SÉCURITÉ DES SYSTÈMES EMBARQUÉS

AVANCÉ | ATELIER | FAISABLE À DISTANCE | RÉALISABLE EN ANGLAIS

FFCNCERCERXCS08 | PRIX : 3 720 € | DURÉE : 5 JOURS

Pauses et déjeuners offerts

PRÉSENTATION

Un système embarqué est vulnérable à des attaques au niveau physique contre ses composants. Par exemple, l'utilisateur d'une set-top box peut vouloir récupérer les flux vidéo diffusés, un pirate peut vouloir récupérer les secrets contenus dans une carte à puce ou un ennemi peut vouloir récupérer le programme de vol d'un drone militaire qu'il a abattu.

La formation présente l'état de l'art des différentes attaques physiques auxquelles sont exposés les systèmes embarqués, les conditions dans lesquelles elles peuvent être réalisées et les contre-mesures à déployer pour s'en protéger.

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 de 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
- Spécificités de la sécurité des systèmes embarqués
- Principe des attaques matérielles et logicielles

Rappels de sécurité pour les systèmes embarqués
- Algorithmes de cryptographie standard s
- 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

Pratique d'attaques physiques des systèmes embarqués
- Exemples d'attaques par canaux auxiliaires
- Extraction d'un mot de passe sur un microcontrôleur
- Réalisation d'une attaque différentielle sur un circuit cryptographique
- Exemples de contre-mesures

Gouvernance de la sécurité et gestion de risques
- Certification Critères Communs pour les circuits électroniques
- Analyse de risques

Sécurité logicielle des systèmes embarqués
- Attaques logicielles par l'exemple
- Mécanismes de protection dans les processeurs récents
- Vulnérabilités et attaques au niveau micro-architecture
- Démarrage sécurisé
- Protections pro-actives

Synthèse et conclusion

PUBLIC/PRÉREQUIS

Développeurs 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 tirer pleinement profit de cette formation.

RESPONSABLE(S)

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.

MODALITÉS PÉDAGOGIQUES

La formation comprend des travaux pratiques qui permettent de valider les notions abordées.