RSX112 - Sécurité et réseaux

Valide le 09-07-2018

Code : RSX112

6 crédits

Responsabilité nationale :
EPN05 - Informatique / Jean-pierre ARNAUD

Contact national :
EPN05 - Informatique
33.1.25, 2 rue Conté
75003 Paris
01 40 27 28 49
Mariella Annicchiarico
mariella.annicchiarico@lecnam.ne

Présentation

Prérequis

Ce cours s'appuie sur des connaissances de base en programmation, en systèmes informatiques et en réseaux. Pour s'inscrire les élèves doivent posséder un niveau de connaissances correspondant à la réussite des deux premières années de licence L1 et L2 ou du DPCT Cnam.

Objectifs pédagogiques

Ce cours présente les principaux aspects de la sécuritédes réseaux. Il présente les problèmes généraux de sécurité (confidentialité, intégrité, authentification, protection, non répudiation). et les solutions types connues pour ces problèmes. Il présente la mise en oeuvre de ces solutions dans l'architecture Internet.

Programme

Contenu

1) Introduction :
- Positionnement des problèmes de sécurité
- Risques et menaces, contexte normatif, méthodologies d'analyse de sécurité (Marion, Melisa, Mehari).
- Les différents problèmes à résoudre.
- Situation des protocoles de sécurité dans l'architecture Internet.
- Contexte légal et aspects juridiques.
2) Protection de l'accès aux données et protection des interfaces dans les systèmes
- Gestion des droits dans les systèmes : politiques discrétionnaires et obligatoires.
- Architectures de machines à anneaux et à capacités.
- Exemple de la protection dans les systèmes de fichiers, dans les répertoires de pages Web. .
3) Protection dans les réseaux
- Mécanismes de filtrages des messages, murs pare-feux (firewalls).
4) Cryptographie
- Introduction aux problèmes de cryptographie
- Cryptographie à clés secrètes : concepts généraux, exemple des chiffres DES, IDEA, RC4, AES.
- Cryptographie à clé publique : concepts généraux, exemple du RSA.
- Fonctions de hachage sécuritaire : exemples MD5, SHA.
5) Protocoles de sécurité dans les réseaux
- Protocoles de confidentialité : mise en oeuvre des méthodes de chiffrement par blocs, par flots
- Protocoles d'intégrité et d'authentification des messages : MAC et signatures
- Protocoles d'authentification des usagers : protocoles à mots de passe (Radius), protocoles à clés publiques.
- Mécanismes de protection contre les virus.
6) Mise en oeuvre des protocoles de sécurité
- Infrastructures à clés publiques (PKI)
- Sécurité de la couche liaison (L2TP, protection des réseaux WIFI)
- Sécurité au niveau réseau : IPSEC
- Sécurité au niveau transport : SSL, TLS.
- Sécurisation du DNS : normes DNSSEC
- Sécurité du courrier électronique : SMIME, mécanismes anti spam.
- Sécurité des applications Web : sécurisation http, sécurisation des services Web.
- Introduction aux techniques de détection d'intrusion (IDS).

Bibliographie

Titre	Auteur(s)
'Cryptographie appliquée' , Thomson Publishing, Paris 1995	Bruce Schneier
'Codage, cryptologie et applications', Presses polytechniques et universitaires romandes 2004	Bruno Martin
'Cryptographie en pratique', Wiley 2003, Vuibert 2004	Niels Ferguson , Bruce Schneier
'Les protocoles de sécurité de l'Internet', Dunod, 2002	Stéphane Natkin