IT-Security

Summary

Prof. Dr.-Ing. Ulrike Meyer

Chapter 1: Introduction

- **Security goals**
  - Confidentiality, Integrity, Availability
- **Examples for attacks against these goals**
- **Definition of security services and security mechanisms**
  - Which of them aim at prevention, detection, or deterrence
- **Categorization of attackers according to**
  - Skills
  - Knowledge on and access to target
  - Computational resources
  - Motivation

Chapter 2: Symmetric Encryption (1)

- **Definition of an encryption scheme**
- **Kerckhoffs' principle**
- **Examples for classical ciphers**
  - Caesar cipher (easily breakable with brute force due to short key length)
  - Monoalphabetic substitution cipher (easily breakable with frequency analysis)
- **Perfect Secrecy**
  - Shannon's theorem
  - One-time pad and perfect secrecy of the one-time pad
  - Practical problems with the one-time pad
- **Computational Security**

Chapter 2: Symmetric Encryption (2)

- **Modeling attacks against ciphers**
  - W.r.t power of the attack (ciphertext-only attack, known-plaintext attack…)
  - W.r.t. attack result ((partial) plaintext recovery, (partial) key recovery)
  - W.r.t technique used (brute force, time-memory trade-off, differential, algebraic..)
- **Block ciphers versus stream ciphers**
  - How are they defined
  - What's the problem with key stream re-use when a stream cipher is used
- **Basic facts on DES, 2DES, 3DES, AES**
  - Key sizes, block sizes, attacks
  - Meet-in-the-middle attack on 2DES

Chapter 2: Symmetric Encryption (3)

- **Modes of encryption (ECB, CBC, CFB, OFB, CTR, GCM)**
  - Encryption / decryption, properties
- **Stream ciphers and block ciphers alone do not provide integrity**
  - Understand that plaintext encrypted with a stream cipher can be changed by anyone

Chapter 3: Integrity (1)

- **Definitions for**
  - hash function, cryptographic hash function, pre-image resistance, 2nd pre-image resistance, collision resistance, relations between the properties
- **Complexity of brute force attacks against ideal hash functions**
- **Basic facts on MD-5, SHA-1, SHA-2, SHA-3**
  - Length of hash value, broken / not broken (yet ;-))
- **Definition message authentication code**
- **HMAC, CMAC constructions in detail**
  - Including advantage of HMAC over other constructions
  - Including advantage of CMAC over CBC-MAC

Chapter 3: Integrity (2)

- Methods for replay protection
- Ways to combine integrity protection and encryption
- Galois Counter Mode (GCM)

Chapter 4: Asymmetric Cryptography (1)

- **RSA key generation, encryption, decryption in detail**
  - Extended Euclidian algorithm
  - Including security proofs and why we need Optimal Asymmetric Encryption Padding
  - Details on how OAEP works and adds semantic security to RSA
- **Symmetric versus asymmetric encryption**
- **RSA Backdoors general idea and examples**
- **Definition of digital signatures**
  - Details of RSA-Signatures (with hashing)
  - Why we hash messages before signing

Chapter 4: Asymmetric Cryptography (2)

- **Type of attacks against signature schemes**
  - wrt power of attacker (key-only etc…)
  - wrt result of the attack, e.g. total break, existential forgery,...
- **Type of attacks against signature schemes**
  - wrt power of attacker (key-only etc…)
  - wrt result of the attack, e.g. total break, existential forgery,...
- **Comparison of MACs and digital signatures**
- **Details on key generation, signature generation/verification in DSS**
- **Details on Diffie-Hellmann key agreement and MitM against DH**

Chapter 5: Authentication and Key Agreement (1)

- **Definition of entity authentication**
  - Correctness, resistance against transfer, impersonation resistance
  - mutual vs. unilateral authentication
- **Example Building Blocks for unilateral and mutual authentication**
  - With time stamps, with random challenges, with signatures, with MACs
  - Understand the problem of reflection attacks in this context
- **Definiton of the properties of session key establishment protocols**
  - key agreement vs. key transport protocols
  - authenticated key establishement
  - explicit key authentication, implicit key authenticaiton, key freshness, perfect forward secrecy, known key attacks

Chapter 5: Authentication and Key Agreement (2)

- **Analyze key establishment protocols w.r.t. these properties**
- **Diffie-Hellmann,**
  - Man-in-the middle attack in DH, implicit key authentication in Diffie-Hellmann, authenticated DH
- **Trusted Third Parties in Key Establishment**
  - Main idea of Key distribution center, example protocol
  - Main idea of Certification authorities,
    - Example authenticated DH with certificates
    - Content of a certificate
    - Certificate verification
    - Certificate revocation
    - Chains of certificates

Chapter 5: Authentication and Key Agreement (3)

