

Principles of Information Security CS 5323 Lecture Eight

Prof. William Winsborough
September 25, 2007

Business

- Return and discuss test today
 - Average score was 38
 - The high was 50
 - The low was 24
- I plan to have another exam covering material we (read and) discussed in class October 11
 - This one will be worth about 20% of the final grade

25 September 2007

Winsborough CS 5323 Lecture 8

2

Access Control Matrix Model

- Let A be the set of actions that can be performed on objects
- The state of the authorization system is given by a triple (S,O,M) in which
 - S is the set of subjects the system has currently
 - O is the set of objects the system has currently
 - $M[s,o] \subseteq A$ contains the access rights subject $s \in S$ currently has for object $o \in O$

25 September 2007

Winsborough CS 5323 Lecture 8

3

Capabilities

- Stores rights in association with the subject
- Each subject s has an unforgeable token that specifies $M[s,o_1], M[s,o_2], \dots, M[s,o_n]$, where $\{o_1, o_2, \dots, o_n\}$ enumerates O
- Used for discretionary access control
- Difficult to enumerate subjects that have access to a given object
- Difficult to revoke rights

25 September 2007

Winsborough CS 5323 Lecture 8

4

Access Control Lists

- Stores rights in association with the object
 - Much more common
- Each object o has associated with it a list of subjects together with their rights on o
 - List specifies $M[s_1,o], M[s_2,o], \dots, M[s_n,o]$, where $\{s_1, s_2, \dots, s_n\}$ enumerates S

25 September 2007

Winsborough CS 5323 Lecture 8

5

Intermediate Abstractions

- Groups aggregate users
 - Invites use of *negative permissions*, which can cause *policy conflicts* (and hampers efficiency)
- *Privileges* aggregate operations (OS level)
- Roles aggregate operations at the application level
 - In this sense, activating a role resembles invoking an application

25 September 2007

Winsborough CS 5323 Lecture 8

6

Protection Rings

- Linearly ordered protection number relates subjects (processes) and objects
 - Subjects are numbered according to how trusted they are
 - Objects are numbered according to how important their integrity is
- Example ordering
 - 0 – operating system kernel
 - 1 – operating system
 - 2 – utilities
 - 3 – user processes

25 September 2007

Winsborough CS 5323 Lecture 8

7

Partial Orders

- Not all elements (labels) have to be comparable
- Def: Given a set (of security labels) L and a relation $\leq \subset L \times L$, (L, \leq) is a partial ordering if it is
 - Reflexive: for all $a \in L$, $a \leq a$
 - Transitive: for all $a, b, c \in L$, if $a \leq b$ and $b \leq c$, then $a \leq c$
 - Anti-symmetric: for all $a, b \in L$, if $a \leq b$ and $b \leq a$, then $a = b$

25 September 2007

Winsborough CS 5323 Lecture 8

8

Examples

- $(\wp(X), \subseteq)$, the powerset of a set X ordered by subset
- $(\mathbb{N}, |)$, the natural numbers ordered by “divides”
- (Σ^*, \leq) , the set of strings ordered by prefix ($\beta \leq \alpha$ if there is a string γ such that $\alpha = \beta\gamma$)
- VSTa Microkernel uses (Σ^*, \leq) in which $\Sigma = \mathbb{N}$
 - As in most systems, the policy is that a subject labeled α can read an object labeled β if $\beta \leq \alpha$

25 September 2007

Winsborough CS 5323 Lecture 8

9

Lattices

- Lattices are partial orders in which least upper bounds and greatest lower bounds are guaranteed to exist

25 September 2007

Winsborough CS 5323 Lecture 8

10

Multilevel Security

- Mandatory Access Control (MAC) policies and multilevel security policies of the “Orange Book” are based on earlier procedures based on security level and clearance
- Need-to-know policies were based on:
 - H , a set of (linearly ordered) *classifications*
 - C , a set of *categories*; a *compartment* is a set of categories
 - Security labels have the form (h,c) , in which $h \in H$ is a security level and $c \subseteq C$ is a compartment
 - The partial ordering \leq of security labels is given by $(h_1, c_1) \leq (h_2, c_2)$ iff $h_1 \leq_H h_2$ and $c_1 \subseteq c_2$

25 September 2007

Winsborough CS 5323 Lecture 8

11