Sécurité

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

En bref

Code Ametys: N8AN02C

Présentation

Objectifs

Introduire la notion de sécurité des systèmes et des réseaux.
Développer les mécanismes de cryptographie et autres mécanismes de sécurité.
Analyser les risques et évaluer la sécurité des systèmes.

Description

– Notions de base
– Menace, vulnérabilités, attaques, intrusions et risques de sécurité
– Introduction à la cryptographie
– Chiffrement symétrique :DES, 3DES, IDEA, AES
– Chiffrement asymétrique : RSA, ElGamal, Diffie Hellman
– Fonctions de Hachage et contrôle d'intégrité : MD5, SHA-1, SHA-2, MAC, HMAC, ...
– Signature électronique
– Certificats et infrastructures de gestion de clés
– Protocoles d'authentification : Défi-Réponse, S-Key, OTP, Zéro-Knowledge, Fiat-Shamir
– Applications : pare-feux, SSL / TLS, IPSec, Kerberos, PGP
– Les critères communs (norme ISO 15408 pour l'évaluation de la sécurité)

– Méthodes d'analyse des risques : la méthode EBIOS (Expression des besoins et identification des objectives de sécurité)

Pré-requis obligatoires

- Protocoles avancés de l'Internet
- Systèmes répartis
- Réseaux des opérateurs de téléphonie