INF3510 Information Security
University of Oslo
Spring 2011

Review

Audun Jøsang

Lecture 1:
Intro and Fundamental Security Concepts

- Understand information security properties/services
  - CIA
  - Authentication
  - Non-repudiation
- Difference between security service and mechanism
  - See e.g. X.800 Table 1
- Understand authorization and the confusion around its definition
  - The importance of having a security policy

Lecture 2:
Security Management + physical + human factor

- ISO/IEC 27001
  - Title & Purpose
  - Structure of ISMS
- ISO/IEC 27002
  - Title & Purpose
  - Know titles of 11 objectives
- Know components of information security:
  - technical, physical, procedural

Lecture 3:
Risk Managemet and Business Continuity

- Risk management principles
  - Risk : (Threat + Vulnerability = Likelihood), Impact/Consequence
  - Process – main steps from PDCA
  - Qualitative v. quantitative
- Business Continuity Planning principles
  - BIA, downtime, options for alternative sites

Lecture 4: Computer Security

- Processor architecture and privilege levels
- Virtual machines
  - Platform model and security advantages
- Security Evaluation
  - Main principles of TCSEC and Common Criteria

Lecture 5: Cryptography

- Symmetric ciphers
- Asymmetric ciphers
- Hash functions
- Message Authentication Code
- Digital signature
- Diffie-Hellmann key exchange

Lecture 6: Key Management and PKI

- NIST SP800-57 Key Management
  - Key State transition diagram
    - Know the different states
  - Meaning of “protection” and “processing”
  - Importance of cryptoperiods
- 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

Lecture 7: Authentication

- Difference between message authentication and user authentication
- User authentication methods
- Biometrics
- Passwords
  - Entropy, usability, trade-off
- Non-repudiation
  - digital signature
  - WYSIWYS property

Lecture 8:
Identity and Access Management

- Meaning of entity/identity/identifier/digital identity
- Identity management models
  - Management of user identities
  - Management of Service Provider identities
- Meaning of mandatory/discretionary AC
- Security models
  - Bell - La Padula
  - Brewer - Nash / Chinese Wall
  - RBAC (Role Based Access Control)
    - Be able to draw and explain the “RBAC-beast”

Lecture 9: Communication Security

- Understand how communication security services can be placed on different layers
  - See e.g. X.800 Table 2.
- Meaning of authentication protocol
- HTTP Basic Authentication / Digest Authentication
- SSL/TLS
- IPSec

Lecture 10: Perimeter Security

- Firewall types
  - Strengths and weaknesses
- Intrusion detection system types
  - Strengths and weaknesses
- WLAN Security
  - Phases of connecting and disconnecting

Lecture 11: Digital Forensics

- Main steps digital forensics
- Chain of Custody
- Order of volatility

Lecture 12:
Privacy and Regulatory Requirements

- History of privacy
- OECD principles
  - Name and explain some principles
- Title of important privacy laws and regulations
- Conflict with privacy

Lecture 13:
Application Security and Operations Security

- Buffer Overflow
- SQL Injection
- Cross-Site Scripting
- Malware and botnets

Final Exam

- Partially based on workshop questions.
  - Many workshop questions are not suitable as exam questions
- 10 questions, each worth 10%
- 4 hours working time
  - Approx. 20 minutes for each question
  - Leaves 40 minutes to check and review
- Write concisely
  - Straight to the point
  - Briefly

- Good Luck ☺