Security for Embedded Systems Bootcamp

Course Description

This training provides a deep background for security for embedded systems including the greatest and latest attacks & countermeasures for microcontrollers, microprocessors and FPGAs.

The first part of the training starts by introducing the elementary terms and attack surface on embedded systems as well as building blocks that consist of security solutions such as random numbers, encryption, and authentication, digital signatures, secured boot and tampering.

The second part of the training is dedicated to hardware security and covers secure hardware architectures, Root of Trust, PUF, multicore and many-cores protections, memory protection (volatile and non-volatile), side-channel protections, circuit level protection and FPGA security.

The third part of the training is dedicated to software security and covers common software attacks, defensive software security architectures, data protection techniques, and firmware protection.

The course shows the difference security solutions applied to MCUs, MPUs and FPGAs and explore the quality of the various solutions and design tradeoffs such as power consumption, silicon area and performance.

The training uses design example that accompanies the training material and provide a system level security understating by demonstrating the theory with real use-case.

Course Duration

3 Days (Also available as 6 half-days)

Goals

1. Understand the need for embedded systems security
2. Understand the threat and vulnerability landscape of Embedded Systems
3. Be able to perform threat modeling and risk assessments
4. Understand the challenges of designing secure Embedded Systems
5. Learn the concepts of designing secure Embedded Systems
6. Master the fundamental building blocks of Embedded Security
7. Get familiar with Embedded Systems Security best practices

Intended Users

Hardware, software, system engineers and team leaders that would like to understand what security is in embedded systems and apply that in projects

Table of Contents

Day 1 – Introduction to Embedded Systems Security

- **Introduction**
  - Cyber security definition and terms
  - Attack types
  - Threat terminology
  - Cyber security requirements
  - Embedded systems security challenges

- **Embedded Systems Threat Landscape**
  - Attacking Embedded Systems
  - Attacker's arsenal state-of-the-art tools
  - Embedded Systems attack surface & taxonomy
  - Local and remote attacks on Embedded Systems

- **Designing Secure Embedded Systems**
  - Structure and flow of a full security protocol and possible threats
  - Use case examples of attacking embedded system and possible solutions

- **Embedded Systems Security Best Practices**
  - Securing Embedded Systems
  - Secure by design
  - Threat modeling & security analyses
  - Security standards for Embedded Systems

- **Modern Embedded Systems Protections**
  - Root of Trust
  - Secure boot process
  - Hardware based security
  - Security monitoring
  - Device tampering detection
  - Secure OTA updates

- **Cryptography 101**
  - Cryptography terminology
  - Cryptography in Embedded Systems
  - Symmetric key cryptography
  - Asymmetric key cryptography
  - Cryptographic Hash functions
  - Digital signature
  - Digital certificates
  - Randomness

Day 2 – Embedded Systems Hardware Security

- **Introduction**
  - Hardware security evolution
  - Hardware attack types & taxonomy
  - Hardware attack surface
  - Hardware Trojans

- **Secure Hardware Architectures**
  - Hardware architecture types
  - Privilege levels
  - Example of Intel SGX and Arm Trustzone
  - Today's limitation of secure architectures
  - HSM, TMP and TXT
  - Crypto managers
  - Crypto accelerators

- **Hardware Root of Trust (RoT)**
  - Functions of RoT
  - RoT and secret key
  - Attacks and measurements

- **Physically Unclonable Functions (PUF)**
  - What is PUF and how does it work?
  - PUF use cases
  - PUF based RoT

- **Multiprocessor & Many-Core Protection**
  - SMP protections
  - Bus traffic protections
  - Many-core trust boundary
  - Performance challenges

- **Memory Protection**
  - Sources & types of attacks on memory
  - Confidentiality and integrity protections
  - Memory access pattern protections
  - Security of non-volatile memories

- **Circuit Level Protection**
  - Power domain isolation
  - Secure RTC & monotonic counters
  - Tamper detection
  - Using fuses
  - Secure JTAG
  - Secure I/O peripherals

- **Side-Channel Threats & Protections**
  - Side and covert channels
  - Timing side channels inside a processor
  - Timing side channels in memory hierarchy
  - Meltdown, Spectre and Foreshadow
  - Speculative side channels
  - Defense strategies

- **Security in Modern FPGAs**
  - Why is FPGA security important?
  - FPGA security & Trust vulnerabilities
  - FPGA state-of-the-art defenses
  - Hardware Trojan in FPGA and detection methods
  - Supply chain attacks protection

Day 3 – Embedded Systems Software Security

- **Introduction**
  - Characteristics of Embedded software security
  - Embedded software security challenges
  - Software attack surface deep dive

- **Common Software Attacks**
  - Web application security
  - Network attacks
  - Memory corruption attacks
  - Attacks on Firmware
  - Software attacks on hardware
  - Hardware attacks on software

- **Defensive Security Architectures**
  - Micro-kernel vs monolith
  - Independent security levels
  - Core security requirements
  - Access control
  - I/O virtualization
  - Hypervisors
  - Virtualization
  - Containerization
  - (TEE) Trusted Execution Environment

- **Data Protection**
  - Data-in-motion protocols
  - Securing data in motion
  - Data-at-rest protocols
  - Securing data at rest

- **Firmware Security**
  - Secure Boot
  - Secure Firmware storage
  - Anti-reversing / obfuscation
  - Code polymorphism
  - Kernel security
  - Exploit mitigation
  - Firmware security best practices