Outline for January 10, 2003

Reading: Chapters 13, 23.1–23.2

Discussion Problem

Bureaucracies have their own version of the English language with which you must become familiar. To help you do so, here are some common phrases. See if you can translate them.

1. Scintillate, scintillate, asteroid minikin.
2. Members of an avian species of identical plumage congregate.
3. Surveillance should precede saltation.
4. Pulchritude possesses solely cutaneous profundity.
5. It is fruitless to become lachrymose over precipitately departed lacteal fluid.
6. Freedom from incrustations of grime is contiguous to rectitude.
7. The writing implement is more potent than the rapier.
8. It is fruitless to attempt to indoctrinate a superannuated canine with innovative maneuvers.
9. Eschew the implement of correction and vitiate the scion.
10. The temperature of the aqueous content of an unremittingly galled saucepan does not reach 212 degrees Farenheit.
11. Upon vacating these premises all illuminations are to be extinguished.

Outline for the Day

1. Principles of Secure Design
   a. Principle of Least Privilege
   b. Principle of Fail-Safe Defaults
   c. Principle of Economy of Mechanism
   d. Principle of Complete Mediation
   e. Principle of Open Design
   f. Principle of Separation of Privilege
   g. Principle of Least Common Mechanism
   h. Principle of Psychological Acceptability
2. Penetration Studies
   a. Why? Why not direct analysis?
   b. Effectiveness
   c. Interpretation
3. Flaw Hypothesis Methodology
   a. System analysis
   b. Hypothesis generation
   c. Hypothesis testing
   d. Generalization
4. System Analysis
   a. Learn everything you can about the system
   b. Learn everything you can about operational procedures
   c. Compare to other systems
5. Hypothesis Generation
   a. Study the system, look for inconsistencies in interfaces
   b. Compare to other systems' flaws
   c. Compare to vulnerabilities models
6. 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
7. 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
8. Peeling the Onion
   a. You know very little (not even phone numbers or IP addresses)
   b. You know the phone number/IP address of system, but nothing else
   c. You have an unprivileged (guest) account on the system.
   d. You have an account with limited privileges.
9. Example Penetration Studies
   a. Michigan Terminal System
   b. Burroughs System
   c. Attacking the Organization Directly