# CS3600 – Summer AY04
# Reading Assignments by Section

| Section | Topic | Textbook Reading |
|---|---|---|
| 1 | Introduction | Chap 1, pp 1-27 |
| 2 | I & A<br>DAC | Chap 4, pp 209-226 |
| 3 | MAC | Chap 5, pp 229-244 |
| 4 | Design and<br>Implementation Issues | Chap 4, pp 179-183<br>Chap 4, pp 183-194 optional<br>Chap 5, pp 250-267 |
| 5 | Malicious Software | Chap 3, 95-140 |
| 6 | System Accreditations and<br>Evaluations | Chap 5, pp 273-297<br>Chap 8, pp 506-508<br>Chap 8, pp 508-529 optional |
| 7 | Cryptography Basics | Chap 2, pp 35-77<br>Chap 10, pp 642-666 |
| 8 | Cryptographic Protocols | Chap 2, pp 77-81 |
| 9 | Networks I,<br>Basics | Chap 7, pp 363-387 optional intro[1]<br>Chap 7, pp 387-436 |
| 10 | Networks II,<br>TCP,<br>Firewalls,<br>Intrusion Detection | Chap 7, pp 450-473 |
| 11 | Networks III,<br>Public Key Infrastructure | Chap 2, 81-88 |

[1] If you already know about how networks work, you can skip this section without missing anything.

# Reading Questions

Book: Security in Computing, by Pfleeger

## Section 1
## Introduction

Chapter 1 (pp. 1-27)

1. How are the terms *threat*, *control*, and *vulnerability* related?
2. Confidentiality, Integrity and Availability: which two are most alike? Why?
3. Confidentiality, Integrity and Availability: which one is least understood? Why?
4. Note: sidebar 1-3 claims that outsider attacks are now considered the greater threat. You should know that this is still a minority opinion.
5. How does risk relate to threat and vulnerability?
6. What five categories of controls does the author provide?

## Section 2
## Access Control I: I&A and DAC

Chapter 4 (pp. 209-226)

1. Note: I left out the pages on access control (pp 194-209) because I thought it was not well presented, i.e., I thought it would confuse rather to teach.
2. What vulnerability is "object reuse" trying to control?
3. For face recognition, hand geometry, fingerprint, and voice recognition, what does the author report as the false negative (false rejection) and false positive (false acceptance) rates?
4. Critical Thinking: When it comes to false positive and false negative rates, what are your expectations for a password-based system?
5. When a system is receiving username and password from someone trying to gain access, why should the error messages be vague if something goes wrong?
6. Application: If a system allowed users to select any password, as long as it was between 7 and 10 characters in length (inclusive), and the character set available was [A-Z, a-z, 0-9], approximately how many passwords are possible?
7. What is the purpose of "salt" in the Unix password scheme?
8. When an operating system is enforcing an access control policy, why is authentication so essential?

## Section 3
## Access Control II: MAC

Chapter 5 (pp. 229-244)

1. What is the author's definition of a trusted operating system?

# Section 4
# Building Secure Systems

Chapter 4 (pp. 179-183)

1. What is the basis of protection?
2. Which form of separation provides the most security?
3. What security concern is the result of modern operating systems being portable across different CPU architectures?

Chapter 5 (pp. 250-267)

4. What is a practical problem when dealing with computer-generated audit logs?
5. What is a security kernel?
6. Note: the author's use of reference monitor is not consistent with the lecture notes. We will use the definition in the lecture notes.

# Section 5
# Malicious Software and Attacks

Chapter 3 (pp. 95-140)

No questions. This reading serves mostly to (hopefully) provide additional clarification of what is presented in class.

# Section 6
# System Certification, Accreditation, and Evaluation

Chapter 5 (pp. 273-297)

1. What is the largest single source of operating system vulnerabilities?
2. What three techniques does the author say can be used to provide some measure of confidence that a system is correctly enforcing its policies?
3. Of the above three techniques, which is most widely used?
4. Which technique is most rigorous? In other words, which technique will provide the most assurance?
5. Note: you don't need to understand the example proof on pages 278-280.
6. What are the two difficulties in applying formal verification methods?
7. How is validation different from verification?

Chapter 8 (pp. 506-508)

No questions.

# Section 7
# Basics of Cryptography

Chapter 2 (pp. 25-77)

1. Why can simple encryption be difficult to break when used on short messages?
2. If a cryptanalyst has both the ciphertext and the corresponding plaintext, why would he still want to determine what the encryption key is?

Chapter 10 (pp. 642-666)

3. What is a product cipher?
4. What is “the most serious objection” raised about DES?

# Section 8
# Cryptographic Protocols

Chapter 2 (pp. 77-81)

No questions.

# Section 9
# Network Security I

Chapter 7 (pp. 363-387)

Optional reading – no questions.

Chapter 7 (pp. 387-436)

1. Why is the risk of attack greater when computers are attached to a network?
2. What does the author say is the single most significant motivation for a hacker?
3. From a security standpoint, what should you assume about the communication links between network nodes?
4. What is a SYN flood?
5. When is link encryption most appropriate?
6. Note: the author’s statements about VPNs and link encryption are misleading, if not altogether wrong.

# Section 10
# Network Security II

Chapter 7 (pp. 450-473)

1. In general, why does the author say that a router is not a good place to do filtering of unwanted network traffic coming into an organization's network? [Note that this opinion is not universally shared.]
2. Why does the author say that a firewall is best put on a dedicated device?
3. According to "security experts", what is the preferred default behavior of firewalls?
4. What does it mean to run an IDS in stealth mode?
5. What is the potential result if too many false positives are raised by an IDS?

# Section 11
# Public Key Infrastructure

Chapter 2 (pp. 81-88)

1. What must people be able to do with certificates before they will widely used for electronic commerce?
2. What hinders this from happening?