# Lecture 9 Outline (April 17, 2015)

**Reading:** §23.3–4, §2 **Assignment**: Homework 1, due April 17, 2015

1. Greetings and felicitations!
2. Discussion problem of the day
3. NRL
   a. Goal: Find out how vulnerabilities enter the system, when they enter the system, and where they are
   b. Axis 1: inadvertent (RISOS classes) vs. intentional (malicious/nonmalicious)
   c. Axis 2: time of introduction (development, maintenance, operation)
   d. Axis 3: location (hardware, software: OS, support utilities, applications)
4. Aslam
   a. Goal: Treat vulnerabilities as faults
   b. Coding faults: introduced during software development
      i. Synchronization errors
      ii. Validation errors
   c. Emergent faults: introduced by incorrect initialization, use, or application
      i. Configuration errors
      ii. Environment faults
   d. Introduced decision procedure to classify vulnerabilities in exactly one category
5. Models of Attacks
   a. Example attack: *rsh* and synflooding
   b. Capabilities and requires/provides models
   c. Attack trees
6. Access Control Matrix
   a. Subjects, objects, and rights
   b. Primitive commands: create subject/object, enter right, delete right, destroy subject/object
   c. Commands and conditions: create-file, various flavors of grant-right to show conditions and nested commands
   d. Copy flag
   e. Attenuation of privileges

---

***Discussion question***. 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?