Hardware Hacking and Embedded Device Security Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The proliferation of Internet of Things (IoT) and connected embedded devices across industries from smart homes and wearables to industrial control systems (ICS) and automotive electronics has drastically expanded the global attack surface. These devices, often deployed with insufficient security measures, represent critical vulnerabilities, making Hardware Hacking and Embedded Device Security a paramount concern. Hardware Hacking and Embedded Device Security Training Course is designed to equip security professionals and engineers with the hands-on reverse engineering and penetration testing skills necessary to identify and mitigate physical attacks, logic flaws, and firmware vulnerabilities at the root hardware level. Attendees will move beyond conventional network and application-layer defenses, mastering the use of specialized tools and techniques to dissect, analyze, and exploit real-world electronics, thereby cultivating a proactive defense mindset essential for securing the next generation of digital infrastructure.

This course immerses participants in the practical methodology of an attacker, focusing on the complete lifecycle of a hardware penetration test. Key learning areas include component identification, probing communication interfaces like UART, SPI, I2C, and JTAG, memory dumping, firmware extraction, and binary reverse engineering. By simulating sophisticated physical security bypasses and non-invasive attacks such as side-channel and fault injection techniques students gain invaluable experience in uncovering deep-seated security flaws that often bypass standard software testing. Graduates will possess the expertise to design, audit, and fortify secure embedded systems, safeguarding against emerging cyber-physical threats and ensuring product security throughout the supply chain.

Programme Curriculum

Hardware Hacking and Embedded Device Security Training Course

Introduction

The proliferation of Internet of Things (IoT) and connected embedded devices across industries from smart homes and wearables to industrial control systems (ICS) and automotive electronics has drastically expanded the global attack surface. These devices, often deployed with insufficient security measures, represent critical vulnerabilities, making Hardware Hacking and Embedded Device Security a paramount concern. Hardware Hacking and Embedded Device Security Training Course is designed to equip security professionals and engineers with the hands-on reverse engineering and penetration testing skills necessary to identify and mitigate physical attacks, logic flaws, and firmware vulnerabilities at the root hardware level. Attendees will move beyond conventional network and application-layer defenses, mastering the use of specialized tools and techniques to dissect, analyze, and exploit real-world electronics, thereby cultivating a proactive defense mindset essential for securing the next generation of digital infrastructure.

This course immerses participants in the practical methodology of an attacker, focusing on the complete lifecycle of a hardware penetration test. Key learning areas include component identification, probing communication interfaces like UART, SPI, I2C, and JTAG, memory dumping, firmware extraction, and binary reverse engineering. By simulating sophisticated physical security bypasses and non-invasive attacks such as side-channel and fault injection techniques students gain invaluable experience in uncovering deep-seated security flaws that often bypass standard software testing. Graduates will possess the expertise to design, audit, and fortify secure embedded systems, safeguarding against emerging cyber-physical threats and ensuring product security throughout the supply chain.

Course Duration

5 days

Course Objectives with Strong Trending Keywords

1. Master the Hardware Hacking Methodology and IoT Penetration Testing framework from reconnaissance to exploitation.
2. Proficiently use essential Hardware Hacking Tools including logic analyzers, multimeters, oscilloscopes, and bus pirates.
3. Execute non-invasive and semi-invasive Physical Attacks to bypass device tamper-proofing and security mechanisms.
4. Identify, probe, and communicate over common Embedded Communication Protocols
5. Perform Firmware Extraction and subsequent Binary Reverse Engineering using tools like Ghidra or IDA Pro.
6. Analyze Embedded Operating Systems to uncover root access vulnerabilities.
7. Comprehend and exploit weaknesses in Bootloader Security and implement robust Secure Boot processes.
8. Implement and audit Cryptographic Accelerators and secure storage mechanisms like Hardware Security Modules (HSM) and Secure Elements.
9. Understand and mitigate advanced attacks such as Side-Channel Analysis and Fault Injection
10. Apply learned techniques to industry-specific devices, focusing on Automotive Cybersecurity and Industrial IoT Security.
11. Develop practical skills in Schematic and PCB Analysis for identifying hidden test points and key components.
12. Establish a Root of Trust and design for security in development practices
13. Conduct and document professional-grade Embedded Device Security Audits and present actionable findings.

