Outline for October 24, 2022

Reading: *text*, §18.3, 24.3–24.4.1

Assignments: Homework 3, due November 11;
Progress report, due Nov 11 (Note change in due date!)

1. Virtual machines
   (a) Type 1 and type 2 hypervisors
2. Sandboxes
3. Covert channels
   (a) Storage channes
   (b) Timing channels
4. Vulnerability models
   (a) PA model
   (b) RISOS
   (c) NRL
   (d) Aslam
5. Example flaws
   (a) *fingerd* buffer overflow
   (b) *xterm* race condition
6. RISOS
   (a) Goal: Aid managers, others in understanding security issues in OSes, and work required to make them more secure
   (b) Incomplete parameter validation — failing to check that a parameter used as an array index is in the range of the array;
   (c) Inconsistent parameter validation — if a routine allowing shared access to files accepts blanks in a file name, but no other file manipulation routine (such as a routine to revoke shared access) will accept them;
   (d) Implicit sharing of privileged/confidential data — sending information by modulating the load average of the system;
   (e) Asynchronous validation/Inadequate serialization — checking a file for access permission and opening it non-atomically, thereby allowing another process to change the binding of the name to the data between the check and the open;
   (f) Inadequate identification/authentication/authorization — running a system program identified only by name, and having a different program with the same name executed;
   (g) Violable prohibition/limit — being able to manipulate data outside one's protection domain; and
   (h) Exploitable logic error — preventing a program from opening a critical file, causing the program to execute an error routine that gives the user unauthorized rights.