3IF1160 - Sécurité réseau et matérielle

Responsables : **Guillaume HIET**

Langues d'enseignement : **FRANCAIS**

Campus où le cours est proposé : **CAMPUS DE RENNES**

Nombre d'heures d'études élèves (HEE) : **60**

Nombre d'heures présentielles d'enseignement (HPE) : **36**

Année académique : **2024-2025**

Niveau avancé : **non**

Présentation, objectifs généraux du cours :

L'infrastructure réseau est un élément essentiel d'un système d'information. Assurer en profondeur la sécurité d'une organisation dans son ensemble passe nécessairement par un contrôle fin et une supervision constante de l'architecture du réseau informatique et des fonctions individuelles qui y sont opérées. Ce module d'enseignement a pour objectif d'approfondir les compétences en réseau des élèves ingénieurs en s'orientant plus particulièrement sur l'analyse des risques de sécurité liés au réseau informatique et sur les méthodes de déploiement et de configuration des contre-mesures appropriées. Des éclairages particuliers seront plus spécifiquement apportés sur certains aspects, comme le contrôle de l'accès au réseau, la configuration des pare-feux ou l'établissement de tunnels sécurisés.

Il est de plus en plus important de combiner des aspects logiciel et matériels afin de prendre en compte les nouvelles attaques logicielles. Par exemple des vulnérabilités matérielles telles que Spectre ou Meltdown peuvent être exploitées par des attaques purement logicielles. De telles attaques peuvent être exécutées à distances et ne requièrent pas d'accès physique à la plateforme matérielle ciblée. D'un autre côté, des fonctionnalités matérielles peuvent être utilisées pour mieux détecter et répondre aux attaques logicielles traditionnelles, telles que celles exploitant des corruptions de la mémoire. Il est donc nécessaire d'étudier avec attention la sécurité des interfaces logiciel/matériel, à la fois en termes d'attaque et de défense.

Période(s) du cours (n° de séquence ou hors séquence) :

SD9

Prérequis :

Enseignements de première année :

- Réseaux et Sécurité

Enseignements de deuxième année :

- Nouveaux Paradigmes Réseau
- Architecture des ordinateurs
- Système d'exploitation

Plan détaillé du cours (contenu) :

Cours 1 (3h) : Introduction et enjeux, architecture, supervision, cadre réglementaire
TP 1 (3h) : Protection de l'accès au réseau (802.1X, RADIUS)
TP 2 (3h) : IPsec
TP 3 (3h) : Fonctionnement d'un SOC/NOC
Cours 2 (3h) : Pare-feux avancés
TP 4 (3h) : Configuration de pare-feux
Cours 3 (3h) : Sécurité du wifi
Cours 4 (3h) : Sécurité du routage
Cours 5 (3h) : Introduction aux mécanismes de sécurité matériel
Cours 6 (3h) : Attaques contre la micro-architecture
TP 5 : Attaques par canaux auxiliaires contre le cache
TP 6 : Enclaves

Déroulement, organisation du cours :

Cours magistraux : 18h
Travaux pratiques : 18h

Organisation de l'évaluation :

Le module est évalué au travers de travaux pratiques (rapports et soutenances).

Moyens :

Enseignants :

- Guillaume Hiet (CentraleSupélec) ;
- Ruben Salvador (CentraleSupélec) ;
- Christophe Bidan (CentraleSupélec) ;
- Jean-François Calvez (Orange Cyberdefense).

Du matériel réseau spécifique sera mis à disposition pour les TP.

Acquis d'apprentissage visés dans le cours :

À la fin de cet enseignement, l'étudiant sera capable de :

- Concevoir une architecture de réseau informatique garantissant de bonnes propriétés de sécurité ;
- Configurer des équipements réseau dans le respect des recommandations de l'ANSSI et du Référentiel Général de Sécurité ;
- Configurer et maintenir des tunnels IPsec ;
- Administrer et superviser le contrôle d'accès au réseau ;
- Anticiper et contenir les risques de sécurité liés aux communications radio et au routage dynamique.
- Réaliser des attaques par canaux auxiliaire exploitant le cache d'un microprocesseur
- Développer une application reposant sur une enclave d'un microprocesseur

Description des compétences acquises à l'issue du cours :

C2 - Analyse, design and implement complex systems made up ofscientific, technological, social and economic dimension