Outline: Lecture 5

Date: April 12, 2011
Topic: Silicon Biology

1. Discussion: classes and testing over the Internet
2. Malware
   a. What it is
   b. Trojan horses
      i. Regular
      ii. Replicating Trojan horses: the animal game
   c. Computer viruses
      i. Basic: boot sector, executable, TSR viruses
      ii. Hiding: stealth viruses
      iii. Morphing: encrypted, polymorphic viruses
      iv. General: macro viruses
   d. Computer worms
   e. Rabbits, bacteria
   f. 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. Static analysis: signature scanning
   d. Heuristic analysis: emulation, generic decryption
   e. Restricting execution
      i. Distinguishing between data and instructions
      ii. Restricting access rights (sandboxing, jailing)
      iii. Checking statistical characteristics
      iv. preventing, detecting changes to specific files