

Outline for March 15, 2006

Reading: text, §22 (except 22.6)

1. Greetings and felicitations!
2. Malicious logic
 - a. Quickly review Trojan horses, viruses, bacteria; include animal and Thompson's compiler trick
 - b. Logic Bombs, Worms (Schoch and Hupp)
3. Ideal: program to detect malicious logic
 - a. Can be shown: not possible to be precise in most general case
 - b. Can detect all such programs if willing to accept false positives
 - c. Can constrain case enough to locate specific malicious logic
 - d. Can use:
 - 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)