CS 5430

Mandatory Access Control, part 2

Prof. Clarkson

Spring 2017

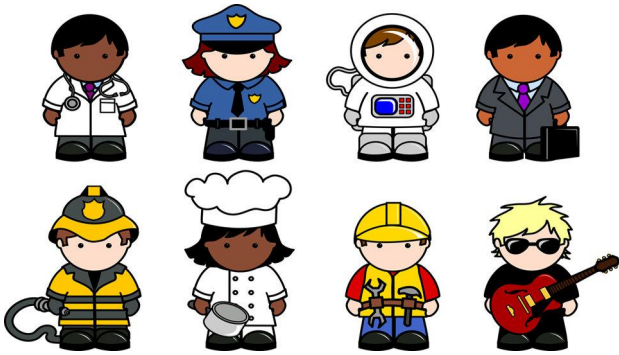
Review: MAC

- 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
- Five case studies:
  1. Multi-level security (military)
  2. Brewer-Nash (consulting firm) // in the middle of this
  3. Role-based access control (organization)
  4. Clinical information systems (medicine)
  5. Clark-Wilson (business)

3. 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

4. CLINICAL INFORMATION SYSTEMS

Medical systems

US:

- Privacy became a concern in medical information systems ca. mid 1990s
- 1996: Health Insurance Portability and Accountability Act (HIPAA)

- No one's happy:
  - privacy advocates consider it inadequate
  - hospitals complain it raises costs
  - patient advocates report it's used by hospital staff as an excuse to be unhelpful

Medical systems

UK:

- 1995-6: attempt by government to centralize all medical records
  - single electronic record that follows you from conception to autopsy
  - security was going to be based on MLS, but that wasn't a good match: e.g., what security level should prescriptions be?
- British Medical Association (BMA) engaged security researchers to develop a policy for clinical information systems
- BMA model [Anderson 1996]
  - guided by stated ethics of medical societies, and advice of practicing clinicians
  - adopted by Union of European Medical Organizations in 1996
  - pilot implementations fielded in private practice and hospital systems in England in late 1990s

BMA model

- Patient: individual who is subject of medical records
  - or an agent for that person who can give consent to be treated
  - patients who are mentally incapacitated, unconscious, or dead: "it's complicated"
- Medical records: information about health, history, or treatment that identifies patient
  - assumes records are about a single individual; obstetrics/gynecology are not
- Clinician: health-care professional who has access to medical records
  - licensed, bound by professional obligation of confidentiality: *"Patients have a right to expect that you will not pass on any personal information which you learn in the course of your professional duties, unless they agree."* [General Medical Council]
  - e.g. doctor, nurse, dentist, pharmacist
  - debates over whether telephone staff, social workers, etc. are included

BMA access control

- A patient may have many medical records
  - Many records within a practice
  - Many practices at which a patient
- **Access control lists:** each medical record (object) has an ACL
  - Identifies which clinicians (subject) have access
  - Only clinicians may be on the ACL, not administrators, lawyers, police, insurance company, employer, ...
  - Being on ACL conveys right to **read and append**
  - No read-only access: auditors and researchers who would need this instead get full access to a temporary copy of record

BMA access control

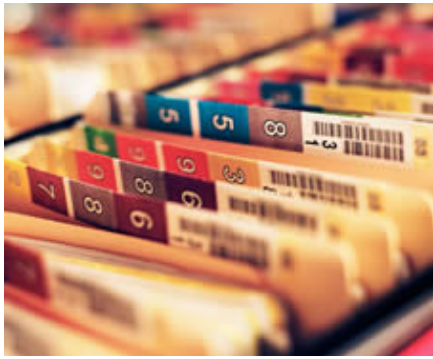
- **Groups:**
  - Clinicians work in teams, so subjects in ACL might be groups
  - Static, e.g., all the clinicians at a small practice
  - Dynamic, e.g., any clinician on duty in patient's ward
- Altering the ACL:
  - One clinician on ACL is marked as responsible
  - Only responsible clinician may alter ACL
- Patient's access:
  - Patient does have read access to own record
  - And "append objection" access
  - In practice these not supported by software

BMA record management

Creation

- Can occur when:
  - New patient registers at a practice
  - Patient is referred from another practice
  - Patient wants to discuss a new highly sensitive condition
- Clinician creates record
  - That clinician is added to the ACL (and presumably marked responsible)
  - Any referring clinician also added to ACL

BMA record management



Access

- Each record carries log of access (read or append) with the subject's identity, date, and time
- Possible to reconstruct record as it existed at any point in time
- Life-critical entries in record require special approval, e.g., Do Not Resuscitate order

BMA record management

Copy between records

- Clinician might want to append information derived from record A to record B
- Permitted if B's ACL is a subset of A's
  - May restrict the set of readers
  - Similar to "no write down" in MLS: can't make information more public
- Or permitted if patient gives consent
  - Similar to declassification by trusted subject in MLS

BMA record management

Copy between records

- Instead of copying, might want to enter into record B "see record A"
- But indicating presence of secret records can itself violate consent
- Example from Netherlands:
  - Implementation: when patient diagnosed with cancer, records removed from computer system.
  - Result: insurers inferred patient had cancer when they saw a blank record
- Possible solution: flag in record to prompt clinician to ask "is there anything else you want to tell me?"

BMA record management

Deletion

- No information may be deleted from record
- Most primary records must be kept for 8 years
  - Some records kept longer, esp. cancer and genetic diseases
  - Clinicians certainly want to keep records until after malpractice suit could be brought
- Can patients insist that their record be destroyed?

BMA consent and notification

- Responsible clinician must obtain consent from patient when:
  - Record is created
  - ACL is modified
  - Responsibility is transferred
- And in each situation notify patient of subjects on ACL
- Consent normally obtained in advance
  - But in emergency or statutory situations may be delayed
  - Delayed consent results in after-the-fact notification
    - Typically occurs annually by letter
    - Patient might then detect unauthorized access

BMA aggregation

- Risky to give any one clinician access to too many records: might be corrupted or blackmailed or hacked, compromising privacy
- So patients must receive special notification if such clinician added to ACL
- What's "too many"?
  - Not uncommon for all clinicians at hospital (maybe 2,000) to be able to access all patients (maybe a million or more)
  - But if 300 such hospitals share an information system, that would mean 600,000 staff have access to the entire population of the US (about 300 million)
  - Typical countermeasure is declaration that unjustified access results in dismissal

5. CLARK-WILSON

Commercial systems

[Clark and Wilson 1987]

- Studied commercial systems rather than military
- Primary goal is **integrity**, not confidentiality
  - Prevent fraud
  - Prevent error
- Two main techniques:
  - Well-formed transactions
  - Separation of duty

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)
- e.g. if error discovered enter a new transaction that accounts for error rather than amending old transaction

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 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

- Integrity verification procedures (IVPs):
  - test whether CDIs satisfy constraints, hence state is valid
  - e.g. teller balancing drawer at opening and closing of window
- 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

Clark-Wilson rules

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

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

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
- Separation of duty
- Certification as distinct from enforcement

Recap: MAC

- Mandatory access control (MAC)
  - **philosophy:** central authority *mandates* policy
  - information belongs to the authority, not to the individual users
- Five case studies:
  1. Multi-level security (military)
  2. Brewer-Nash (consulting firm)
  3. Role-based access control (organization)
  4. Clinical information systems (medicine)
  5. Clark-Wilson (business)

Upcoming events

- [today] A5 due, A6 out

"Whatsoever I shall see or hear in the course of my profession…if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets." – Hippocratic Oath