

CS590U

## Access Control: Theory and Practice

Lecture 2 (August 28<sup>th</sup>)  
More Project Ideas & Access  
Control Matrix Models



### An Advertisement

---

- Security Reading Group
  - Meeting weekly on Mondays 3pm-4pm
  - Upcoming meeting is on Wednesday Sep 3<sup>rd</sup>
  - Place: Conference room in REC 216
  - Mailing list: security-reading-group@cs
    - to join, log on to a CS machine and run mailer, then type command add ... to security-reading-group



## Another Advertisement

---

- Reading group on trust
  - Topic: Trust establishment, reputation systems, trust management, and their applications to e-commerce, P2P, and ad-hoc networks
  - Wednesdays at 10:30am
  - Place: conference room in REC 216

3



## Yet Another Advertisement

---

- CERIAS Computer Security Seminar (CS590E)
  - Wednesdays 4:30pm to 5:30pm
- We need speakers!
- Anyone giving a conference talk in the Fall?
- Do you know anyone doing so?
- Anyone just want to give a talk?

4



## Reminders

---

- Pre-proposal due next Thursday
  - Affect whether you will be able to do the project you are most interested in
  
- See me after class if you are interested in a project that I didn't list references

5

More Project Ideas



## More Project Ideas (See Syllabus for Details)

---

- Security Analysis of Administrative Models for RBAC
- Using Constraint Datalog to Analyze XrML and XACML
- Distributed Evaluation for RT<sub>1</sub>

7



## RTML

---

- Develop a standard format for expressing credentials and policies in RT
- Continue previous work
  - See paper on syllabus.
- Also need to consider needs driven by other applications, such as ATN

8



## Cryptographic Approaches to ATN

---

- Zero-knowledge proof
- Storing cryptographic commitments in credentials rather than actual values
- Using secure multi-party computation protocols

9



## Fuzzier Project Topics

---

- Access Control for XML documents
- Access Control in Computer Supported Collaborative Work (Groupware)
- Access control requirements in healthcare, financial industry, or universities, etc.

10

## The Access Matrix Model



### History

---

- Lampson'1971
  - "Protection"
- Refined by Graham and Denning'1972
  - "Protection---Principles and Practice"
- Harrison, Ruzzo, and Ullman'1976
  - "Protection in Operating Systems"



## Access Matrix

- A set of subjects  $S$
- A set of objects  $O$
- A set of rights  $R$
- An access control matrix
  - one row for each subject
  - one column for each subject/object
  - elements are right of subject on another subject or object

13



## Special Rights in Graham-Denning Model

- Each subject/object has an owner
- Each subject has a controller (which may be itself)
- A right may be transferable or nontransferable

		Objects				
Subjects	$S_1$	$S_2$	$S_3$	$O_1$	$O_2$	$O_3$
$S_1$	control			owner	read write	
$S_2$		control	read*			execute
$S_3$			control		owner	



## Eight Commands in Graham-Denning Model

---

1. subject  $x$  creates object  $o$ 
  - no precondition
  - add column for  $o$
  - place 'owner' in  $A[x,o]$
2. subject  $x$  creates subject  $s$ 
  - no precondition
  - add row and column for  $s$
  - place control, 'owner' in  $A[x,s]$

15



## Eight Commands in Graham-Denning Model

---

3. subject  $x$  destroys object  $o$ 
  - precondition: 'owner' in  $A[x,o]$
  - delete column  $o$
4. subject  $x$  destroys subject  $s$ 
  - precondition: 'owner' in  $A[x,s]$
  - delete row and column for  $s$

16



## Eight Commands in Graham-Denning Model

---

5. subject  $x$  grants a right  $r/r^*$  on object  $o$  to subject  $s$ 
  - precondition:  $\text{'owner'}$  in  $A[x,o]$
  - stores  $r/r^*$  in  $A[s,o]$
6. subject  $x$  transfers a right  $r/r^*$  on object  $o$  to subject  $s$ 
  - precondition:  $r^*$  in  $A[x,o]$
  - stores  $r/r^*$  in  $A[s,o]$

17



## Eight Commands in Graham-Denning Model

---

7. subject  $x$  deletes right  $r/r^*$  on object  $o$  from subject  $s$ 
  - precondition:  $\text{'control'}$  in  $A[x,s]$  or  $\text{'owner'}$  in  $A[x,o]$
  - delete  $r/r^*$  from  $A[s,o]$

18



## Eight Commands in Graham-Denning Model

---

8. subject  $x$  checks what rights subject  $s$  has on object  $o$  [ $w := \text{read } s, o$ ]
  - precondition: `control' in  $A[x, s]$  OR `owner' in  $A[x, o]$
  - copy  $A[s, o]$  to  $w$

19



## The HRU Model

---

- Generalize Access Matrix models to allow one to specify an arbitrary set of commands
- Consider properties of an access control system when state changes

20



## Protection System

---

- A protection system has
  - a finite set of generic rights
  - a finite set of commands

21



## Commands

---

- A command has the form

```
command a( $X_1, X_2, \dots, X_k$ )
  if
     $r_1$  in ( $X_{s1}, X_{o1}$ ) and ... and  $r_m$  in ( $X_{sm}, X_{om}$ )
  then
    op1 ... opn
  end
```

22



## Primitive Operations

---

- enter  $r$  into  $(X_s, X_o)$
- delete  $r$  from  $(X_s, X_o)$
- create subject  $X_s$
- create object  $X_o$
- delete subject  $X_s$
- delete object  $X_o$

23



## A Protection System as a State Transition System

---

- The matrix is the state
- State changes by executing commands
- The (Simple) Safety Analysis Problem
  - determine whether a specific subject could get certain access to a specific object in some state

24



## Simple Safety Analysis is Undecidable

---

- Any Turing machine can be encoded using a protection system
- Surprising? Maybe not.
  - the commands basically give full power of programming languages

25



## Why Care About Simple Safety Analysis?

---

- Suppose that there exists an algorithm to decide safety, how can we use it?

26