Chapter 6: Mobile and Embedded Device Security

Introduction to Mobile Devices

- Types of Mobile Devices include the following:
- **Tablets** are portable computing devices that generally lack a built-in keyboard or mouse
- **Smartphones** have all of the tools of a feature phone plus an OS that allows it to run apps and access the Internet
- **Wearables** are devices that can be worn by the user instead of carried
- The most common of these devices is the smart watch

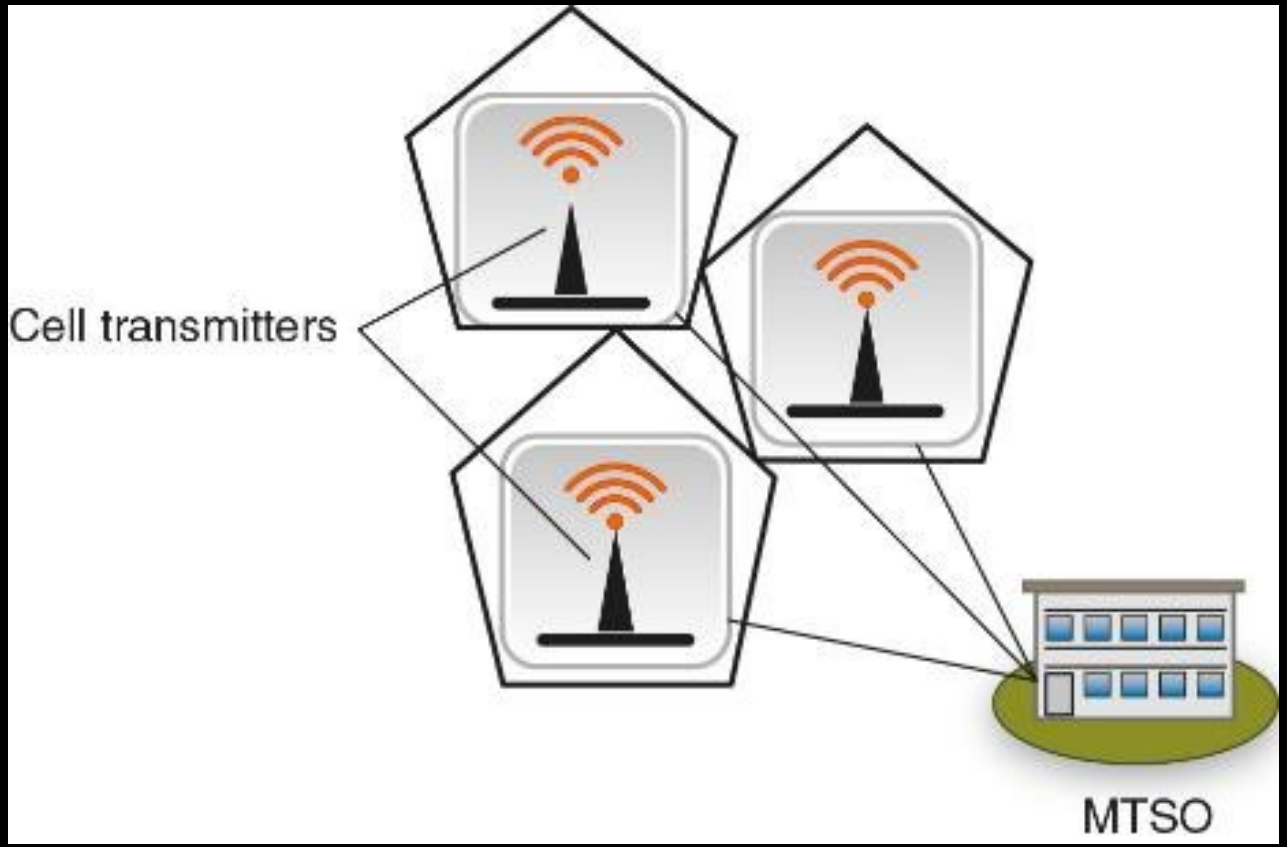
Introduction to Mobile Devices

- Types of Mobile Devices include the following (continued):
- **Portable computers** are devices that closely mirror the functionality of desktop computers
- They are smaller, self-contained devices that can easily be transported from one location to another while running on battery power
- A web-based computer contains a limited version of an OS and a web browser with an integrated media player

