CYBERSÉCURITÉ : ATTAQUES MATÉRIELLES PAR CANAUX CACHÉS

Du 5 au 7 avril à Lannion (22)

Durée : 3 jours (21h) **Prix : 1 650 € HT (1 200 € HT pour les adhérents Cap'Tronic)**

PUBLIC

Ingénieurs, techniciens, chefs de projet, responsables qualité dans des PMEs, startups, grands groupes, exerçant dans des bureaux d'études en conception, développement et intégration de cartes électroniques ou de systèmes embarqués logiciels/matériels de domaines nécessitant de la sécurité.

PREREQUIS

Connaissances de base en électronique numérique. Connaissances en programmation C ou Python. Éventuellement notions en cryptographie appliquée.

OBJECTIFS

L'objectif de cette formation est :
- Appréhender des problématiques et enjeux en cybersécurité liées aux attaques physiques
- Vous approprier les bases des attaques par canaux auxiliaires
- Connaître quelques éléments de protection simples contre certaines attaques
- Pratiquer et analyser différentes attaques et protections sur plateforme expérimentale (la formation intègre une importante partie de travaux pratiques)

LIEU

ENSSAT - 6 Rue de Kerampont - 22300 LANNION

INTERVENANT

ENSSATT

PROGRAMME

Pour toute entreprise désireuse de commercialiser un produit connecté ou intelligent, analyser la question de sa cybersécurité devient un incontournable pour mettre sur le marché. Tous les marchés sont en effet potentiellement impactés par les cyberattaques et la sécurité tend à devenir un standard bientôt demandé, que cela soit par les autorités compétentes ou par les clients directement.
Par ailleurs la mobilité et l'isolement toujours croissants des produits connectés (souvent accessibles physiquement) conjuguée à la multiplicité des mobiles d'attaques et à l'importance des coûts associés à une cyberattaque, rendent de plus en plus nécessaire de s'intéresser à la question.

Cette formation s'attachera à montrer que les systèmes électroniques embarqués, même conçus à partir de solutions robustes au niveau théorique, doivent être implantés de façon à résister un minimum à des attaques matérielles par canaux cachés comme l'analyse de la consommation d'énergie, du rayonnement électromagnétique et du temps de calcul.

Jour 1

- **Introduction à la sécurité numérique et aux attaques physiques :**
  - Place des blocs/routines de cryptographie dans les systèmes de sécurité
  - Revue des principales possibilités d'attaques (théoriques, informatiques, physiques)
  - Évolution de l'importance des attaques physiques pour les systèmes électroniques/informatiques embarqués
  - Rappels sur des algorithmes cryptographiques classiques (Chiffrements symétrique/asymétrique)

- **Étude des principes des attaques par canaux cachés :**
  - Identification de vulnérabilités et sources cachées d'information
  - Présentation des attaques directes (principes et exemples historiques)

- **Prises en main du banc d'attaque :**
  - Mise à niveau C et/ou Python
  - Présentation des différents composants et instruments
  - Travaux pratiques : première utilisation du banc d'attaque et des logiciels associés (sur cas simple)

Jour 2

- **Attaques simples :**
  - Présentation des principes et des algorithmes
  - Travaux pratiques sur un crypto-système simple
  - Analyse des limitations des attaques simples

- **Attaques avancées basées sur des statistiques :**
  - Présentation des principes et des algorithmes (rappel des notions de statistiques nécessaires)
  - Travaux pratiques sur plateforme expérimentale
  - Analyse du coût et du taux de réussite des attaques

Jour 3

- **Contre-mesures et protections :**
  - Présentation des principes (p. ex. masquage, uniformisation, randomisation)
  - Exemples concrets
  - Travaux pratiques : attaque de crypto-systèmes protégés

- **Analyse de compromis coût–performance–sécurité**

Moyens pédagogiques : Support de cours - Exercices pratiques - Mises en situation
Moyens permettant d'apprécier les résultats de l'action : Evaluation de l'action de formation par la remise d'un questionnaire de fin de stage.
Moyen permettant de suivre l'exécution de l'action : Feuilles de présence signées par chaque stagiaire et le formateur par journée de formation.
Sanction de la formation : Attestation de présence
