SEC6 - 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

- Access to a Linux machine
- Access to a shared filesystem to save and share their work.
- PDF course material
- I.MX8mQEVK evaluation board

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

Target Audience

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

Course Outline

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