oSEC6 - Embedded Security for NXP i.MX-based processors

Objectives

- Understand the unique security challenges faced by embedded systems and i.MX-based processors and learn how to identify potential attack vectors and threats.
- Learn about the latest security standards and best practices for embedded systems, and how to apply them to i.MX-based processors.
- Learn about secure boot and firmware protection mechanisms, and how to implement them on i.MX-based processors.
- Understand the principles of secure network communication and how to implement secure network protocols, such as TLS/SSL, IPSec/IKE, WiFi security, Bluetooth, BLE and UWB
- Learn about the best practices for IoT security at different layers of communication
- Understand the fundamentals of firmware update and management, and how to implement secure firmware update processes and OTA updates

Course Environment

- Theoretical course
  - PDF course material (in English).
  - Course dispensed using the Teams video-conferencing system.
  - The trainer answers trainees' questions during the training and provide technical and pedagogical assistance through the Teams video-conferencing system.
- Practical activities
  - Practical activities represent from 40% to 50% of course duration.
  - Code examples, exercises and solutions
  - One Online Linux PC per trainee for the practical activities.
  - The trainer has access to trainees' Online PCs for technical and pedagogical assistance.
  - Eclipse environment and GCC compiler.
  - QEMU Emulated board or physical board connected to the online PC (depending on the course).
  - Some Labs may be completed between sessions and are checked by the trainer on the next session.
- Downloadable preconfigured virtual machine for post-course practical activities
- At the start of each session the trainer will interact with the trainees to ensure the course fits their expectations and correct if needed

Prerequisites

- Familiarity with computer architecture
- Programming skills: Some programming experience, particularly in C
- Knowledge of NXP Implementation and ARM implementations
- Basic understanding of Security Algorithms and Secure coding
- Basic knowledge about Communication and Network protocols
- Basic knowledge in Embedded Linux

Duration

- Total: 12 hours
- 2 sessions, 6 hours each
- From 40% to 50% of training time is devoted to practical activities

- Some Labs may be completed between sessions and are checked by the trainer on the next session

Target Audience

- Any embedded systems engineer or technician with the above prerequisites.

Evaluation modalities

- The prerequisites indicated above are assessed before the training by the technical supervision of the traineein his company, or by the trainee himself in the exceptional case of an individual trainee.
- Trainee progress is assessed in two different ways, depending on the course:
  - For courses lending themselves to practical exercises, the results of the exercises are checked by the trainer while, if necessary, helping trainees to carry them out by providing additional details.
  - Quizzes are offered at the end of sections that do not include practical exercises to verifythat the trainees have assimilated the points presented
- At the end of the training, each trainee receives a certificate attesting that they have successfully completed the course.
  - In the event of a problem, discovered during the course, due to a lack of prerequisites by the trainee a different or additional training is offered to them, generally to reinforce their prerequisites,in agreement with their company manager if applicable.

Plan

First Day

Introduction to embedded security for NXP devices

- Overview of embedded security and its importance
- Threads and attack vectors specific to embedded systems
  - Common attack vectors
  - Malware and exploits
  - Threat landscape for embedded systems
- NXP and security features
  - i.MX Applications processors
  - Layerscape processors
  - ARM MCUs
  - S32 Automotive platform
  - QorIQ platform

Secure Development

- Secure coding practices
  - Code reviews and audits
  - Input validation and sanitization
  - Memory management and buffer overflows
- Static and dynamic code analysis tools
  - Using static analysis tools
  - Using dynamic analysis tools
- Secure development lifecycle for i.MX NXP-based devices
  - Requirements gathering and threat modeling
  - Design and implementation
  - Testing and validation
  - Deployment and maintenance

Exercise: *Using static and dynamic analysis tools to find vulnerabilities*

i.MX secure boot, firmware protection and Hardware assisted security

- Secure boot on NXP Devices
  - Introduction to secure boot
  - Secure boot implementation
  - Secure boot verification and toubleshooting
- Firmware protection on NXP devices
  - Introduction to firmware protection
  - Techniques for protecting firmware on NXP devices
  - Implementation of firmware protection
- Hardware assisted security on NXP devices
  - Introduction to hardware assisted security
  - ARM security features
  - Implementation of hardware assisted security

Exercise: *Implementing secure boot on NXP iMX*

Second Day

Network Security for NXP-based Devices

- Network Architecture i.MX-based processors
  - Overview of network communication protocols for embedded systems
  - Secure communication protocols
  - Designing a secure network architecture
- Transport Layer Security (TLS)
  - Introduction to TLS and SSL
  - Implementing TLS/SSL
  - Secure communication using TLS/SSL
- IPSec and IKE
  - IPSec Fundamentals
  - IKE Fundamentals
  - IPSec and IKE configuration on NXP devices
  - Advanced IPSec and IKE topics
- WiFi security
  - Overview of WiFi security mechanisms and standards
  - Implementing secure WiFi communication
  - Best practices
- Bluetooth and BLE Security
  - Introduction
  - Security Fundamentals
  - Bluetooth Security on NXP Devices
  - Advanced Bluetooth Security Topics
- Secure Ultra-wideband
  - Introduction to Ultra-Wideband
  - UWB security Fundamentals
  - UWB security on NXP devices
  - Advanced UWB Security Topics

IoT security

- Introduction to IoT Security
  - Unique security challenges faced by IoT devices
  - Overview of the common attack vectors and threats faced by IoT devices
- IoT security best practices
- Securing IoT devices at the network layer
  - IoT-specific network security protocols
- Access control and secure data transfer
  - Overview of authentication and authorization mechanisms for IoT devices
  - Discussion of secure data transfer protocols for IoT, such as MQTT and HTTPS

- The role of application-level encryption in securing IoT devices

Firmware update and management for NXP devices

- Introduction to firmware update and management
  - Importance of firmware updates in maintaining the security of embedded systems
  - Overview of firmware update methods including manual and over-the-air (OTA) updates
- Secure firmware update processes
- OTA update mechanisms
  - Overview of OTA update mechanisms
  - Implementing OTA updates, including server-side and device-side
  - Best practices for OTA updates, including testing and deployment

Renseignements pratiques

Duration : 12 hours
Cost : 2150 € HT