Lecture 26 Outline

November 21, 2016

Reading: §23* **Assignments**: Homework 5, due Dec. 2

1. Computer virus
   a. Boot sector infector
   b. Executable infector
   c. Multipartite
   d. TSR (terminate and stay resident)
   e. Stealth
   f. Encrypted
   g. Polymorphic
   h. Metamorphic
   i. Macro
2. Computer worm
3. Bots, botnets
4. Bacterium, rabbit
5. Logic bomb
6. Adware, spyware
7. Ransomware
8. Phishing
9. Ideal: program to detect malicious logic
   a. Can be shown: not possible to be precise in most general case
   b. Can constrain case enough to locate specific malicious logic
10. Defenses
    a. Scanning defenses
    b. Data and instructions
    c. Information flow metrics
    d. Reducing rights
    e. Specifications as restrictions
    f. Limiting sharing
    g. Statistical analysis