USEEK7 - Network security

Mis à jour le 17-09-2024

Code : USEEK7

Unité spécifique de type cours

6 crédits

Responsabilité nationale : EPN03 - Electroniques, électrotechnique, automatique et mesure (EEAM) / Pengwenlong GU

Contact national :

EPN03 - Easy

292 rue Saint-Martin
11-B-2
75141 Paris Cedex 03
01 40 27 24 81
Virginie Dos Santos Rance
virginie.dos-santos-rance@lecnam.net

Présentation

Prérequis

Not applicable as this Specific Unit (US) is an integral part of a coherent degree.

Objectifs pédagogiques

This course covers the main aspects of network security. It presents general security problems (confidentiality, integrity, availability, authentication and access control, non-repudiation), known standard solutions for these problems and their implementation in the Internet architecture.

Compétences

- Understand security issues.
- Manage risks related to information technology.
- Deploy appropriate solutions according to the confidentiality, integrity and availability constraints of business applications.

Programme

Contenu

0) Introduction to IT security and risk management (ISO 27000 standards)

1) Cryptographic primitives:

- Cryptographically strong random number generators
- Historical approaches: codes, steganography, encryption
- Kerckhoffs principle
- Taxonomy of cryptanalysis techniques. Example clock attack on smart cards.
- Friedman's coincidence index
- Historical algorithms: Caesar, Vigenère, Playfair, ADFGVX, Enigma
- Unconditional security of the one-time pad (Vernam cipher)
- Shannon's information theory and consequences on algorithmic security
- Turing's complexity theory, and computational security. NP-complete problems.
- Semantic security, cryptogram indistinguishability and non-malleability.
- Symmetrical ciphers: stream (A5/1, RC4, ChaCha20), block (DES, AES) and their operating modes (ECB, CBC, CTR)
- Arithmetic notions: modulo n congruences, Euclidean division, GCD, LCM, Euclid's algorithm, Bézout relations, Chinese remainder theorem, Euler indicator
- Public-key cryptography: backpack, RSA, OAEP padding, Diffie-Hellman, elliptical curves. Non-repudiation and digital signatures.
- Cryptographic hash functions: birthday attacks, Merkle-Damgård constructs (MD5, SHA1 and 2), RFC2104 HMACs, sponge functions (SHA3).
- Public Key Infrastructures: X509v3 certificates, certification authorities, double key pair deployments and encryption private key escrow, revocation (CRL, OCSP RFC6960). Hands-on labs deploying a certification authority, enabling encryption on a web server (HTTPS) and on electronic mail (S/MIME).
- Applications of quantum theory and consequences on cryptosystem security: Shor and Grover algorithms.

2) Access controls and information security:

- Authentication: via password (storage techniques : hashing and salt), biometrics (fingerprints, iris recognition…) and token (smart card...) Strong / multifactor authentication.
- Authorization: access control lists and capacities
- Hierarchical security models (Bell-LaPadula, Biba…) and compartments. Examples with SELinux and Windows 10. Discretionary vs. Mandatory Access Control.
- CIA classification (FIPS 199, ISO 27000): impact scale and controls.

- Access management: role-based access control. Segregation of duties and least privilege.
- Identity management: generic and privileged accounts
- Covert channels: example with Covert_TCP
- Inference control in statistical databases

3) Availability and dependability:

- Failures, MTBF and MTTR
- ANSI/TIA-942 standard and Datacenter availability levels
- Server availability
- Local storage reliability and virtualization: RAID levels, logical volume management
- Storage centralization and optimization: Storage Area Networks (SAN), SCSI protocol, Fiber Channel, storage tiering, thin provisioning, over-subscription and thin persistence. Block-level deduplication. World-Wide Names, FC Zoning and LUN masking. SAN fabrics, multi-pathing and ALUA. FCoE and iSCSI.
- Network redundancy at the link layer: LACP IEEE 802.3ad, multi-switch extensions (Virtual Ports channels), or active/passive mode. VLAN loop management with Multiple Spanning Tree (802.1q)
- Recovery Time Objective (RTO)
- High Availability: physical HA clusters, server virtualization (“compute”): license impact
- Disaster Recovery and Business Continuity Planning: maximum admissible data loss (RPO)
- SAN-to-SAN data replication, synchronous (metropolitan networks) or asynchronous
- Stretched VLAN between Data Centers, Network Virtualization (VXLAN) and Overlay Transport Virtualization

4) Security protocols

- Basic authentication primitives: challenge/response, nonces, mutual authentication schemes, perfect forward secrecy, timestamps
- TCP-based authentication, and sequence number prediction. Example with SMTP (email).
- Zero-Knowledge Proofs: transcription, simulators. Examples based on graph isomorphisms, Hamiltonian circuits, and the Feige-Fiat-Shamir protocol. Iteration parallelization.
- Transport Layer Security: SSL/TLS
- Network layer security: IPSec, IKE, AH/ESP
- Applicative layer security: Kerberos (Active Directory), KDC, TGT and resource tickets
- Link-layer security: GSM security architecture. Roaming, authentication and confidentiality. 3G/4G changes.

Modalités de validation

- Examen final

Description des modalités de validation

Final exam.

Bibliographie

Titre	Auteur(s)
Applied Cryptography	Bruce Schneier
'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