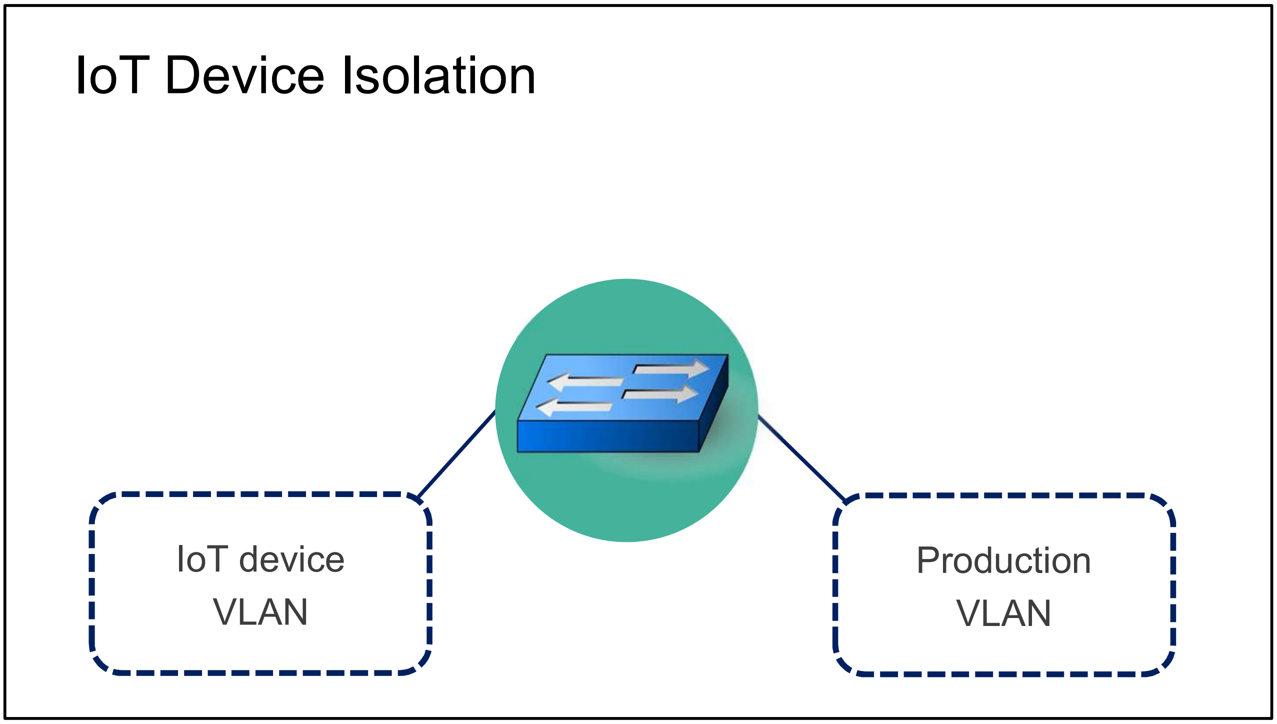
Mobile Device Constraints

- CPU
  - Limited power
  - Lightweight cryptography
  - Elliptic Curve Cryptography (ECC) uses a small crypto key size
- Battery
  - Limited power duration
- Limited transmission range
- Limited device access
  - Rooting (Android)
  - Jailbreaking (Apple)