Mobile Device Connectivity Methods

- The following are different connectivity methods used to connect mobile devices to networks:
  - **Cellular –** coverage area for a cellular telephony network is divided into cells
    - Transmitters are connected through a mobile telecommunications switching office (MTSO) that controls all of the transmitters in the cellular network
- **Wi-Fi** – a wireless local area network (WLAN) is designed to replace or supplement a wired local area network (LAN)

Cellular Network



Mobile Device Connectivity Methods

- The following are different connectivity methods used to connect mobile devices to networks:
  - **Bluetooth** – uses short-range radio frequency transmissions and provides rapid device pairings
  - **USB connections** – different types and sizes of Universal Serial Bus (USB) connectors on mobile devices can be used for data transfer between devices

Enterprise Deployment Models

Model name	Description	Employee actions	Business actions
Bring your own device (BYOD)	Employees use their own personal mobile devices for business purposes.	Employees have full responsibility for choosing and supporting the device.	This model is popular with smaller companies or those with a temporary staff.
Corporate owned, personally enabled (COPE)	Employees choose from a selection of company approved devices.	Employees are supplied the device chosen and paid for by the company, but they can also use it for personal activities.	Company decides the level of choice and freedom for employees.
Choose your own device (CYOD)	Employees choose from a limited selection of approved devices but pay the upfront cost of the device while the business owns the contract.	Employees are offered a suite of choices that the company has approved for security, reliability, and durability.	Company often provides a stipend to pay monthly fees to wireless carrier
Virtual desktop infrastructure (VDI)	Stores sensitive applications and data on a remote server accessed through a smartphone	Users can customize the display of data as if the data were residing on their own mobile device.	Enterprise can centrally protect and manage apps and data on server instead of distributing to smartphones.
Corporate owned	The device is purchased and owned by the enterprise.	Employees use the phone only for company-related business.	Enterprise is responsible for all aspects of the device.

Enterprise Deployment Models

- The following are benefits of the BYOD, COPE, and CYOD models for the enterprise:
  - Management flexibility
  - Less oversight
  - Cost savings
  - Simplified IT infrastructure
  - Reduced internal service
  - Increased employee performance

Enterprise Deployment Models

- The following are **user** benefits of the BYOD, COPE, and CYOD models:
  - Choice of device
  - Choice of carrier
  - Convenience

Mobile Device Risks

- The increasing reliance of businesses on mobile devices means that employees must have access to sensitive data
  - This has heightened the interest of threat actors toward mobile devices
- There are several security risks associated with using mobile devices, including the following:
  - Mobile device vulnerabilities, connection vulnerabilities, and access untrusted content

Mobile Device Vulnerabilities

- Mobile device vulnerabilities include the following:
  - **Physical security** – mobile devices are frequently lost or stolen
  - **Limited updates** – security patches and updates for mobile OSs are distributed through **firmware over-the-air (OTA) updates**
  - **Location tracking** – mobile devices using geolocation are at increased risk of targeted physical attacks
    - A related risk is GPS tagging
  - **Unauthorized recording** – by infecting a device with malware, a threat actor can spy on an unsuspecting victim and record conversations or videos

Connection Vulnerabilities

Name	Description	Vulnerability
Tethering	A mobile device with an active Internet connection can be used to share that connection with other mobile devices through Bluetooth or Wi-Fi.	An unsecured mobile device may infect other tethered mobile devices or the corporate network.
USB On-the-Go (OTG)	An OTG mobile device with a USB connection can function as either a host (to which other devices may be connected such as a USB flash drive) for **external media access** or as a peripheral (such as a mass storage device) to another host.	Connecting a **malicious flash drive** infected with malware to a mobile device could result in an infection, just as using a device as a peripheral while connected to an infected computer could allow malware to be sent to the device.
Malicious USB cable	A USB cable could be embedded with a Wi-Fi controller that can receive commands from a nearby device to send malicious commands to the connected mobile device.	The device will recognize the cable as a Human Interface Device (similar to a mouse or keyboard), giving the attacker enough permissions to exploit the system.
Hotspots	A hotspot is a location where users can access the Internet with a wireless signal.	Because public hotspots are beyond the control of the organization, attackers can eavesdrop on the data transmissions and view sensitive information.

