Lecture 18: Mandatory Access Control

CS 5430

3/28/2018

Review: Access control

- Subject: principal to which execution can be attributed
- Object: data or resource
- Operation: performed by subject on object
- Right: entitlement to perform operation

Mandatory Access Control

- Mandatory access control (MAC)
  - not Message Authentication Code (applied crypto), nor Media Access Control (networking)
  - **philosophy:** central authority *mandates* policy
  - information belongs to the authority, not to the individual users
- Examples:
  1. Multi-level security (confidentiality, military)
  2. Biba model (integrity, military)
  3. Clark-Wilson (integrity, business)
  4. Role-based access control (hybrid, organization)
  5. Brewer-Nash (hybrid, consulting firm)

Multi-Level Security/Bell-LaPadula

- Objects and principals have labels $L = (S, C)$
  - Unclassified ≤ Confidential ≤ Secret ≤ Top Secret
  - {} ⊆ {crypto} ⊆ {crypto, U.S.}
  - (Unclassified,{}) ⊑ (Secret,{}) ⊑ (Top Secret, {crypto, U.S.})
- **P may read O iff L(O) ⊑ L(P)**
  - object's classification must be below (or equal to) subject's clearance, eg.,
  - "no read up"
- **P may write O iff L(P) ⊑ L(O)**
  - object's classification must be above (or equal to) subject's clearance
  - "no write down"
- L1 ⊑ L2 means “L1 may flow to L2”

MLS for Integrity (Biba Model)

- Objects and principals have integrity labels
  - Trusted $\sqsubseteq$ Untrusted
- **P may read O iff L(O) $\sqsubseteq$ L(P)**
  - object's classification must be below (or equal to) subject's clearance, eg.,
  - "no read up"
- **P may write O iff L(P) $\sqsubseteq$ L(O)**
  - object's classification must be above (or equal to) subject's clearance
  - "no write down"
- L1 $\sqsubseteq$ L2 means “L1 may flow to L2”

Mandatory Integrity for Business Applications

[Clark and Wilson 1987]

- Studied commercial systems rather than military
- Primary goal is **integrity**, not confidentiality
  - Prevent fraud
  - Prevent error

Clark-Wilson model

- Two levels of security:
  - Constrained: high integrity information, crucial to business, e.g., bank account balances
  - Unconstrained: low integrity information, nonessential to business, e.g., gift selected by customer when account opened
- Constrained data items (CDIs) are meant to satisfy integrity constraints, e.g. teller balance constraint
  - Valid state: all CDIs satisfy their constraints
  - Otherwise invalid
- Unconstrained data items (UDIs) don't have integrity constraints

Clark-Wilson model

- Transformation procedures (TPs):
  - change system from one valid state to another valid state
  - operate on associated CDIs
  - implement **well-formed transactions**
  - e.g., deposit, withdraw, transfer
- Integrity verification procedures (IVPs):
  - test whether CDIs satisfy constraints, hence state is valid
  - e.g. teller balancing drawer at opening and closing of window

Clark-Wilson rules

- **Enforcement rules (ERs):**
  - Followed by system
  - Goal is to enforce the integrity policy
  - Online checking
- **Certification rules (CRs):**
  - Followed by security officer of business
  - Goal is to certify that system will obey integrity policy
  - Offline checking

Commercial systems

Well-formed transactions:

- Transition system from one state to another
- Maintain invariants over state
- e.g. bank teller
  - Trained to perform only certain kinds of transactions from their drawer
  - Maintain invariant: (yesterday's balance) + (today's deposits) – (today's withdrawals) = (today's balance)
- Implemented by transformation procedures (TPs)

Clark-Wilson rules

Rules for well-formed transactions:

- **CR:** IVPs must ensure that CDIs are in a valid state
- **CR:** TPs must maintain validity as invariant
- **ER:** A TP may modify only its associated CDIs
- **CR:** A TP that accepts UDIs as input must validate them as part of transforming them into CDIs

Commercial systems

Separation of duty:

- Transactions require multiple principals
- Principals mutually certify that transaction performed properly
- e.g. purchasing:
  - Purchasing agent creates order, sends order to supplier, receiving agent, and accounting
  - Supplier ships goods to receiving
    - Receiving clerk checks goods against original order and updates inventory
  - Supplier sends invoice to accounting
    - Accountant checks invoice against original order
  - All four principals work together to detect fraud and error

Clark-Wilson rules

Rules for separation of duty:

- **CR:** Users must be authorized to invoke TPs

  part of what security officer is meant to check as part of this certification is that separation of duty is actually part of the authorization policy

- **ER:** Only the security officer may change the authorization policy, and the security officer may not invoke TPs
- **ER:** The system must check that **authorization** policy before performing TPs on behalf of a user
- **ER:** The system must **authenticate** users
- **CR:** All TPs must append enough **audit** information to reconstruct the operation to an append-only CDI

Clark-Wilson rules

Rules for separation of duty:

- **CR:** Users must be authorized to invoke TPs

  part of what security officer is meant to check as part of this certification is that separation of duty is actually part of the authorization policy

- **ER:** Only the security officer may change the authorization policy, and the security officer may not invoke TPs
- **ER:** The system must check that **authorization** policy before performing TPs on behalf of a user
- **ER:** The system must **authenticate** users
- **CR:** All TPs must append enough **audit** information to reconstruct the operation to an append-only CDI

Gold standard

Contributions of Clark-Wilson

- Difference of concerns between commercial and military security models
- Authorized programs
- Certification as distinct from enforcement

ROLE-BASED ACCESS CONTROL

Jobs

- Your access rights depend on job you are performing
  - Student in one class
  - TA in another class
  - Prof in another class?