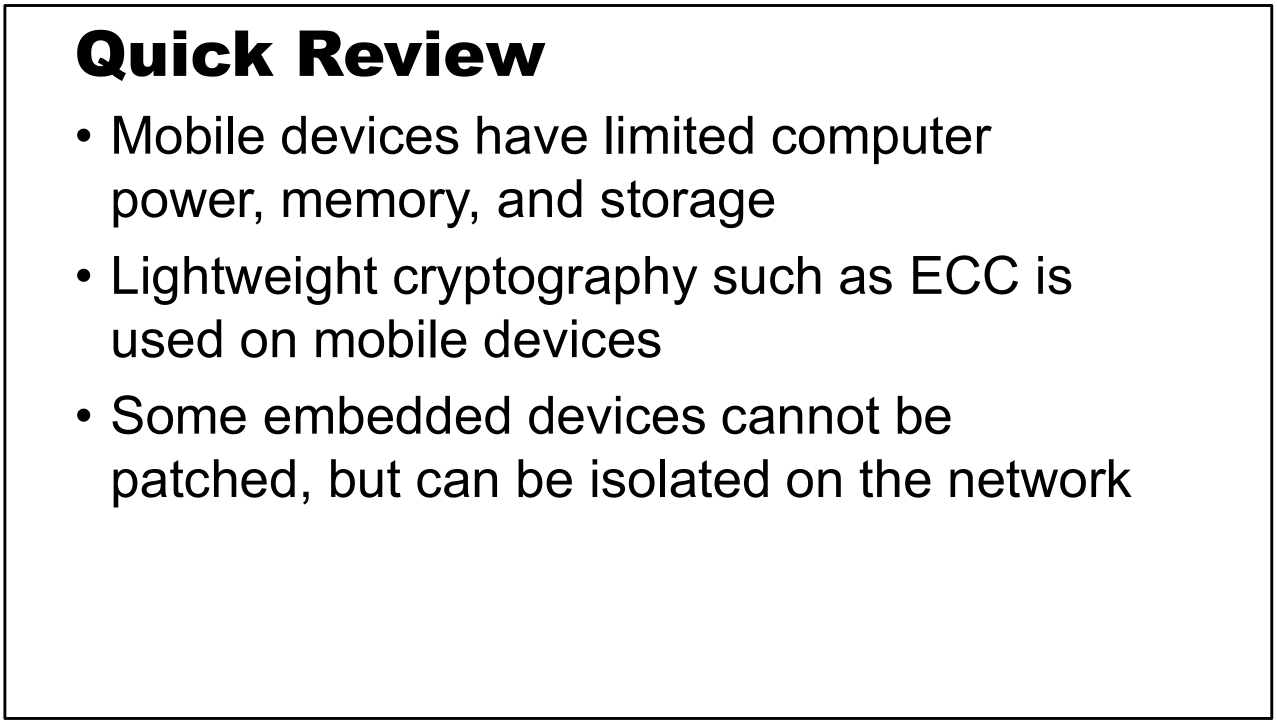


Device Constraints

- Unable to patch firmware
  - Embedded devices
  - IoT devices
- Unable to change defaults or authentication settings
- Mitigation
  - Replace device
  - VLAN device isolation

