2016 CS4264 (Principles of Computer Security)

Final exam: 12/9 (Friday morning), 10:05AM-12:05PM in New Classroom Building 120
Close book, close note. Please do not leave the classroom during the exam.

The exam may cover everything discussed in the lectures, including lectures before the midterm. Guest lectures are not included. The advanced topics discussed in the final week are not included.

Types of questions (similar to homework and midterm problems):
- Given a security goal, to analyze vulnerabilities of a system
- Given a security goal, to propose solutions
- To compare various security techniques
- To explain security concepts
- May contain True/False questions

Examples of topics:
Comparing various network security protocols (SSL, IPSec, WPA, HTTPS) and understanding their different purposes and security guarantees in terms of CIAAAA properties. If Alice needs to send a confidential email to Bob, which protocols are needed to achieve this security goal?

Why is WEP protocol is? How do the improvement protocols work? Why wireless security is important?

The security of wireless network authentication

What is same origin policy in web security?

What are the defenses against web exploits such as XSS, XSRF, SQL injection, HTTP session hijacking?

Describe the different categories of malcode (worm, virus, trojan), their differences, and approaches to detect malware. What would a system admin of an organization do to avoid DoS attacks, phishing, hosting bots (and sending spam), hack-in of user accounts, defaced websites, etc.?

What are the differences of firewalls, IDS, IPS, anomaly detection techniques? Use firewall rules to filter traffic.

How does mix net work for anonymous routing? How are messages encrypted, formed, and routed? How does TOR realize hidden service?

If you are a website owner, what user authentication mechanisms can you adopt? What are the threats to each mechanism?

How do RSA encryption and signature schemes work? What is the RSA multiplicative property and its consequences?

What are the basic techniques used by symmetric key based crypto-systems? What are the properties of a cryptographic hash function? Message authentication code.

What is SYN flood? How can it be prevented?

What is stack-based buffer overflow? How can it be prevented?