Outline for October 20, 2005

Reading: D. Libes, "Choosing a Name for Your Computer" ftp://ftp.rfc-editor.org/in-notes/fyi/fyi5.txt (Aug. 1990).

1. Email
   a. How it works
   b. Security issues
   c. How secure is email?
2. Privacy-Enhanced Mail
   a. Goals
   b. How confidentiality works
   c. How integrity and authenticity work
   d. Combining the two
   e. Armoring
   f. Sending the message
   g. PEM and PGP (GPG)
3. Identity
   a. Principles and identities
   b. Files and objects
   c. Users, groups, roles
   d. Computers: names, addresses, and the DNS
   e. On the web: cookies and such
   f. Anonymity

Puzzle of the Day

Microsoft spent February, 2002, teaching its programmers how to check their code for security vulnerabilities and how to spot common security flaws. Yet many Microsoft programs have security vulnerabilities. What problems do you think Microsoft encountered, and will encounter, in trying to find and clean up the vulnerabilities in its systems?