Accessing Untrusted Content

- Users can circumvent the built-in installation limitation on their smartphone (called **jailbreaking** on Apple iOS or **rooting** on Android devices) to download from an unofficial third-party app store (called **sideloading**)
- Untrusted content can invade mobile devices through SMS, MMS, and RCS text messaging
- Mobile devices can access untrusted content using *QR* codes
  - An attacker can create an advertisement listing a reputable website but include a QR code that contains a malicious URL

Protecting Mobile Devices

- The following configurations should be considered:
  - Use Strong Authentication - verifying the authentic user of a device involves requiring a strong passcode and restricting unauthorized users with a screen lock
  - Options include using:
    - A passcode
    - A PIN
    - A fingerprint or facial recognition
    - A pattern connecting dots to unlock the device

Protecting Mobile Devices

- The following configurations should be considered (continued):
  - **Segmentation** separates business data from personal data on mobile devices
  - Users can apply **containerization**, or separating storage into business and personal “containers”
  - It helps companies avoid data ownership privacy issues and legal concerns regarding a user’s personal data stored on the device

Protecting Mobile Devices

- Enable Loss or Theft Services
  - Several security features can be used to locate a lost or stolen device
  - If a lost or stolen device cannot be located, it may be necessary to perform a remote wipe

Protecting Mobile Devices

Security feature	Explanation
Alarm	The device can generate an alarm even if it is on mute.
Last known location	If the battery is charged to less than a specific percentage, the device's last known location can be indicated on an online map.
Locate	The current location of the device can be pinpointed on a map through the device's GPS.
Remote lockout	The mobile device can be remotely locked and a custom message sent that is displayed on the login screen.
Thief picture	Thieves who enter an incorrect passcode three times will have their picture taken through the device's on-board camera and emailed to the owner.

Protecting Mobile Devices

- **Mobile Device Management** (**MDM**) tools allow a device to be managed remotely by an organization
- **Mobile Application Management** (**MAM**) covers application management, which comprises the tools and services responsible for distributing and controlling access to apps
- **Mobile Content Management** (**MCM**) supports the creation and editing and modification of digital content by multiple employees
- **Unified Endpoint Management** (**UEM**) provides capabilities for managing and securing mobile devices, applications, and content

Question

- Ozan has received a phone call from his supervisor that a new employee has attempted to download and install an unapproved app that allows her to circumvent the built-in limitations on her Android smartphone. What is this called?

Answer

- Ozan has received a phone call from his supervisor that a new employee has attempted to download and install an unapproved app that allows her to circumvent the built-in limitations on her Android smartphone. What is this called?
- Rooting. Users who circumvent the installed built-in limitations on their smartphone are jailbreaking on Apple iOS devices and rooting on Android devices.

Embedded Systems

- Computing capabilities can be integrated into appliances and other devices
- An **embedded system** is computer hardware and software contained within a larger system designed for a specific function
- Protection of these devices needs to be considered

Types of Devices

- Hardware and Software
  - One of the most common hardware components is the **Raspberry Pi**, which is a low-cost, credit-card-sized computer motherboard
    - A device similar to the Raspberry Pi is the Arduino
  - A **field-programmable gate array (FPGA)** is a hardware “chip” that can be programmed by the user to carry out one or more logical operations
  - A **system on a chip (SoC)** combines all the required electronic circuits of the various computer components on a single chip
    - SoCs often use a **real-time operating system (RTOS)**

Types of Devices

- Industrial Systems
  - **Industrial control systems (ICSs)** collect, monitor, and process real-time data so that machines can directly control devices such as valves, pumps, and motors without human intervention
  - ICSs are managed by **supervisory control and data acquisition (SCADA)** systems
  - SCADA systems help maintain efficiency and provide information on issues to help reduce downtime

