RSX112 - Sécurité des réseaux

Mis à jour le 11-04-2024

Code : RSX112

Unité d'enseignement de type cours

6 crédits

Volume horaire de référence (+/- 10%) : **50 heures**

Responsabilité nationale : EPN05 - Informatique / 1

Contact national :

EPN05 - Informatique

2 rue Conté
75003 Paris
01 40 27 22 40
Agnès Lapierre
agnes.lapierre@lecnam.net

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, du DUT informatique ou du diplôme d'établissement Analyste programmeur/Technicien développeur (DPCT) Cnam.

Il est conseillé de suivre ou d'avoir suivi l'unité d'enseignement NFA009 ou UTC505.

Objectifs pédagogiques

Ce cours présente les principaux aspects de la sécurité des réseaux. Il présente les problèmes généraux de sécurité (confidentialité, intégrité, disponibilité, authentification et contrôle d'accès, non-répudiation), les solutions-types connues pour ces problèmes et leur mise en œuvre dans l'architecture Internet.

Programme

Contenu

0) Introduction à la sécurité et à la gestion des risques informatiques

1) Primitives cryptographiques :

- Propriétés de sécurité, de contrôle d'accès et de sûreté de fonctionnement
- Approches historiques : codage, stéganographie, chiffrement
- Principe de Kerckhoffs
- Taxinomie des techniques de cryptanalyse : KPA, CPA, CCA. Exemple d'attaque sur la carte à puce via l'horloge.
- Niveau de sécurité
- Analyse des fréquences (Al-Kindi). Indice de coïncidence de Friedman
- Algorithmes historiques : César, Vigenère, Playfair, ADFGVX, Enigma.
- Sécurité inconditionnelle de l'algorithme du masque à usage unique (chiffre de Vernam)
- Théorie de l'information de Shannon et conséquences sur la sécurité des algorithmes
- Théorie de la complexité de Turing, et notion de sécurité calculatoire. Problèmes NP-complets.
- Sécurité sémantique, indistinguabilité des cryptogrammes, randomisation du chiffrement et non-malléabilité
- Générateurs de nombres aléatoires : NRBG et DRBG. Sources d'entropie. Technique d'élimination de biais de Von Neumann. Générateurs pseudo-aléatoires : affine, Mersenne Twister, cryptographiquement forts. Confidentialité persistante. Générateurs de Windows, Fortuna, Python3, Perl, Java, Linux getentropy(). Instructions x86 RDRAND et RDSEED.
- Chiffres symétriques en continu : LFSR (A5/1), RC4, ARX : ChaCha20.
- Chiffres par bloc : chiffres itérés, attaque par glissement, attaque des anniversaires. Chiffres de Feistel (DES), double et triple DES, attaque 'meet-in-the-middle'. Blanchiment par la clé (DESX), construction XEX.
- AES : algorithme, implémentation matérielle x86 AES-NI et AVX-512 VAES, performances.
- Autres algorithmes : IDEA, Blowfish, RC6, TEA, GOST Magma/Kuznyechik.
- Modes opératoires pour le chiffrement : ECB, CBC, CTR, CFB, OFB, XTS.
- Bourrage binaire et par octets. Attaques sur l'oracle de bourrage. ciphertext stealing (CTS).
- Intégrité et codes d'authentification de messages : CBC-MAC, CMAC/OMAC1.
- Chiffrement authentifié : les différentes façons de combiner chiffrement et MAC. Authenticated Encryption with Associated Data (AEAD): CCM, construction de Wegman-Carter, GCM, Poly1305, OCB3, GCM-SIV. Mesure et comparaison des performances.
- Mise à niveau arithmétique : relation de congruence modulo n, division euclidienne, PGCD, PPCM, algorithme d'Euclide, relation de Bézout, théorème des restes chinois, indicatrice

d'Euler
- Cryptographie à clé publique : sac-à-dos, RSA, bourrage OAEP, Diffie-Hellman, courbes elliptiques. Non-répudiation et signatures digitales.
- Fonctions de hachage cryptographique : attaque des anniversaires, constructions de Merkle-Damgård (MD5, SHA1 et 2), construction HMAC RFC2104, fonctions éponge (SHA3).
- Infrastructures de gestion de clés : certificats X.509 v3, autorités de certification, déploiement en double paire de clés et séquestre de clés privées, révocation (CRL, OCSP RFC6960). TP consistant à déployer une autorité de certification, activer le chiffrement sur un serveur web (HTTPS) et sur le courrier électronique (S/MIME).
- Applications de la théorie quantique et conséquences sur la sécurité des cryptosystèmes : algorithmes de Shor et de Grover.

