

**CMPSCI 177 - Computer Security - Fall 2011**  
**FIRST APPROXIMATION AT FINAL EXAM TOPICS**

**TERMINOLOGY** - Be familiar with the terminology: spoofing, browsing, 0-day exploit, covert channels (storage and timing), Trojan horse, trap door, malware, badware, worm, virus, spyware, security, confidentiality, integrity, privacy, defense-in-depth, denial-of-service, buffer overflow, canaries, reference monitor, tiger team, false positive, false negative.

**SECURITY PRINCIPLES** - Understand and be able to give examples of least privilege, economy of mechanism, complete mediation, open design, separation of privilege, least common mechanism, psychological acceptability, and fail-safe defaults. Be able to discuss how these principles are satisfied/or not by a particular systems.

**SECURITY MODELS AND POLICIES** - Know the models their differences, similarities, and when one is more appropriate than the others. In particular, understand the Bell-LaPadula, Integrity (Biba), Lattice, and Noninterference models. Understand the Basic Security Theorem and the difference between a mandatory policy and a discretionary policy. Understand need-to-know and trusted processes. Be prepared to discuss the UCSB College of Engineering Acceptable Use Policy, which you all agreed to (*If you did not, then you better get a copy and review it*).

**SECURITY MECHANISMS** - Understand the function of and when to use capabilities, access control lists, authentication mechanisms, biometric and behavioral systems, secure attention key, statistical inference mechanisms.

**NETWORK SECURITY** - Know the relevant layers of the TCP/IP protocol stack. Understand the different network discovery tools that are available and how a multistep attack works. Be able to explain how IP Spoofing, TCP Spoofing, UDP Spoofing, and Session Hijacking work.

**CRYPTOGRAPHY** - Know the difference between public key encryption systems and conventional encryption systems. Know how encryption is used to detect data modification (block ciphers), how it is used for user authentication, and how digital signatures work. Know how to use a salt when encrypting passwords and what benefits it gives. You need not know all of the encryption algorithms and crypto analysis techniques, but you are expected to be able to perform some simple crypto analysis.

**BUFFER OVERFLOWS** - Understand how a stack-based overflow works and how a canary can be used to detect an overflow attempt. Understand how Address Space Layout Randomization (ASLR) works and how it can thwart a buffer overflow attempt.

**INTRUSION DETECTION** - Know the different approaches to intrusion detection, such as threshold detection, profile-based detection, anomaly detection, and misuse detection. Know the strengths and weaknesses of each approach and how different methods can be used to complement each other. Understand how alert correlation gives a more accurate "big picture" of the attack landscape.

**MALWARE** - Know the different types of malware and how they are similar/different. Understand polymorphic and metamorphic approaches to obfuscating malware, and be able to give examples of each. Understand generally how the Torpig botnet infection occurs and explicitly how Torpig domain flux works.

**ONLINE BANKING** - Understand the threats to online banking systems and how they relate to the goals for the system.

### **GENERAL COMMENTS**

You should be able to compare the different security models, security mechanisms, security architectures, and protection techniques that we have studied and to generally evaluate their advantages and disadvantages. I do not want you to memorize facts; I do want you to understand the general concepts and how they relate to one another. You will be expected to be able to apply what you've learned to a *new* problem.

### **GENERAL INFORMATION**

The exam will consist of a closed book portion and an open book portion. The closed book portion will be given first. You are to bring *all* notes, papers, homework solutions, and other handouts that you received in class, or that were posted on the web, to the exam. The exam will refer to some of these handouts and extra copies *will not* be available at the exam. If you are not sure whether you have everything, check with your fellow students before the exam. *You will not be able to use calculators, laptops, or cell phones during the exam.*

**FINAL EXAM TIME** -- Tuesday December 6, 2011, 4:00pm - 7:00pm, Phelps 1401

*Note:* By the end of the quarter please return any papers or books that you may have borrowed from me during the quarter.