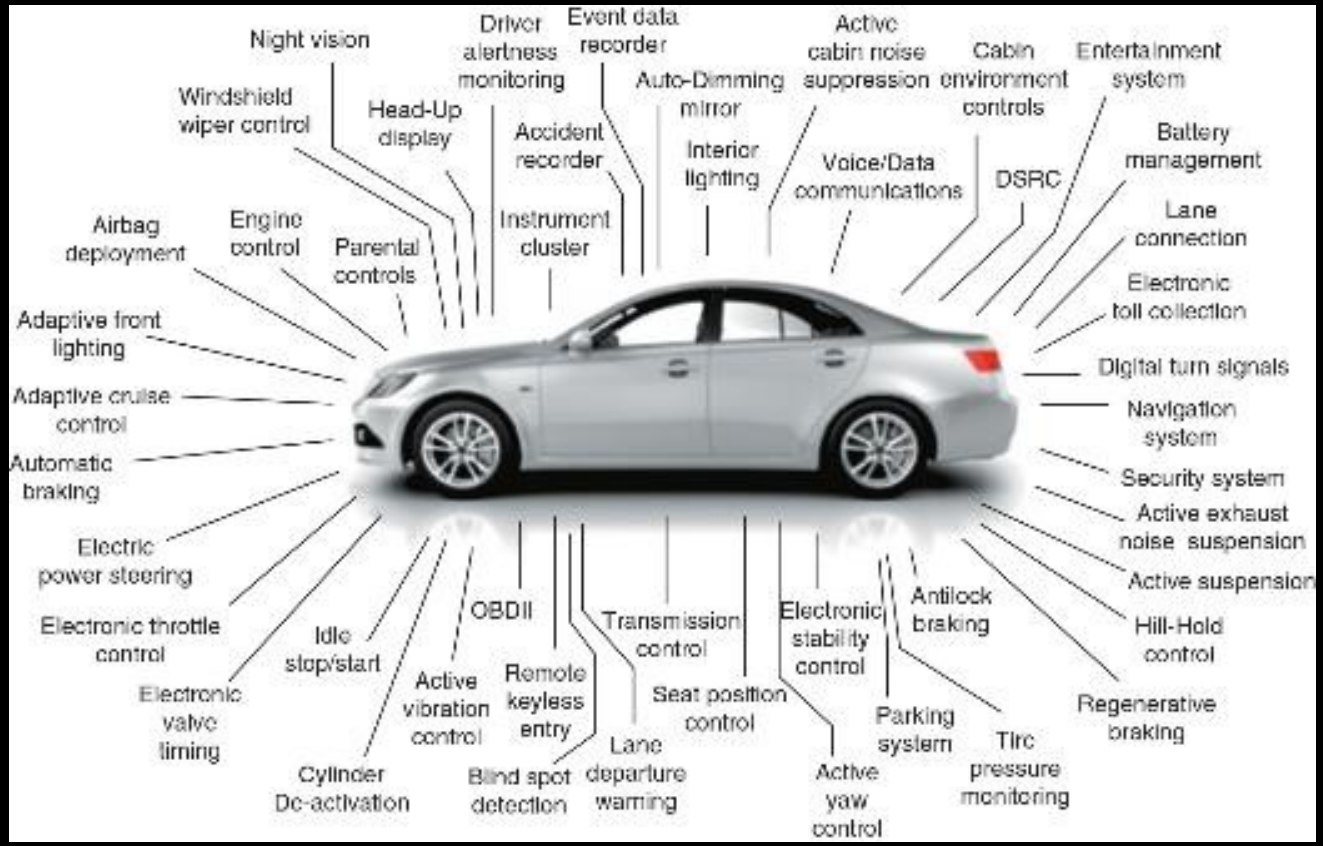
Types of Devices

- Specialized Systems
  - Digital smart meters are used to measure the amount of utilities consumed
    - Smart meters have several advantages over analog meters
  - Other specialized systems include medical systems, aircraft, and vehicles
    - Embedded systems in cars use sonar, radar, and laser emitters to control brakes, steering, and the throttle

Types of Devices

Action	Analog meter	Smart meter
Meter readings	Employee must visit the dwelling each month to read the meter.	Meter readings are transmitted daily, hourly, or even by the minute to the utility company.
Servicing	Annual servicing is required in order to maintain accuracy.	Battery replacement every 20 years.
Tamper protection	Data must be analyzed over long periods to identify anomalies.	Can alert utility in the event of tampering or theft.
Emergency communication	None available	Transmits “last gasp” notification of a problem to utility company.

