Training Course on Embedded Cybersecurity and Secure Boot

Professional Development Training Course Outline

Category	Engineering	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Introduction

This intensive training course provides a crucial deep dive into Embedded Cybersecurity and Secure Boot, equipping participants with the specialized knowledge and practical skills required to design and implement resilient, trustworthy embedded systems. Training Course on Embedded Cybersecurity and Secure Boot focuses on identifying and mitigating vulnerabilities across the entire embedded system lifecycle, from hardware design to firmware deployment and ongoing operation. Attendees will gain hands-on expertise in critical concepts such as root of trust, secure boot chains, trusted execution environments (TEE), cryptographic implementations, and secure firmware updates (OTA). This course is meticulously crafted to empower engineers to protect their embedded products against evolving cyber threats, ensuring data integrity, system authenticity, and operational reliability in an increasingly connected world.

The program emphasizes a proactive and defense-in-depth approach, exploring trending topics like supply chain security, hardware security modules (HSM), side-channel attack countermeasures, and compliance with industry security standards (e.g., NIST, IEC 62443). Participants will learn to conduct threat modeling, risk assessment, and implement secure coding practices specific to resource-constrained embedded environments. By the end of this course, attendees will possess the expertise to architect and implement comprehensive cybersecurity solutions for embedded devices, ensuring protection against tampering, unauthorized access, and intellectual property theft. This training is indispensable for professionals seeking to safeguard critical infrastructure, consumer electronics, and IoT devices from sophisticated cyberattacks.

Programme Curriculum

Training Course on Embedded Cybersecurity and Secure Boot

Introduction

This intensive training course provides a crucial deep dive into Embedded Cybersecurity and Secure Boot, equipping participants with the specialized knowledge and practical skills required to design and implement resilient, trustworthy embedded systems. Training Course on Embedded Cybersecurity and Secure Boot focuses on identifying and mitigating vulnerabilities across the entire embedded system lifecycle, from hardware design to firmware deployment and ongoing operation. Attendees will gain hands-on expertise in critical concepts such as root of trust, secure boot chains, trusted execution environments (TEE), cryptographic implementations, and secure firmware updates (OTA). This course is meticulously crafted to empower engineers to protect their embedded products against evolving cyber threats, ensuring data integrity, system authenticity, and operational reliability in an increasingly connected world.

The program emphasizes a proactive and defense-in-depth approach, exploring trending topics like supply chain security, hardware security modules (HSM), side-channel attack countermeasures, and compliance with industry security standards (e.g., NIST, IEC 62443). Participants will learn to conduct threat modeling, risk assessment, and implement secure coding practices specific to resource-constrained embedded environments. By the end of this course, attendees will possess the expertise to architect and implement comprehensive cybersecurity solutions for embedded devices, ensuring protection against tampering, unauthorized access, and intellectual property theft. This training is indispensable for professionals seeking to safeguard critical infrastructure, consumer electronics, and IoT devices from sophisticated cyberattacks.

Course duration

10 Days

Course Objectives

1. Understand the fundamental principles of embedded cybersecurity and attack vectors.
2. Design and implement a robust secure boot process for embedded devices.
3. Establish a hardware-rooted "Root of Trust" for system integrity.
4. Utilize cryptographic primitives (AES, RSA, ECC) effectively in embedded applications.
5. Implement secure firmware update (OTA) mechanisms with integrity checks and authentication.
6. Understand and apply Trusted Execution Environments (TEE) for sensitive operations.
7. Conduct threat modeling and risk assessment specific to embedded systems.
8. Implement secure communication protocols (TLS/DTLS) for IoT connectivity.
9. Mitigate common software vulnerabilities (buffer overflows, injection attacks) in embedded code.
10. Explore hardware security modules (HSM) and secure elements for key management.
11. Implement countermeasures against physical and side-channel attacks.
12. Understand supply chain security implications for embedded components.
13. Apply secure coding guidelines (e.g., MISRA C Security) for robust development.

Organizational Benefits

1. Enhanced security posture of embedded products, reducing vulnerability to cyberattacks.
2. Mitigation of financial and reputational damage from security breaches.
3. Compliance with evolving industry security standards and regulations.
4. Protection of intellectual property embedded within devices.
5. Reduced risk of product recalls due to security flaws.

6. Faster time-to-market for secure products by integrating security early in design.
7. Increased customer trust in their connected devices and solutions.
8. Improved ability to respond to and remediate emerging security threats.
9. Development of highly robust and resilient embedded systems.
10. Competitive advantage in markets demanding secure and trustworthy devices.

Target Participants

- Embedded Software Engineers
- Firmware Developers
- System Architects
- IoT Device Developers
- Hardware Engineers involved in security design
- Security Analysts focused on embedded systems
- Technical Leads managing embedded product development

Course Outline

Module 1: Introduction to Embedded Cybersecurity

- **Understanding Embedded Systems Security Landscape:** Unique challenges, common attack vectors (physical, software, network).
- **The CIA Triad in Embedded Systems:** Confidentiality, Integrity, Availability.
- **Embedded vs. IT Security:** Key differences and shared principles.
- **Attacker Mindset:** Understanding motivations and techniques.
- **Case Study:** Analyzing a real-world embedded system hack (e.g., vehicle ECU compromise).

Module 2: Threat Modeling and Risk Assessment

- **STRIDE Threat Model:** Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege.
- **Attack Trees and Attack Graphs:** Visualizing attack paths.
- **Risk Assessment Methodologies:** Likelihood and impact analysis.
- **Security Requirements Engineering:** Translating threats into design requirements.
- **Case Study:** Performing a threat model for a smart door lock system.

