



Clinical Information Systems Security Model

Clinical Information Systems Security Model

- 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

- 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

- 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*

- 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

- 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.

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; B-LP on the subjects accessing the objects
 - May matter when looking for insiders in the medical environment



ORCON

- 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)