Lecture 10, April 20

ECS 235B, Foundations of Computer and Information Security

Spring Quarter 2026

Clinical Information Systems Security Policy

- Intended for medical records
  - Conflict of interest not critical problem
  - Patient confidentiality, authentication of records and annotators, and integrity are
- Entities:
  - Patient: subject of medical records (or agent)
  - Personal health information: data about patient's health or treatment enabling identification of patient
  - Clinician: health-care professional with access to personal health information while doing job

Assumptions and Principles

- Assumes health information involves 1 person at a time
  - Not always true; OB/GYN involves father as well as mother
- Principles derived from medical ethics of various societies, and from practicing clinicians

Access

- Principle 1: Each medical record has an access control list naming the individuals or groups who may read and append information to the record. The system must restrict access to those identified on the access control list.
  - Idea is that clinicians need access, but no-one else. Auditors get access to copies, so they cannot alter records

Access

- Principle 2: One of the clinicians on the access control list must have the right to add other clinicians to the access control list.
  - Called the *responsible clinician*

Access

- Principle 3: The responsible clinician must notify the patient of the names on the access control list whenever the patient's medical record is opened. Except for situations given in statutes, or in cases of emergency, the responsible clinician must obtain the patient's consent.
  - Patient must consent to all treatment, and must know of violations of security

Access

- Principle 4: The name of the clinician, the date, and the time of the access of a medical record must be recorded. Similar information must be kept for deletions.
  - This is for auditing. Don’t delete information; update it (last part is for deletion of records after death, for example, or deletion of information when required by statute). Record information about all accesses.

Creation

- Principle: A clinician may open a record, with the clinician and the patient on the access control list. If a record is opened as a result of a referral, the referring clinician may also be on the access control list.
  - Creating clinician needs access, and patient should get it. If created from a referral, referring clinician needs access to get results of referral.

Deletion

- Principle: Clinical information cannot be deleted from a medical record until the appropriate time has passed.
  - This varies with circumstances.

Confinement

- Principle: Information from one medical record may be appended to a different medical record if and only if the access control list of the second record is a subset of the access control list of the first.
  - This keeps information from leaking to unauthorized users. All users have to be on the access control list.

Aggregation

- Principle: Measures for preventing aggregation of patient data must be effective. In particular, a patient must be notified if anyone is to be added to the access control list for the patient's record and if that person has access to a large number of medical records.
  - Fear here is that a corrupt investigator may obtain access to a large number of records, correlate them, and discover private information about individuals which can then be used for nefarious purposes (such as blackmail)

Enforcement

- Principle: Any computer system that handles medical records must have a subsystem that enforces the preceding principles. The effectiveness of this enforcement must be subject to evaluation by independent auditors.
  - This policy has to be enforced, and the enforcement mechanisms must be auditable (and audited)

Compare to Bell-LaPadula

- Confinement Principle imposes lattice structure on entities in model
  - Similar to Bell-LaPadula
- CISS focuses on objects being accessed; Bell-LaPadula on the subjects accessing the objects
  - May matter when looking for insiders in the medical environment

Compare to Clark-Wilson

- CDIs are medical records
- TPs are functions updating records, access control lists
- IVPs certify:
  - A person identified as a clinician is a clinician;
  - A clinician validates, or has validated, information in the medical record;
  - When someone is to be notified of an event, such notification occurs; and
  - When someone must give consent, the operation cannot proceed until the consent is obtained
- Auditing (CR4) requirement: make all records append-only, notify patient when access control list changed

Originator Controlled Access Control

- Problem: organization creating document wants to control its dissemination
  - Example: Secretary of Agriculture writes a memo for distribution to her immediate subordinates, and she must give permission for it to be disseminated further. This is “originator controlled” (here, the “originator” is a person).

Requirements

- Subject $s \in S$ marks object $o \in O$ as ORCON on behalf of organization X. X allows o to be disclosed to subjects acting on behalf of organization Y with the following restrictions:
  1. o cannot be released to subjects acting on behalf of other organizations without X's permission; and
  2. Any copies of o must have the same restrictions placed on it.

