Lecture 11

Access Control

1

1

Recall: Security Services

- Confidentiality: ensure data secrecy
- Integrity: ensure that data is not altered
- Authentication: assert who originated data
- Access Control and Authorization: prevent misuse of resources = control access to them
- Availability: assure access to resources, permanence, non-erasure

2

2

Access Control (AC)

- **A "language" for expressing access control policies: who can access what, how and when …**
- **Enforcement of access control**
  - Identify all resources (objects) and their granularity
  - Identify all potential entities that might use objects (subjects)
  - Specify rules for subject/object interaction
  - Guard them in real time

3

3

Model and Terminology

- **Users: humans**
- **Principals: user accounts**
- **Subjects:** processes running on behalf of principals
- **Objects:** resources
  - files, memory regions, processes,
  - peripherals/devices: cameras, printers, routers, plotters, disks, etc.

4

4

Focus of Access Control

- **What a subject is allowed to do**

- **What may be done with an object**

5

5

Access Modes

- **"Look" at an object, e.g.:**
  - Read file
  - Check printer queue
  - Read screen
  - Query database
  - Turn on/use microphone, etc., etc.

- **"Change" an object, e.g.:**
  - Write/append/erase file
  - Print on a printer
  - Display on screen
  - Use speakers (audio out)
  - Send packets via WiFi/Bluetooth, etc., etc.

6

6

Access Modes

4 mode of access: execute, read, append, and write

	Execute	Read	Append	Write
Observe		X		X
Alter			X	X

7

7

UNIX/Linux/*x Operating Systems

- **execute:** execute (program) file, search directory
- **read:** read from file, list directory
- **write:** write (re-write or append) file, create or rename file in directory

8

8

AC Types

Who is in charge of setting the local AC policy?

- **Discretionary Access Control (DAC):** resource owner
- **Mandatory Access Control (MAC):** system-wide policy

9

9

Access Control Structures

- **MAC: Access Control Matrix**
- **MAC: Access Control Lists**
- **DAC: Capabilities**

10

10

Access Control Matrix (ACM)

Object

Subject

	Bill.doc	Edit.exe	Fun.com
Alice	{0}	{execute}	{execute,read}
Bob	{read,write}	{execute}	{execute,read,write}

Note: a real ACM can be huge and SPARSE!

11

11

Access Control Lists (ACLs)

Keep access rights to an object with that object:

- **ACL for bill.doc:**
  - **Bob: read, write**
- **ACL for edit.exe:**
  - **Alice: execute;**
  - **Bob: execute**
- **ACL for fun.com:**
  - **Alice: execute, read;**
  - **Bill: execute, read, write**

- As many ACLs as there are objects
- Each ACL must be either signed or stored in a protected place
- Faster/better when # subjects << # objects

12

12

Capabilities 1/2

- **Capabilities are associated with Discretionary Access Control (DAC)**
- **Reason: difficult to get full view of who has permission to access an object**

13

13

Capabilities 2/2

Keep access rights with the subject:

- **Alice's capabilities:**
  - **[edit.exe:execute];**
  - **[fun.com:execute,read]**
- **Bob's capabilities:**
  - **[bill.doc:read,write]**
  - **[edit.exe:execute]**
  - **[fun.com:execute,read,write]**

- As many capabilities as there are subject/object pairs
- Each capability either signed or otherwise protected
- Hard to revoke in a distributed setting:
  owners and objects must keep track of all issued capabilities
- Faster when # subjects >> # objects

14

14

In Summary

- **Centralized Systems:**
  - **MAC and ACLs are better**
- **Distributed Systems:**
  - **DAC and Capabilities are better**

15

15

ROLE BASED ACCESS CONTROL (RBAC)

16

16

RBAC Basics

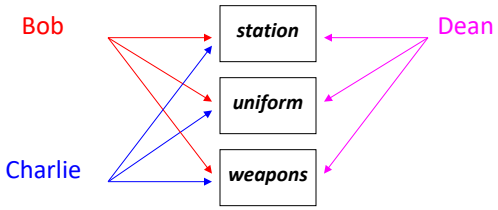
- Users are associated with roles
- Roles are associated with permissions
- A user has permission only if it has a role associated with that permission
- Similar to ACL → uses groups as subjects, not users

17

17

Example: Cops (User/Permission Association)

Bob, Dean, and Charlie are cops.

