UNIK4250 Security in Distributed Systems
University of Oslo
Spring 2012

Review

Audun Jøsang

Part 1
Background and Basic Concepts

- The importance of policy in information security
- Meaning of “authorization” and the related confusion in the literature
- Security services/properties
  - CIA
  - Authentication
  - Non-repudiation
- Relationship between security service and mechanism
  - See X.800 Table 1
- Meaning of ”network security”
  - Communication security
  - Network perimeter security

Part 2
Symmetric Encryption and Message Confidentiality

- Types of attack (ciphertext only, known plaintext, chosen plaintext, chosen ciphertext, chosen text)
- Substitution and transposition in ciphers
- Modes of operation
  - ECB, CBC, CFB, OFB, CTR
- DES (Feistel), AES
  - Architecture & Specificaitons
- Stream cipher
  - Architecture

    Characteristics, strengths and weaknesses

Part 3
Public-Key Cryptography and Message Authentication

- RSA
  - Principle, key generation, operation
  - Usage for confidentiality and integrity
- Diffie-Hellmann
  - Algorithm & Properties
- Elliptic curve crypto algorithgm principle
- Hash functions
  - Properties, SHA-1, SHA-2 family, SHA-3 competition
- MAC and HMAC
  - Properties & Construction
- Non-repudiation
- DSS and DSA (Digital Signature Algorithms)

Part 4
Key Distribution and User Authentication

- PKI
  - Meaning of CA and RA, and root
  - PKI models/trust structures
  - X.509 Certificates
    - Know meaning: binding id+key
    - No need to know all elements of certificates
- User Authentication
  - Methods
    - Tokens
    - Passwords: entropy, usability, trade-off
    - Biometrics and modalities

Part 5
Transport Layer Security

- SSL/TLS
  - Protocol family
  - Security services
- SSH
  - Protocol family
  - Security services

Part 6
Mobile Network Security

- 2G (GSM), 3G (UMTS), 4G (LTE) technologies
- 2G (GSM) Security
  - Vulnerabilities and attacks
- 3G (UMTS) Security
  - How 2G vulnerabilities were fixed

Part 7
Wireless Network Security

- IEEE 802.11 WLAN
  - Architecture
- WLAN Security and Access Control
  - WEP
  - WPA & WPA2

Part 8
Semantics in mobile networks

- Security challenges
  - – Person: electronic traces, privacy, anonymity
  - – Things (IoT): security, privacy, dependability
- Policies
  - – User, Company, Service providers
  - – Authorities

Part 9
IP Security

- IPSec
  - Security Services and modes
  - VPN architectures
- IPSec Key management

Part 10
DNSSEC

- DNS security challenge
- DNSSEC Architecture
- Trust model
- Root signing ceremony
- Applications of DNSSEC

Part 11
Firewalls + IDS

- Firewalls
  - – Types, advantages & disadvantages
  - – Architectures, TLS proxy

- IDS
  - – Types, advantages & disadvantages

- IPS = Firewalls + IDS

Part 12
Cyber Security

- Purpose of cyber security networks
- Beer network of Trust
- Role of
  - Malware analysis
  - PEN testing
  - Forensics
  - Law enforcement authorities

Exam

- Similar in style to previous exam
- 10 questions, from all parts, except P8 and P12
- Answer 8 of the 10 questions
  - each worth 10 points, thus max total of 80
- 4 hours working time
  - Typically use approx. 20 minutes for each question
  - Leaves 60+ minutes to check and review
- Write concisely
  - Straight to the point, brief answers
- Good Luck ☺