

Principles of Information Security CS 5323 Lecture Seven

Prof. William Winsborough
September 20, 2007

Business

- Read Gollmann Chapter 5 for Tuesday 9/25
- Test today – first part of the hour

20 September 2007

Winsborough CS 5323 Lecture 7

2

Access Control Basics

- Chapter 4 from Gollmann
- AC can be performed at several levels
 - (Service)
 - Application
 - Operating system
 - Hardware
- AC is a pretty effective means of managing *integrity*
- Except in systems that exist rarely outside the military, AC is not very effective at preserving *confidentiality*
 - As soon as data is released, control over it is lost and the recipient must be trusted

20 September 2007

Winsborough CS 5323 Lecture 7

3

Reference Monitor

- Enforcement point between subject and object
- Mediates all action requests
 - Determines whether the requested action is authorized on the designated object
 - If so, permits the action to be performed on the object

20 September 2007

Winsborough CS 5323 Lecture 7

4

Some Terminology

- Principals are entities that can be granted access rights and can make statements
- Subjects are active entities that operate on behalf of one or more principals
 - Actions are permitted based on the access rights of the represented principal
 - Subjects are also objects
- An important case in which a principal may not be a person:
 - Source code may be considered a principal (Java), and as such may be granted extensive or limited access rights, depending on code integrity level

20 September 2007

Winsborough CS 5323 Lecture 7

5

Access Modes

- *Access modes* encode actions that can be performed on a given object
 - Term mainly used in OS (file system) context
- *Observe* versus *alter*
 - Lots of different variants across different systems
- Unix file system access modes
 - File: Read, write (but not read), execute
 - Directory: List, create or rename, search

20 September 2007

Winsborough CS 5323 Lecture 7

6

Ownership

- In *discretionary* AC models, resources have owners
 - Owners determine who is authorized for which actions on their resources
- In *mandatory* AC models, essentially the system owns everything
 - A system-wide policy determines access rights for all objects

20 September 2007

Winsborough CS 5323 Lecture 7

7

Access Control Matrix Model

- Let A be the set of actions that can be performed on objects
- System is a state machine in which state is given by (S, O, M) ,
 - $M[s, o] \subseteq A$ gives access rights of subject $s \in S$ for object $o \in O$

20 September 2007

Winsborough CS 5323 Lecture 7

8

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

20 September 2007

Winsborough CS 5323 Lecture 7

9

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

20 September 2007

Winsborough CS 5323 Lecture 7

10

Intermediate Abstractions

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

20 September 2007

Winsborough CS 5323 Lecture 7

11