INF3510 Information Security
University of Oslo
Spring 2010

Lecture 15

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: Cryptography

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

Lecture 3: 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 4: Authentication

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

Lecture 5:
Security Models and Access Control

- 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”
  - Also have general/high level (not detailed) knowledge of the Clark-Wilson and the Biba models

Lecture 6: 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 7:
Identity and Access Management

- Meaning of entity/identity/identifier/digital identity
- Identity management models
  - Management of user identities
  - Management of Service Provider identities
- Zooko's triangle
- Federation
- SAML

Lecture 8: Perimeter Security

- Firewall types
  - Strengths and weaknesses
- Intrusion detection system types
  - Strengths and weaknesses

Lecture 9:
Physical Security and the Human Factor

- Environmental Security
- CPTED
- Physical Access Control

- Social Engineering Attacks and Defences

Lecture 10:
Computer Security and Trusted Systems

- Microprocessor security protection rings
- Trusted Computing principles
- TPM (Trusted Platform Module)
  - Understand that it's new technology with currently few practical applications
  - Understand theoretical possibilities and practical limitations

Lecture 11:
Security Management and Security Development

- ISO/IEC 27001
  - Purpose
  - Structure of ISMS
- ISO/IEC 27002
  - Purpose
  - Know titles of 11 objectives
- Secure Development Lifecycle
  - structure

Lecture 12:
Risk Managemet and Business Continuity

- Risk management principles
  - Risk – Threat – Vulnerability
  - Process – main steps from SP800-30
- Business Continuity Planning principles
  - BIA, downtime, options for alternative sites

Lecture 13:
Application Security and Trust Management

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

- Difference between soft security and traditional info sec
- Purpose of trust and reputation systems

Lecture 14:
Privacy and Computer Forensics

- History of privacy
- OECD principles
  - Name principles
- Privacy problems in Web 2.0

- Meaning of computer forensics
- 4 main steps of computer forensics

Final Exam

- Largely based on workshop questions.
- 10 questions, each worth 10%
- 3 hours working time
  - Approx. 15 minutes for each question
  - Leaves 30 minutes to check and review
- Write concisely
  - Straight to the point
  - Briefly

- Good Luck ☺