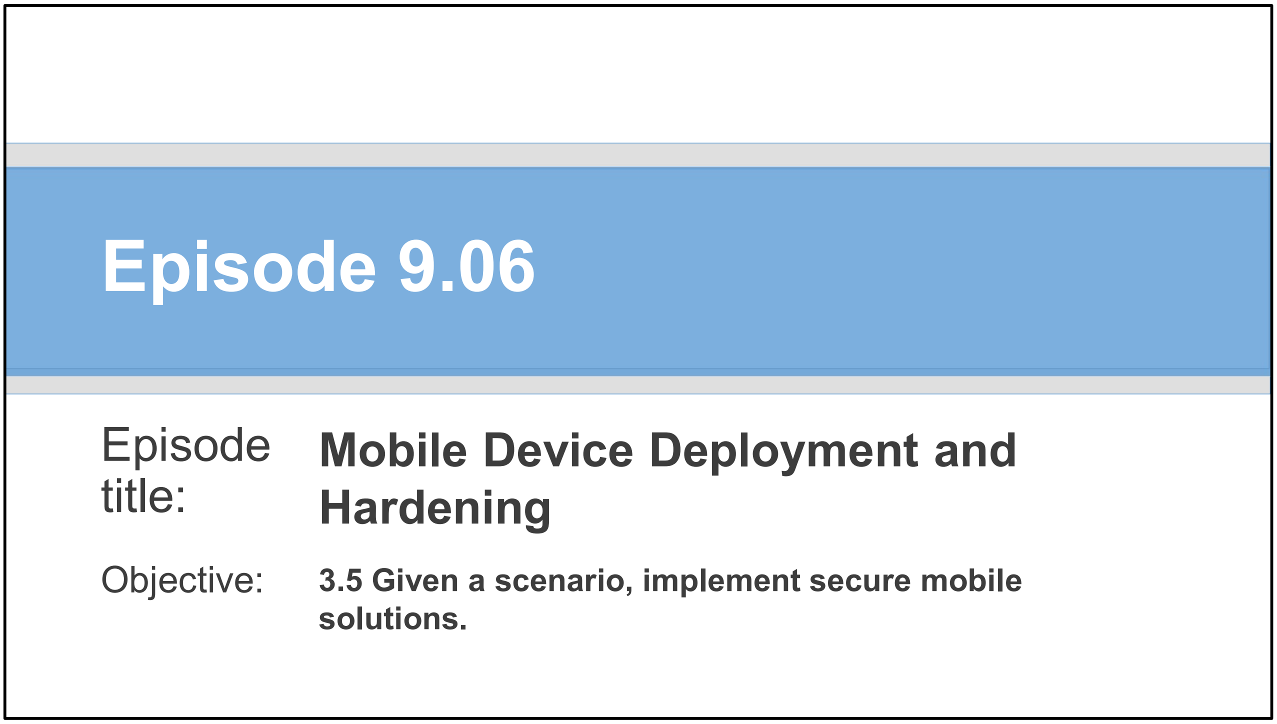


IoT Device Isolation



Quick Review

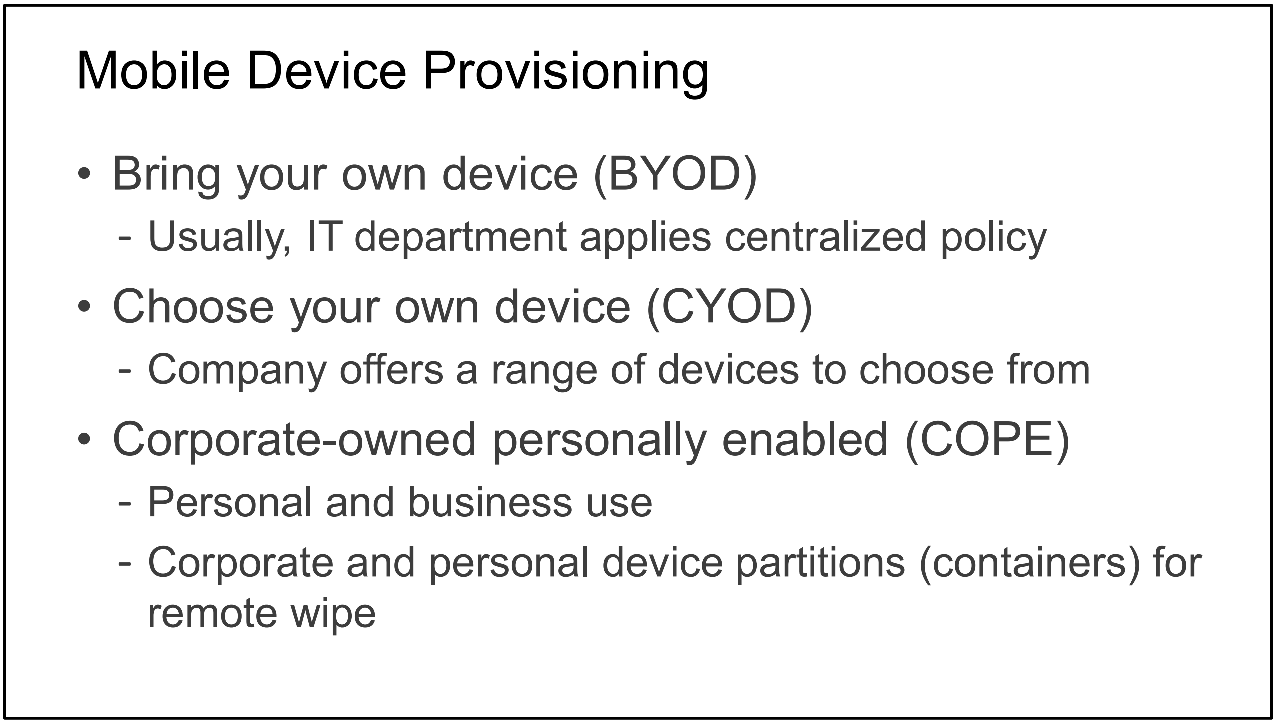
- Mobile devices have limited computer power, memory, and storage
- Lightweight cryptography such as ECC is used on mobile devices
- Some embedded devices cannot be patched, but can be isolated on the network