DAC Fails

- Owner can set any desired permissions
  - This makes 2 unenforceable

MAC Fails

- First problem: category explosion
  - Category C contains o, X, Y, and nothing else. If a subject $y \in Y$ wants to read o, $x \in X$ makes a copy o'. Note o' has category C. If y wants to give $z \in Z$ a copy, z must be in Y—by definition, it's not. If x wants to let $w \in W$ see the document, need a new category C' containing o, X, W.
- Second problem: abstraction
  - MAC classification, categories centrally controlled, and access controlled by a centralized policy
  - ORCON controlled locally

Combine Them

- The owner of an object cannot change the access controls of the object.
- When an object is copied, the access control restrictions of that source are copied and bound to the target of the copy.
  - These are MAC (owner can’t control them)
- The creator (originator) can alter the access control restrictions on a per-subject and per-object basis.
  - This is DAC (owner can control it)

Digital Rights Management (DRM)

- The persistent control of digital content
- Several elements:
  - Content: information being protected
  - License: token describing the uses allowed for the content
  - Grant: part of a license giving specific authorizations to one or more entities, and (possibly) conditions constraining the use of the grant
  - Issuer: entity issuing the license
  - Principal: identification of an entity, used in a license to identify to whom the license applies
  - Device: mechanism used to view the content

Example: Movie Distribution by Downloading

- Content: movie itself
- License: token binding palying the movie to the specific downloaded copy
- Grant: movie can be played on some specific set of equipment provided the equipment is located in a geographical area
- Issuer: movie studio
- Principal: user who downloaded the movie
- Device: set of equipment used to play the movie; it manages the licenses, principle, and any copies of the movie

Relationships

Elements related, and the relationship must satisfy all of:

1. The system must implement controls on the use of the content, constraining what users can do with the content
   - Encrypting the content and providing keys to authorized viewers fails this, as the users can distribute the keys indiscriminantly
2. The rules that constrain the users of the content must be associated with the content, not the users
3. The controls and rules must persist throughout the life of the content, regardless of how it is distributed and to whom it is distributed

Conditions

- Stated using a rights expression language
- Example: Microsoft's PlayReady uses a language supporting temporal constraints such as
  - Allowing the content to be viewed over a specific period of time
  - Allowing a validity period for the license
  - Allowing constraints on copying, transferring, converting the content
  - Allowing geographical constraints
  - Allowing availability constraints (for example, content can't be played when being broadcast)

Example: Microsoft PlayReady DRM

Setup

- Content is enciphered using AES
- Key made available to a license server, encrypted content to a distribution server

Play

- Client downloads content, requests license
- License server authenticates client; on success, constructs license and sends it
- Client checks the constraints and, if playback allowed, uses the key in the license to decipher content

Example: Apple's FairPlay DRM

Set up system to play using iTunes

- iTunes generates globally unique number, sends it to Apple's servers
- Servers add it to list of systems authorized to play music for that user
  - At most 5 systems at a time can be authorized

Obtain content using iTunes

- Content enciphers by AES with a master key
- Master key locked with a randomly generated user key from iTunes
- iTunes sends user key to Apple server; stored there and in iTunes, encrypted

Example: Apple's FairPlay DRM

Play content using iTunes

- iTunes decrypts user key
- iTunes uses user key to decrypt master key
- iTunes uses master key to decrypt content
- Note it need not contact Apple servers for authorization

Authorize new system

- Apple server sends that system all user keys stored on server

Example: Apple’s FairPlay DRM

Deauthorize system

- System deletes all locally stored user keys
- Notifies Apple servers to delete globally unique number from list of authorized computers

Copying content to another system

- Cannot be decrypted without user key, which is not copied

Oops …

- Sony BMG developed rootkit to implement DRM on a music CDs
  - Only worked on Windows systems; users had to install a proprietary program to play the music
  - Also installed software that altered functions in Windows OS to prevent playing music using other programs
  - This software concealed itself by altering kernel not to list any files or folders beginning with “sys” and storing its software in such a folder
  - On boot, software contacted Sony to get advertisements to display when music was played
  - Once made public, attackers created Trojan horses with names beginning with “sys (like “sysdrv.exe”)
- Result: lawsuits, flood of bad publicity, and recall of all such CDs

Role-Based Access Control

- Access depends on function, not identity
  - Example:
    - Allison, bookkeeper for Math Dept, has access to financial records.
    - She leaves.
    - Betty hired as the new bookkeeper, so she now has access to those records
  - The role of “bookkeeper” dictates access, not the identity of the individual.

