Lecture 6 Outline

Reading: *text*, §29; [Bellovin, 2007] **Assignments due:** Homework #1, due April 13, 2001 at 11:55pm

Discussion Problem. After the first Gulf War ended in 1991, some generals realized that the Iraqi networks had been remarkably resilient. As soon as the Allies destroyed one station, the network promptly routed around it. The generals discovered that the Iraqis were using Internet routing protocols, which were designed for resiliency. Several promptly suggested that those protocols should be classified. What are the problems with doing this?

1. Review of robust programming principles
   a. Paranoia
   b. Stupidity
   c. Dangerous implements
   d. Can't happen
2. Robust library
   a. Interface
   b. Internal structures
   c. Tokens and their generation and analysis
   d. Functions
3. Secure design
   a. Simplicity
   b. Restrictiveness
4. 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
   f. Principle of separation of privilege
   g. Principle of least common mechanism
   h. Principle of least astonishment