Lecture 7 Outline (April 13, 2015)

Reading: §23.2–4, [PTE12]

Assignments: Program 1, due April 15, 2015
Homework 1, due April 17, 2015

1. Greetings and felicitations!
   a. Welcome to room 6 Olson!
   b. Remember that I had to move Monday's office hours to 9:00-9:50am, so I will not hold office hours today from 2:10pm–3:00pm
2. Discussion problem of the day
3. Penetration Studies
4. Examples
   a. Burroughs system
   b. Corporate site
5. Vulnerability models
   a. PA model
   b. RISOS
   c. NRL
   d. Aslam
6. Example Flaws
   a. *fingerd* buffer overflow
   b. *xterm* race condition
7. 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.

Discussion question. From Sun Tzu, *The Art of War*, James Clavell, *ed*., Dell Publishing, New York, NY (1983), p. 11:

> All warfare is based on deception. Hence, when able to attack, we must seem unable; when using our forces, we must seem inactive; when we are near, we must make the enemy believe we are far away; when far away, we must make him believe we are near. Hold out baits to entice the enemy. Feign disorder, and crush him. If he is secure at all points, be prepared for him. If he is in superior strength, evade him. If your opponent is of a choleric temper, seek to irritate him. Pretend to be weak, that he may grow arrogant. If he is taking his ease, give him no rest. If his forces are united, separate them. Attack him where he is unprepared, appear where you are not expected.

What does this say to an attacker trying to break into a computer system? To the system administrator or security officer trying to defend that system?