Definitions

- Role *r*: collection of job functions
  - *trans*(*r*): set of authorized transactions for *r*
- Active role of subject *s*: role *s* is currently in
  - *actr*(*s*)
- Authorized roles of a subject *s*: set of roles *s* is authorized to assume
  - *authr*(*s*)
- *canexec*(*s*, *t*) iff subject *s* can execute transaction *t* at current time

Axioms

Let S be the set of subjects and T the set of transactions.

- *Rule of role assignment*: $(\forall s \in S)(\forall t \in T)\ [canexec(s, t) \rightarrow actr(s) \neq \varnothing]$.
  - If s can execute a transaction, it has a role
  - This ties transactions to roles
- *Rule of role authorization*: $(\forall s \in S)\ [actr(s) \subseteq authr(s)]$.
  - Subject must be authorized to assume an active role (otherwise, any subject could assume any role)

Axiom

- *Rule of transaction authorization*:

$$(\forall s \in S)(\forall t \in T)\ [canexec(s, t) \rightarrow t \in trans(actr(s))].$$

  - If a subject *s* can execute a transaction, then the transaction is an authorized one for the role *s* has assumed

Containment of Roles

- Trainer can do all transactions that trainee can do (and then some). This means role r contains role r' ($r > r'$). So:

  $(\forall s \in S)[\ r \in authr(s) \wedge r > r' \rightarrow r' \in authr(s)\ ]$

Separation of Duty

- Let r be a role, and let s be a subject such that $r \in auth(s)$. Then the predicate $meauth(r)$ (for mutually exclusive authorizations) is the set of roles that s cannot assume because of the separation of duty requirement.
- Separation of duty:

$$(\forall r_1, r_2 \in R)\ [\ r_2 \in meauth(r_1) \rightarrow [\ (\forall s \in S)\ [\ r_1 \in authr(s) \rightarrow r_2 \notin authr(s)\ ]\ ]\ ]$$

RBAC Hierarchy

- $RBAC_0$: basic model (you just saw it)
- $RBAC_1$: adds role hierarchies to $RBAC_0$
- $RBAC_2$: adds constraints to $RBAC_0$
- $RBAC_3$: adds both role hierarchies, constraints to $RBAC_0$
  - It combines $RBAC_1$ and $RBAC_2$

$RBAC_0$, Formally

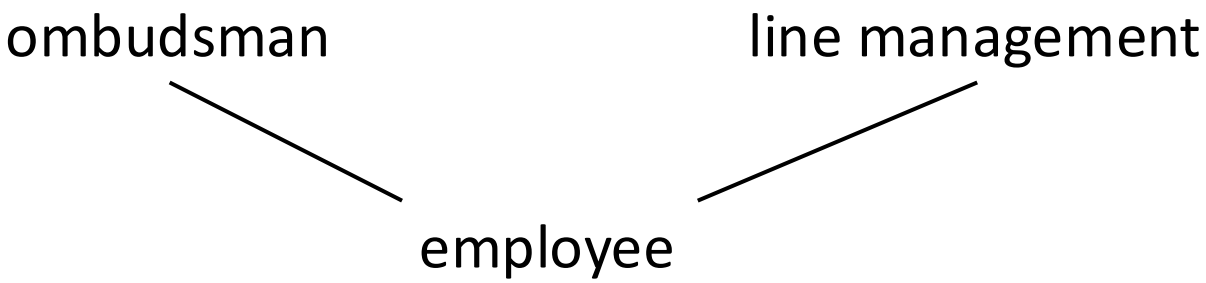
- Set of users U, roles R, permissions P, sessions S
- Relation $PA \subseteq P \times R$ mapping permissions to roles
- Relation $UA \subseteq U \times R$ mapping users to roles
- Function *user*: $S \rightarrow U$ mapping each session to a user
- Function *roles*: $S \rightarrow 2^R$ mapping each session s $\in S$ to a set of roles $roles(s) \subseteq \{ r \in R \mid (user(s), r) \in UA \}$, where s has permissions

$$\bigcup_{r \in roles(s)} \{ p \in P \mid (p, r) \in PA \}$$

  - When a user assumes role r during session, r and hence the user assuming r gets the set of permissions associated with r

