Outline for May 29, 2003

1. Security testing
    a. Property-based testing
2. What is malicious logic?
3. Trojan horses
    a. Propagating Trojan horses
4. Computer viruses
    a. Boot sector infectors
    b. Executable infectors
    c. Multipartitie infectors
    d. TSR viruses
    e. Stealtth viruses
    f. Encrypted viruses
    g. Polymorphic viruses
    h. Macro viruses
5. Computer worms
    a. Original work
    b. Internet worm
6. Rabbits and Logic Bombs
7. Countermeasures
    a. Separate data and instructions
    b. Limit protection domain: flow control, reduction of rights
        i. Karger’s knowledge-based subsystem
        ii. Sandboxing
    c. Limit sharing
    d. Detect alteration of files
    e. Specification-based behavior
        i. Proof-carrying code
    f. Statistical analysis