CPSC 91 Computer Security

Final Exam Study Guide

Probability Theory

- Random Variable, sample space, events and probability distribution function
- Properties of distribution functions
- Conditional Probability
- Independence
- Law of Total Probability
- Bayes' Theorem
- Analysis of Randomized Algorithms using Bayes' Theorem

The question in probability will likely be a variant of a question that appeared on Assignment 1. It will not be about combinatorial counting. For example, no calculations of probability of poker hands or counting permutations. Counting colored balls in urns is fair game though.

Symmetric Cryptography

- Block Ciphers
- Pseudorandom Functions and their security
- Pseurorandom Permutations and their security
- Symmetric Encryption
- Symmetric Encryption Security: key recovery, message recovery, semantic security (CPA and CCA)
- Block cipher modes of operations (big picture only)
- Message Authentication codes and their security (big picture)
- NO REDUCTIONS

See Midterm 1 Study Guide for the list of security definitions.

Public Key Cryptography

- How public key encryption differs from symmetric key encryption
- How public key signature differs from message authentication codes
- Why public key certificates are necessary

Networking

Network layers, and what protocol belongs to what level.

How each of the following works and high level view of what is contained in the headers and what it does:

- Internet Protocol
- UDP and TCP
- DNS resolution

User Authentication

- Authentication Factors
- How to make good passwords
- How to exchange passwords
- How to store passwords
- How to use passwords as keys

Security Protocols

- Kerberos
- secure email (PGP)
- SSL/TLS
- SSH (what little we covered about it)
- IPsec
- Wireless Security
- Onion Routing and Tor
- Firewalls and Intrusion Detection

You should also be able to find and exploit flaws in simple network protocols.

Network Attacks

How the following attacks are conducted and how they could be countered:

1. Man-in-the-Middle attack
2. Replay attacks
3. SYN flood
4. unsecure wireless
5. corrupted router

System Attacks and Internet Threats

1. Viruses and their Stealth Strategies
2. Buffer Overflows and their possible effects
3. Code Injection Attacks (XSS, SQL injection, eval exploits)

For each of these attacks, you should also know of possible countermeasures