Day 14 - Integrity models and Hybrid models
Integrity

- Commercial and industrial firms are more concerned with accuracy
  - My bank balance may be disclosed but worse if modified without authorization
  - An inventory list may be disclosed but worse if modified without authorization
Requirements of Commercial Policies

1. Users will not write their own programs, but will use existing production programs and databases.

2. Programmers will develop and test programs on a non-production system; if they need access to actual data, they will be given production data via a special process, but will use it on their development system.

3. A special process must be followed to install a program from the development system onto the production system.

4. The special process in requirement 3 must be controlled and audited.

5. The managers and auditors must have access to both the system state and the system logs that are generated.
Separation of duty

- If two or more steps are required to perform a critical function, at least two different people should perform the steps.
- e.g. moving a program from the developmental environment to the production environment
  - If the developer has made a mistake or performed a malicious act, then the installer’s process of checking and validating should catch the problem.
Separation of function

- Developers do not develop new programs on the production system
- Developers do not process production data on the development system
  - Depending on sensitivity of data, developers and testers may get a sanitized version of the data
Auditing

- Process of analyzing systems to determine what actions took place and who performed them.
- Commercial systems must emphasize recovery and accountability
  - Must maintain extensive logs to allow for auditing
Will the Bell-LaPadula model work for confidentiality?

- “Clearance” level is not typical in a commercial enterprise.
- Access is provided on a per user basis
  - Too many categories and security levels needed
  - Model will become too complex
  - Difficult to control the proliferation of categories and levels
- Aggregating public info could help in deducing confidential information
  - Model needed to track what questions have been asked
Biba Integrity model

• Intuition for *Integrity Levels*
  • The higher the level, the more confidence
    • that a program will execute correctly
    • that data is accurate and/or reliable
  • Note relationship between integrity and trustworthiness
  • Important point: *integrity levels are not security levels*
Biba’s Model

• Similar to Bell-LaPadula model
  1. \( s \in S \) can read \( o \in O \) iff \( i(s) \leq i(o) \)
  2. \( s \in S \) can write to \( o \in O \) iff \( i(o) \leq i(s) \)
  3. \( s_1 \in S \) can execute \( s_2 \in S \) iff \( i(s_2) \leq i(s_1) \)
The Biba Model - an example
Hybrid Policies

- Overview
- Clinical Information Systems Security Policy
- Chinese Wall Model
Clinical Information Systems

Security Policy

• Intended for medical records
  • Patient confidentiality, authenticity of records and annotators, and integrity

• 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)