EECS565 Intro to Computer and Information Security

Exam 3 Review

Professor Fengjun Li

Exam 3

- Time: Thursday, April 27, 4:00 – 5:15pm
- Location: G415

- You can bring one cheat sheet to the exam (letter-size, double-sided)

Exam 3

- Format
  - Multiple Choice
  - T/F **with justification**
  - Short Answer
    - Encryption/decryption, security analysis, etc.

Exam 3

- Coverage: Lecture 19 to Lecture 22
  - Network security (about 60%)
  - Firewall and IDS (about 40%)
  - ~~Web security (20%)~~

Network Security

- Network Vulnerabilities
  - What makes network vulnerable?
- Attacks
  - Packet sniffing
  - Spoofing: SYN spoofing, how would anti-spoofing help?
  - Flooding: UDP flood, SYN flood
  - Smurf attack
  - DoS attacks: reflection, amplification

Network Security

- Controls
  - Design: separation, single point of failure, redundancy, recovery, encryption (link vs. end-to-end)
  - Protocols: SSL/TLS
    - Provides additional security services
    - From TLS 1.2 to TLS1.3
  - Protocols: IPsec
    - Transport Mode vs. Tunnel Mode
    - AH vs. ESP

Firewall and IDS

- Firewall
  - Types of firewalls: strengths and limitations
  - What can be protected, and what cannot?
- IDS
  - Fundamental assumption: intruder behavior differs from legitimate users
  - Host-based IDS vs. Network IDS
  - Signature-based IDS vs. anomaly detection IDS
  - Detection quality, Bayesian detection rate, and the base rate fallacy