INF3510 Information Security
University of Oslo
Spring 2014

Review

Audun Jøsang

General Security Concepts

- Understand information security properties/services
  - CIA (Confidentiality, Integrity and Availability) definitions
  - Definition of information security (ISO27001)
- Understand meaning of other security services
  - authentication,
  - non-repudiation,
  - access control
- Understand 2 interpretations of authorization
- Perspectives on information protection:
  - During storage, transmission, processing
  - Preventive, detective, corrective

Information Security Management

- Know ISO27K Series
- ISO/IEC 27001
  - Title & Purpose
- ISO/IEC 27002
  - Title & Purpose
- NIST SP800 series: know that it is alternative to ISO27K
- Difference between security control and security service
- Categories of security controls
  - technical, physical, administrative
- Principle for selecting security controls
  - Based on risk analysis, proportionality

Computer Security

- TCB and Reference Monitor
  - Definition and requirements
- Protection rings in microprocessor architecture
- Memory protection principles
  - No-Execute, ASLR, Stack Cookies
- Virtual machines
  - Understand hypervisor, VM/Guest OS, Host OS
  - Type 1 and Type 2 virtualisation architecture
  - Protection Ring assignment to hypervisor, Host, VM, Apps etc.

Cryptography

- Symmetric ciphers
  - Parameters (block and key size) of DES and AES
- Principles of hash functions
  - Hash sizes of main functions: MD5, SHA-1, SHA-2
- MAC (Message Authentication Code)
  - Basic principle: keyed hash function
- Asymmetric ciphers
  - Understand usage of keys in encryption and digital signature
  - Digital signature, understand practical usage combined with hash
- Diffie-Hellmann key exchange
- Hybrid Crypto systems

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 – Public-Key Infrastructure
  - Meaning of CA and RA, and root
  - Purpose of self-signed certificates
  - PKI models/trust structures
  - X.509 Certificates
    - Know meaning: binding id+key
    - No need to know all elements of certificates

User Authentication

- Categories of credentials for user authentication
  - Knowledge, Ownership, Inherence
- Password security, hashing, salting
- Biometrics systems
  - Criteria for biometric characteristics
- E-Government user authentication frameworks
  - Assurance levels
  - Requirement classes
    - Authentication Method strength
    - Credential Management Assurance
    - Registration Assurance

Identity and Access Management

- Meaning of entity/identity/identifier/digital identity
- Identity management models
  - Silo model / Federated model
- Facebook and FEIDE federation scenarios
- Meaning and principle of MAC, DAC, RBAC and ABAC
- Role of XACML in distributed access control architectures

Communication Security

- SSL/TLS
  - Protocols
  - Key establishment
  - Usage of keys
  - option for exchanging session key using Diffie-Hellmann
- Meaningful server authentication
  - Properties of names
  - Zooko's triangle
  - Petname systems
- IPSec
  - Options

Perimeter Security

- Firewall types
  - Strengths and weaknesses
  - Principles of application gateway proxies
  - TLS/SSL stripping
- Intrusion detection system types
  - Strengths and weaknesses

Application Security

- What is OWASP and the top 10 vulnerabilities list
  - No need to know all 10
- Main vulnerabilities
  - SQL Injection
  - XSS - Cross-Site Scripting
  - CSRF – Cross-Site Request Forgery
  - Broken authentication and session management
- Malware and botnets
- Patching procedures
- Back-up procedures
- Data destruction principles

Forensics, Risk Management and BCP

- The written exam has limited focus on:
  - Forensics
  - Risk Management
  - BCP (Business Continuity Planning)
- Some elements of the above topics might be superficially relevant for questions on the written exam, but the topics need not be studied in detail for the exam.

Marking Scheme

- Approximate weighing:
  - Home exam: 40%,
  - Written exam 60%
- You must pass both exams to pass the course.
  - Score100% on home exam, and score 30% on written exam normally gives mark F.
  - Score 100% on home exam and score 40% on written exam $\rightarrow$ combined score 64% which normally corresponds to mark C.
  - Written exam shows what you have learnt during course
    - Not strictly needed to score $\geq$ 40% on home exam to pass
- Thus, it is important that you don't fail the written exam!

Written Exam

- Same style as 2012 written exam
- Sometimes 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 ☺