Outline for May 3, 2013

Reading: §8.1–8.2, [KR02][1] **Assignments due:** Homework #3, due May 10, 2013

1. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
2. Problem with instantiation of Bell-LaPadula Model
   a. Covert channel example: what is "writing"?
   b. Composition of lattices
   c. Principles of autonomy and security
3. Deterministic noninterference
   a. Model of system
   b. Example
   c. Relationship of output to states
   d. Projections and purge functions

Table of Notation

notation	*meaning*
S	set of subjects s
Σ	set of states σ
O	set of outputs o
Z	set of commands z
C	set of state transition commands (s, z), where subject s executes command z
C^*	set of possible sequences of commands $c_0, \ldots, c_{n_i}$
ν	empty sequence
c_s	sequence of commands
$T(c, \sigma_i)$	resulting state when command c is executed in state σ_i
$T^*(c_s, \sigma_i)$	resulting state when command sequence c_s is executed in state σ_i
$P(c, \sigma_i)$	output when command c is executed in state σ_i
$P^*(c_s, \sigma_i)$	output when command sequence c_s is executed in state σ_i
$proj(s, c_s, \sigma_i)$	set of outputs in $P^*(c_s, \sigma_i)$ that subject s is authorized to see
$\pi_{G,A}(c_s)$	subsequence of c_s with all elements (s, z), $s \in G$ and $z \in A$ deleted
$dom(c)$	protection domain in which c is executed
$\sim^{dom(c)}$	equivalence relation on system states
$\pi'_d(c_s)$	analogue to π above, but with protection domain and subject included

[1] This is available in the Resources area of SmartSite; look in the folder "Handouts"