Target Audience

1. Cybersecurity Professionals and Penetration Testers
2. Embedded System Developers and Hardware Engineers.
3. IoT Security Researchers and Vulnerability Analysts.
4. Digital Forensics Investigators.
5. Product Security Engineers
6. Security Architects designing Secure Boot and Hardware Root of Trust mechanisms.
7. Ethical Hackers specializing in Cyber-Physical Systems
8. Professionals in regulated industries dealing with device security compliance.

Course Modules

1. Fundamentals of Hardware & Embedded Systems

- Component Identification & Datasheet Analysis.
- Essential Hacking Toolkit.
- PCB Reconnaissance & Probing.
- Case Study: Disassembling a Smart Home Hub to map internal components and power architecture.
- Basic soldering/desoldering practice and continuity testing on a custom target board.

2. Embedded Communication Protocol Analysis

- UART & Serial Exploitation.
- SPI & I2C Bus Sniffing/Manipulation.
- JTAG & SWD Debugging Interfaces.
- Case Study: Exploiting a Network Router's JTAG port to bypass login security and dump configuration.
- Using a logic analyzer to passively sniff SPI traffic and actively using a Bus Pirate to read from an I2C EEPROM.

3. Firmware Extraction and Analysis

- Memory Dumping Techniques.
- Firmware Image Identification.
- Binary Reverse Engineering
- Case Study: Analyzing a Wearable Device's firmware to discover hardcoded API keys and internal logic.
- Extracting flash memory using a programmer and executing basic static analysis on the embedded Linux filesystem using binwalk and firmware-mod-kit.

4. Advanced Hardware Attack Vectors

- Side-Channel Analysis.
- Fault Injection (FI) Techniques.
- Hardware Trojans & Supply Chain Attacks.
- Case Study: Demonstrating a Power Analysis attack against a simple AES implementation to recover the secret key.
- Performing a clock glitching attack on a target microcontroller to bypass a hardware-enforced boot check.

5. Wireless and RF Hacking Fundamentals

- Bluetooth Low Energy (BLE) Hacking.
- Zigbee/Z-Wave Security
- Software Defined Radio (SDR) Basics.

- Case Study: Exploiting a BLE pairing vulnerability in a smart lock to gain unauthorized access.
- Capturing and analyzing a BLE connection setup, identifying a potential pairing weakness.

6. Embedded Operating System and Software Exploitation

- U-Boot & Bootloader Exploitation.
- Kernel and Driver Vulnerabilities.
- Memory Corruption in Embedded C/C++.
- Case Study: Leveraging a U-Boot environment variable flaw on an industrial gateway to drop into a root shell.
- Exploiting a simple stack-based buffer overflow in a vulnerable application running on a target device.

7. Automotive and Industrial Embedded Security

- CAN Bus Hacking.
- OBD-II Diagnostics Security.
- Industrial Control System (ICS)/SCADA Device Analysis
- Case Study: Simulating an attack on a vehicle's CAN Bus to manipulate dashboard indicators or essential functions.
- Using a CAN Bus tool to sniff traffic from an automotive target and identify specific control messages.

8. Defense and Secure Design Principles

- Secure Boot and Trusted Execution Environments
- Hardware-Based Protection Mechanisms.
- Anti-Tamper & Anti-Cloning Measures.
- Case Study: Reviewing the Platform Security Architecture for hardening commercial IoT designs.
- Implementing and testing a basic Cryptographic Authentication scheme on a target device's boot process.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

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

Register Online Now

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