

CSE 498U/598U – Computer Security

Class 21: Friday, October 11

Reminders

- Homework
 - Final Project Proposal Due Oct 15 @ 5 PM
 - Exam Wed, Oct 13
 - Mid-Semester Evaluation Due Oct 15
 - Reading / Web Browsing
 - Review for the exam
-

Schedule

Monday

Exam Review

Wednesday

Mid-Term Exam

Lecture Outline

Exam 1 Review

Key Points

- See review handout

Introduction

- What is the difference between confidentiality vs. integrity vs. availability?
- Which of the above three areas is easiest/hardest to measure/design for?
- What is a salami attack?
- What is a replay attack?
- What is repudiation of origin?

Encryption

- What is the difference between plaintext and ciphertext?
- How do you write the functions (symbolically) for encryption?
- What is the difference between an asymmetric and symmetric key?
- What is a substitution cipher?
- What is the difference between a substitution and a transposition cipher?
- Why is regularity/predictability bad for an encryption system?
- What is a Vernam cipher?
- What is a one-time pad?
- What is the difference between key distribution with a public/private key and key distribution with a symmetric (secret) key?
- What are the pros/cons of a stream vs. block cipher?
- What is confusion and how does it differ from diffusion?
- Describe the basic DES operation
- Why do double-DES and triple-DES take different times to crack?
- What is a knapsack?
- What is a super-increasing knapsack?
- Describe the Merle-Hellman Knapsack algorithm
- Describe how RSA works
- [From yesterday] What makes a knapsack problem hard versus easy?
- What was the primary weakness of the Merle-Hellman knapsack?
- Why would you want to pad plaintext with random bits?
- What is a cryptographic checksum and what is its purpose?
- What are the properties of a strong hash function?
- What is the pigeonhole principle?
- How is a nonce different from a sequence number?
- Why must one be careful when using sequence numbers?
- Describe a protocol that can withstand replays and external modifications.
- Describe briefly how SSL works
- Why does SSL have the extensive handshake process?
- [From Monday] Why is certificate revocation hard?

Authentication

- What are the four basic forms of authentication?
- Does it matter if your password is longer than 8 characters on a UNIX system?
- What is a password salt and why does it make cracking passwords harder?
- Using Anderson's rule, why is it only a lower bound on the probability of cracking?
- What makes a challenge/response system unique?

- Why are biometrics not a perfect solution?
- What is PAM?
- Describe a hybrid system that employs multiple authentication mechanisms.

Steganography

- How is steganography different from encryption?
- What is the purpose of a watermark?
- Describe why steganography on a JPEG is harder than on a simple bitmap.

O/S Considerations

- What is the difference between a fault versus an error versus a failure?
- Describe what happens in a buffer overflow attack.
- Why is penetrate/patch not effective?
- What is incomplete mediation?
- Describe the 4 different kinds of separation.
- What is relocation and how does it apply to O/S memory interactions?
- What is least privilege?
- What is the difference between a security policy and a security mechanism?
- How might you detect the JPEG virus?
- How might you obfuscate the virus? Is there a point at which this will no longer work?
- Be able to conduct on a trust analysis on a system.
- What is the difference between a MAC vs. DAC?
- Describe Bell La Padula.
- Describe the Biba integrity model.
- How can you incorporate both Biba and Bell La Padula together?
- What is RBAC?
- Describe 4 out of the 8 design principles in detail.
- What is a principal in the context of identity?
- Describe the difference between a CA issuance versus authentication policy.
Why should there be different policies rather than a set policy for all?