Faysal Aziz

IoT Security Lab

Practical security for connected systems, from BLE to firmware updates.

FA-0267 · 2-day

Cybersecurity

Introduction

Connected systems are no longer simple devices with wireless features attached. They are full product ecosystems made up of firmware, mobile apps, APIs, cloud services, wireless communication, update mechanisms, and hardware trust anchors. A weakness in any one layer can affect the safety, reliability, and integrity of the whole system.

This 2-day hands-on workshop is designed for engineering leads, embedded developers, firmware/software engineers, and full-stack architects working on connected products. The instructor has **over 30 years of industry experience** and will use **real industry-demanded content**, not an academic-only approach.

Learning outcomes

By the end of the workshop, participants will be able to:

- Understand key security risks in connected and IoT systems.
- Analyse BLE security fundamentals, pairing models, and attack surfaces.
- Perform controlled wireless and BLE packet analysis in a lab environment.
- Recognise mobile application reverse engineering concepts relevant to IoT products.
- Identify common API, communication, and session security weaknesses.
- Understand secure boot, Root of Trust, firmware signing, and FOTA security.
- Apply threat modelling to connected-system design.
- Identify, mitigate, and verify security gaps through practical lab exercises.

Prerequisites

Participants should have:

- Basic Linux or Unix command-line familiarity.
- Basic networking knowledge.
- Programming or scripting experience.
- General understanding of embedded systems, firmware, APIs, mobile apps, or cloud-connected products.
- A laptop with administrator privileges for lab setup.

Recommended Pre-Work and Setup

- Laptop prepared with a Linux environment, virtual machine, or WSL where applicable.
- Ability to install workshop tools before the training.
- Basic review of BLE concepts, HTTP APIs, TLS, and public-key cryptography.
- All hands-on activities will be performed only in controlled and authorised lab environments.

Training outline

1. Connected Systems Security Overview

1. IoT security landscape
2. Device, firmware, mobile, API, cloud, and wireless trust boundaries
3. Common security weaknesses in connected products
4. Secure engineering responsibilities across the product lifecycle

2. BLE Protocol and Security Fundamentals

1. BLE architecture, roles, advertising, scanning, and connections
2. GAP, GATT, services, characteristics, and descriptors
3. Pairing, bonding, encryption, and key management
4. BLE legacy pairing and LE Secure Connections
5. Pairing models: Just Works, Passkey, Numeric Comparison, and Out-of-Band

6. BLE privacy, device identity, and security levels

3. BLE Attack Surface and Packet Analysis

1. Advertising data exposure
2. Service and characteristic enumeration
3. Weak permissions and unauthorised read/write risks
4. Pairing weaknesses and insecure device states
5. Controlled BLE traffic capture and packet inspection
6. Lab analysis of BLE communication and security gaps

4. Wireless Interception and Controlled Lab Analysis

1. Wireless security testing principles
2. Authorised lab scope and safe testing boundaries
3. Radio-layer versus application-layer analysis
4. Wireless metadata and communication pattern review
5. Verification of wireless security controls

5. Mobile Application Reverse Engineering Concepts

1. Mobile app role in connected-system ecosystems
2. Static and dynamic analysis concepts
3. App permissions, configuration, storage, and endpoints
4. Hardcoded secrets and insecure local storage
5. BLE workflow discovery from mobile app logic
6. Transport security and certificate validation review

6. API, Communication, and Session Security

1. IoT API architecture patterns
2. User, device, and service authentication
3. Authorisation weaknesses and access-control failures
4. Session handling, token storage, and token lifecycle
5. TLS, request integrity, replay protection, and secure communication
6. Common API vulnerabilities affecting connected products

7. Secure Boot, Root of Trust, and Firmware Security

1. Secure boot principles and chain of trust
2. Hardware and software Root of Trust
3. Bootloader security responsibilities
4. Firmware integrity and authenticity validation
5. Firmware signing and key protection
6. Anti-rollback and downgrade protection
7. Secure FOTA design, delivery, verification, and recovery

8. Threat Modelling and Secure Engineering Practices

1. Asset, trust boundary, and data flow identification
2. Attack surface mapping for connected systems
3. Threat modelling across provisioning, operation, update, and decommissioning
4. Translating threats into security requirements
5. Secure design review and security acceptance criteria
6. Security testing and regression verification

9. Hands-On Practical Labs

1. BLE discovery and enumeration
2. BLE advertising and GATT analysis
3. BLE pairing and permission review
4. Controlled packet analysis
5. Mobile app structure and endpoint review
6. API authentication, authorisation, and session testing
7. Firmware update security review
8. Secure boot and firmware signing design review
9. Threat modelling exercise
10. Mitigation and verification workshop

Disclaimer

This outline is provided as a professional training guideline for planning purposes. The trainer may amend, restructure, substitute, or adjust the content, lab sequence, tools, depth of coverage, or delivery approach as deemed appropriate based on participant readiness, client priorities, available equipment, technical feasibility, and training objectives, without prior notice.

© 2026 Faysal Aziz · Kuala Lumpur

https://faysalaziz.com/courses/iot-security-lab/