ECE 471/571: Fundamentals of Information and Network Security
Final Exam Preparation Guide

Exam open date: Monday, May 6, 2024, 12am
Exam due date: Monday, May 6, 2024, Midnight

1. The exam will be open book, open note, 150-minutes online timed quiz in D2L. The format is similar to the midterm exam. There will be about 8 sections of problems that you need to answer/solve. Example types of the questions are: T/F, multiple choices, short answers, and numerical analysis/calculation. For the latter type, the answers are expected to include some analysis and calculation (you need to show the intermediate steps, and a calculator is allowed (non-programmable)). Input your final answers in the online quiz, and write down your explanation/analysis to support your answer in a separate worksheet and upload it right after the exam to D2L final exam folder.

2. Graduate students (ECE571) and undergraduate students (ECE471) will receive different sets of exam questions (more than 50% of the questions will be different). Generally speaking, graduate students can expect relatively more in-depth questions (such as those involving more modular arithmetic and probability calculations). However, the amount of calculations will not be much in the exam.

3. Generally speaking, anything that has been covered in the lectures on and before 4/29, 2024 might be tested in the exam. Although more focus will be put on the knowledge learnt after the midterm exam, any concept learnt throughout this course may still relevant in the final exam. Reviewing the lecture notes (power-points) on Piazza, in-class exercises on Tophat (or D2L quizzes), the homework assignments & project would all be helpful.

4. <u>Have a deep understanding of the principles and concepts, and how to apply them in scenarios relevant to information and network security is more important than just knowing the details</u>. More specifically, the following topics are considered fundamentals in this course. You are expected to know them by heart. The main topics after the midterm are listed as follows:

    - Public Key Cryptography
        - Diffie-Hellman key exchange: know how to use Diffie-Hellman to establish a shared number between two remote parties; understand what Man-in-the-Middle attack is and how to defend against it.

    - Key Management
        - Key distribution: KDCs and CAs: why are they needed? How to do key distribution/management with KDCs or CAs? What information is included in a ticket/certificate?

    - Understand certificate authorities, and how are certificates being verified.
    - The public key infrastructure: the common models, e.g., bottom-up, top-down, with name constraints, etc; the certificate chains.

- Authentication:
    - What information is generally used in authentication? –what you know, what you have, what you are, and where you are.
    - Principles of password based authentication, eavesdropping, database reading, and password guessing attacks (online and offline).
    - Authentication protocol design principles; be familiar with the known security handshake pitfalls: what are the common attacks? How do they work? How to defend against them? E.g., replay attack, reflection attack. Role of nonces.
    - Mutual authentication, session key establishment, forward secrecy.

- Internet Security Issues
    - TCP/IP security vulnerabilities and attacks, such as ARP cache poisoning, DDoS attack (smurf attack), IP address spoofing (ICMP protocol), eavesdropping, TCP Sync flooding attack, etc
    - How can these attacks be realized, what layer do they correspond to, and how can they be defended using which security protocol below.

- Kerberos:
    - The function of Kerberos V4 and the security services it provides.
    - Basic model and configuration.
    - The authentication mechanisms used in Kerberos Authentication – the concepts of KDC, long-term authentication key, session key, ticket, ticket-granting ticket, authenticator, credential, etc. (You need to know the messages exchanged and the major content in the messages, and their security values)
    - The scalability of Kerberos authentication, the inter-realm authentication mechanism (again, you need to know the messages involved)

- IPSec
    - The three protocols in IPSec – AH, ESP, IKE. The security services each protocol provides and the relationship among them
    - Concepts of Security Association (database), Security Policy (database), and SPI.
    - Two modes – Transport mode and Tunnel modes. The difference between the two modes and the suitable application scenarios.
    - What process is applied to the packet by AH and ESP (You need to know the processing to the level of header structure)
    - Understand how VPN works, and its relation to IPSec.

- SSL/TLS:
    - The security services SSL/TLS provides.
    - Understand the different mechanisms, protocols used in server authentication and client authentication.

    - Compare Kerberos, IPSec, and SSL, understand the different scopes of applicability and implementation locations in TCP/IP protocol stack.

- Malicious Software:
    - Types of Malicious Software, the Nature of Viruses, Worms.

- Intrusion Detection
    - Basic methods: Statistical Anomaly Detection, Rule-Based Intrusion Detection
    - The Base-Rate Fallacy
    - Password Management: Password Protection. Evaluate the strength of a password.

- Firewalls
    - Types of Firewalls: Packet Filtering Firewall, Stateful Inspection Firewalls, Application-Level Gateway
    - Firewall rules: understand and apply.