Outline for November 22, 2005

**Reading:** “FBI Alerts Public to Recent E-Mail Scheme,” Federal Bureau of Investigation, Department of Justice (Nov. 21, 2005).

1. Virus Defenses
   a. Can constrain case enough to locate specific malicious logic, using:
      i. Type checking (data vs. instructions)
      ii. Limiting rights (sandboxing)
      iii. Limiting sharing
      iv. Preventing or detecting changes to files
      v. Prevent code from acting beyond specification (proof carrying code)
      vi. Check statistical characteristics of programs (more authors than known, constructs in object files not corresponding to anything in the source)

2. Safety on the Web: WWW
   a. Unfriendly applets
   b. Unfriendly images and pixels
   c. Site and content filtering software
   d. PHP, CGI, and all that: server side problems
   e. Redirection
   f. Naming problems

3. Safety on the Web: Email
   a. Attachments, worms, and viruses
   b. Spam
      i. Joe jobs
      ii. Relaying through third parties
      iii. Zombies
   c. Anti-spam technologies
      i. Authentication and authorization services
      ii. Reputation services
      iii. Challenge-response
      iv. Port blocking and rate limiting
      v. Preventing relaying
      vi. Spam filtering
      vii. Image blocking
   d. Phishing
Puzzle of the Day

When you examine a system for security problems, or design a system with strengthened security, creativity in anticipating problems is a major factor in the success of your work. Here are some creative answers to the riddle, “Why did the chicken cross the road?” A child might answer: “To get to the other side.” But what would others answer?

Plato:
Aristotle:
Karl Marx:
Timothy Leary:
Captain James T. Kirk:
Machiavelli:
Jack Nicholson:
Oliver Stone:
Albert Einstein:
Ralph Waldo Emerson:
Ernest Hemingway:
Colonel Sanders: