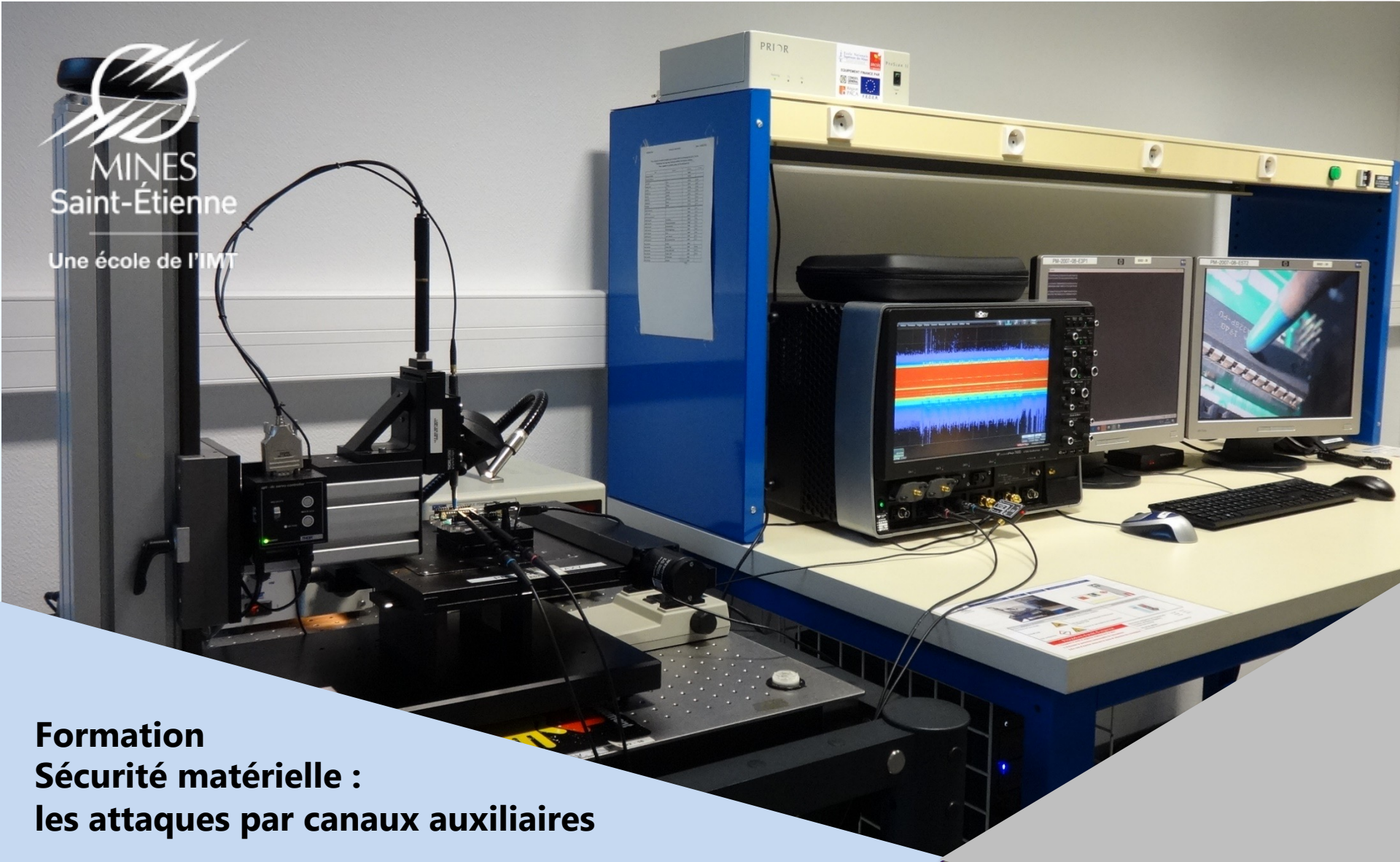


MINES
Saint-Étienne

Une école de l'IMT

Formation
Sécurité matérielle : les attaques par canaux auxiliaires

Centre Microélectronique de Provence, Gardanne

www.mines-stetienne.fr

INSPIRING INNOVATION SINCE 1816

Objectifs professionnels :

- Compréhension des menaces liées aux attaques matérielles
- Acquérir une première expérience pratique d'une attaque par canaux auxiliaires

Objectifs pédagogiques :

