Threats and Vulnerabilities Associated with Specialized Technology

Chapter 5

Episode 5.01

Mobile and IoT

Objective 5.1 Explain the threats and vulnerabilities associated with specialized technology.

- Mobile
- Internet of Things (IoT)

Mobile

- Access points
  - Any place where a device connects via Wi-Fi, then into the network infrastructure
  - Common place for vulnerabilities
- VPNs
  - Virtual private network
  - Establish secure connection using insecure access point
- Network vulnerabilities
  - Mobile device has to connect to IT infrastructure
    - Wi-Fi or cellular
    - Older cellular technologies were very insecure
    - Newer technologies are more secure and use encryption

Mobile

- Device vulnerabilities
  - Securing mobile devices is challenging
  - Provisioned for multi-use
  - Can’t secure one device for many different uses
- Operating system vulnerabilities
  - Operating systems update frequently
    - Competition between OS manufacturers
    - Patch bugs and security vulnerabilities

Mobile

- App vulnerabilities
  - Improper platform usage
  - Insecure data storage
  - Insecure authentication
  - Insecure authorization
  - Code quality vulnerabilities

Internet of Things (IoT)

- Smaller devices connecting to the Internet and doing things autonomously
  - Increased risk of compromise
- Botnet
  - Collection of compromised devices used to launch a DDoS attack
- Mirai botnet
  - Malware that compromised a lot of insecure IoT devices
  - Successful DDoS attack

Internet of Things (IoT)

- IoT devices are ubiquitous
- Users often not concerned about security
- Many devices are not hardened
- Default credentials are easy to find

Episode 5.02

Embedded and Firmware Systems (RTOS, SoC, and FPGA)

Objective 5.1 Explain the threats and vulnerabilities associated with specialized technology.

- Embedded
- Real-time operating system (RTOS)
- System-on-Chip (SoC)
- Field programmable gate array (FPGA)

Embedded

- Special-purpose software
- Low-power processor
- Often no external storage
- Software can be burned into the firmware
- Could just be hardware only
- Limited ability to monitor or patch

Real-time Operating System (RTOS)

- Devices that require low-latency input processing
  - Vehicles
  - Manufacturing
  - Aviation
  - Medical
- Vulnerabilities allow threats to underlying performance guarantees

System on a Chip (SoC)

- Software and hardware integrated on a single chip
- Used in special-purpose applications
- SoC is efficient and cost effective
- Vulnerabilities can affect the entire SoC environment (hardware and software)

Field Programmable Gate Array (FPGA)

- Combination of SoC and embedded system
- Programmable chip with the ability to be modified and reprogrammed in the field
- Must use special device to overwrite the firmware
  - Upgradable
- Cost effective
- Simplicity sometimes leads to vulnerabilities

Episode 5.03

Access and Vehicles Risk

Objective 5.1 Explain the threats and vulnerabilities associated with specialized technology.

- Physical access control
- Vehicles and drones
  - CAN bus

Physical Access Control

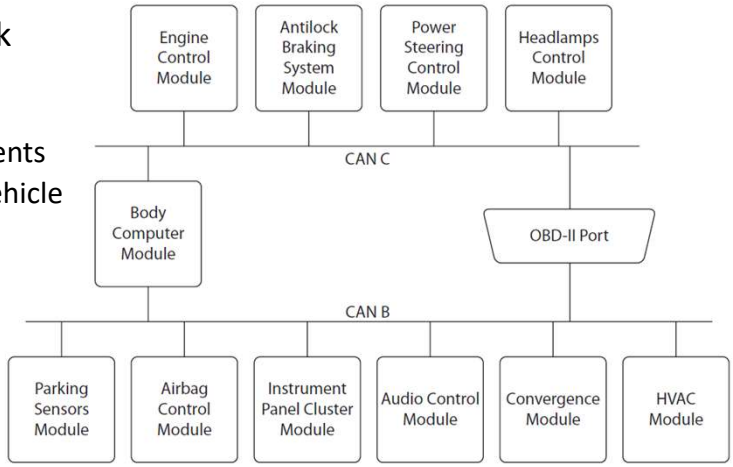
- Example: RFID
  - Radiofrequency identification
  - Chip that uniquely communicates with receiver
- Physical readers make reverse engineering and spoofing possible
- Vulnerabilities can allow attackers to bypass access control
- Replay and cloning are popular attack methods

Vehicles

- Vehicles of all types are increasingly connected
- Internet connectivity
  - Access to many subsystems
  - Control of some subsystems
  - Also opens up vulnerabilities

Typical CAN Bus Configuration

- Controller Area Network (CAN bus)
  - Defines communication among vehicle components
  - CAN exploits (to alter vehicle operation) have been demonstrated



Source: Chapman, B., & Maymí, F. (2020). *CompTIA CySA+™ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)*, 134.

Drones

- Can be malicious
  - Controlled by an attacker
- Can be innocent
  - Drone operators may have their drones hijacked and used for malicious purposes
- Many options for attacks

Episode 5.04

Automation and Control Risk

Objective 5.1 Explain the threats and vulnerabilities associated with specialized technology.

- Building automation systems
- Workflow and process automation systems
- Industrial control system
- Supervisory control and data acquisition (SCADA)

- Modbus

Building Automation Systems

- Network of connected cyber-physical devices
  - Combination of computing device that has impact on physical world
  - Examples:
    - Robots
    - Lighting
    - Environmental control
    - Physical access
    - Smoke detection
    - Fire suppression
- Vulnerabilities can impact a building's usability, inhabitability, and safety

Workflow and Process Automation Systems

- Systems that direct and/or control workflow
  - Project management
  - Document management
  - Software Configuration Management (SCM)
- Value is in autonomy
  - Vulnerabilities can include malicious workflow alterations
- Important to externally audit desired workflow

Industrial Control System (ICS)

- Cyber-physical systems
  - Software to control physical behavior
- Common in manufacturing and warehousing/distribution
- Other applications include elevators and HVAC systems
- Remote Terminal Units (RTU) or Programmable Logic Controllers (PLC)
  - Connect physical world to computers
- PLCs commonly use firmware
  - Difficult to monitor or upgrade

Supervisory Control and Data Acquisition (SCADA)

- Special class of ICS
- Controls cyber-physical systems
- SCADA vulnerabilities
  - Communications with remote facilities
  - Autonomous operation of remote facilities
  - SCADA is not modular
- Modbus
  - SCADA (PLC) communication standard
  - Security not part of its design