Episode 9.06

Episode title: **Mobile Device Deployment and Hardening**

Objective: **3.5 Given a scenario, implement secure mobile solutions.**

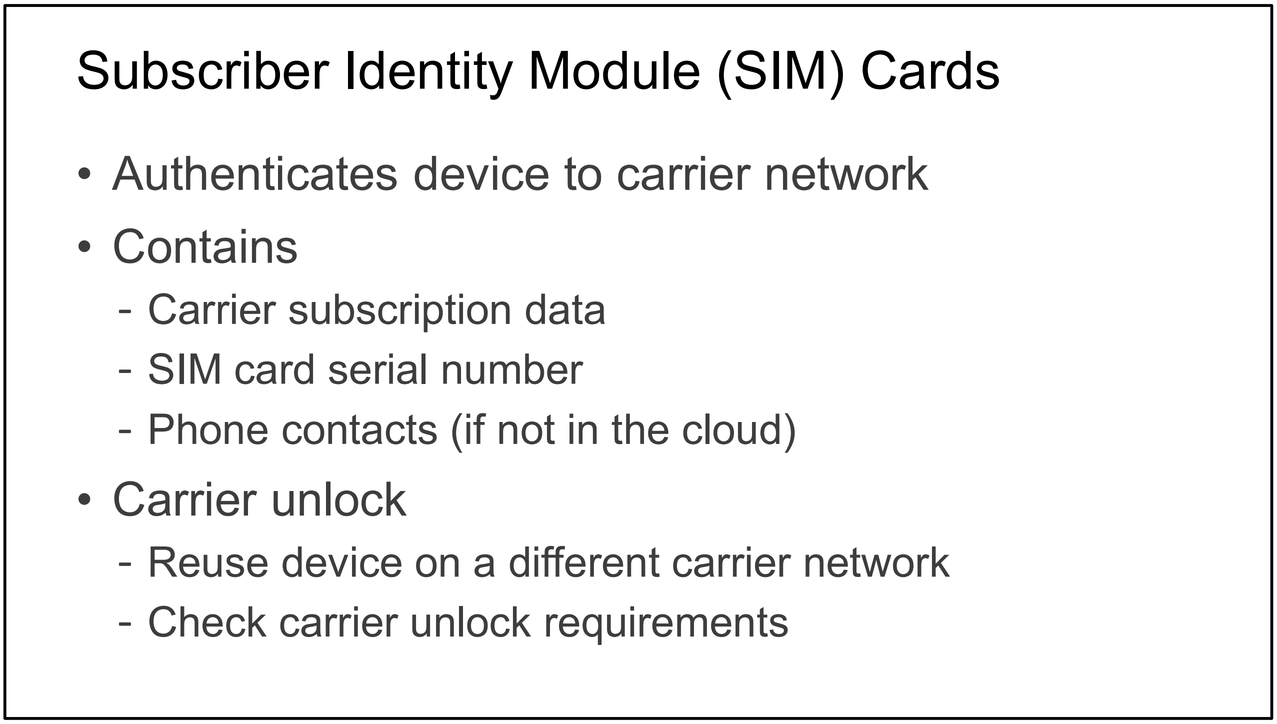


Mobile Device Provisioning

- Bring your own device (BYOD)
  - Usually, IT department applies centralized policy
- Choose your own device (CYOD)
  - Company offers a range of devices to choose from
- Corporate-owned personally enabled (COPE)
  - Personal and business use
  - Corporate and personal device partitions (containers) for remote wipe

