INF3510 Information Security
University of Oslo
Spring 2012

Review

Audun Jøsang

Lecture 1:
Intro and Fundamental Security Concepts

- Understand information security properties/services
  - CIA
  - User Authentication
  - Data Authentication and 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 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, Semi-Quantitative, Quantitative Risk Estimation
  - Know main elements of ISO 27005 Risk Management Process
- Business Continuity Planning principles
  - Difference between BCP and Risk Management
  - Principle for BIA,
  - downtime, options for alternative sites

Lecture 4: Computer Security

- Processor architecture and privilege levels
- Virtual machines
  - Architectures with advantages/disadvantages
  - Protection Ring Options
- Security Evaluation
  - Difference between TCSEC and Common Criteria
  - Terms of Common Criteria

Lecture 5: Cryptography

- Symmetric ciphers
  - Parameters (block and key size) of DES and AES
  - Names of modes of operation
  - Details of CBC and CTR mode
- Hash functions
- Message Authentication Code
- Asymmetric ciphers
  - Digital signature
- Diffie-Hellmann key exchange
- Hybrid Crypto systems

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:
User Authentication

- Difference between data authentication and user authentication
- User authentication methods
- HTTP Digest Authentication
- Biometrics systems principles and trade-offs
- E-Authentication Frameworks
  - Levels of Norwegian e-authentication framework
  - Practical solutions

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
  - Silo model / Federated model
- Meaning of MAC and DAC
  - Bell - La Padula
- OpenID
- OAuth

Lecture 9: Communication Security

- Understand how communication security services can be placed on different layers
  - See e.g. X.800 Table 2.
- SSL/TLS
  - Protocols
  - Key establishment
- IPSec
  - Options

Lecture 10: Perimeter Security

- Firewall types
  - Strengths and weaknesses
  - Principles of application gateway proxies including TLS proxies
- Intrusion detection system types
  - Strengths and weaknesses

Lecture 11: Digital Forensics

- Main steps digital forensics
- Chain of Custody
- Order of volatility
- Live acquisition vs. post-mortem acquisition

Lecture 12:
Application Security and Operations Security

- SQL Injection
- Cross-Site Scripting
- Malware and botnets
- Patching procedures
- Back-up procedures
- Data destruction principles

Lecture 13:
Privacy and Regulatory Requirements

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

Marking Scheme

- Approximate weighing:
  - Home exam: 40%,
  - Written exam 60%
- You must pass both exams to pass the course.
  - A student who scores 100% on the home exam, but only 30% on the written exam will fail the course.
  - A student who scores 100% on the home exam and 40% on the written exam normally gets 64% which corresponds to mark C.
- Thus, it is important that you don’t fail the written exam!

Written 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 ☺