CSE413 – Security of Information Systems 2020

PhD Furkan Gözükara, Toros University

https://github.com/FurkanGozukara/Security-of-Information-Systems-CSE413-2020

Lecture 13

Review Recap

Composed from Prof. Audun Jøsang & Nils Gruschka, University of Oslo, Information Security 2018 Lectures

Source : https://www.uio.no/studier/emner/matnat/ifi/INF3510/v18/lectures/

General Security Concepts

- Understand information security properties/services
  - Definition of information security (ISO27000)
  - Definitions of CIA (Confidentiality, Integrity and Availability) services
  - Privacy and GDPR
- Meaning of, and difference between other security concepts
  - authentication
  - non-repudiation
  - access control
  - authorization
- Perspectives on security controls:
  - 3 categories of security controls: physical, technical, administrative
  - Preventive, detective, corrective security controls.
  - Security controls during storage, transmission, processing.

Security Management

- Know what ISO27K series is about
- ISO27000, ISO27001& ISO27002
  - Title and purpose of each standard
- Elements of ISMS (cycle)

Cryptography

- Hash functions and symmetric ciphers
  - Status/usage of SHA-1, SHA-2 and SHA-3
  - Parameters (block and key size) of AES
- 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
- Hybrid Crypto systems
- Threat to classical crypto from quantum computing

Key Management

- Key distribution problem. Understand requirements for
  - Key distributions with and without PKI
  - Type of protection needed (confidentiality or integrity)
- Certificates and PKI:
  - Ideas, content, issuing, managing
  - PKI trust model
  - Revocation: CRL, OCSP
  - CAA, CT

Risk Management

- Understand the factors that contribute to risk
  - Attacker/threat agent, vulnerability, impact
  - And how they are related: Understand diagram
  - Risk management process (ISO 27005)
- Threat scenario modelling:
  - Attacker centric, architecture centric, and asset centric
- Models for risk level estimation:
  - Qualitative
  - Quantitative
- Risk treatment strategies
  - Reduce, share, retain/accept, avoid

Computer Security

- Protection rings in microprocessor architecture
- Virtual machines
  - Understand hypervisor, VM/guest OS, host OS
  - Type 1 and type 2 virtualization architecture
  - Protection ring assignment to hypervisor, host, VM, apps etc.
- Security advantages of running VMs
- Boot security (UEFI)
- Security functions supported by TPM

Incident Response and Forensics

- Elements if IR (Incident Response) policy
- Types of IR teams: permanent, virtual, hybrid
- Phases of IR

User Authentication

- Types of authentication tokens
  - Clock-based, counter-based, challenge-response
- Password security, hashing, salting
- Biometrics systems
  - Criteria for biometric characteristics
- E-Government user authentication frameworks
  - Assurance levels
  - eIDAS
  - Assurance requirement classes
    - Authentication Method strength
    - Credential Management Assurance
    - Registration Assurance

Identity and Access Management

- Meaning of entity/identity/identifier/digital identity
- IAM phases (configuration and operation) with steps.
- Identity management models
  - Silo model / federated model
  - Advantages and disadvantages of silo and federated models
- Centralized/distributed federation models
- Facebook Connect federation scenario
- Meaning and principle of MAC, DAC, RBAC and ABAC

Communication Security

- TLS
  - Protocols
  - Security services
  - Key establishment (RSA / DH)
  - TLS stripping attack / HSTS
- IPSec
  - Modes (Tunnel, Transport)
  - Key exchange
  - Tor

Perimeter Security

- Firewall types
  - Principles of different firewalls
  - Strengths and weaknesses
- Location of entities: DMZ or production network
- TLS inspection in firewalls
- Intrusion detection principles

Application Security

- Malware types
- What is OWASP and the top 10 vulnerabilities list
  - No need to know all 10
- Explain main vulnerabilities
  - SQL Injection
  - XSS - Cross-Site Scripting
  - Broken authentication and session management
- Secure Software development
  - Security by design
  - Secure agile software development