Outline for January 15, 2008

Reading: text, §13; [Be07]

Announcement: Michael Clifford's office hours will be in 55 Kemper. My office hours for Wednesday, January 16, are moved to 2:00–3:00PM, and my office hours on Thursday, January 17, are *cancelled*.

Discussion Problem. After the first Gulf War, 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. Secure design
   a. Simplicity
   b. Restrictiveness
2. 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 psychological acceptability