- Existence of jobs is relatively stable in organization
  - Even if over time the people who perform them change jobs
  - Better not to directly assign rights to user

- Instead, associate rights with the job...

Roles and rights

Role: job function or title

- Users are assigned to roles
- Subjects executing on behalf of users can activate a role to indicate it is now performing that job
  - Least Privilege
  - Amplification of Privilege

Roles and rights

- Roles can be hierarchical
  - e.g. TA, prof
  - Hierarchy is a *partial order*
- Multiple roles may be active simultaneously
- Can be constraints on which roles users can simultaneously be assigned
  - e.g. cannot be both Student and TA in same course
  - provides possibility for Separation of Duty

Roles and rights

- **Rights:**
  - Rights are assigned to roles, not directly to users
  - Relation on (role, obj, rights)
- Role-based access control (RBAC) policy: role assignment plus rights assignment

Roles vs. groups

- Group:
  - set of users
  - can be assigned rights
- Role:
  - set of users
  - can be assigned rights
- **Differences?**
  - Roles are hierarchical and can inherit rights
  - Roles can be activated and deactivated

RBAC, DAC, MAC

Is RBAC a DAC or MAC policy?

- Role assignments typically dictated by organization: MAC
- Right assignments might come from organization or from owners of objects: MAC or DAC

BREWER-NASH

Conflict of interest

Setting: consulting firm

- e.g., stock exchange, investment bank, law firm
- Consultant represents two clients
  - Best interest of those clients conflict
  - Consultant could help one at expense of the other
  - Consultant has a conflict of interest (COI)
- Norms (laws, regulations, ethics) prohibit consultant from exploiting COI
- After some time (days, years, never), COI might expire

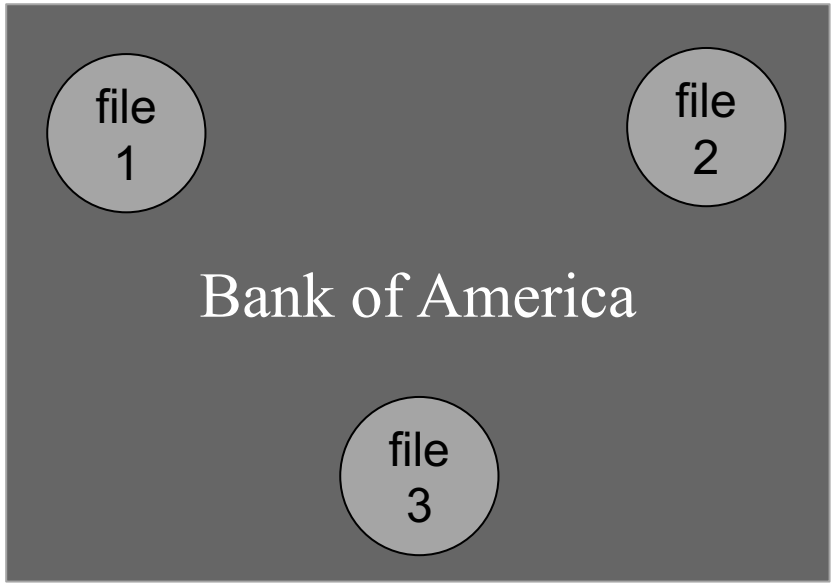
Conflict of interest

- Typical paper implementation:
  - Consultant maintains public CV
    - Entry in CV for each client
    - Entry has been sanitized and approved by client, e.g., "Sep 2015-Apr 2016: consulted on security requirements for a new branch accounting system for a major US retail bank"
  - Manager checks CV before assigning consultant to new client
  - Client receives CV to double-check from their perspective
- Brewer and Nash [1989] invented a MAC policy for this setting
  - Often known as Chinese Wall (CW)
  - Other names: ethics wall, screen

