Lecture 7 Outline

April 19, 2016

Reading: *text*, §24.1–24.2; [Bis07a, Bis07b, Wei95] **Assignments due:** Homework 2, on Apr. 19

1. Greetings and felicitations!
2. Puzzle of the Day
3. Penetration Studies
   a. Why? Why not direct analysis?
   b. Effectiveness
   c. Interpretation
4. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization
5. System Analysis
   a. Learn everything you can about the system
   b. Learn everything you can about operational procedures
   c. Compare to other systems
6. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to other systems' flaws
   c. Compare to vulnerabilities models
7. Hypothesis testing
   a. Look at system code, see if it would work (live experiment may be unneeded)
   b. If live experiment needed, observe usual protocols
8. Generalization
   a. See if other programs, interfaces, or subjects/objects suffer from the same problem
   b. See if this suggests a more generic type of flaw
9. Elimination
10. Where to start
    a. Unknown system
    b. Known system, no authorized access
    c. Known system, authorized access
11. Examples
    a. Burroughs system
    b. Corporate site
12. Attacks
    a. Attack trees
    b. Requires-provides model
    c. Incident response
13. Types of malicious logic
    a. Trojan horse
       i. Replicating Trojan horse
       ii. Thompson's compiler-based replicating Trojan horse
    b. Computer virus
       i. Boot sector infector
       ii. Executable infector

iii. Multipartite
iv. TSR (terminate and stay resident)
v. Stealth
vi. Encrypted
vii. Polymorphic
viii. Metamorphic
ix. Macro

c. Computer worm
d. Bacterium, rabbit
e. Logic bomb
f. Keystroke logger
g. Ransomware
h. Botnets

Discussion Problem. Many European countries (and a few others, too) have a "right to forget". This enables a citizen to demand the removal of information about them from search engine results. It is an attempt to implement privacy, which can be defined as the right of the individual to control the dissemination of information about himself or herself, and to control what is done with that information.

1. What technical problems does doing this entail?
2. Assuming this cannot be implemented directly, what might be done to achieve a similar effect?
3. What problems might arise when someone, or some organization, exercises this right?