

## Principles of Information Security CS 5323 Lecture Eight

Prof. William Winsborough  
September 25, 2008

## Business

- Recall:
  - Read chapter 8
  - No class Thursday Oct. 2
    - I'm giving a keynote talk that day at PST2008, Sixth Annual Conference on Privacy, Security and Trust, Fredericton, New Brunswick, Canada
  - Tuesday October 7 will be devoted to review
    - Bring your questions
  - Thursday October 9 will be midterm 1
    - It will cover material from the first 7 chapters and lectures through Thursday 9/25
- Questions from previous lectures?

25 September 2008

Winsborough CS 5323 Lecture 8

2

## Chapter 7: Hybrid Policies

- Overview
- Chinese Wall Model
- Clinical Information Systems Security (CISS) Policy
- ORCON
- RBAC

25 September 2008

Winsborough CS 5323 Lecture 8

3

## Overview

- Chinese Wall Model
  - Focuses on conflict of interest
- CISS Policy
  - Combines integrity and confidentiality
- ORCON
  - Combines mandatory, discretionary access controls
- RBAC
  - Base controls on job function

25 September 2008

Winsborough CS 5323 Lecture 8

4

## ORCON

- Problem: organization creating document wants to control its dissemination
  - Example: Secretary of Agriculture writes a memo for distribution to her immediate subordinates, and she must give permission for it to be disseminated further. This is "originator controlled" (here, the "originator" is a person).

25 September 2008

Winsborough CS 5323 Lecture 8

5

## Requirements

- Subject  $s \in S$  marks object  $o \in O$  as ORCON on behalf of organization  $X$ .  $X$  allows  $o$  to be disclosed to subjects acting on behalf of organization  $Y$  with the following restrictions:
  1.  $o$  cannot be released to subjects acting on behalf of other organizations without  $X$ 's permission; and
  2. Any copies of  $o$  must have the same restrictions placed on it.

25 September 2008

Winsborough CS 5323 Lecture 8

6

## DAC Fails

- Owner can set any desired permissions
  - This makes 2 unenforceable

25 September 2008

Winsborough CS 5323 Lecture 8

7

## MAC Fails

- First problem: category explosion
  - To simulate ORCON in BLP, one could create a new category  $C$  that is part of the label of  $o$  and included in the categories for which owner-organization and possessor-organization members have clearance
  - But this creates too many categories to be practical
- Second problem: category management
  - MAC classification, categories centrally controlled, and access controlled by a centralized policy
  - ORCON controlled locally

25 September 2008

Winsborough CS 5323 Lecture 8

8

## ORCON Combines MAC and DAC

- The owner (possessor) of an object cannot change the access controls of the object.
- When an object is copied, the access control restrictions of that source are copied and bound to the target of the copy.
  - These are MAC (owner (possessor) can't modify access rights)
- The creator (originator) can alter the access control restrictions on a per-subject and per-object basis.
  - This is DAC (creator can modify access rights)

25 September 2008

Winsborough CS 5323 Lecture 8

9

## RBAC

- Access depends on function, not identity
  - Example:
    - Allison, bookkeeper for Math Dept, has access to financial records.
    - She leaves.
    - Betty hired as the new bookkeeper, so she now has access to those records
  - The role of “bookkeeper” dictates access, not the identity of the individual.

25 September 2008

Winsborough CS 5323 Lecture 8

10

## Definitions

- Role  $r$ : collection of job functions
  - $trans(r)$ : set of authorized transactions for  $r$
- Active role of subject  $s$ : role  $s$  is currently in
  - $actr(s)$
- Authorized roles of a subject  $s$ : set of roles  $s$  is authorized to assume
  - $authr(s)$
- $canexec(s, t)$  iff subject  $s$  can execute transaction  $t$  at current time

25 September 2008

Winsborough CS 5323 Lecture 8

11

## Axioms

- Let  $S$  be the set of subjects and  $T$  the set of transactions.
- *Rule of role assignment*:  
 $(\forall s \in S)(\forall t \in T) [canexec(s, t) \rightarrow actr(s) \neq \emptyset]$ .
  - If  $s$  can execute a transaction, it has an active role
  - This ties transactions to roles
- *Rule of role authorization*:  
 $(\forall s \in S) [actr(s) \in authr(s)]$ .
  - Subject must be authorized to assume an active role (otherwise, any subject could assume any role)

25 September 2008

Winsborough CS 5323 Lecture 8

12

## Axiom

- *Rule of transaction authorization:*  
 $(\forall s \in S)(\forall t \in T)$   
[*canexec*(*s*, *t*)  $\rightarrow$  *t*  $\in$  *trans*(*actr*(*s*))].  
– If a subject *s* can execute a transaction, then the transaction is an authorized one for the role *s* has assumed

25 September 2008

Winsborough CS 5323 Lecture 8

13

## Containment of Roles

- Trainer can do all transactions that trainee can do (and then some). This means role *r* contains (or dominates) role *r'* (*r* > *r'*)  
 $(\forall s \in S)[r' \in \text{authr}(s) \wedge r > r' \rightarrow r \in \text{authr}(s)]$

25 September 2008

Winsborough CS 5323 Lecture 8

14

## Separation of Duty

- Let *r* be a role, and let *s* be a subject such that *r*  $\in$  *auth*(*s*). Then *meauth*(*r*) (for mutually exclusive authorizations) is the set of roles that *s* cannot be assigned because of the separation of duty requirement.
- (Static) separation of duty:  
 $(\forall r_1, r_2 \in R) [r_2 \in \text{meauth}(r_1) \rightarrow$   
[ $(\forall s \in S) [r_1 \in \text{authr}(s) \rightarrow r_2 \notin \text{authr}(s)] ] ]$

25 September 2008

Winsborough CS 5323 Lecture 8

15

## Key Points

- Hybrid policies deal with both confidentiality and integrity  
– Different combinations of these
- ORCON model neither MAC nor DAC  
– Actually, a combination
- RBAC model controls access based on job function

25 September 2008

Winsborough CS 5323 Lecture 8

16