2) Contrôle d'accès et sécurité de l'information :

- Authentification : par mot de passe (techniques de stockage : hachage et sel), biométrie (empreintes digitales, reconnaissance de l'iris), et par objet transporté (jeton, carte à puce…). Authentification forte à plusieurs facteurs.
- Autorisation : contrôle d'accès par liste (ACL) ou capacité.
- Modèles de sécurité hiérarchiques (Bell-LaPadula, Biba…) et à compartiments. Exemples avec SELinux et Windows 10. Politiques discrétionnaires et obligatoires.
- Classification CIA (FIPS 199, ISO 27000) : échelle d'impact et mesures de sécurité
- Gestion des accès : contrôle d'accès à base de rôles. Principe de séparation des tâches et du moindre privilège.
- Gestion des identités : comptes génériques et accès privilégiés
- Canaux cachés : exemple avec Covert_TCP
- Contrôle d'inférence dans les bases de données statistiques

3) Disponibilité et sûreté de fonctionnement :

- Défaillances, MTBF et MTTR.
- Norme ANSI/TIA-942 et niveaux de disponibilité d'un Datacenter
- Disponibilité des serveurs
- Fiabilisation et virtualisation du stockage local : RAID, gestion des volumes logiques
- Centralisation et optimisation du stockage : réseaux SAN (Storage Area Networks), protocoles SCSI, Fibre Channel, storage tiering, thin provisioning, over-subscription et thin persistence. Déduplication niveau bloc. World-Wide Names, Zoning FC et LUN masking. SAN fabrics, chemins multiples et ALUA. Évolutions FCoE et iSCSI.
- Redondance réseau en couche liaison : LACP IEEE 802.3ad, extensions multi-commutateurs (virtual port channels) ou mode actif/passif. Gestion des boucles en présence de VLAN avec Multiple Spanning Tree 802.1q
- Temps de rétablissement (RTO)
- Haute disponibilité : cluster physiques HA et virtualisation des serveurs ('compute') : impact sur les licences
- Plan de reprise et de continuité d'activité : perte de données maximale admissible (RPO)
- Réplication des données entre SAN, synchrone (réseaux métropolitains) ou asynchrone
- VLAN étendus entre Datacenters, virtualisation réseau (VXLAN) et Overlay Transport Virtualisation

4) Protocoles de sécurité

- Primitives élémentaires des protocoles d'authentification : Challenge/Response, nonces, authentification mutuelle, confidentialité future, estampilles temporelles
- Authentification basée sur le protocole TCP et attaque par prédiction des numéros de séquence. Exemple avec le protocole de courrier électronique (SMTP).
- Protocoles de preuve à divulgation nulle de connaissance : transcription, simulateur. Exemples avec les isomorphismes de graphes, les circuits hamiltoniens et le protocole Feige-Fiat-Shamir. Parallélisation des itérations.
- Sécurité en couche transport : Secure Sockets Layer/Transport Layer Security (SSL/TLS)
- Sécurité en couche réseau : IPSec: IKE, AH/ESP
- Sécurité en couche applicative : Kerberos (Active Directory): KDC, tickets maîtres (TGT) et

ressources.
- Sécurité en couche liaison : architecture du GSM. Itinérance, authentification et confidentialité. Evolutions 3G/4G.

Modalités de validation

- Contrôle continu
- Examen final

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
'Security Engineering', 2d Edition, Wiley, 2008	Ross Anderson
'Handbook of applied cryptography', CRC Press, 2001	Alfred J. Menezes, Paul C. van Oorschot et Scott A. Vanstone