Outline for November 15, 2005

Reading: K. Thompson, "Reflections on Trusting Trust," *Communications of the ACM* **27** (8) pp. 761–763 (Aug. 1984).

1. Recording property electronically
   a. Goals of recording property
   b. Overview of process
   c. Architecture of a solution
   d. Tests and problems
   e. Current state of e-recordation in California
2. Malicious logic
   a. Trojan horses, including replicatiing Trojan horses
   b. Computer viruses
      i. Boot sector infectors
      ii. Executable infectors
      iii. Multipartite viruses
      iv. TSR viruses
      v. Stealth viruses
      vi. Encrypted viruses
      vii. Polymorphic viruses
      viii. Macro viruses
   c. Computer worms
   d. Rabbits, bacteria
   e. Logic bombs
3. Defenses
   a. Cannot write a program to detect computer viruses without error
   b. Can detect all such programs if willing to accept false positives
   c. 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)

Puzzle of the Day

When you play certain Sony music CDs on your Windows system, the CD installs special software to play Sony's CDs. This software enforce Sony's Digital Rights Management (DRM) policies. This software cloaks itself so the user cannot see many associated files, by hiding files whose name begins with "sys". It also installs a new version of the CD device driver that restricts the number of times you can copy the Sony CD. The software mimiced a type of program that compromises a system once the attacker has gained administrator privileges; this program is called *root-kit*.

The software was discovered by a Windows expert who noticed a problem with his system. After considerable work, and publicity, he posted that:

- Sony denied that the rootkit poses a security or reliability threat despite the obvious risks of both.
- Sony claims that users don't care about rootkits because they don't know what a rootkit is.
- The installation provides no way to safely uninstall the software.
- Without obtaining consent from the user, Sony's player informs Sony every time it plays a "protected" CD.

Do you believe Sony's actions are an effective way to enforce its rights to protect its music? What are its drawbacks