

Outline for April 12, 2005

Reading: §4.5, 5.1, 5.2–5.2.2, 5.3

Discussion

“Our ancestors, and those who were considered to be wise, were accustomed to say that it was necessary to control Pistoia by means of factions and Pisa by means of fortresses; so they fostered strife in various of their subject towns, so as to control them more easily. In those days, when there was stability of a sort in Italy, this was doubtless sensible; but I do not think it makes a good rule today. I do not believe any good at all ever comes from dissension. On the contrary, on the approach of the enemy, cities which are so divided inevitably succumb at once; the weaker faction will always go over to the invader, and the other will not be able to hold out.”¹

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

Outline

1. High-Level Policy Languages
 - a. Characterization
 - b. Example: DTEL
2. Low-Level Policy Languages
 - a. Characterization
 - b. Example: Tripwire configuration file
3. Goals of Confidentiality Policies
4. Bell-LaPadula Model with Levels Only
 - a. Security Levels
 - b. Simple Security Property
 - c. *-Property
 - d. Basic Security Theorem
5. Bell-LaPadula Model
 - a. Compartments
 - b. BLP as lattice structure
 - c. Simple Security Property
 - d. *-Property
 - e. Basic Security Theorem
6. DG/UX B2 UNIX System
 - a. Hierarchy of levels
 - b. Labels, explicit and implicit
 - c. MAC tuples
7. Tranquility
 - a. Strong tranquility
 - b. Weak tranquility

1. Niccolò Machiavelli, *The Prince*, George Bull trans., Penguin Books, New York, NY ©1995, p. 67