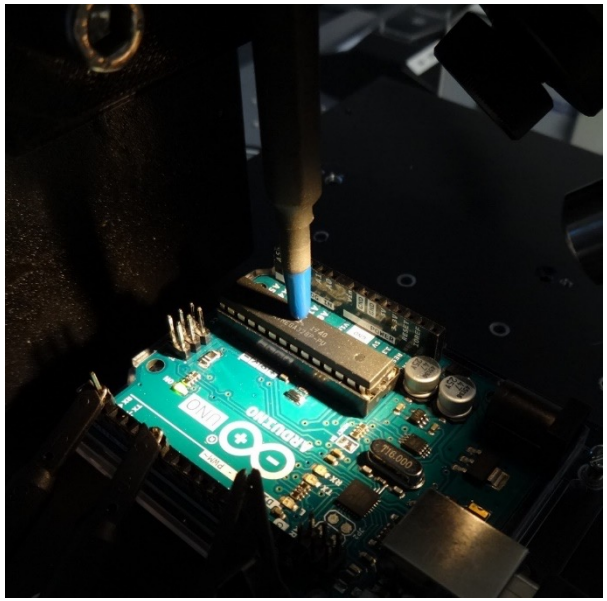
- Une journée dédiée à la sensibilisation théorique et pratique de la sécurité matérielle :
  1. Un cours théorique des mécanismes de fuite d'informations à l'exécution d'algorithmes cryptographiques
  2. Une séance de travaux pratiques de mise en œuvre d'une attaque par mesure du rayonnement électromagnétique de l'algorithme AES
  3. Une introduction aux schémas de protections face aux attaques matérielles

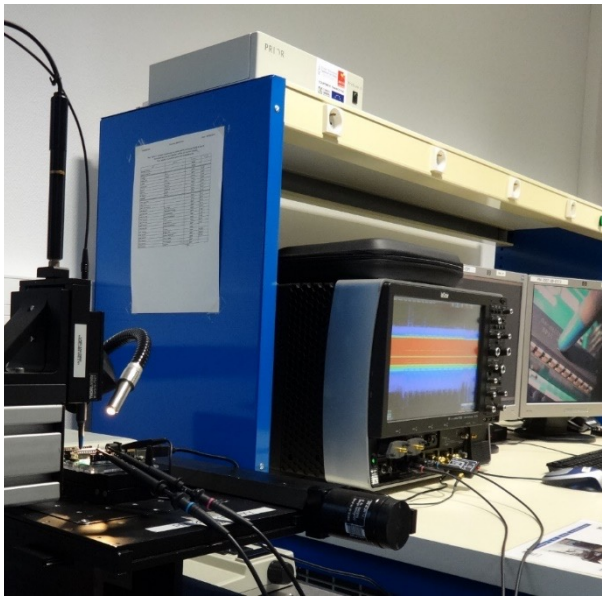
Équipe animatrice :

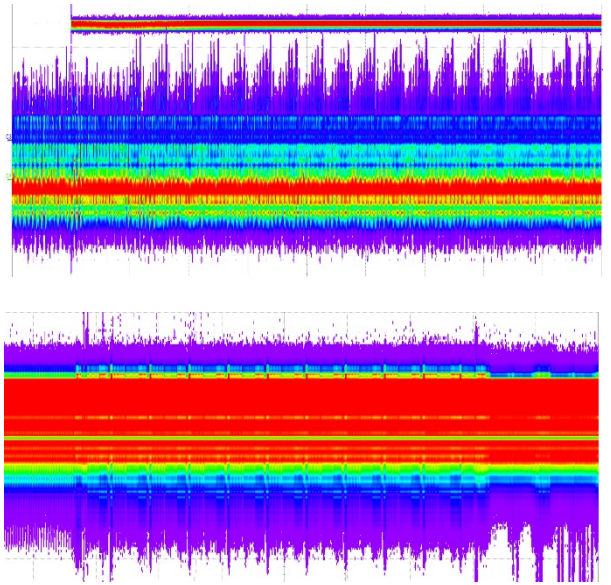
- Olivier Potin, enseignant-chercheur du département Systèmes et Architectures Sécurisés (SAS)
- Anne-Lise Ribotta, ingénieur responsable du laboratoire sécurité du département SAS

Public :

- Les ingénieurs des systèmes embarqués souhaitant évaluer les risques d'attaques matérielles







Programme :

Première ½ journée

- Généralités sur la cryptographie
- Introduction aux attaques physiques (Type, classification, exemples)
- Attaques par canaux auxiliaires (Modèle de fuites, processus physique, type, exemples)

Deuxième ½ journée

- Présentation du cas d'étude : Extraction de la clé symétrique de l'AES sur Arduino UNO
- Présentation des schémas de protections

Prix de la formation : 1 500 € TTC

Ce prix comprend :

- les pauses café et déjeuner
- les supports de cours
- la maquette utilisée pendant le TP
- les scripts de pilotage

Équipement nécessaire :

- Un PC sur lequel est installé :
- une version récente de Python
- l'IDE Arduino® pour faciliter la prise en main de la maquette
- le logiciel open-source Lascar de Ledger Donjon®

Documentation et matériel fourni :

- les supports de cours
- la maquette utilisée pendant le TP
- les scripts de pilotage

Inscription :

auprès de Olivier Potin
par mail : olivier.potin@emse.fr
ou par téléphone : 04.42.61.67.37

Adresse :

MINES Saint-Etienne
Centre de Microélectronique de Provence
880, Avenue de Mimet
F-13541 Gardanne
http://www.mines-stetienne.fr/plans-dacces/

N° SIRET : 18009202500105

N° de déclaration d'activité comme prestataire de formation : 84420300642

INSPIRING INNOVATION SINCE 1816