- **Typical password-based authentication between client and server**
  - Relation between randomly selected passwords and effective key length
  - Password based user authentication by a server
    - Advantage storing cryptographic hashes of passwords over plaintext / encrypted storage
  - Purpose of salting passwords
  - Dictionary attacks on password files
- **Typical password-based authentication between two peers**
  - MAC-keys generated from password
  - Vulnerability against offline password cracking

Chapter 6: Network Security Protocols (1)

- **IPSec**
  - Transport mode vs tunnel mode
  - Security services offered by ESP and AH
    - What does an IP packet look like that is protected with ESP/AH in tunnel/transport mode
    - Which part of the packet is encrypted/integrity protected in ESP/AH in tunnel/transport mode
  - Fields in AH and ESP protocol headers / ESP trailer
  - Replay protection in ESP and AH
  - Main content of SAs and SA selectors
  - Inbound / outbound processing overview

Chapter 6: Network Security Protocols (2)

- **IPSec**
  - IKE v2 protocol details
    - In particular: how do initiator and responder authenticate each other?
    - What's the basis for the key agreement?
    - How are security algorithms for IKE itself / for ESP and/or AH negotiated?
- **TLS 1.3**
  - Understand the details of the handshake protocol
    - Different options to authenticate the handshake (mutual or unilateral authenticaiton with signatures, PSK-based authentication only, DH with PSK)
    - Properties these different options have
- **Comparison between IPSec and TLS including main use cases**

Chapter 7: Email, DNS, SSH (1)

- **Email Security**
  - End-to-end vs hop-by-hop protection of email
  - End-to-end security goals
  - Basic principle used in PGP and S/MIME (hybrid encryption, signatures for non-repudiation...)
  - Web of trust in PGP
    - Introducer Trust, certificate trust, key legitimacy
  - Main ideas of DKIM, SPF, and DMARC

Chapter 7: Email, DNS, SSH (2)

- **DNS**
  - General operation of DNS
    - Concept and types of resource records
    - Recursive and interative queries
    - Purpose of caching
  - Security issues of DNS
    - Authenticity of resource records
      - cache poisoning
    - Confidentiality
  - DNSSec
    - New types of resource records
    - Keys used in DNSSec and how they are distributed and authenticated

Chapter 7: Email, DNS, SSH (3)

- **SSH**
  - Details on the transport layer protocol
    - Including the mandatory key exchange method
    - Including algorithm negotiation
  - User authentication protocol
    - Including the details on the three user authentication protocols (public key, password, host-based)

Chapter 8: Denial of Service Attacks

- **Classification of DoS attacks w.r.t. the type of resource they target**
  - network bandwith, system resources, appplication resources
  - Example attack for each type
    - Flodding with ICMP echo requests, SYN Flooding, HTTP Flood
- **Source address spoofing**
- **DDoS attacks**
- **Principle of a reflection attack**
  - Amplification attack as a subtype of reflection attacks
- **Preventive defense mechanisms**

Chapter 9: Access Control, Firewalls, IDSs (1)

- **Access Control**
  - Discretionary vs. Mandatory access control
  - Access control subjects, objects rights
  - Access control matrices and Access control lists
  - How do different Discretionary access control systems differ
    - Who can change acl associated with an object
    - How ACLs apply to privileged user
    - Support of groups and wildcards
    - Handling of contradictory permissions
    - Default settings

Chapter 9: Access Control, Firewalls, IDSs (2)

- **Access Control**
  - Access Control in UNIX file systems
    - rights
    - changing rights
    - meaning of rights on directories
    - user ids
  - Roll based Access Control
    - Main idea
  - Attribute based access control
    - Main idea

Chapter 9: Access Control, Firewalls, IDSs (3)

- **Firewalls**
  - Packet filters
  - Firewall policy
    - First match policy
    - Comprehensiveness of a fire wall policy
  - Interpret rules in a simple packet filtering policy
    - Find redundant rules
    - Find (half-)shadowing rules
    - Combine rules
  - Stateful firewall and why we need them
  - What is a DMZ

Chapter 9: Access Control, Firewalls, IDSs (4)

- **Intrusion Detection Systems**
  - Components of an IDS
  - Basic assumption underlying any iDS
  - Definition of detection rate and false alarm rate
  - Base rate fallacy problem
  - Anomaly detection vs. misuse (signature based) detection
  - Host based vs. network-based intrusion detection
  - Inline vs. passive network-based intrusion detection

Chapter 10

- **Types of Malware w.r.t. spreading**
  - worms, viruses, trojans
- **Botnets**
  - Command and Control Infrastructures
  - DGAs
- **Buffer Overflows**
  - Basic principle
  - Explain on an example if given a vulnerable piece of code
  - Types of defenses
- **Typical malware payloads**

Good Luck!

… and don’t forget to look at the exercises and e-tests as well!!!!