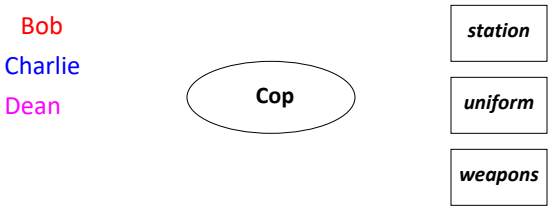


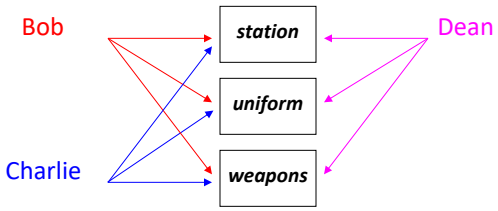
18

18

Example: RBAC

Bob, Dean, and Charlie are cops.

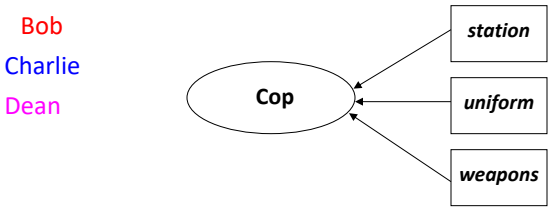


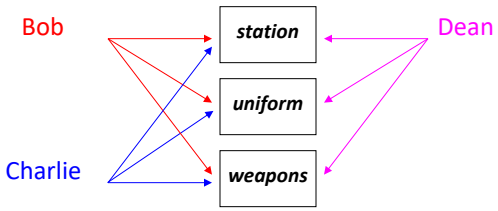


19

19

Example: RBAC

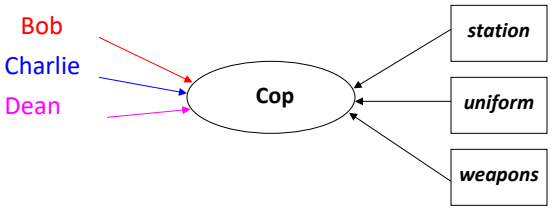




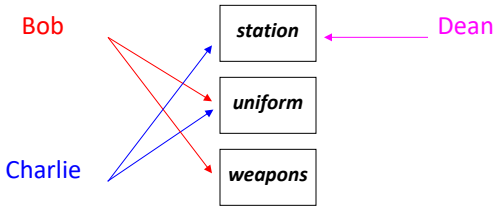
20

20

Example: RBAC



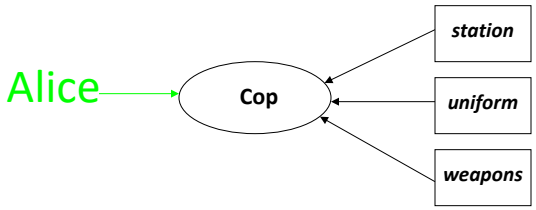
Here RBAC doesn't work …

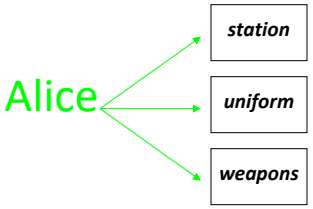


21

21

Example: Alice becomes a Cop





22

22

Some further light readings

https://en.wikipedia.org/wiki/Role-based_access_control

https://en.wikipedia.org/wiki/Bell-LaPadula_model

https://en.wikipedia.org/wiki/Biba_Model

23

23

ADIOS!

24

24