

Attaques matérielles, composants matériels pour la sécurité



Component
École Nationale
Supérieure
d'Électrotechnique
d'Électronique
d'Informatique
d'Hydraulique
et des
Télécommunications

In brief

> **Code:** NEIT3B

Presentation

Objectives

- Composants matériels pour la sécurité (virtualisation, IO-MMU, TPM)
 - Attaques matérielles (canaux auxiliaires) et contre-mesures
 - Classes d'attaques Spectre, Meltdown, rowhammer et canaux auxiliaires temporels à l'aide des caches
-

Description

L'objectif de ce cours est de présenter les principales attaques réalisées depuis le matériel ainsi que les contre-mesures associées. Un balayage des composants d'un système sera réalisé en identifiant l'utilité et les risques associés à la présence de chacun de ces composants. Certains de ces risques seront illustrés par des attaques récentes, soit en reconfigurant les composants concernés, soit en réalisant une étude matérielle et physique de ces composants. Aussi, des contre-mesures seront présentées avec les dernières avancées en terme de protection matérielle réalisées par les fondeurs de processeurs et de chipset.

A l'issue de ce cours, l'étudiant devra être capable d'obtenir une vue globale des échanges entre les composants matériels d'un système d'information, en considérant aussi bien les composants logiciels et réseaux que matériels. Il sera capable de comprendre le fonctionnement d'une attaque sur le matériel, de la décrire et d'expliquer les mécanismes de

protection associés. Il sera également capable d'identifier les composants critiques d'un système, d'analyser les vulnérabilités pouvant cibler ces composants, de déterminer les contre-mesures permettant de les protéger et de mettre en œuvre ces contre-mesures.