Services Nationaux du CNFM
PCM - Pôle CNFM de Montpellier
Université Montpellier - LIRMM - CC 477 - 161 rue Ada
34095 MONTPELLIER Cedex 5, France

Formation
Sécurité Numérique des Systèmes Intégrés
9-10 Mai 2017, Montpellier

Le CNFM organise une formation de deux jours sur :

Sécurité Numérique des Systèmes Intégrés

Cette formation est ouverte à l'ensemble des acteurs du monde industriel.

Date et Lieu :

Cette formation aura lieu du **9 Mai 9h30** au **10 Mai 17h30** à Montpellier.
Pôle CNFM de Montpellier
161 rue Ada - Bâtiment 3
34095 Montpellier Cedex 5

Contact: Florent Bruguier, Tél : +33 (0) 4 67 14 86 43, florent.bruguier@cnfm.fr

---

Sécurité Numérique des Systèmes Intégrés

Résumé

Cette formation a pour objectif de sensibiliser aux enjeux de la sécurité matérielle. Après une revue des principaux algorithmes cryptographiques, le but sera de comprendre leurs vulnérabilités potentielles, en mettant en pratique ce que l'on appelle communément les attaques par canaux cachés. Les stagiaires seront amenés à réaliser des expérimentations sur la plateforme SECNUM, plateforme de Sécurité Numérique et seront confrontés à des cas très pratiques.

Objectifs

A la fin de cette formation, les stagiaires seront capables:

- D'appréhender les enjeux de la sécurité numérique.
- De comprendre les mécanismes mis en jeux par les attaques par canaux cachés.
- De réaliser des mesures de consommation et d'émissions électromagnétiques en vue d'attaquer un système cryptographique.
- De coder une attaque du premier ordre (DPA, CPA, CEMA...).
- De mettre en place des contremesures sur un système cryptographique.

Personnes concernés

Chercheurs, enseignants, enseignants-chercheurs, doctorants

Pré-requis

Afin de profiter au mieux de cette formation, une connaissance minimale des bases de l'électronique et des systèmes numériques est nécessaire.

Contenu de la formation

Jour 1
Matin

- Introduction à la cryptographie et la cryptanalyse : Terminologie et définitions
- Enjeux de la sécurité numérique
- Les algorithmes de chiffrement symétriques
- Les algorithmes de chiffrement asymétriques
- Principe des attaques par canaux cachés

Après-midi

- Présentation de la Plateforme SECNUM
- Mise en place d'une attaque sur un processeur exécutant un AES (Consommation)
- Campagne d'acquisition
- Implémentation de l'attaque sur Matlab (CPA)
- Analyse des résultats

Jour 2
Matin

- Mise en place d'une attaque sur un cryptoprocesseur AES (Emissions EM)
- Campagne d'acquisition
- Implémentation de l'attaque sur Matlab (CEMA)
- Analyse des résultats

Après-midi

- Principe des contremesures (Dissimulation et Masquage)
- Mises en application sur un processeur généraliste de deux exemples (Dissimulation et Masquage)

Modalités d'inscription :

Les frais d'inscription de 800 euros HT comprennent les séances de cours, les séances de TP et les 2 repas de midi.
Les frais annexes de mission/déplacement sont à la charge des participants.

Pour toute information complémentaire vous pouvez contacter :

Mme Chantal BLANC

Tel : (33) (0)4 67 14 96 84, Email : spcm@cnfm.fr

Fax : +33 (0) 4 67 14 96 85

Formation
Sécurité Numérique des Systèmes Intégrés

9 au 10 mai 2017

Formulaire d'inscription

Ce formulaire d'inscription doit être rempli et renvoyé par courriel ou par fax *(04 67 14 96 85)* à :
Chantal BLANC (spcm@cnfm.fr)

Date limite d'inscription : 27 avril 2017

NB : Le nombre de places étant limité à 8, celles-ci seront attribuées selon le principe du « premier inscrit, premier servi ».
Si le nombre de participant inscrit au 27 avril 2017 est insuffisant nous nous réservons la possibilité d'annuler cette formation à cette date.

ATTENTION : Si la formation est confirmée au 16 avril, en cas d'annulation de votre part après le 2 mai 2017, les frais d'inscription vous seront facturés.

Prix de la formation : 800 € HT

Titre/Nom : …… Prénom : ……..……

Université/Entreprise: ……...

Adresse : ……..……..……

……..……..……..……..……....

Ville : ……..Code Postal : ……..

Tel : ……Fax : …… Email : ……..

Signature :