FO9CS08 3 600 € 5 jour(s)

[Formation] Sécurité des systèmes embarqués

OBJECTIFS

- Décrire les menaces existantes sur les systèmes embarqués
- Identifier les enjeux de la sécurité des systèmes embarqués
- Rappeler les principes de sécurité des systèmes des processeurs
- Décrire les différentes attaques physiques contre les systèmes embarqués
- Décrire les mécanismes de sécurité existants et les mettre en place
- Expliquer la certification Critères Communs
- Décrire le principe de démarrage sécurisé d'un système embarqué

PROGRAMME

Introduction

Principales menaces sur les systèmes embarqués

- Principe des attaques matérielles et logicielles

Rappels de sécurité pour les systèmes embarqués

- Algorithmes de cryptographie standard
- Implémentations matérielles et logicielles, vulnérabilités
- Exemples pratiques de sécurisation de systèmes embarqués

Principes des attaques physiques des systèmes embarqués

- Attaques par canal auxiliaire et canal caché
- Attaques par injection de fautes
- Protections

ATELIER AVANCÉ

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

Techniciens et ingénieurs spécialistes dans le développement de systèmes sensibles, responsables de projets critiques (amenés à faire évaluer leur projet par les CESTI selon les critères communs).

Une connaissance des bases de la sécurité, des mathématiques et de l'électronique numérique sont nécessaires afin de tirer pleinement profit de la formation.

COORDINATEURS

Ulrich KUHNE

Enseignant-chercheur à Télécom Paris au sein du département Communication et Électronique. Ses activités de recherche sont axées sur la sûreté et la sécurité des circuits électroniques et des systèmes embarqués. Il s'intéresse en particulier aux attaques par canaux auxiliaires, ainsi qu'à la conception et à la validation de nouvelles techniques de protections contre des attaques physiques et logicielles.

MODALITES PEDAGOGIQUES

Des séances de cours magistraux pour introduire les concepts fondamentaux.

Pratique d’attaques physiques des systèmes embarqués

- Exemples d’attaques par canaux auxiliaires
- Analyse sur un crypto-processeur réel
- Exploitation des fautes injectées
- Exemples de contremesures

Attaque diverses des systèmes embarqués

- Rétro-conception matérielle
- Contrefaçon, chevaux de Troie matériels
- Contre-mesures

Certification Critères Communs appliquée aux circuits électroniques

Sécurité logicielle des systèmes embarqués

- Attaques logicielles par l’exemple
- Mécanismes de protection standard
- Règles de codage pour la sécurité
- Mécanismes de protection dans les processeurs récents
- ARM Trustzone, PAC, Intel SGX, MPX, etc.
- Exemples d’utilisation
- Vulnérabilités au niveau microarchitecture
- Démarrage sécurisé
- Mises à jour sécurisée du « firmware »

Synthèse et conclusion

En fonction des profils des participants, des travaux pratiques ou des démonstrations peuvent être proposés dans le but de s’approprier les concepts théoriques de la formation.

Un accès aux moyens techniques utilisés dans les laboratoires de recherche universitaires de Télécom Paris est proposé aux stagiaires de la formation.