Computer Security

Reagan Shirk

October 15, 2020

Midterm Review

Introduction to Cryptography

- Basic security concepts: confidentiality, integrity, availability
- Introduction to Cryptography
  - Secret key cryptography
    - Sender and receiver share the same key
    - Applications: communication over insecure channel, secure storage, authentication, integrity check
  - Hash function: map a message of arbitrary length to a fixed-length short message
    - Desirable properties: performance, one-way, weak collision free, strong collision free

DES

- DES is festiel, AES is not
- Parameters:
  - Block size (input/output 64 bits)
  - Key size (56 bits)
  - Number of rounds (16)
  - Subkey generalization algorithm
  - Round function

Modes of Block Cipher Operations

- ECB - electronic code block
- CBC - cipher block chaining
- OFB - output feedback
- CFB - cipher feedback
- CTR - counter

Double/Triple DES

- Understand how it works

Meet in the Middle Attack

Hash Functions and Applications

MD5

SHA