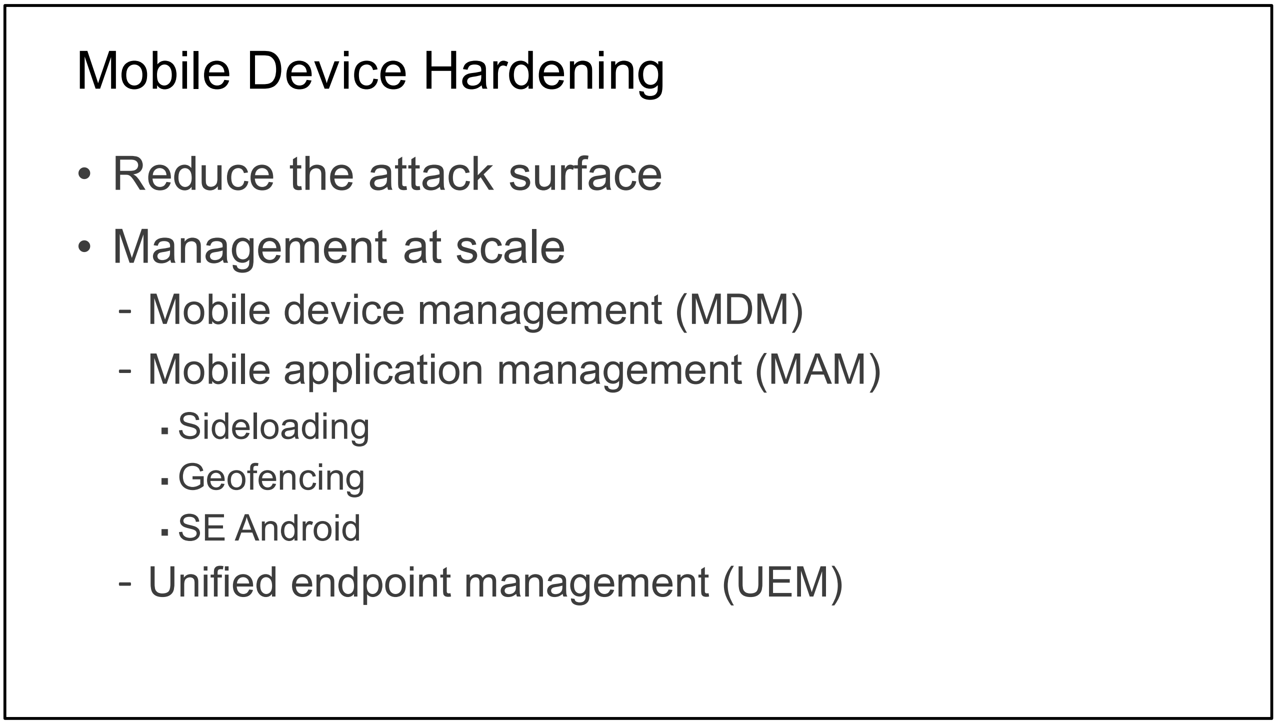
SIM Card

8901260962
[redacted]
40.40
ting
Wifi Analyzer
dSploit
Fing
File Manage..
Settings
ColorNot



