SEC2 - Sécurité avancée des systèmes embarqués

Créer des systèemes embarqués connectés sécurisés

Objectifs

- Comment manipuler les fichiers et les répertoires de manière sécurisée
- Découvrir comment protéger vos programmes contre les entrées malveillantes des utilisateurs
- Considération du logiciel du système sécurisé
- Caractéristiques matérielles des systèmes embarqués pour la sécurité
- Méthodologie et cadre de développement de logiciels sécurisés
- Appréhender le contexte et l'utilisation des hyperviseurs et de la virtualisation des systèmes
- Découvrir les contrôles et outils de sécurité

Pré-requis

- Quelques notions de programmation sont souhaitables (quel que soit le langage)
- Quelques notions de cryptographie et Linux

Environnement du cours

- Cours théorique
  - Support de cours au format PDF (en anglais)
  - Cours dispensé via le système de visioconférence Team
  - Le formateur répond aux questions des stagiaires en direct pendant la formation et fournit une assistance technique et pédagogique
- Au début de chaque demi-journée 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

Durée

- Totale : 12 heures
- 2 sessions, 6 heures chacune

Plan du cours

Première session

System Software Consideration

- The Operating System
- Multiple Independent Levels of Security
  - Information Flow
  - Data Isolation
  - Damage Limitation
  - Periods Processing
  - Tamper Proof

    - Evaluable
- Core embedded Operating system Security Requirements
    - Memory Protection
    - Virtual Memory
- Guard Pages
- Location obfuscation
    - Fault Recovery
    - Impact of Determinism
    - Secure Scheduling
- Hypervisors and System Virtualization
    - Introduction to System Virtualization
    - Applications of System Virtualization
    - Environment Sandboxing
    - Virtual Security Appliances
- Hypervisor Architectures
- Paravirtualization
- Leveraging Hardware Assists for Virtualization
    - ARM TrustZone
- Hypervisor Security
- I/O Virtualization
- Remote Management
- Assuring Integrity of the TCB
    - Trusted Hardware and Supply Chain
    - Secure Boot
    - Static versus Dynamic Root of Trust
    - Remote Attestation

Exercise : Memory Protection (MPU)
Exercise : ARM TrustZone
Exercise : Secure Boot

Deuxième session

Data Protection Protocols for Embedded Systems

- Data-in-Motion Protocols
    - Generalized Model
    - Choosing the Network Layer for Security
    - Ethernet Security Protocols
    - IPsec versus SSL
    - IPsec
    - SSL/TLS
    - Embedded VPN Clients
    - DTLS
    - SSH
    - Custom Network Security Protocols
    - Secure Multimedia Protocols
    - Broadcast Security
- Data-at-Rest Protocols
    - Choosing the Storage Layer for Security
    - Symmetric Encryption Algorithm Selection
    - Managing the Storage Encryption Key

Testing for Security

- Basic Testing Methods
    - White-Box Testing
    - Black-Box Testing

    - Grey-Box Testing
- Fuzz-Testing