Embedded Systems in Cars



Types of Devices

- **Internet of Things** (**IoT**) is connecting any device to the Internet for the purpose of sending and receiving data to be acted upon
  - IoT devices include wearable technology as well as every home automation items such as thermostats, coffee makers, tire sensors, slow cookers, keyless entry systems, washing machines, electric toothbrushes, headphones, and light bulbs
- It is estimated that in 2022, the average number of connected devices per household was 22

Types of Devices

- **Internet of Things** (**IoT**) is connecting any device to the Internet for the purpose of sending and receiving data to be acted upon
  - IoT devices include wearable technology as well as every home automation items such as thermostats, coffee makers, tire sensors, slow cookers, keyless entry systems, washing machines, electric toothbrushes, headphones, and light bulbs
- It is estimated that in 2022, the average number of connected devices per household was 22

Security Considerations

- There are significant security concerns surrounding SCADA systems, specialized systems, and IoT devices
  - These devices have a low **resilience** to resist attacks
- Improving security of these systems begins with knowing the security constraints
- There are also specific hardening techniques and technologies for ICS and SCADA systems, some of which are being addressed by new legislation and regulations

Security Considerations

- One security constraint involves adding cryptography to embedded devices
  - Cryptographic algorithms require time and energy, which is in short supply for small, low-power devices
  - This results in a resource versus security constraint

Security Considerations

- The following are some of the steps that can be taken to harden SCADA and ICS system:
  - Clearly define security roles, responsibilities, and authorities for managers, system administrators, and users
  - Identify security requirements
  - Disconnect unnecessary connections to the SCADA network
  - Do not rely on proprietary protocols to protect the network
  - Test to identify and evaluate possible attack scenarios
  - Evaluate and strengthen the security of all connections to the SCADA network

Security Considerations

- Federal and state laws have recently been passed to address protection of embedded devices and IoT
- The Internet of Things (IoT) Cybersecurity Improvement Act of 2020 requires agencies to increase cybersecurity for IoT owned or controlled by the federal government
- California and Oregon passed state laws addressing IoT security that went into effect in 2020
  - The laws require that connected devices be equipped with “reasonable security features”

Security Considerations

- Regulatory bodies have begun mandating protections on IoT devices
- In late 2022, the U.S. Food and Drug Administration (FDA) gained new powers from legislators to set minimum security standards for medical-device manufacturers

Application Security

Attack	Description	Defense
Executable files attack	Trick the vulnerable application into modifying or creating executable files on the system	Prevent the application from creating or modifying executable files for its proper function
System tampering	Use the vulnerable application to modify special sensitive areas of the OS (Microsoft Windows registry keys, system startup files, etc.) and take advantage of those modifications	Do not allow applications to modify special areas of the OS
Process spawning control	Trick the vulnerable application into spawning executable files on the system	Take away the process spawning ability from the application

Application Development Concepts

- General Concepts
  - Developing an application requires completing the following stages:
    - Development, testing, staging, and production
- An **application development lifecycle model** is a conceptual model that describes the different stages involved in creating an application
- The **waterfall model** uses a sequential design process
- The **agile model** takes an incremental approach, which allows for software issues to be incrementally discovered

Application Development Concepts

- **SecDevOps** is the process of integrating secure development best practices and methodologies into application software development and deployment processes using the agile model
  - SecDevOps applies automated courses of action to develop code as quickly and securely as possible that enables the following:
    - Continuous monitoring
    - Continuous validation
    - Continuous integration
    - Continuous delivery
    - Continuous deployment

Secure Coding Techniques

- Several coding techniques should be used to create secure applications and limit data exposure or disclosing sensitive data to attackers
- These techniques include:
  - Determining how encryption will be implemented
  - Ensuring that memory management is handled correctly so as not to introduce memory vulnerabilities

