



IoT and Embedded Device Security Course: Firmware, Protocols and Secure Lifecycle



IoT and Embedded Device Security Course: Firmware, Protocols and Secure Lifecycle

Introduction:

IoT and embedded device security, covering firmware, protocols and secure lifecycle, is a 5-day course for device security, product security, firmware engineering and solution architecture teams, ending with a Connected Device Security Plan. Smart city sensors, utility meters and connected medical devices often ship with default credentials, exposed debug ports, unsigned updates and unauthenticated messaging, which leaves whole fleets open to takeover. Nominees already design, build or assess connected products, and the course is taught as a hands-on lab on development boards, captured firmware images and test brokers. CoreConcept Training Center delivers this IoT and embedded device security course.

Course Objectives:

- Build a device threat model that maps attacker entry points across hardware interfaces, firmware, radio links and cloud back ends
- Specify a hardware root of trust and secure boot chain that verifies every firmware stage before execution
- Extract and analyse firmware images to locate hardcoded secrets, outdated components and unsafe default settings
- Harden MQTT, CoAP and BLE communication with mutual authentication, topic access control and protected pairing
- Design device identity provisioning with X.509 certificates and a signed, rollback-protected over-the-air update process
- Produce a Connected Device Security Plan with fleet telemetry rules, vulnerability disclosure and end-of-life decommissioning

Target Audience:

- Device and product security functions responsible for the security architecture of connected products
 - Firmware and hardware engineering functions that build sensors, gateways, meters and medical device controllers
 - Security testing functions that assess connected devices before procurement or release
 - Solution architecture functions that integrate device fleets with brokers, cloud services and update servers
 - Smart city, utility and healthcare technology functions that operate large fleets of field devices
-

Course Outline:

Day 1: Connected Device Attack Surface and Threat Modelling

- OWASP IoT Top 10 Weaknesses Mapped to Field Devices
- STRIDE Threat Modelling of Sensor, Gateway and Cloud Paths
- Attack Tree Construction for Smart Meter Takeover Scenarios
- Device Data Flow Diagram With Trust Boundaries Marked
- Current-State Security Review of a Deployed Device Fleet

Day 2: Device Security Baselines, Root of Trust and Secure Boot

- Device Cybersecurity Capability Baseline for Identification and Update
- IEC 62443-4-2 Component Requirements for Embedded Devices
- OWASP ISVS Verification Levels Applied to Product Requirements
- Hardware Root of Trust Using Secure Elements and TPMs
- Secure Boot Chain With Signed Bootloader Stages and Fuses

Day 3: Firmware Extraction, Binary Analysis and Hardware Interfaces

- OWASP FSTM Stages for Firmware Acquisition and Analysis
- UART, JTAG and SWD Debug Port Discovery and Lockdown
- Binwalk Filesystem Extraction and Hardcoded Credential Search
- SBOM Generation and Outdated Component Vulnerability Matching
- IoTGoat Vulnerable Firmware Emulation and Exploitation Exercise

Day 4: Protocol Weaknesses, Device Identity and Signed OTA Updates

- MQTT Broker Authentication, Topic ACLs and Keepalive Abuse
- CoAP Over DTLS With Pre-Shared Keys and Certificates
- BLE Pairing Modes, Passive Sniffing and Replay Attacks
- X.509 Device Certificate Provisioning and Rotation at Manufacture
- Signed OTA Update Packages With Rollback and Downgrade Protection

Day 5: Lab on a Case Fleet and Connected Device Security Plan

- Case Fleet Briefing for Smart Streetlights, Meters and Infusion Pumps
 - Threat Model and Secure Boot Gap Findings for Case Devices
 - Fleet Telemetry Rules for Detecting Cloned or Compromised Devices
 - Coordinated Vulnerability Disclosure and End-of-Life Decommissioning Policy
 - Connected Device Security Plan Completion and Peer Review
-

Skills You Will Gain:

- Device Threat Modelling
- Secure Boot Design
- Firmware Binary Analysis
- Debug Interface Lockdown
- IoT Protocol Hardening
- Device Certificate Management
- OTA Update Assurance
- Fleet Anomaly Detection

Why Attend This Course:

- Deliver a Connected Device Security Plan to the product security lead and the fleet operations manager for one device family
- Decide whether a device can be released or procured by checking its boot chain, debug ports and update signing
- Avoid fleet-wide takeover, cloned devices and bricked units caused by default credentials and unsigned updates
- Brief engineering and procurement colleagues with a firmware review checklist and a protocol hardening baseline

Conclusion:

Back at work, the participant hands the product security lead and the fleet operations manager a Connected Device Security Plan for one device family in smart city, utility or healthcare service. They use it to decide which release or procurement gates a device must pass, which certificates and update signing keys need stronger protection, and which telemetry rules flag a cloned or compromised unit. After the first release or update campaign under the plan, the unit should review closed firmware findings, devices still lacking an individual identity and alerts raised against confirmed incidents.

Frequently Asked Questions FAQ:

What should participants know before an IoT and embedded device security course?

Participants should already work on connected products or their security, read network captures and use a Linux command line. Basic knowledge of TLS and public key certificates helps. No firmware reverse engineering experience is assumed, and a description of a device family they support makes the lab work more relevant.

How does IoT and embedded device security differ from an IoT business strategy or embedded programming course?

It concentrates on attacking and protecting the device itself: boot chain, firmware, debug ports, radio and messaging protocols, identity and updates. Business IoT courses plan use cases and pilots, and embedded programming courses teach writing drivers and real-time tasks rather than securing them.

Why do signed over-the-air updates matter in IoT and embedded device security?

Field devices stay in service for many years and new weaknesses appear after release. Signed, rollback-protected updates let the operator fix them remotely while stopping attackers from installing modified or older vulnerable firmware, which could otherwise lead to the takeover of a whole fleet.

What does a participant take back from the IoT and embedded device security course?

Each participant takes back a Connected Device Security Plan covering a threat model, root of trust and secure boot design, firmware review findings, protocol hardening settings, certificate provisioning, an update signing process and fleet telemetry rules, ready to adapt to a device family in their organisation.