$RBAC_1$, Intuitively

- Add containment of roles to $RBAC_0$ (this is the hierarchy)
  - It's a partial ordering
- Each role less powerful than its containing role
  - Containing role contains job functions (permissions) of the contained role
- Can define *private roles* in which one role is subordinate to two others, and those two are not related



$RBAC_1$, Formally

- Set of users U, roles R, permissions P, sessions S
- Partial order $RH \subseteq R \times R$
  - Write $(r_1, r_2) \in R$ as $r_1 \geq r_2$
- Relation $PA \subseteq P \times R$ mapping permissions to roles
- Relation $UA \subseteq U \times R$ mapping users to roles
- Function *user*: $S \rightarrow U$ mapping each session to a user
- Function *roles*: $S \rightarrow 2^R$ mapping each session $s \in S$ to a set of roles $roles(s) \subseteq \{ r \in R \mid (\exists r' \geq r)(user(s), r') \in UA \}$, where s has permissions

$$\bigcup_{r \in roles(s)} \{ p \in P \mid (\exists r'' \geq r)(p, r'') \in PA \}$$

  - When a user assumes role r with subordinate role r' during session, r and hence the user assuming r gets the set of permissions associated with r, and hence with r'

$RBAC_2$ and $RBAC_3$

- $RBAC_2$ adds constraints on values that components can assume to $RBAC_0$
  - Example: user can be in only one role at a time
  - Example: make 2 roles mutually exclusive
- $RBAC_3$ provides both role hierarchies and constraints that determine allowable values for relations and functions
  - Combines $RBAC_1$ and $RBAC_2$
- Can be extended to manage role and privilege assignments
  - A set of administrative roles *AR* and permissions *AP* defined disjointly from *R* and *P*
  - Constraints allow $ap \in AP$ to be assigned to $ar \in AR$ only, and $p \in P$ to $r \in R$ only

Role Engineering

- *Role engineering*: defining roles and determining needed permissions
- Often used when two organizations using RBAC merge
  - Roles in one organization rarely overlap with roles in other
  - Job functions often do overlap
- *Role mining*: analyzing existing roles, permission assignments to determine optimal assignment of permissions to roles
  - *NP*-complete, but in practice optimal solutions can be approximated or produced

Case Study: Traducement

Designed to model electronic recordation

- What is recordation?
- Why do it electronically?
- Models and recordation
- Example: approach and problems

Recordation

- Recording title to real property
  - Real estate purchases
- Recording liens, *etc*.
  - Mortgage holders and such
- In California, County Recorders do this
  - No standards other than statutory ones
  - No state office oversees them

Goals of Recordation

- Establish title
- Establish priority of liens, *etc*.
- Protection of Public
  - Permanence of records
  - Fraud prevention (no secret conveyance, *etc*.)
- Recording triggers release of funds
  - It’s the official record of property ownership

Requirements of a Solution

1. A signed document cannot be altered (although new signatures may be appended);
2. A document may require multiple signatures;
3. A document submitted to the recorder's office may be revoked by any signatory until the document is recorded, but is no longer eligible for additional signatures;
4. The recorder may only append information to the document (*i.e.*, sign it); and
5. If the document is recorded, it becomes a public record immutable to all parties.

