

Chapter 7 HYBRID POLICIES

- Few organizations limit their security objectives to confidentiality and integrity.
- Most organizations desire both in some mixture.
- This chapter presents two such models:
 - The *Chinese Wall* model
 - The *Clinical Information Systems* security model
- Two other models present alternative views:
 - Originator controlled access control lets the creator determine who should access the data and how.
 - Role-based access control formalizes the more common notion of groups of users.

7.1 Chinese Wall model

- Derived from the British laws concerning conflict of interest.
- Refers equally to confidentiality and integrity.
- Consider the database of an investment house.
 - Consists of company records.
 - Suppose Anthony counsels Bank of America and Citibank.
 - Anthony has a potential conflict of interest.
 - Hence, Anthony cannot counsel both banks.

Chapter 7 HYBRID POLICIES

- **Definitions**

- The *objects* of the database are items of information related to a company.
- A *company dataset* (CD) contains objects related to a single company.
- A *conflict of interest* (COI) class contains the datasets of companies in competition.
 - *COI (O)*: represents the COI class that contains object *O*.
 - *CD(O)*: the company dataset that contains object *O*. The model assumes that each object belongs to exactly one COI class.
 - Anthony has access to the objects in the CD of Bank of America.
 - Because the CD of Citibank is in the same COI class, Anthony cannot gain access to the objects in Citibank's CD (shown in Figure 7-1).
 - Hence, the structure of the database provides the required ability.

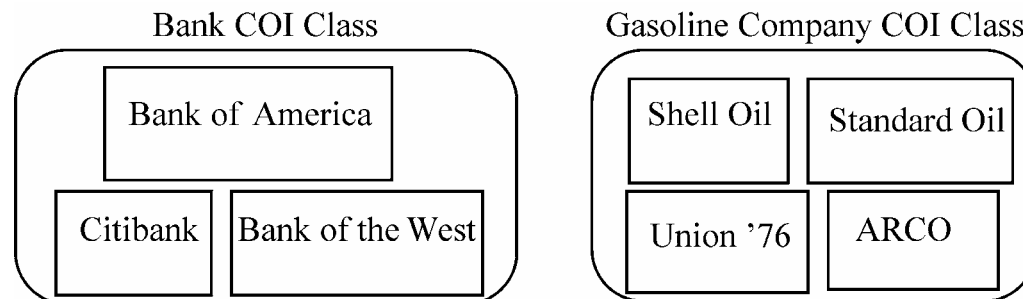


Figure 7-1. The Chinese Wall model database with two COI classes

Chapter 7 HYBRID POLICIES

- **Suppose Anthony worked first worked on Bank of America's portfolio, and was then transferred to Citibank's portfolio.**
 - Much of the information Anthony learned from Bank of America's portfolio will be current.
 - Hence, he can guide Citibank's investments using information about Bank of America - a conflict of interest!
 - This leads to the following rule.
- **$PR(S)$ is the set of objects that S has read.**
- **CW-Simple Security Condition, Preliminary Version: S can read O if and only if either of the following is true:**
 1. **There is an object O' such that S has accessed O' and $CD(O') = CD(O)$.**
 2. **For all objects O' , $O' \in PR(S) \Rightarrow COI(O') \neq COI(O)$.**
 - Initially, $PR(S) = \emptyset$, and the initial read requested is granted.
 - Bank of America's COI class = Citibank's COI class.
 - Anthony cannot access an object in Bank of America's CD because he has accessed an object in Citibank's CD.
 - Two consequences of this rule affect subjects rights:
 - Once a subject reads any object in a COI class, the only other objects in that COI class that the subject can read are in the same CD as the read object.
 - The minimum # of subjects needed to access every object in a COI class is the same as the # of CDs in that COI class.
 - If the gasoline company COI class has 4 CDs, then at least 4 analysts are needed to access all information in the COI class.
 - Hence, any trading house must have at least 4 analysts to access all information in that COI class without creating a conflict of interest!