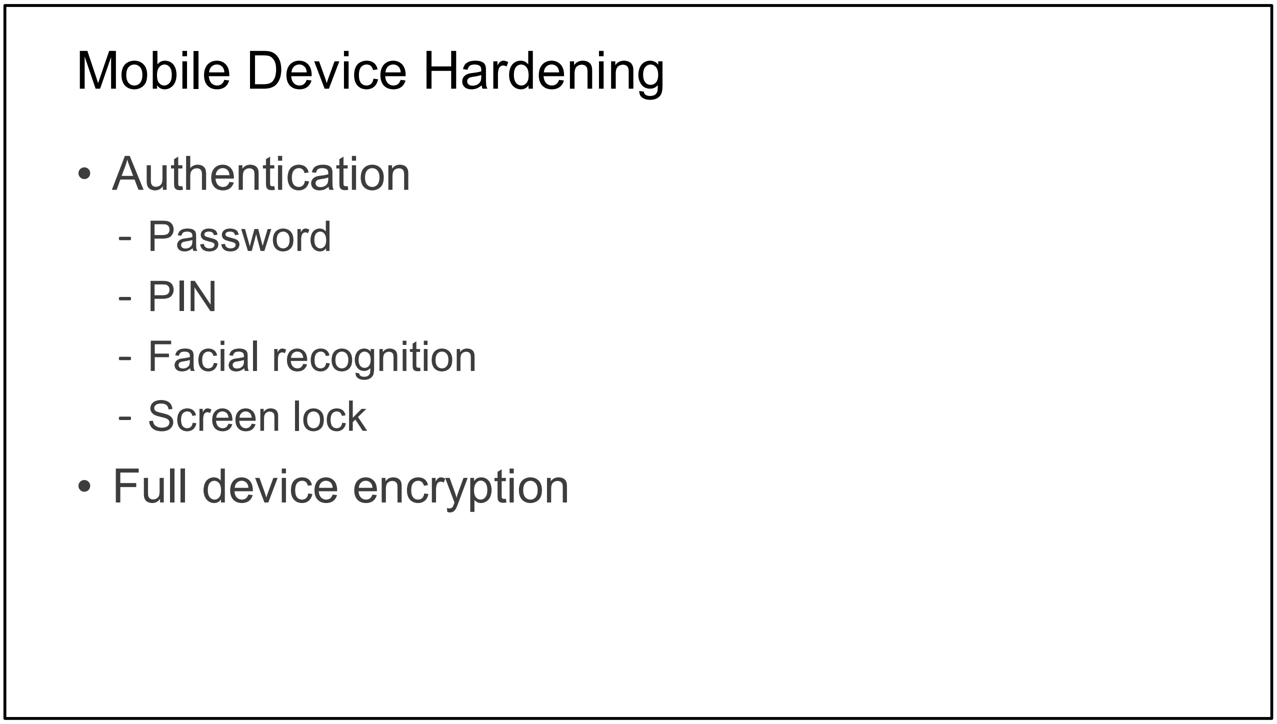
Subscriber Identity Module (SIM) Cards

- Authenticates device to carrier network
- Contains
  - Carrier subscription data
  - SIM card serial number
  - Phone contacts (if not in the cloud)
- Carrier unlock
  - Reuse device on a different carrier network
  - Check carrier unlock requirements



