Introduction to Computer Security
Midterm Exam
Fall 2008

This is a closed-book, closed-notes exam.

1. True or False. [15 points]

   (a) Covert channels are easily detected and eliminated.

   (b) Storage channels can be addressed with well known security engineering techniques.

   (c) The Orange book attempts to correct issues that led to paralysis under the Common Criteria.

   (d) The Bell La Padula model is used in the context of mandatory access control.

   (e) The Bell La Padula model supports discretionary access control.

   (f) The Biba model addresses confidentiality.

   (g) The protection state enforced by the Chinese Wall model at any particular point in time can be described with BLP.

   (h) The 1972 Anderson report failed to identify network security as an important field deserving further study.

2. Short Answer. [15 points]

   Please give a **short** description of each of the following:

   (a) Integrity

   (b) Confidentiality

   (c) Availability

   (d) Access Control Matrix

   (e) Originator controlled access control

   (f) Separation of duty

   (g) Common Criteria

   (h) British Medical Association policy for clinical information

3. Usability. [15 points]

   Ross Anderson stresses usability as a critical issue in practical computer security. He points out that many of the most devastating security failures have had a significant human component. Give an anecdote about usability in the domain of voting that supports Anderson's thesis.

4. Integrity Models [15 points]

   Contrast the Biba and Clark-Wilson integrity models. You may wish to use examples, such as the voting machine case study, to illustrate your points. Please address:

   (a) Simplicity of mechanism.

   (b) Guidance to security architects in developing requirements.

   (c) Protection from external threats.

   (d) Protection from internal threats.

   (e) Integration with existing security practices in government and industry.

5. Telephone Fraud [20 points]

   Outline the telephone fraud detection problem. In your discussion please address the following points:

   (a) Define "subscription fraud" and "superposition fraud."

   (b) How does the concept of "Communities of Interest" apply to telephone fraud detection?

   (c) What data sources are used in telephone fraud detection?

   (d) Define and contrast "guilt by association" and "linkage using COI-based matching".

6. Virtualization [20 points]

   How does virtualization address the confinement problem? If security is a primary objective do you expect the virtual machine monitor (VMM) to be optimized for: simplicity, performance, or feature richness? Discuss.