Sécurité et Cryptographie (INFO731_IDU)

Composante
POLYTECH
2026-2027

En bref

- **Langues d'enseignement:** Français
- **Ouvert aux étudiants en échange:** Oui

Présentation

Description

Ce cours présente une introduction aux principes et à la pratique de la sécurité des réseaux et des systèmes informatiques. Les sujets abordés seront la cryptographie, la sécurité des réseaux et des systèmes d'exploitations, les mécanismes de propagation des vers et virus, et la gestion d'incident de sécurité. Nous traiterons aussi de sujet liés à la sécurité des applications mobiles, des systèmes de paiement et de la sécurité des données.

Objectifs

Ce cours vise à doter les étudiants des connaissances théoriques et pratiques nécessaires pour protéger les systèmes d'information contre les menaces numériques. Voici les principaux objectifs :

1. **Comprendre les fondamentaux de la cybersécurité** : notions de confidentialité, intégrité, disponibilité, authentification et non-répudiation.
2. **Identifier les types de menaces et d'attaques** : virus, ransomwares, phishing, attaques par déni de service (DDoS), ingénierie sociale, etc.
3. **Maîtriser les outils et techniques de protection** : pare-feu, antivirus, systèmes de détection d'intrusion (IDS), chiffrement, gestion des identités et des accès (IAM).
4. **Apprendre à concevoir des architectures sécurisées** : appliquer les bonnes pratiques pour renforcer la sécurité des réseaux, des applications et des bases de données.
5. **Comprendre les enjeux légaux et éthiques** : conformité réglementaire (RGPD, NIS2, etc.), responsabilité numérique, respect de la vie privée.

6. **Développer des capacités d'analyse et de réaction** : analyser un incident de sécurité, réaliser un plan de réponse aux incidents, mettre en œuvre un plan de continuité d'activité.
7. **Se sensibiliser à la sécurité dans le cycle de développement logiciel**(DevSecOps) : intégrer la sécurité dès la phase de conception.

Heures d'enseignement

CM	Cours Magistral	13,5h
TD	Travaux Dirigés	22,5h
TP	Travaux Pratiques	4h

Plan du cours

Introduction à la cryptographie de sécurité
Cryptographie symétrique Cryptographie asymétrique Fonctions de hachage
Gestion des clés et PKI
Sécurité du réseau - Attaques
Sécurité du web
IPSec VPN et pare-feu
Détection d'intrusion
Authentification des utilisateurs
Sécurité des programmes
Logiciels malveillants

Compétences visées

-Maîtriser les fondamentaux de la sécurité informatique : cryptographie, protocoles sécurisés, authentification, contrôle d'accès.

-Configurer et sécuriser des infrastructures réseau : pare-feu, VPN, systèmes de détection/prévention d'intrusion (IDS/IPS).

-Analyser et détecter les vulnérabilités : réaliser des audits de sécurité, tests d'intrusion (pentests), analyse de failles.

-Développer et intégrer des applications sécurisées : appliquer les principes du développement sécurisé (DevSecOps).

-Mettre en œuvre des politiques de sécurité : gestion des identités et des accès (IAM), segmentation réseau, chiffrement des données.

Compétences acquises

Macro-compétence	Micro-compétences

Infos pratiques

Lieux

- Annecy-le-Vieux (74)