INF3510 Information Security
University of Oslo
Spring 2015

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 security controls:
  - 3 categories of security controls: Physical, Technical, Administr.
  - Security controls during storage, transmission, processing.
  - Preventive, detective, corrective security controls.

Security Management and Human Factors

- Know what ISO27K series is about
- ISO/IEC 27001
  - Title & Purpose
- ISO/IEC 27002
  - Title & Purpose
- Perspectives on personnel integrity:
  - How to strengthen staff integrity,
  - When is support and check of staff integrity important
- Perspectives on personnel as security protection
  - What is a social engineering attack
  - Understand balance between being too naïve and too paranoid

Risk Management

- Understand the factors that contribute to risk
  - Attacker/threat agent, vulnerability, impact
  - And how they are related: Diagram
- Understand factors that contribute to attacker strength
  - Competence/Capacity and Motivation
- Threat scenario modelling:
  - Attacker centric, architecture centric, and asset centric
- Flow chart for Risk Management Process in ISO27005
- Models for risk level estimation:
  - Qualitative
  - Quantitative

Computer Security

- Approaches for strengthening computer platform security
- Protection rings in microprocessor architecture
- 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.
- Principle of buffer overflow, and protection mechanisms
- Security functions supported by TPM
- Security function supported by UEFI

Cryptography

- Symmetric ciphers
  - Parameters (block and key size) of 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

- Key distribution problem. Understand requirements for
  - Number of keys i.c.o. symmetric and asymmetric keys.
  - Number of key distributions with and without PKI
  - Type of protection needed /confidentiality or integrity)
- 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
- IAM phases and steps: diagram.
- Identity management models
  - Silo model / Federated model
  - Advantages and disadvantages of silo and federated models
- Facebook Connect federation scenario
- Meaning and principle of MAC, DAC, RBAC and ABAC

Communication Security

- TLS/SSL
  - Protocols
  - Key establishment
  - TLS/SSL stripping attack
- HSTS: Http Strict Transport Security
  - How it works
  - Policy enforcement
- IPSec
  - Options

Perimeter Security

- Firewall types
  - Strengths and weaknesses
  - Principles of application gateway proxies
  - TLS/SSL stripping
- TLS/SSL inspection in firewalls
  - How it works
  - How to know when TSL/SSL stripping is used

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
- Secure Software development
  - Microsoft SDL
  - Secure agile software development
  - Software fuzzing

Forensics and BCP

- The written exam has limited focus on:
  - Forensics
  - 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: approximately 0.4
  - Written exam: approximately 0.6
- You must pass both exams to pass the course.
  - E.g. score 100% on home-ex. and score 50% on written-ex. → total score 70% which normally gives mark C.
  - Score100% on home exam, and score 30% on written exam normally gives mark F.
  - Written exam shows what you have learnt during course
- It is important that you don't fail the written exam!
  - Not strictly needed to score ≥ 40% on home exam to pass
  - But score around 40% on written exam carries heavy weight

Written Exam

- Same style as 2014 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 ☺