CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-5-security_implications_of_embedded_systems
Title: Security Implications of Embedded Systems
Subtitle: CompTIA Security+ (SY0-501)

3.5 Security Implications of Embedded Systems

- 3.5 Explain the security implications of embedded systems.
    - SCADA/ICS
        - Highly sought out targets
        - Perform critical tasks within essential services
        - Can present multiple attack vectors
        - Many interconnection to massively complex systems
        - These systems can have a very long life cycle
        - Often lack security
        - Considerations:
            - Interuption of vital services
            - Process Redirection
            - Manipulation of operational data
            - Nation State/APT vulnerable
            - Hard-coded default passwords
            - Susceptible to Zero Day threats
    - Smart devices/IoT
        - Wearable technology
        - Home automation
        - IoT
            - Insecure Web Interfaces
            - Insufficient Authentication/Authorization
            - Insecure Network Services
            - Lack of Transport Encryption/Integrity Verification
            - Privacy Concerns
            - Insecure Software/Firmware
            - Insufficient Security Configurability
            - Insecure Software/Firmware
            - Poor Physical Security
    - HVAC
        - Server rooms need environmental controls
        - Copper thieves see HVAC systems as easy money
        - Implement security controls like alarms, cameras and high-intensity strobe lights
        - Log all vistors arriving and leaving the building
        - If technicians visit, confirm internal contact and ensure that an emply escorts the technician, never leaving them completely untattended
        - Back in 2014 Qualys said there were more than 55,000K HVAC systems connected to the Internet
        - Audit and log all remote access capabilities of the HVAC system and document the findings
        - Target exploit was believed to be stolen credentials from the company providing HVAC services
    - SoC
    - RTOS
        - General purpose operating systems utilize a scheduler to give the appearance of full multitasking by rapidly switching between applications
        - RTOS try to use scheduling predictability to satisfy real-time requirements
    - Printers/MFDs
        - midrange printers can contain HDDs, RAM and an OS
        - Printers are vary propriatary so each model can present its's own set of vulnerabilities
    - Camera systems
        - IP based cameras are very vulnerable
    - Special purpose
        - Medical devices
        - Vehicles
        - Aircraft/UAV