How to Record Something

Submission

- Presentation of documents to recorder

Validation

- Check for conformance with statutory requirements
- Calculate fees

Storage

- Record documents, index and provide locators
- Filming and/or imaging the documents to create archival record

Return documents

Modeling the Process

- Confidentiality not an issue
  - Exception: some fees may be
- Integrity a *critical* issue
  - Originator must be able to file document
  - Document must be correct, legal
  - Document immutable
- Availability may, may not be issue

Electronic Commerce

- Model many are trying to use, but there are substantial differences:
  - Emphasis on privacy inappropriate
  - Nothing exchanged (no non-fungible property involved)
  - Not immutable; you can erase an electronic transaction
  - Does not establish title
  - Does not deal with liens

Traducement

- Model designed for electronic recordation
  - a signed document cannot be altered (although new signatures may be appended)
  - a document may require multiple signatures
  - a document submitted to the recorder's office may be revoked by any signatory until the document is recorded, but additional signatures may not be added
  - the recorder may only append information to the document (i.e., sign it)
  - if the document is recorded, it becomes a public record immutable to all parties.

Key Notions

- *Publishing* document
  - Cannot modify it further
  - Making it available to larger community
- *Signing* document
  - Associates authors with documents
- Common to legal documents
  - Unusual in other documents

Entities

- Subjects
  - *Authors* contribute in some way to the document to be filed
  - *Recorders* attest to the completion of document, converting it into official record
- Objects
  - Documents to be filed

Definitions

- Author set *AS*
  - Attribute of object that specifies set of users who wrote to object
  - No author can be removed from author set
- Signer set *SS*
  - Attribute that specifies users who approve the object, contents
  - Any reader can add themselves to this set

Create Rule

- User *u* creates object *o*:
  - *o* indelibly stamped with creation time
  - $o'(AS) = \{ u \}$
  - $o'(SS) = \varnothing$

Alteration Rule

- User *u* alters object *o*:
  - $o'(AS) = \{ u \} \cup o(AS)$
  - $o'(SS) = \varnothing$

Signature Rule

- User u signs object o:
  - $o'(AS) = o(AS)$
  - $o'(SS) = \{ u \} \cup o(SS)$

Example

- Peter drafts document
  - $d(AS)$ = { Peter }, $d(SS) = \varnothing$
- Paul approves
  - $d(AS)$ = { Peter }, $d(SS)$ = { Paul }
- Mary makes some changes
  - $d(AS)$ = { Peter, Mary }, $d(SS) = \varnothing$
- Everyone says it's fine
  - $d(AS)$ = { Peter, Mary }
  - $d(SS)$ = { Peter, Paul, Mary}

Copy Rule

- User *u* copies object *o* to *x*:
  - $x'(AS) = o(AS)$
  - $x'(SS) = o(SS)$

Proposition

- A user is in the *signer set* of an object if and only if the document has not been modified since the user was added to the signer set.
- *Proof*

  ($\Rightarrow$) Let $u \in o(SS)$. Creation, alteration rules set $o(SS) = \varnothing$; by induction, not used. Signature, copy do not alter $o(SS)$.

Proof (*con't*)

- *Proof*

  (⇐) Assume *o* not modified since *u* added to *o*(*SS*).
  - Signature or copy rule applied
  - Signature rule adds to *o*(*SS*); does not delete any elements
  - Copy rule copies original *o*(*SS*); does not delete any elements
  - Induction gives the result

Preconditions

1. Each document in the system has an author set list identifying all users who created or modified that document
2. Each document in the system has a signer set list identifying all users who approve that document.

Theorem

- If a system satisfies the preconditions, then the system still satisfies the preconditions after any sequence of applications of the creation, alteration, signature, and copy rules.
- *Proof*: Let a system satisfy preconditions in state s_0. Apply one of the rules to transition to state s_1.

Applying Rules

- Create rule
  - New document created; *o*(*AS*) is creator only (#1 met) and *o*(*SS*) empty (#2 met)
- Alteration rule
  - Add user to *o*(*AS*), so *o*(*AS*) contains only new user, members of old *o*(*AS*) (#1 met); *o*(*SS*) cleared, so no-one has approved of it (#2 met)

Applying Rules

- Signature rule
  - Document not changed so *o*(*AS*) not changed (#1 met); add signer to *o*(*SS*), as signer approves of (unchanged) document (#2 met)
- Copy rule
  - Create new instance of document, so no changes (#1 met); signers approved of content and no changes to that (#2 met)