CSCI 454/554 Computer and Network Security

Final Exam Review

Topics covered by Final

- Topic before Midterm 20%
- Topic after Midterm 80%

- Date: 05/11/2016 2:00pm – 5:00pm
- Place: the same classroom

Open notes/close book exam

No laptop/tablet/smartphones etc.

Topics covered by MidTerm

- Topic 1. Basic Concepts
- Topic 2. Basic Cryptography
- Topic 3. Secret Key Cryptography
- Topic 4. Hash Functions
- Topic 5. Basic Number Theory and Public Key Cryptography

Topics covered after MidTerm

- Topic 6. Identification and Authentication
- Topic 7. Trusted Intermediaries
- Topics 8.1-2 IPsec and IKE
- Topic 8.3 SSL/TLS
- Topic 8.4 Firewalls and IDS
- Topic 8.5 Malicious Logic

Topic 6. Identification and Authentication

- Be able to explain the concepts of authentication and identification. Be able to give examples of authentication mechanisms.
- Be able to explain general approaches for authentication in large networks using trusted intermediaries (KDC and CA), and explain what are KDC, CA, and CRL.
- Be able to explain the general basis of user authentication (what the user knows, where the user can be reached, what the user is, and what the user has).

Topic 6. Identification and Authentication (cont'd)

- Be able to explain what is password based user authentication, threats to password based authentication, how to store user passwords in computer systems.
- Be able to explain dictionary attacks (both online and offline). Be able to describe the password salt mechanism used to mitigate dictionary attacks and its effectiveness against online and offline dictionary attacks.
- Be able to explain the one-time password mechanisms, including S/Key and time synchronized authentication tokens.
- Be able to explain biometrics based user authentication and give examples of such approaches. Be able to explain the key metrics for biometrics authentication, including false positives and false negatives.

Topic 6. Identification and Authentication (cont’d)

- Be able to explain typical attacks against authentication protocols, including eavesdropping, deleting, forging, modifying, replaying, reflection attacks, and delaying attacks. Be able to illustrate the above attacks using examples. Be able to describe defenses against the above attacks.
- Be able to describe the Needham-Schroeder protocol. Be able to explain the "old-key attack" against the Needham-Schroeder protocol and the three countermeasures (timestamp, expanded N-S, and Ottay-Ree protocol).

Topic 7. Trusted Intermediaries

- Be able to explain the general way KDC based trusted intermediaries are used.
- Be able to describe the Kerberos V4 protocol, and explain which parts of the protocol help achieve (1) centralized authentication service, (2) protection of user passwords, and (3) anti-replay attack capability.
- Be able to describe Kerberos inter-realm authentication.

Topic 7. Trusted Intermediaries (cont'd)

- Be able to explain the general way PKI is used.
- Be able to explain what is a CA, and describe the ways that multiple CAs are organized in large networks.
- Be able to explain what is CRL and delta CRL.

Topics 8.1-2 IPsec and IKE

- Be able to describe the IPsec architecture, IPsec Security Association (SA), SA bundle, Security Parameter Index (SPI). Explain the purpose of Security Policy Database (SPD), Secure Association Database (SAD), and Internet Key Exchange (IKE) modules in the IPsec architecture.
- Be able to describe the IPsec Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols as well as Tunnel and Transport modes.
- Be able to describe the difference in the authentication capabilities provided by AH and ESP.

Topics 8.1-2 IPsec and IKE (cont'd)

- Be able to describe the anti-replay feature in IPsec ESP.
- Be able to explain the IPsec outbound processing and inbound processing.
- Be able to explain the security principles for Internet key management, particularly the property of Perfect Forward Secrecy (PFS). Be able to describe the (only known) way to achieve PFS (ephemeral D-H).
- Be able to describe the separation of key establishment and key management in Internet key management.
- Be able to describe the SKIP protocol for sessionless IPsec key management.

Topics 8.1-2 IPsec and IKE (cont'd)

- Be able to describe the Oakley key establishment protocol and explain the mechanisms to defeat (1) resource clogging attacks (i.e., Cookie), (2) replay attacks (i.e., nonce), and (3) man-in-the-middle attacks (i.e., with authentication).
- Be able to explain high-level issues of ISAKMP protocol, including the protocol structure (2 phases), protocol message construction (i.e., with different types of payloads), and exchange types. Be able to explain the following ISAKMP exchanges: basic exchange, ID protection exchange, authentication only exchange, aggressive exchange, and informational exchange.

Topics 8.1-2 IPsec and IKE (cont'd)

- Be able to explain the IKE protocol, including the phase 1 exchanges using (1) signature authentication, (2) authentication with public key encryption, (3) authentication with revised public key encryption, and (4) authentication with pre-shared key in both main mode and aggressive mode. In each case, be able to explain how authentication is achieved, how PFS is achieved, and how ID protection is achieved.

Topic 8.3 SSL/TLS

- Be able to explain the basic facts of SSL/TLS, including its protocol architecture, its subprotocols and their objectives, basic SSL functionalities (authentication, secrecy, compression, generation and distribution of keys, security parameter negotiation), and SSL connection and session.
- Be able to describe the SSL record protocol operations (outbound and inbound).
- Be able to describe the SSL handshake protocol operations (4 phases), the generation of master secret and cryptographic parameters.

Topic 8.3 SSL/TLS (cont'd)

- Be able to describe the change cipher spec protocol, and explain how the cryptographic parameters negotiated in the handshake protocol take effect through the change cipher spec protocol.
- Be able to give examles of application protocols that run on top of SSL (https, smtps, nntps, ftps, pop3s, imaps).

Topic 8.4 Firewalls and IDS

- Be able to explain the following concepts:
  - firewall
  - DMZ
  - firewall capabilities, including logging traffic, network address translation, encryption/decryption, application payload transformation
  - limitations of firewalls
- Be able to explain basic firewall technologies
  - packet filters
  - session filters
  - application-level proxies
  - circuit level proxies

Topic 8.4 Firewalls and IDS (cont'd)

- Be able to explain the following basic concepts on IDS
  - Anomaly detection
  - misuse detection (or signature-based detection, rule-based detection)
  - False positive rate
  - False negative rate
  - Host-based IDS
  - Network-based IDS
  - Base rate fallacy

Topic 8.5 Malicious Logic

- Be able to explain the following basic idea of malicious logic
  - Trojan horses
  - Computer viruses
  - Worms
  - Rabbits and bacteria
  - Logic bombs
  - Trapdoor
  - DDoS
- Be able to explain the basic defenses against malicious logic