SEC6 - Sécurité embarquée pour les processeurs NXP i.MX

Objectifs

- Comprendre les enjeux de sécurité propres aux systèmes embarqués et aux processeurs i.MX, et apprendre à identifier les vecteurs d'attaque et les menaces potentiels.
- Découvrir les dernières normes de sécurité et les bonnes pratiques pour les systèmes embarqués, et savoir les appliquer aux processeurs i.MX.
- Découvrir les mécanismes de secure boot et de protection du firmware, et savoir les mettre en œuvre sur les processeurs i.MX.
- Comprendre les principes des communications réseau sécurisées et savoir mettre en œuvre des protocoles réseau sécurisés tels que TLS/SSL, IPSec/IKE, la sécurité WiFi, Bluetooth, BLE et UWB
- Découvrir les bonnes pratiques de sécurité de l'IoT aux différentes couches de communication
- Comprendre les principes de la mise à jour et de la gestion du firmware, et savoir mettre en œuvre des processus de mise à jour sécurisés et des mises à jour OTA

Environnement du cours

- Accès à une machine Linux
- Accès à un système de fichiers partagé pour sauvegarder et partager leur travail.
- Support de cours au format PDF
- Carte d'évaluation I.MX8mQEVK

Prérequis

- Bonne connaissance de l'architecture des ordinateurs
- Compétences en programmation : une expérience de la programmation, en particulier en C
- Connaissance des implémentations NXP et ARM
- Compréhension de base des algorithmes de sécurité et du codage sécurisé
- Connaissances de base sur les protocoles de communication et de réseau
- Connaissances de base en Linux embarqué

Audience visée

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

Plan du cours

Premier jour

Introduction à la sécurité embarquée pour les composants NXP

- Présentation de la sécurité embarquée et de son importance
- Menaces et vecteurs d'attaque propres aux systèmes embarqués
  - Vecteurs d'attaque courants
  - Logiciels malveillants et exploits
  - Le paysage des menaces pour les systèmes embarqués
- NXP et les fonctions de sécurité
  - Processeurs applicatifs i.MX
  - Processeurs Layerscape
  - Microcontrôleurs ARM

    - Plate-forme automobile S32
    - Plate-forme QorIQ

Développement sécurisé

- Pratiques de codage sécurisé
    - Revues et audits de code
    - Validation et assainissement des entrées
    - Gestion de la mémoire et débordements de tampon
- Outils d'analyse statique et dynamique de code
    - Utilisation des outils d'analyse statique
    - Utilisation des outils d'analyse dynamique
- Cycle de développement sécurisé pour les équipements i.MX NXP
    - Recueil des exigences et modélisation des menaces
    - Conception et mise en œuvre
    - Tests et validation
    - Déploiement et maintenance

Secure boot i.MX, protection du firmware et sécurité assistée par le matériel

- Secure boot sur les composants NXP
    - Introduction au secure boot
    - Mise en œuvre du secure boot
    - Vérification du secure boot et résolution des problèmes
- Protection du firmware sur les composants NXP
    - Introduction à la protection du firmware
    - Techniques de protection du firmware sur les composants NXP
    - Mise en œuvre de la protection du firmware
- Sécurité assistée par le matériel sur les composants NXP
    - Introduction à la sécurité assistée par le matériel
    - Fonctions de sécurité ARM
    - Mise en œuvre de la sécurité assistée par le matériel

Deuxième jour

Sécurité réseau pour les équipements à base de composants NXP

- Architecture réseau des processeurs i.MX
    - Présentation des protocoles de communication réseau pour les systèmes embarqués
    - Protocoles de communication sécurisés
    - Conception d'une architecture réseau sécurisée
- Transport Layer Security (TLS)
    - Introduction à TLS et SSL
    - Mise en œuvre de TLS/SSL
    - Communication sécurisée avec TLS/SSL
- IPSec et IKE
    - Principes d'IPSec
    - Principes d'IKE
    - Configuration d'IPSec et d'IKE sur les composants NXP
    - Sujets avancés sur IPSec et IKE
- Sécurité WiFi
    - Présentation des mécanismes et normes de sécurité WiFi
    - Mise en œuvre d'une communication WiFi sécurisée
    - Bonnes pratiques
- Sécurité Bluetooth et BLE
    - Introduction
    - Principes de sécurité

    - Sécurité Bluetooth sur les composants NXP
    - Sujets avancés sur la sécurité Bluetooth
- Ultra-wideband sécurisé
    - Introduction à l'Ultra-Wideband
    - Principes de sécurité de l'UWB
    - Sécurité UWB sur les composants NXP
    - Sujets avancés sur la sécurité UWB

Sécurité de l'IoT

- Introduction à la sécurité de l'IoT
    - Les enjeux de sécurité propres aux équipements IoT
    - Présentation des vecteurs d'attaque et menaces courants visant les équipements IoT
- Bonnes pratiques de sécurité de l'IoT
- Sécuriser les équipements IoT au niveau de la couche réseau
    - Protocoles de sécurité réseau spécifiques à l'IoT
- Contrôle d'accès et transfert de données sécurisé
    - Présentation des mécanismes d'authentification et d'autorisation pour les équipements IoT
    - Discussion des protocoles de transfert de données sécurisés pour l'IoT, tels que MQTT et HTTPS
    - Le rôle du chiffrement au niveau applicatif dans la sécurisation des équipements IoT

Mise à jour et gestion du firmware pour les composants NXP

- Introduction à la mise à jour et à la gestion du firmware
    - Importance des mises à jour de firmware pour maintenir la sécurité des systèmes embarqués
    - Présentation des méthodes de mise à jour du firmware, manuelles et par voie hertzienne (OTA)
- Processus de mise à jour sécurisée du firmware
- Mécanismes de mise à jour OTA
    - Présentation des mécanismes de mise à jour OTA
    - Mise en œuvre des mises à jour OTA, côté serveur et côté équipement
    - Bonnes pratiques pour les mises à jour OTA, y compris les tests et le déploiement