

## Outline for September 29, 2003

**Reading:** Chapter 13

### Discussion Problem

A multinational company employs 10,000 system administrators. It has become very concerned with computer security issues, and (in particular) its vulnerability to attackers, both from the outside and the inside. It has decided to require the system administrators to become certified in security using a test. The testing company will develop a security test using knowledge from industry standard courses and books, test all system administrators, and report their scores as percentiles. The system administrators will then receive training. After a year, the test will be given again, and any system administrator who fails to score above the 50th percentile will be required to undergo further training. This will continue until *all* system administrators score above the 50th percentile.

What do you think of this scheme? What are its merits and demerits?

### Outline for the Day

1. Operational Issues (*con't*)
  - a. Laws and customs
2. Human issues
  - a. Organizational problems
  - b. People problems
3. Principles of Secure Design
  - a. Principle of Least Privilege
  - b. Principle of Fail-Safe Defaults
  - c. Principle of Economy of Mechanism
  - d. Principle of Complete Mediation
  - e. Principle of Open Design