

Principles of Information Security CS 5323 Lecture 14

Prof. William Winsborough
October 23, 2007

Business

- For Tuesday 10/23, read Gollman Chapter 8
- Tuesday 10/30 and Thursday 11/1 you will have guest lectures by Prof. Hugh Maynard about intrusion attacks and their detection

23 October 2007

Winsborough CS 5323 Lecture 14

2

Security Models

- A security model is a formal specification of a system for expressing and enforcing a security policy

23 October 2007

Winsborough CS 5323 Lecture 14

3

State Machines

- Transition systems
 - A set of states
 - A set of inputs Σ
 - Optionally, a set of outputs
 - A transition function $S \times \Sigma \rightarrow S$

23 October 2007

Winsborough CS 5323 Lecture 14

4

State Machines

- Transition systems
 - A set of states, S
 - A set of inputs, Σ
 - Optionally, a set of outputs, Γ
 - A transition function $\delta: S \times \Sigma \rightarrow S \times \Gamma$
- Security properties can be modeled as sets of states that are deemed secure
- If the transition function can be shown to preserve the security property, then when the system is started in a secure state, all reachable states will also be secure

23 October 2007

Winsborough CS 5323 Lecture 14

5

Bell-LaPadula Model (BLP)

- Enforces the multilevel security (MLS) policy
- State machine model
 - Confidentiality
 - Uses an access control matrix and security levels
- Components
 - S , set of subjects
 - O , set of objects
 - $A = \{\text{execute, read, append, write}\}$, access operations
 - (L, \leq) , security levels
- Access matrix
 - $B = \wp(S \times O \times A)$, set of all access matrix tables
 - $b \in B$, an individual access matrix table

23 October 2007

Winsborough CS 5323 Lecture 14

6

BLP State Set

- A state is given by (b, M, f) where
 - b is as above
 - $M = (M_{so})_{s \in S, o \in O}$ is an access permission matrix
 - $f = (f_s, f_c, f_o)$ in which
 - $f_s: S \rightarrow L$ gives the subject's max security level
 - $f_c: S \rightarrow L$ gives the subject's current security level
 - $f_o: O \rightarrow L$ gives the object's classification

23 October 2007

Winsborough CS 5323 Lecture 14

7

Security Policies

- Simple security property
 - No read up
 - State (b, M, f) satisfies simple security if for each $(s, o, a) \in b$ in which a is read or write, $f_o(o) \leq f_s(s)$
- Star property
 - No write down
 - For all $(s, o, a) \in b$, if a is append or write, then $f_c(s) \leq f_o(o)$ and $f_o(o') \leq f_o(o)$ for all $o' \in O$ such that $(s, o', a') \in b$ and a' is read or write

23 October 2007

Winsborough CS 5323 Lecture 14

8

Discretionary Security Property

- (b, M, f) satisfies the ds-property if for each element $(s, o, a) \in b$ we have $a \in M_{so}$

23 October 2007

Winsborough CS 5323 Lecture 14

9

Basic Security Theorem

- A state is *secure* if the ss-, *- , and ds-properties are satisfied
- A transition is secure if it starts and ends at a secure state
- Theorem: if all state transitions are secure and if the initial state is secure, then every reachable state will also be secure
- McLean argued that this definition of security for a transition is too permissive

23 October 2007

Winsborough CS 5323 Lecture 14

10