CS494/594 Computer and Network Security

Review for Midterm Exam

1. Midterm exam will be closed-book, closed-note and 2-hour. One letter-sized double-sided aid sheet is allowed. There will be 10 to 12 questions and simple calculation will be required. The type of answers I am expecting is mostly descriptive. You may want to draw figures for some questions to help illustrate your answer.

2. Generally speaking, anything that has been covered in the lectures up to Chapter 11 (Kaufman) may be tested in the exam.

More specifically, the following topics are considered fundamentals in this course. You are expected to know them by heart. >90% of points will be from the following topics.

- Introduction to Computer Security: (Lecture 1)
  - Understand the concept of the three aspects of security: security attacks (passive/active attacks), security mechanisms, security services; the relationship between them.
  - What are some common security services and security attacks (attacks on integrity, availability, authenticity, and password); Be able to identify the security attacks in terms of the violations of the security services.
  - Malicious software: Understand the common ways for a malicious software to infect a system, and to spread from machine to machine; Understand mechanisms that are used to defend against it (both prevention and detection).

- Introduction of Cryptography (Lecture 2)
  - Two basic encryption techniques: Substitution, Transposition (Permutation).
  - Three types of Cryptography: Secret key, Public key, Hash. What cryptographic tasks they are able to perform, respectively, and how they do it.

- Secret Key Cryptography: (Lectures 3, 4)
  - DES: The input and output of DES; The key length of DES; How to make more secure DES? – Triple DES, how is Triple DES designed, why?
  - How to encrypt large messages? The modes of operation – ECB, CBC, CFB, OFB, CTR. What are the advantages and disadvantages of each mode? How to use CBC to protect both integrity and privacy?
  - Stream cipher: one-time pad, pseudorandom number generator

- Hashes and Message Digest: (Lecture 5)
    - The feature of hash functions: one-way functions. What a hash function can do? How? The randomness requirement for a message digest (how many bits are considered sufficient?).
    - Understand the problem with keyed hash MD(key|message)? How to fix it (HMAC)?

- Public Key Cryptography: (Lecture 6)
    - RSA algorithm: know how public/private keys are generated; how to use public/private keys to encrypt/decrypt/sign/verify messages.
    - Diffie-Hellman key exchange: know how to use Diffie-Hellman to establish a shared number between two remote parties; understand what is Man-in-the-Middle attack and how to defend against it.

- Authentication: (Lectures 7, 8)
    - What information is generally used in authentication? –what you know, what you have, what you are, and where you are.
    - KDCs and CAs: why are they needed? How to do authentication with KDCs or CAs? What information is included in a ticket/certificate?
    - Be aware of the known security handshake pitfalls. Specifically, you need to know: how to choose a good session key (examples), what (or lack of what) causes replay attack and reflection attack, the different uses of the three types of nonce and the pitfalls associated with them.