Chapter 7 HYBRID POLICIES

- **Sanitization**
 - Public information may belong to a CD (e.g., annual stockholder's report).
 - No conflict of interest arises.
 - All sensitive data removed from information before it is released publicly is called sanitization.
 - Hence, the model distinguishes between *sanitized* data and *unsanitized* data.
 - Sanitized data falls under the CW-Simple Security Condition, Preliminary Version, and unsanitized data does not!
 - The CW-Simple Security Condition can be reformulated to include this notion.
- **CW-Simple Security Condition: S can read O if and only if any of the following holds:**
 - There is an object O' such that S has accessed O' and $CD(O') = CD(O)$.
 - For all objects O' , $O' \in PR(S) \Rightarrow COI(O') \neq COI(O)$.
 - O is a sanitized object.
- **Suppose Anthony and Susan work in the same trading house.**
 - Anthony can read objects in Bank of America's CD.
 - Susan can read objects in Citibank's CD.
 - Both can read objects in ARCO's CD.
 - If Anthony could also write to objects in ARCO's CD, then Susan can read that information.
 - So, Susan can indirectly obtain information from Bank of America's CD, causing a conflict of interest!
 - CW-Simple Security Condition must be augmented to prevent this.
- **CW*-Property: A subject S may write to an object O if both of the following conditions hold:**
 1. The CW-Simple Security Condition permits S to read O .
 2. For all *unsanitized* objects O' , if S can read O' , then $CD(O') = CD(O)$.
 - In the above example:
 - Anthony can read objects in Bank of America's CD and ARCO's CD, making condition 1 true.
 - If Bank of America's CD contains unsanitized objects, Anthony can read those objects, making condition 2 false.
 - Hence, Anthony cannot write to objects in ARCO's CD.

Chapter 7 HYBRID POLICIES

7.2 Clinical Information Systems Security Policy

- Medical records require policies that combine confidentiality and integrity.
- Conflict of interest is not a critical problem!
- Critical problems
 - Patient confidentiality
 - Authentication of records and the personnel making entries in those records
 - Assurance that the records have not been changed erroneously
- In the policy, three types of entities are defined:
 - A *patient* is the subject of medical record, or an agent for that person.
 - *Personal health information* is data about a patient's health or treatment enabling identification of the patient.
 - A *clinician* is a health-care professional with access to personal health information while performing his/her job.
- The policy also assumes that personal health information involves one person at a time.
 - This is not true.
 - For example, obstetrics/gynecology records contain information about the father and the mother.
 - In these cases, special rules need to be applied. The policy does not cover them.
 - The policy is guided by principles similar to the certification and enforcement rules of the Clark-Wilson model.
 - These principles are derived from the medical ethics of several medical societies, and from the experience of and advice of practicing clinicians.
- The first set of principles deals with access to the medical records themselves.
- 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.
 - Medical ethics require that only clinicians and the patient have access to the patient's record.

Chapter 7 HYBRID POLICIES

- **Access Principle 2:** One of the clinicians on the access control list (the *responsible clinician*) must have the right to add other clinicians to the access control list.
 - Because the patient must consent to treatment, the patient has the right to know when his/her medical record is accessed or altered.
 - If a clinician who is unfamiliar to the patient accesses the record, the patient should be notified of the leakage of information.
- **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.
 - Erroneous information should be corrected, not deleted, to facilitate auditing of the records.
 - Auditing also requires that all accesses be recorded, along with the data/time of each access and the name of each person accessing the record.
- **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.
- The next set of principles concern record creation and information deletion.
- **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.
 - How long the medical records are kept depends on the circumstances.
 - Normally, the medical records can be discarded after 8 years.
 - However, in some cases, the records are kept longer.
- **Deletion Principle:** Clinical information cannot be deleted from a medical record until the appropriate time has passed.
 - Deletion of a record also depends on the circumstances.

Chapter 7 HYBRID POLICIES

- **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.
 - 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).
- Finally, systems must implement mechanisms for enforcing these principles.
- **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).

Chapter 7 HYBRID POLICIES

- **7.3 Originator Controlled Access Control**
 - Mandatory and discretionary access controls (MACS and DACs) do not handle environments in which the originators of documents retain control over them even after those documents are disseminated.
 - Graubert developed a policy called ORCON (ORiginator CONtrolled) in which a subject can give another subject rights to an object only with the approval of the creator of that object.
 - **EXAMPLE:**
 - The Secretary of Defense of the United States drafts a proposed policy document and distributes it to her aides for comment.
 - The aides are not allowed to distribute the document any further without permission from the secretary.
 - The secretary controls dissemination.
 - Hence, the policy is ORCON.
 - In practice, a single author does not control dissemination; instead, the organization does.
 - Suppose a 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. The object o cannot be released to subjects acting on behalf of other organizations without X 's permission.
 2. Any copies of o must have the same restrictions placed on it.