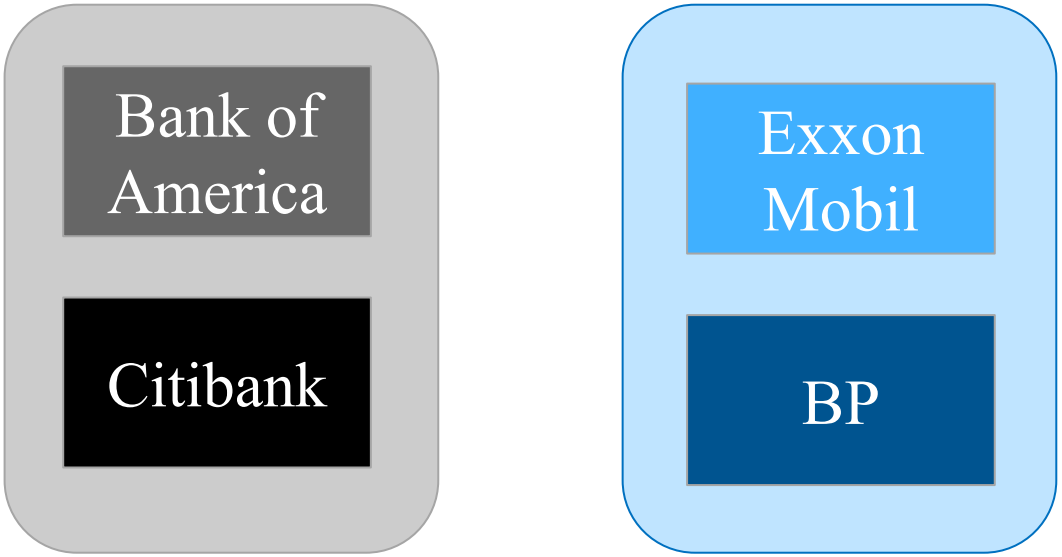
Brewer-Nash model

- Object: contains sensitive information about companies
  - a file about Bank of America's trade secrets
  - but not its addresses, phone numbers, etc.
- Company dataset (CD): all the objects related to a single company
  - all the files about Bank of America
- Conflict of interest class (COI): all the company datasets for which the companies compete
  - all the files about banks

Brewer-Nash model



Brewer-Nash model



CD

COI

Breaches

Prevent two kinds of breaches of the wall:

- One consultant works on more than one CD inside a COI
- Two consultants each work on their own CD inside COI but cooperate to write that information to a shared object

Access control with Brewer-Nash

- When may a subject read an object?
  - **S may read O iff**
    S has never read any O' such that
    COI(O) = COI(O') and CD(O) != CD(O')
  - Subject may not read from two CDs inside same COI
- When may a subject write an object?
  - **S may write O iff**
    S has never read any O' such that
    CD(O) != CD(O')
  - Subject may not write to any other CD after reading from one

Reading with Brewer-Nash

- **S may read O iff**
  S has never read any O' such that
  COI(O) = COI(O') and CD(O) != CD(O')
- If S has never read anything, S has free choice of what to read next
- Once S does read object from CD1 in COI1, a
  around S
  - Cannot read other CDs from same COI
  - But can read from different COI
- If S does read from CD2 in COI2, wall changes shape
  - CD1 and CD2 inside wall
  - All other CDs from COI1 and COI2 outside the wall
- Requires tracking history of objects read by subject

Writing with Brewer-Nash

- **S may write O iff**
  S has never read any O' such that
  CD(O) != CD(O')
- If S has never read anything, S has free choice of what to write
- If S has read from CD1, S may write only to CD1
- Requires tracking history of objects read by subject
- If S has read from CD1 and CD2, S may not write at all
  - e.g. read from Bank of America and Exxon Mobil:
    - Now cannot write anywhere
    - Writing to Bank of America could leak info about Exxon Mobil and vv.
- Seems overly prohibitive...

Users with Brewer-Nash

- A **subject** who has read two CDs may not write
- But that need not be true of a **user**
- Track read objects for:
  - user over its lifetime
  - subject over its lifetime (which is shorter than user)
  - distinguish what user has learned vs. what subject has learned
- As with MLS, user can choose to login at lower security level
  - **Attenuation of privilege:** give up the subject's right to read from CDs that have previously been read by user
  - Subject assigned that security level
  - So user could have multiple subjects with different security levels

Users with Brewer-Nash

Example: Alice has read CD1 from COI1 and nothing from COI2

- Alice could login
  - with right to read CD1
  - or without that right
- Then subject on behalf of Alice reads CD2 from COI2: that is recorded for Alice as well and influences future subjects of hers
- Can Alice's subject write?
  - With right to read CD1: no
  - Without right: yes
- Alice's subject always prohibited from reading CD1' from COI1, regardless of whether right to read CD1 is enabled

So if user wants to work with different CDs, they can! Just disable access to the rest.

Mandatory Access Control

- Mandatory access control (MAC)
  - not Message Authentication Code (applied crypto), nor Media Access Control (networking)
  - **philosophy:** central authority *mandates* policy
  - information belongs to the authority, not to the individual users
- Examples:
  1. Multi-level security (confidentiality, military)
  2. Biba model (integrity, military)
  3. Clark-Wilson (integrity, business)
  4. Role-based access control (hybrid, organization)
  5. Brewer-Nash (hybrid, consulting firm)