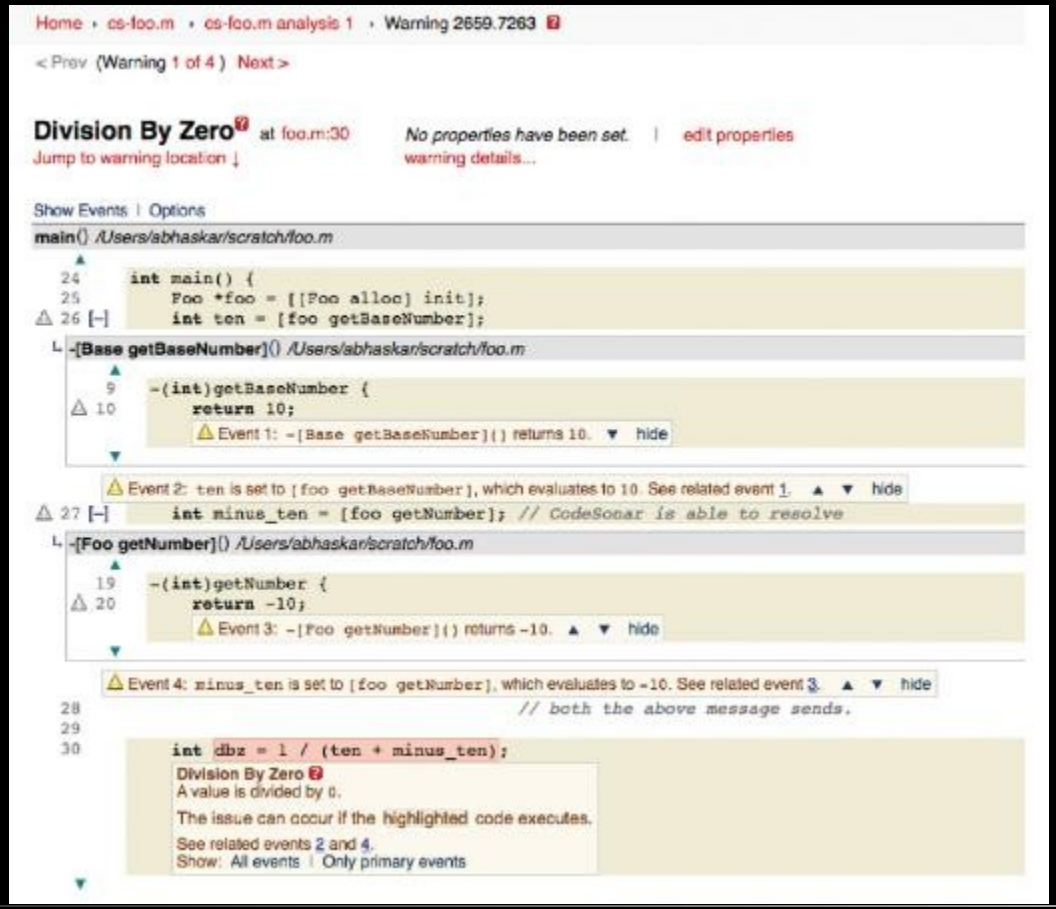
Code Testing

- Testing is one of the most important steps in SecDevOps
- Testing should be performed during the implementation and verification phases of a software development process
- Testing involves static code analysis and dynamic code analysis
- Static Code Analysis
  - **Static code analysis** are tests ran before the source code is even compiled and may be accompanied by manual peer reviews

Code Testing

- Dynamic Code Analysis
  - Security testing performed after the source code is compiled is called **dynamic code analysis** or runtime verification
  - **Fuzzing** is used by dynamic code analysis tools and provides random input to a program in an attempt to trigger exceptions
  - Exceptions could include memory corruption, program crashes, or security breaches

Automated Static Code Analysis



Question

- What is anotherr name for runtime verification?

Answer

- What is anotherr name for runtime verification?
- Dynamic code analysis; Security testing performed after the source code is compiled is a process called dynamic code analysis or runtime verification when all components are integrated and running.