oSEC2 - 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) 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

Durée

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

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

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

Renseignements pratiques

Renseignements : 12 heures
Prochaines sessions : du 31 juillet au 1er août 2025 - Online EurAsia (9h-16h CET)