Security (CS4028)

Lecture 11. Access Control

Chunyan Mu

chunyan.mu@abdn.ac.uk

The School of Natural and Computing Sciences

Schedule

	Week	Lecture 1	Lecture 2	Tutorial
	1	Intro to course & security	Intro to Crypto	I
	2	Symmetric Crypto	Hash	Math for crypto
	3	Asymmetric Crypto-1	Asymmetric Crypto-2	Symmetric Crypto
	4	Signatures	Zero Knowledge Proof	Asymmetric Crypto
	5	Certificates	Authentication	Signature & certificates
⇒	6	Access Control	AC models	Authentication
	7	Information flow control	Information flow control	Access control
	8	Security Mgt	Protocols	Information flow & mgt
	9	Network security	Network security	Protocols
	10	Advanced topics	Advanced topics	Network security
	11	Revision		

Outline

Outline

Security policies

Intuitive questions

Suppose that a human being wants to use or access a protected computer:

- How should we decide whether that user is allowed to use the resource?
- What do we need to know about the user?
- What do we need to know about the resource?
- How might we prevent that user from using the resource?

Security policies

Security policies

- A security policy is a statement of what is and what is not allowed
- A security mechanism is a method, tool, or procedure for enforcing a security policy

Security implementation in real life

- In real life, we add mechanisms to prevent unauthorised access to sensitive resources, e.g.
  - locks, or
  - guards
- How do you gain access to protected resources?
  - locks are opened with keys, and keys must be distributed to users;
  - guards only allow certain people in

These two notions mirror two fundamental ways of controlling access to resources in computer systems!

Computer security issues

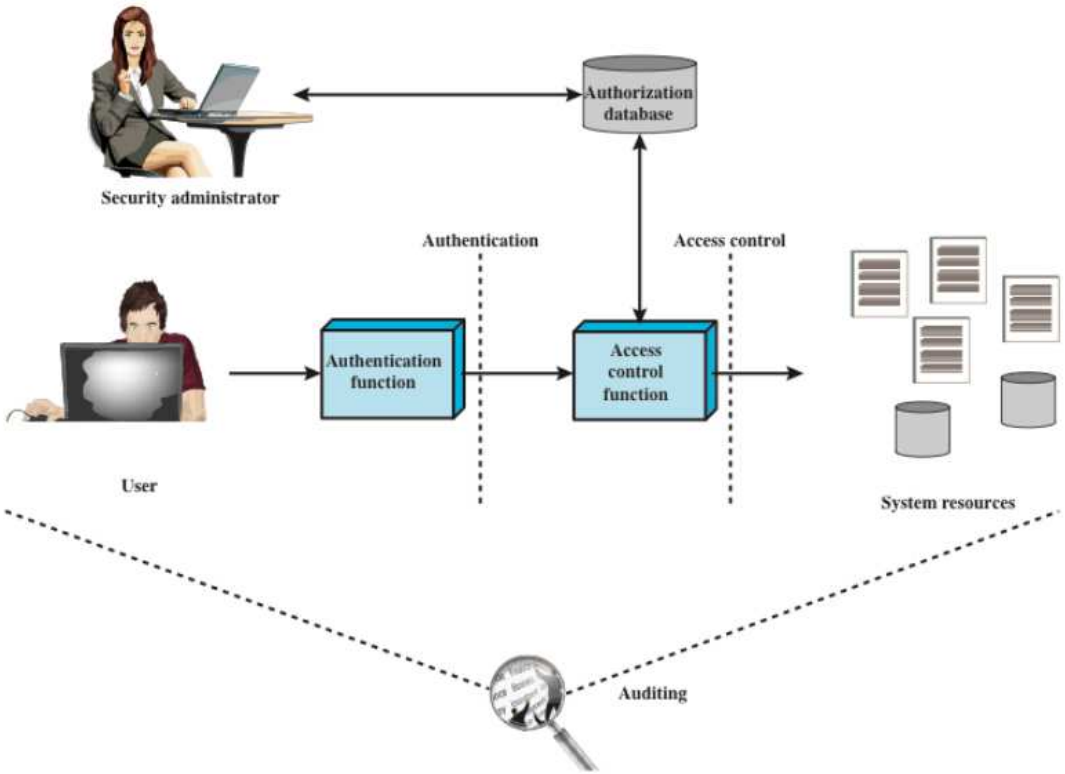
In a computer system, the following issues need to be addressed

- How do we control which people can use the computer system?
- How do we control which programs a user can run?
- How do we control which resources a process can access?
- How do we protect processes that share computer resources from each other?