Module 3: Fundamentals of Cryptography for Embedded Systems

- **Symmetric-Key Cryptography:** AES, DES, block ciphers, stream ciphers.
- **Asymmetric-Key Cryptography:** RSA, ECC, public/private key pairs.
- **Hash Functions and Message Authentication Codes (MACs):** SHA-256, HMAC.
- **Digital Signatures:** Authentication and integrity of code/data.
- **Case Study:** Implementing AES encryption/decryption on a microcontroller for sensitive data.

Module 4: Secure Boot Chain (Root of Trust)

- **Concept of Root of Trust (RoT):** Hardware-anchored security.
- **Chain of Trust:** Boot ROM, primary bootloader, secondary bootloader, OS kernel.
- **Authenticated Boot:** Verifying cryptographic signatures at each stage.
- **Measuring Boot:** Establishing a dynamic root of trust (DRTM).

- **Case Study:** Configuring a microcontroller's hardware security features to establish a secure boot.

Module 5: Trusted Execution Environments (TEE)

- **Introduction to TEEs:** Isolation, secure world, normal world.
- **ARM TrustZone:** Architecture and use cases.
- **Secure Enclaves:** Intel SGX (overview) and other hardware-based TEEs.
- **Applications of TEEs:** Secure key storage, DRM, secure processing.
- **Case Study:** Designing a secure firmware update process leveraging a TrustZone-enabled microcontroller.

Module 6: Secure Firmware Updates (OTA)

- **Challenges of OTA Updates:** Integrity, authenticity, rollback protection.
- **A/B Partitioning:** Dual-bank updates for resilience.
- **Cryptographic Signatures for Firmware:** Ensuring authenticity of updates.
- **Rollback Prevention:** Preventing downgrade attacks.
- **Case Study:** Implementing a secure A/B update mechanism on an IoT device.

Module 7: Secure Communication Protocols

- **TLS/SSL for Embedded Devices:** Handshake, certificates, mutual authentication.
- **DTLS for UDP-based Communication:** Adapting TLS for unreliable networks.
- **MQTT Security:** TLS over MQTT, client certificates, authentication.
- **Protocol Hardening:** Minimizing attack surface, secure configuration.
- **Case Study:** Establishing a secure MQTT connection between an IoT device and a cloud broker using TLS.

Module 8: Hardware Security Modules (HSM) and Secure Elements

- **Role of HSMs/Secure Elements:** Secure key storage, cryptographic acceleration.
- **Types of Secure Elements:** TPM, smart cards, dedicated crypto chips.
- **Key Provisioning and Lifecycle Management:** Secure generation, storage, and deletion.
- **Secure Manufacturing and Provisioning:** Ensuring supply chain integrity.
- **Case Study:** Integrating a dedicated crypto chip (e.g., ATECC608A) for secure key storage and cryptographic operations.

Module 9: Physical and Side-Channel Attacks

- **Physical Attacks:** Tampering, reverse engineering, fault injection.
- **Side-Channel Attacks:** Power analysis (SPA/DPA), electromagnetic analysis (EMA), timing attacks.
- **Countermeasures:** Shielding, obfuscation, masking, random delays.
- **Tamper Detection and Response:** Active and passive tamper detection circuits.
- **Case Study:** Analyzing a simple power analysis attack against an AES implementation and discussing countermeasures.

Module 10: Secure Coding Practices for Embedded Systems

- **Common Software Vulnerabilities:** Buffer overflows, integer overflows, format string bugs.
- **Input Validation and Sanitization:** Preventing injection attacks.
- **Secure Memory Handling:** Avoiding use-after-free, double-free issues.
- **MISRA C/C++ Security Guidelines:** Adhering to secure coding standards.

- **Case Study:** Identifying and fixing common security vulnerabilities in sample embedded C code.

Module 11: Supply Chain Security for Embedded Devices

- **Components Sourcing:** Authenticity and integrity of hardware components.
- **Firmware Origin and Integrity:** Ensuring trusted firmware.
- **Manufacturing Process Security:** Preventing tampering during production.
- **Software Bill of Materials (SBOM):** Tracking open-source and third-party components.
- **Case Study:** Discussing the potential security risks in a typical IoT device supply chain.

Module 12: Embedded Device Hardening

- **Minimizing Attack Surface:** Disabling unused peripherals, services, and ports.
- **Least Privilege Principle:** Running processes with minimum necessary permissions.
- **Firewall and Network Segmentation:** Protecting devices from external threats.
- **Security Configuration Management:** Ensuring secure defaults.
- **Case Study:** Hardening an embedded Linux system for a publicly accessible kiosk.

Module 13: Monitoring and Incident Response for Embedded Devices

- **Security Logging and Auditing:** Capturing relevant security events.
- **Intrusion Detection Systems (IDS) at the Edge:** Detecting anomalous behavior.
- **Remote Attestation:** Verifying the integrity of a remote device.
- **Incident Response Planning:** Procedures for handling security breaches.
- **Case Study:** Setting up basic security logging and anomaly detection on an embedded gateway.

Module 14: Compliance and Industry Standards

- **NIST Cybersecurity Framework for IoT:** Core functions, categories, subcategories.
- **IEC 62443 (Industrial Control Systems Security):** Standards for OT environments.
- **GDPR and Data Privacy:** Implications for IoT devices handling personal data.
- **Product Security Certification:** Common certifications and their requirements.
- **Case Study:** Mapping a fictional embedded product's security features to relevant NIST IoT guidelines.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com