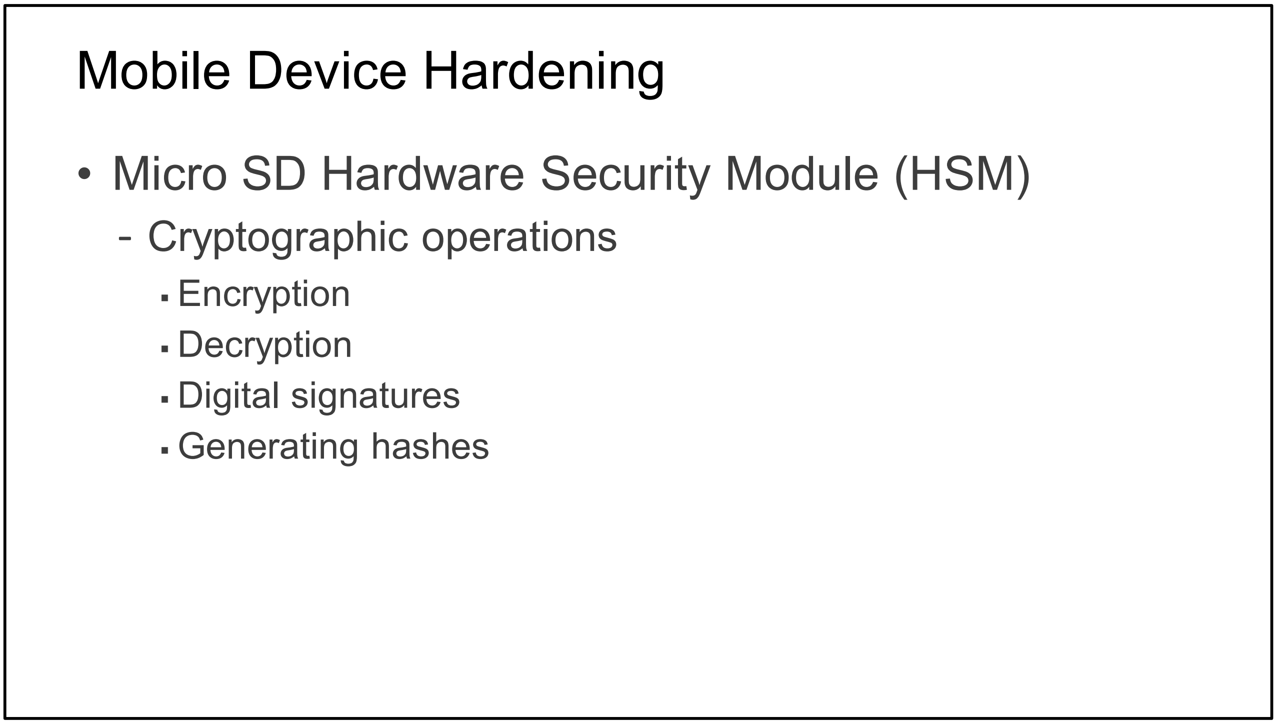
Mobile Device Hardening

- Reduce the attack surface
- Management at scale
  - Mobile device management (MDM)
  - Mobile application management (MAM)
    - Sideloading
    - Geofencing
    - SE Android
  - Unified endpoint management (UEM)



Mobile Device Hardening

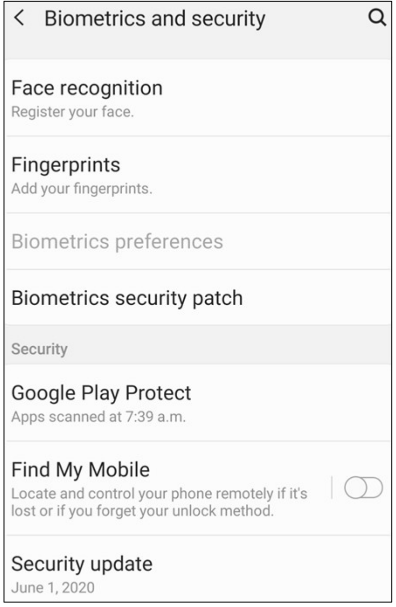
- Authentication
  - Password
  - PIN
  - Facial recognition
  - Screen lock
- Full device encryption



Mobile Device Hardening

- Micro SD Hardware Security Module (HSM)
  - Cryptographic operations
    - Encryption
    - Decryption
    - Digital signatures
    - Generating hashes

Android Smartphone Security Settings



Biometrics and security

Face recognition
Register your face.

Fingerprints
Add your fingerprints.

Biometrics preferences

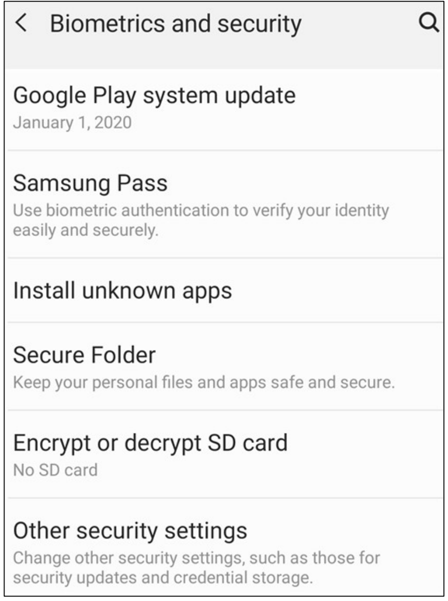
Biometrics security patch

Security

Google Play Protect
Apps scanned at 7:39 a.m.