Fundamental techniques

- Authentication
  - corroborates the identities of users
  - is about who you are
- Access control (authorisation)
  - limits access to program and resources
  - is about what is and what is not allowed to you
  - the main focus of this part of the course
- Audit
  - independent review of system records and activities
  - system controls are adequate
  - compliance with policy and procedures
  - detect breaches
- Information flow control
  - to ensure that the information propagates throughout the execution environment without security violations

AAA: Authentication-Authorisation-Auditing

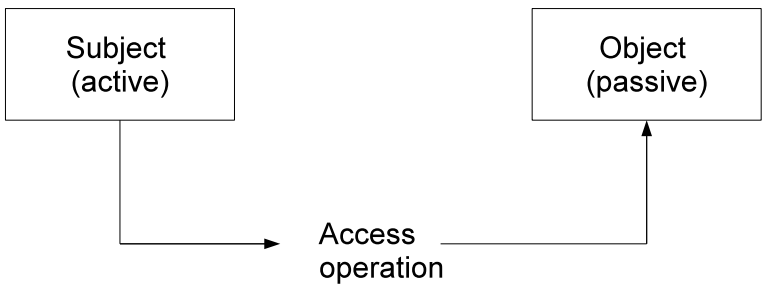


Source: Stalling-Brown "Computer Security"

Outline

What is access control?

- Authentication is about "who you are"; access control is about "who may do what to what".
  - **Subject**: active entity, *e.g* users, processes, etc
  - **Object**: files, directories, devices, etc
- Access control is a generic term for the process(es) by which a computer system controls the **interaction** between *users* and *system resources*

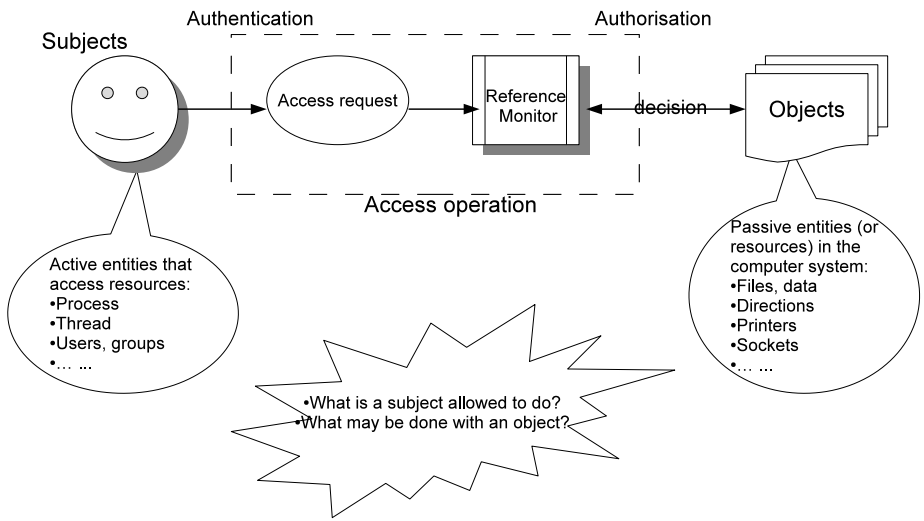


Why use access control?

- Prevents users from having unlimited access to system resources
- Limit access of unauthorised users that manage to break in
- AC is not required if access to resources does not need to be constrained
- Early stand-alone PCs (DOS, Windows 95) could not (and arguably did not need to) enforce access control.

Access control

- A **user** requests **access** (read, write, print, etc.) to a **resource** in the computer system
- The **reference monitor** establishes the validity of the request and returns a decision either granting or denying access to the user



An analogy: Locks and keys

- In a paper-based office, certain documents should only be read by certain individuals
- We could implement security by:
  - storing documents in filling cabinets;
  - and issuing keys to the relevant individuals for the appropriate cabinets
- The reference monitor is the set of (locked) filing cabinets:
  - An access request (an attempt to open a filing cabinet) is granted if the key fits the lock, and denied otherwise.

Reference Monitor

- The reference monitor is the entity within a system (an abstract machine) that mediates all access requests by subjects
- The reference monitor is responsible for authorisation checks
- Access matrix $M : S \times O \rightarrow 2^R$
- Access rights: e.g. read, write, execute
  - e.g. S may read O iff read $\in M(S, O)$

M	...	O	...
...		...	
S	...	$R_1..R_n$	...
...		...	

Access modes

- There are two basic modes of interaction between a subject and an object:
  - observe: look at the content of an object, i.e., read;
  - alter: change the contents of an object i.e., write
- Accessing an object can be regarded as initiating a flow of information
- A subject may observe (read) an object: information flows from object to subject;
- A subject may alter (write to) an object: information flows from subject to object.

