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

Environnement du cours

- Cours théorique
  - Support de cours au format PDF (en anglais) et une version imprimée lors des sessions en présentiel
  - Cours dispensé via le système de visioconférence Teams (si à distance)
  - Le formateur répond aux questions des stagiaires en direct pendant la formation et fournit une assistance technique et pédagogique
- Activités pratiques
  - Les activités pratiques représentent de 40% à 50% de la durée du cours
  - Elles permettent de valider ou compléter les connaissances acquises pendant le cours théorique.
  - Exemples de code, exercices et solutions
  - Pour les formations à distance:
    - Un PC Linux en ligne par stagiaire pour les activités pratiques, avec tous les logiciels nécessaires préinstallés.
    - Le formateur a accès aux PC en ligne des stagiaires pour l'assistance technique et pédagogique
    - Certains travaux pratiques peuvent être réalisés entre les sessions et sont vérifiés par le formateur lors de la session suivante.
  - Pour les formations en présentiel::
    - Un PC (Linux ou Windows) pour les activités pratiques avec, si approprié, une carte cible embarquée.
    - Un PC par binôme de stagiaires s'il y a plus de 6 stagiaires.

- Pour les formations sur site:
  - Un manuel d'installation est fourni pour permettre de préinstaller les logiciels nécessaires.
  - Le formateur vient avec les cartes cible nécessaires (et les remporte à la fin de la formation).
- Une machine virtuelle préconfigurée téléchargeable pour refaire les activités pratiques après le cours
- Au début de chaque session (demi-journée en présentiel) une période est réservée à une interaction avec les stagiaires pour s'assurer que le cours répond à leurs attentes et l'adapter si nécessaire

Audience visée

- Tout ingénieur ou technicien en systèmes embarqués possédant les prérequis ci-dessus.

Modalités d'évaluation

- Les prérequis indiqués ci-dessus sont évalués avant la formation par l'encadrement technique du stagiaire dans son entreprise, ou par le stagiaire lui-même dans le cas exceptionnel d'un stagiaire individuel.
- Les progrès des stagiaires sont évalués de deux façons différentes, suivant le cours:
  - Pour les cours se prêtant à des exercices pratiques, les résultats des exercices sont vérifiés par le formateur, qui aide si nécessaire les stagiaires à les réaliser en apportant des précisions supplémentaires.
  - Des quizz sont proposés en fin des sections ne comportant pas d'exercices pratiques pour vérifier que les stagiaires ont assimilé les points présentés
- En fin de formation, chaque stagiaire reçoit une attestation et un certificat attestant qu'il a suivi le cours avec succès.
  - En cas de problème dû à un manque de prérequis de la part du stagiaire, constaté lors de la formation, une formation différente ou complémentaire lui est proposée, en général pour conforter ses prérequis, en accord avec son responsable en entreprise le cas échéant.

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

Durée : 2 jours
Prix : 2260 € HT