Embedded Systems Security Bootcamp (With LPC55S69)

About this training:

Is your Embedded System secured? Embedded devices have traditionally run in relative isolation and have therefore been protected from a wide range of security threats. Today's devices, however, are often connected to corporate networks, public clouds, or the Internet directly. Medical Devices, IoT Devices, Automotive Systems and Industrial Control System have been increasingly become target for attackers.

The design of security for Embedded Systems is a critical and difficult task!

Embedded Systems Security Boot Camp with the LPC55S69 is a 4-day training covering the know-how of building security and trust into Embedded Systems and devices.

Through lectures and practical hands-on labs, students are guided through the design and implementation of secured Embedded Systems, including preventing and mitigating embedded systems attacks using state of the art and recent innovation security technologies that are available today. All hands-on labs are done using NXP's LPC55S69 Secure Microcontroller.

Intended Audience:

This training is suited for beginners as well as experienced Embedded systems engineers.

Duration: 4 Days (Theory and Hands-on) + Course Completion Certification

Topics covered in this training:

- What Makes Embedded Systems Vulnerable?
- Modern Attacks on Embedded Systems
- Embedded Systems Threat Assessment
- Using Cryptography in Embedded Systems
- Protecting Data In Motion
- Protecting Data At Rest
- Implementing Secure Authentication
- Defensive Software Architectures
- Defensive Hardware Architectures
- Arm's TrustZone
- Hardware Root of Trust
- Secure Boot
- Physical Unclonable Function (PUF)
- Building Security into Existing Projects
- Embedded Systems Security Best Practices

HandsOn Training

Extensive hands-on labs for all topics, demonstrating the attacks as well as the countermeasures within the secure flow to make your system robust and protected:

- Defenses against Stack Buffer Overflow attacks
- Cryptography in Practice (Encryption, Hash Functions, HMAC, Public-Key Cryptography, etc.)
- Using PUF to implement a secure Keys-store
- Implementing Secure Boot (Including Image Encryption)
- Fault Tolerance A/B Firmware Update
- Hands on Arm's Truest Zone
- Securing Peripherals
- System Hardening
- Secure Debug Authentication
- Capstone project: Put everything together!

Attendees will receive the LPC55S69-EVK development board (LPC55S69Xpresso) as well as:

- Virtual Machine with Pre-installed IDE and Tools
- A digital copy of all lecture slides
- A Lab Manual with instructions for all hands-on labs
- Source code starting points for the labs
- Datasheets and User's Manuals for all of the hardware and software tools

Perquisites:

- Basic C/C++ Programming
- Embedded systems programming basic knowledge
- Linux command line (nice to have)

System Requirements:

4 Cores CPU (Intel i5 or Ryzen 5 CPU minimum)

8GB RAM

20GB available disk space

Windows 10 64-bit

One available USB port