FC9CS08 3 100 € 5 jour(s)

Sécurité des systèmes embarqués

OBJECTIFS

- Identifier les enjeux de la sécurité des systèmes embarqués contre les attaques physiques.
- Mettre en place les contre-mesures pour s'en prémunir.
- Expliquer la certification Critères Communs.
- Expliquer les architectures de sécurité des processeurs et le démarrage sécurisé d'un système embarqué.

PROGRAMME

Cryptographie embarquée

- Rappels mathématiques
- Algorithmes standards (DES, AES, RSA, ECC, etc.)
- Algorithmes dédiés à l'embarqué
- Implémentations matérielles et logicielles des algorithmes

Attaques par analyse des canaux auxiliaires

- Présentation des attaques (DPA, CPA, etc.)
- Contre-mesures

Attaques par injection de fautes

- Présentation des attaques
- Techniques d'injection de fautes
- Contre-mesures

Rétro-conception de composants

- Présentation des différentes techniques de rétro-conception
- Contre-mesures

Génération et utilisation d'aléas dans les circuits

- Implémentation de TRNG (True Random Number Generator)
- Implémentation de PUF (Physically Uncloneable Functions

Espionnage des bus de communication dans les systèmes embarqués

- Problématique
- Architectures sécurisées avec chiffrement des bus

Certification

- Certification Critères Communs appliquée aux circuits

ATELIER AVANCÉ

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

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 pour tirer le meilleur parti de cette formation.

COORDINATEURS

Jean-Luc DANGER

Directeur d'Etudes à Télécom Paris. Il anime l'équipe SSH (Secure and Safe Hardware) dont les recherches portentsur les architectures optimales des systèmes embarqués pour répondre aux exigences de sécurité et sûreté de fonctionnement, en plus des contraintes de faible complexité, haut débit, faible latence, faible consommation. Auteur de plus de 200 publications et 20 brevets. Cofondateur de Secure-IC qui propose des circuits numériques sécurisés. Il a aussi travaillé chez PHILIPS, GOUPIL, NOKIA. Ses intérêts de recherche personnels sont la génération d'aléas, les architectures flexibles et sécurisées dans les nouvelles technologies.

MODALITES PEDAGOGIQUES

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

Synthèse et conclusion