Outline for March 6, 2008

Reading: text, §22.1–22.5, 22.7, 23.3–22.4; [AL96]

Discussion Problem. Sun Tzu wrote[1]:

> If we do not wish to fight, we can prevent the enemy from engaging us even though the lines of encampment be merely traced out on the ground. All we need to do is to throw something odd and unaccountable in his way.
>
> Tu Mu relates a strategm of Chu-ko Liang, who in 149 B.C., when occupying Yang-p'ing and about to be attacked by Ssu-ma I, suddenly struck his colors, stopping the beating of the drums, and flung open the city gates, showing only a few men engaged in sweeping and sprinkling the ground. This unexpected proceeding had the intended effect; for Ssu-Ma I, suspecting an ambush, actually drew off his army and retreated.

What does this paragraph say to a system administrator or security officer seeking insight to defend her systems?

Lecture Outline

1. Malicious logic
   a. Bacteria and logic bombs
2. Ideal: program to detect malicious logic
   a. Can be shown: not possible to be precise in most general case
   b. Can detect all such programs if willing to accept false positives
   c. Can constrain case enough to locate specific malicious logic
3. Detection
   a. Type checking (data vs. instructions)
   b. Limiting rights (sandboxing)
   c. Limiting sharing
   d. Preventing or detecting changes to files
   e. Prevent code from acting beyond specification (proof carrying code)
   f. Check statistical characteristics of programs (more authors than known, constructs in object files not corresponding to anything in the source)
4. 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 (*sendmail* large integer flaw, buffer overflow)
   c. Race conditions (*xterm* flaw, signals)
   d. Environment variables (*vi* one-upsmanship)
   e. Not resetting privileges (Purdue Games incident)

1 Sun Tzu, *The Art of War*, James Clavell, *ed*., Dell Publishing, New York, NY ©1983, pp. 26-27