Outline

What is an access control model?

- "*The model has the ability to* ***represent abstractly*** *the elements of computer systems and of security that are relevant to a treatment of classified information stored in a computer system*"
  - Bell-Lapadula, 1976
- A model includes elements that are used to represent the system, such as
  - sets, relations and functions
- In the context of access control, a model typically describes a reference monitor

Why are models useful?

- It may be possible to deduce formal results about the security of the system from the model
  - e.g. given a specification of security policy, we can answer the question "*Does the system maintain the security policy?*"
- A model may also generate rules that can provide a blueprint for an implementation
  - It may also assist in verifying that an implementation meets requirements.

Classification

Access control mechanisms exits two enforce policies.

Discretionary policies (DAC)

- based on identities or other characteristics of users
- ownership of resources is typically important
- Unix access control enforces such a policy
- common in commercial systems

Mandatory policies (MAC)

- are independent of user's identities
- characteristics of resources are important
- access is only allowed if user and object belong to same security domain
- common in government/military systems

Access control matrix

- Introduced by Lampson (1972) and extended by Harrison, Ruzzo and Ullman (1976-8):
  - Columns indexed by objects
  - Rows indexed by subjects
  - Matrix entries are (sets of) access operations
- The foundation of many theoretical security models

	bill.txt	edit.exe	fun.com
Alice	–	$\{x\}$	$\{r, x\}$
Bob	$\{r, w\}$	$\{x\}$	$\{r, w, x\}$

The access control matrix

- A request can be regarded as a triple (s, o, a)
- Indicates that the subject s wants to access object o where a is an access right
- A request is granted (by the reference monitor) if a belongs to the access matrix entry corresponding to subject s and object o

Disadvantages

- The access control matrix is an abstract concept
- It is hard to implement and manage, especially:
  - if the number of subjects and objects is large
  - or if the sets of subjects and objects change frequently

Access Control Lists (ACLs)

- An ACL corresponds to a column in the access control matrix
- The ACL for "fun.com" would be: [(Alice, $\{r, x\}$), (Bob, $\{r, w, x\}$)]
- How would a reference monitor that uses ACLs check the validity of the request (Alice, fun.com, r)?

	bill.txt	edit.exe	fun.com
Alice	–	$\{x\}$	$\{r, x\}$
Bob	$\{r, w\}$	$\{x\}$	$\{r, w, x\}$

Access Control Lists

- Typically represented internally as a (per-object) list of access control entries
  - Each entry includes a user account identifier and an access mask
- An access mask is a bit pattern in which each bit represents a particular access right:
  - if the bit is set then access is granted
  - if 111 represents $\{r, w, x\}$ then 100 represents $\{r\}$ etc
  - If Alice's account identifier is 138 an Bob's is 533, the ACL for "fun.com" would be $[(138, 101), (533, 111)]$

Access Control Lists

- ACLs focus on the objects:
  - Typically implemented at operating system level;
  - Widows NT uses ACLs
- Disadvantage:
  - One major disadvantage of ACLs arises if we want to check the access rights of a particular subject efficiently i.e., if we want to perform "before-the-act per-subject review". This will require looking at every object's ACL.

Capabilities

- Access rights can be kept with the subjects or with the objects
- In the first case, the subject is given a capacity, an unforgeable token that specifies this subject's access rights
- The access rights of our previous example given as capabilities are:
  - Alice's capability: edit.exe: execute; fun.com: execute, read
  - Bob's capability: bill.txt: read, write; edit.exe: execute; fun.com: execute, read, write

Capabilities

- The notion of a capability is, in some sense, the dual of an ACL.
- A capability list corresponds to a row in the access control matrix.
- e.g. Alice's capability list would be: edit.exe: execute; fun.com: execute, read
- how would such a reference monitor check the validity of the request (Alice, fun.come, r)?

	bill.txt	edit.exe	fun.com
Alice	–	$\{x\}$	$\{r, x\}$
Bob	$\{r, w\}$	$\{x\}$	$\{r, w, x\}$

Capabilities

- Typically, capabilities are associated with discretionary access control.
  - when a subject creates a new object, it can give other subjects access to this object by granting them the appropriate capabilities
  - when a subject (process) calls another subject, it can pass on its capability, or parts thereof, to the invoked subject

