

Outline for February 3, 2003

Reading: text, §5.2.1–5.2.2, 5.3, 6.1–6.2

Discussion Problem

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 stratagem 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.¹

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

Outline for the Day

1. Bell-LaPadula Model
 - a. Compartments
 - b. BLP as lattice structure
 - c. Simple Security Property
 - d. *-Property
 - e. Basic Security Theorem
2. DG/UX B2 UNIX System
 - a. Hierarchy of levels
 - b. Labels, explicit and implicit
 - c. MAC tuples
3. Tranquility
 - a. Strong tranquility
 - b. Weak tranquility
4. Integrity models
 - a. Requirements
 - i. Users won't write their own programs, but will use existing programs, databases, etc.
 - ii. Programmers develop and test programs on non-production systems
 - iii. Installing a program from the development system requires a special process
 - iv. This process must be controlled and auditable
 - v. System managers must be able to access the system state and the system logs
 - b. Separation of duty
 - c. Separation of function
 - d. Auditing
5. Biba: mathematical dual of BLP
 - a. P may read O if $L(P) \leq L(O)$ and $C(P) \subseteq C(O)$
 - b. P may write O if $L(O) \leq L(P)$ and $C(O) \subseteq C(P)$
 - c. Combined with BLP: continue example

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