Find My Mobile
Locate and control your phone remotely if it's lost or if you forget your unlock method.

Security update
June 1, 2020



Biometrics and security

Google Play system update
January 1, 2020

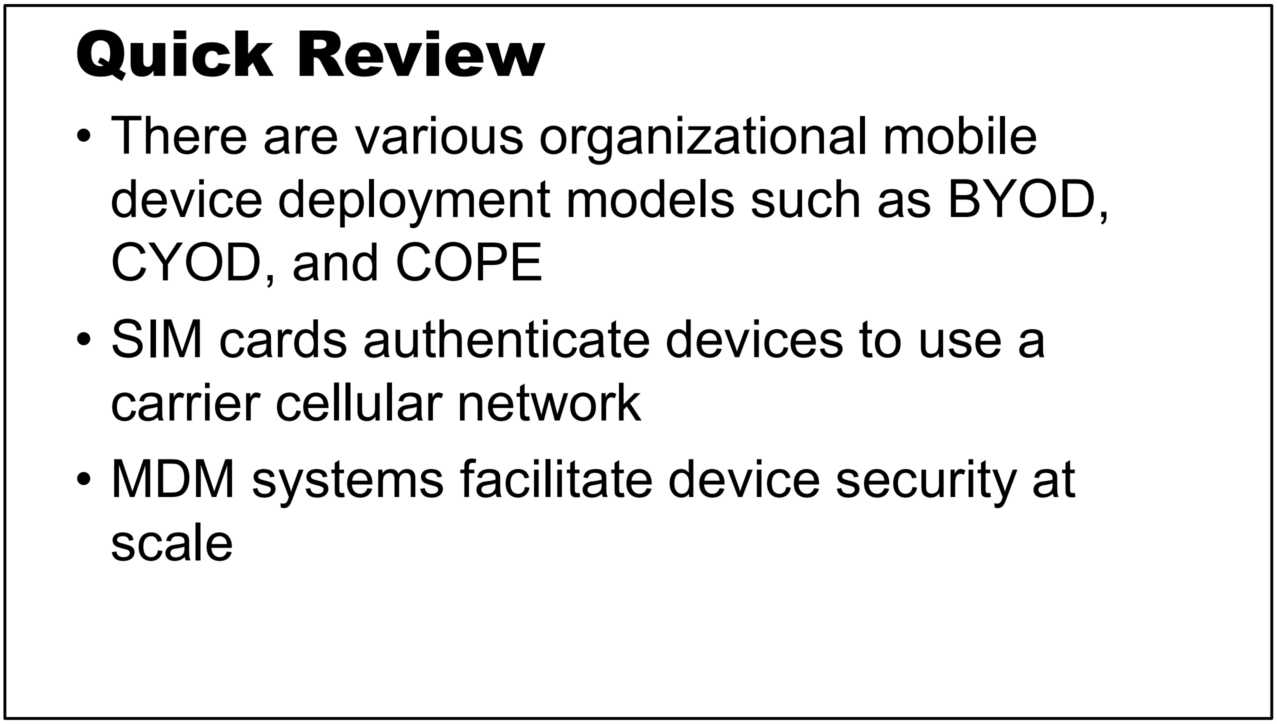
Samsung Pass
Use biometric authentication to verify your identity easily and securely.

Install unknown apps

Secure Folder
Keep your personal files and apps safe and secure.

Encrypt or decrypt SD card
No SD card

Other security settings
Change other security settings, such as those for security updates and credential storage.



Quick Review

- There are various organizational mobile device deployment models such as BYOD, CYOD, and COPE
- SIM cards authenticate devices to use a carrier cellular network
- MDM systems facilitate device security at scale