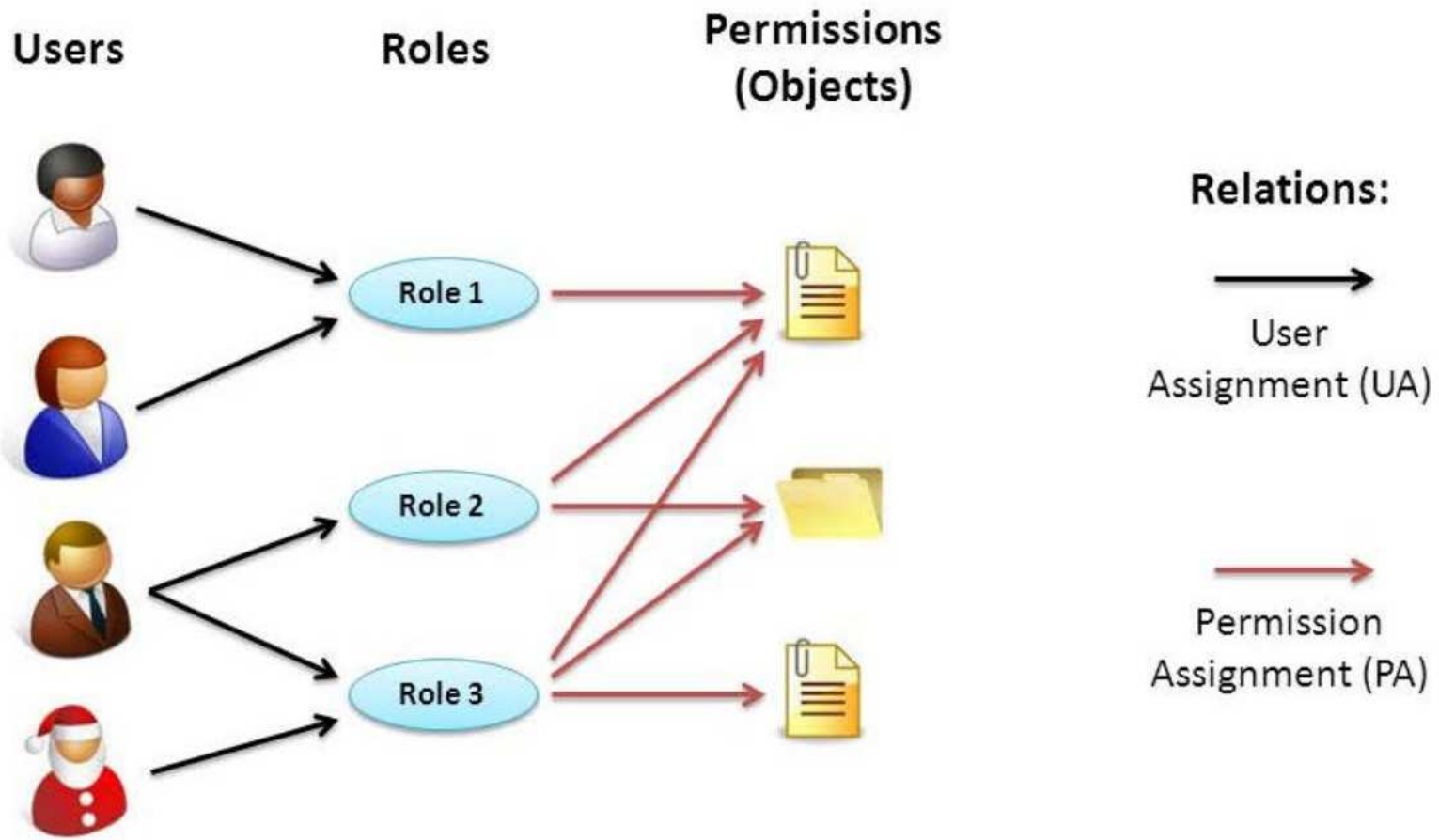
Capabilities: disadvantages

- It is difficult to get an overview of who has permission to access a given object
- It is difficult to revoke a capability:
  - either the operating system has to be given the task
  - or users have to keep track of all the capabilities they have passed on;
  - this problem is particularly awkward when the rights in the capability include the transfer of the capability to third parties

Other approaches to access control

- Role-based Access Control
  - Policy bases access control approvals on the jobs the user is assigned
- Rule-based (or Procedure-oriented) Access Control
  - A list of rules, maintained by the data owner, determines which users have access to objects
- Content-dependent Access Control
  - Access control based on what is contained in the data

RBAC: Role-based Access Control



Outline

Summary

Access control

- Notions, requirements, and fundamental model of access control.
- Essential access control structures, classification, approaches.

Next lecture: security models

- BLP model
- Biba model
- Chinese wall model