Outline for April 13, 2004

Reading: Chapter 23.3–23.4

Discussion Problem

"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."[1]

1. What does this paragraph say to an attacker who is trying to penetrate a system?
2. What does this paragraph say to a system administrator or security officer seeking insight to defend her system?

Outline for the Day

1. Common Implementation Vulnerabilities
   a. Unknown interaction with other system components (DNS entry with bad names, assuming finger port is finger and not chargen)
   b. Overflow (year 2000, *lpr* overwriting flaw, *sendmail* large integer flaw, *su* buffer overflow)
   c. Race conditions (*xterm* flaw, *ps* flaw)
   d. Environment variables (*vi* one-upsmanship, *loadmodule*)
   e. Not resetting privileges (Purdue Games incident)
2. Robust Programming
   a. Principles

1. Sun Tzu, *The Art of War*, James Clavell, *ed.*, Dell Publishing, New York, NY ©1983, p. 11