Chapter 7 HYBRID POLICIES

- **DACs are insufficient for this purpose.**
 - The owner of an object can set any desired permissions.
- **MACs are theoretically sufficient but they have a serious drawback:**
 - **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 the copy o' is in C .
 - » If y wants to give $z \in Z$ a copy, z must be in Y - by definition, it is not.
 - » If x wants to let $w \in W$ see the document, there is a need for a new category C' containing o, X, W .
 - **Second problem: abstraction**
 - » Organization that use categories grant access to individuals on a “need to know basis.”
 - » There is a formal, written policy that determines who needs the access based on common characteristics and restrictions.
 - » However, this requires a central clearing house for categories.
 - » The creation of categories to enforce ORCON implies local control of categories, and a set of rules dictating who has access to each security level.
 - » ORCON is a decentralized system of access control.
 - » No centralized set of rules controls access to data; access is at the complete discretion of the originator.
 - » Hence, the MAC representation of ORCON is not suitable!
 - **A solution is to combine features of the MAC and DAC models.**
 1. The owner of an object cannot change the access controls of the object.
 2. When an object is copied, the access control restrictions of that source are copied and bound to the target of the copy.
 3. The creator (originator) can alter the access control restrictions on a per-subject and per-object basis.
 - » The first two rules are from mandatory access controls. The system controls all accesses.
 - » The third rule is discretionary, and gives the originator power to determine who can access the object.
 - » Hence, the hybrid system is neither MAC nor DAC.

Chapter 7 HYBRID POLICIES

7.4 Role-Based Access Control (RBAC)

- The ability, or need, to access information may depend on one's job functions.
- **EXAMPLE:** Allison is the bookkeeper for the Dept. of Mathematics.
 - She has access to all departmental accounts.
 - She becomes head accountant of the University's Office of Admissions
 - She no longer has access to Math department's accounts.
 - The Math department hires Sally as its new bookkeeper.
 - Now, Sally has full access to all accounts of the Math department.
 - Access to the accounts is a function of the job of the bookkeeper; it is not tied to any particular individual.
- This suggests associating access with the particular job of the user.

Chapter 7 HYBRID POLICIES

- **Definitions**
 - **A role is a collection of job functions.**
 - Each role r is authorized to perform one or more transactions.
 - The set of authorized transactions for r is written $trans(r)$.
 - **The active role of a subject s , written $actr(s)$, is the role that s is currently performing.**
 - **The authorized roles of a subject s , written $authr(s)$, is the set of roles that s is authorized to assume.**
 - **The predicate $canexec(s, t)$ is true if and only if the subject s can execute the transaction t at the current time.**
- **Three rules reflect the ability of a subject to execute a transaction.**
 - Let S be the set of subjects and T the set of transactions.
 - **Axiom 1: The rule of role assignment is $(\forall s \in S)(\forall t \in T) [canexec(s, t) \rightarrow actr(s) \neq \emptyset]$.**
 - It simply says that if a subject can execute any transaction, then that subject has an active role.
 - This binds the notion of execution of a transaction to the role rather than to the user.
 - **Axiom 2: The rule of role authorization is $(\forall s \in S) [actr(s) \subseteq authr(s)]$.**
 - It means that the subject must be authorized to assume its active role.
 - The subject cannot assume an unauthorized role.
 - **Axiom 3: The rule of transaction authorization is**
$$(\forall s \in S)(\forall t \in T)[canexec(s, t) \rightarrow t \in trans(actr(s))].$$
 - It says that a subject cannot execute a transaction for which its current role is not authorized.
- **The forms of these axioms restrict the transactions that can be performed.**
 - They do not ensure that the allowed transactions can be executed.
 - They state rules that must be satisfied before a transaction can be executed.

Chapter 7 HYBRID POLICIES

- **Containment of Roles: Some roles subsume others.**
 - **EXAMPLE 1**
 - A trainer can perform all actions of a trainee, as well as others.
 - This can be viewed as containment, which suggests a hierarchy of roles.
 - **EXAMPLE 2**
 - Many operations are common to a large number of roles.
 - Instead of specifying the operation once for each role, one specifies it for a role containing all other roles.
 - Granting access to a role R implies that access is granted for all roles containing R .
 - This simplifies the use of the RBAC model and its implementation.
- **Separation of duty**
 - RBAC model can model the separation of duty.
 - The goal is to specify the separation of duty centrally.
 - The key is to recognize that the users in some roles cannot enter other roles.
 - For 2 roles r_1 and r_2 bound by separation of duty: $(\forall s \in S) [r_1 \in authr(s) \rightarrow r_2 \notin authr(s)]$
- **Capturing the notion of mutual exclusion requires a new predicate.**
- **Let r be a role, and let s be a subject such that $r \in authr(s)$. 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.**
 - This definition together with the above example, the separation of duty can be summarized as $(\forall r_1, r_2 \in R) [r_2 \in meauth(r_1) \rightarrow [(\forall s \in S) [r_1 \in authr(s) \rightarrow r_2 \notin authr(s)]]]$.