Lecture 5

Hybrid Policies:
The Nature of Life is to Progress

Wholeness Statement

Situations arise where pure confidentiality or pure integrity policies are not adequate. Today we look at a few hybrid policy models that are concerned with both. As more and more applications become concerned with security, the field of computer security continues to progress. The nature of life is to grow and progress.

Overview

Four hybrid policy models

1. The Chinese Wall model is appropriate for investment counselors. It increases the trust of their clients in their advice. Trust means integrity.
2. Clinical Information Systems Security Policy
   - Patients want their medical records to be confidential.
   - But records must not be changed inappropriately, e.g., doctors cannot change records because of a malpractice suit.
3. Originator Controlled Access Control
   - Controls how one's work is disseminated
   - Controls its integrity also (so no one can modify your work and attribute it to you).
4. Role-Based Access Control
   - Based on the roles we looked at in Lecture 2, we can restrict read access, that is confidentiality.
   - But we can also restrict access based on separation of duty which is an integrity concern.

Chinese Wall Model

Chapter 7.1

Chinese Wall (CW) Model

Models a security policy that refers equally to confidentiality and integrity, and deals with conflict of interest.

- The Chinese Wall Model also distinguishes between sanitized and unsanitized data
- Sanitized Data: Public, unrestricted information
- Unsanitized Data: Confidential information

Definition 7-1/7.2 A *company dataset* (CD) contains objects (items of information) related to a single company

Definition 7-3 A *conflict of interest* (COI) *class* contains the datasets of companies in competition.

Let *COI(O)* represent the COI class that contains object O.

Let *CD(O)* be the company dataset that contains object O.

Let *PR(S)* be the set of objects that S has previously read.

- The model assumes that each object belongs to exactly one COI class.

CW-Simple Security Condition

S can read O if and only if any of the following holds.

1. There is an object O' such that S has accessed O' and CD(O') = CD(O)
2. For all objects O', if O' in PR(S), then COI(O) != COI(O').
3. O is a sanitized object

- Thus a subject can read unsanitized objects from only one CD of a COI.

Consider the following:

- Anthony and Susan work in the same trading house.
- Anthony can read BankCOI.BankOfAmerica and Susan can read BankCOI.Citibank.
- Both can read GasCompanyCOI.ARCO.
- If Anthony can also write to GasCompanyCOI.ARCO, then he can read information from BankCOI.BankOfAmerica and write it to GasCompanyCOI.ARCO, and then Susan can read that information.
- The following prevents this from happening

CW-*-Property

A subject S may write an unsanitized object O if and only 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).

- This means that all the unsanitized objects that S can read have to be from the same CD as O
- Thus if a subject can read unsanitized objects from more than one CD, then it cannot write unsanitized objects to any CD
- Prevents transfer of “inside” information from one CD into a different CD for someone else to read

Main Point

1. Chinese Wall deals with conflict of interest. Such conflicts are prevented by keeping certain data confidential to eliminate integrity concerns that might arise. TM lets its practitioners live 200% of life, because inner and outer are one.

Clinical Information Systems Security Policy

Chapter 7.2

Patient confidentiality

Most patients are unwilling to share their personal health information with administrators

Integrity concerns:

1. Doctor changing record because of a malpractice suit
2. Less confidentiality will increase integrity problems, e.g., if health records are used in hiring, then the desire to modify them will increase.
3. If patients cease to believe that their clinical confidences will be respected, they will suppress relevant information, leading not just to inaccurate records but to poor treatment of individual patients and to an increased risk to others.
4. What if a patient walks in and says he is somebody else.

Definitions

Definition 7-4. A *patient* is the subject of medical records, or an agent for that person who can give consent for the person to be treated.

Definition 7-5. *Personal health information* is information about a patient's health or treatment enabling that patient to be identified.

Definition 7-6. A *clinician* is a health-care professional who has access to personal health information while performing his or her job.

"As usual with policy models, we will attempt to translate the application requirements into a set of rules that say which subject can access which object. Here a subject may be a computer user (such as a doctor, health administrator or outside hacker) or a computer program acting on behalf of a user; the objects are the information held in the system, and may include programs and data; and access may include the ability to read, write and execute objects"

- One assumption is that each record is about only one person (not necessarily the case with obstetrics, pediatric, psychiatric or pediatric records.)

Access Principles

Access Principle 1: Each medical record has an access control list naming the individuals or groups who may read and append information to it. The system shall prevent anyone not on the access control list from accessing the record in any way.

Access Principle 2: One of the clinicians on the access control list (called the *responsible clinician*) must have the right to add other clinicians to the access control list.

Access Principle 3: The responsible clinician must notify the patient of the names on the access control list whenever the patients medical record is opened. Except in emergency, or in the case of statutory exemptions, the responsible clinician must obtain the patient's consent.

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.

- Note: this also helps detect identity theft

Creation Principle: A clinician may create a record, with the clinician and the patient on the access control list. If the record is opened as a result of a referral, the referring clinician may also be on the access control list.

Deletion Principle: Clinical information cannot be deleted until the appropriate time period has expired.

- Note: appropriate varies based on the nature of the records. Keeping records may help a doctor delay with relapses of a disease. Append rather than delete.

Confinement Principle: Information derived from record A may be appended to record B if and only if B's access control list is contained in A's.

Aggregation Principle: There shall be effective measures to prevent the aggregation of personal health information. In particular, patients must receive special notification if anyone is to be added to their access control list when that person already has access to personal health information on a large number of people.

- Show me the records of all females aged 35 with two daughters aged 13 and 15 who both suffer from eczema
- In the form you filled out yesterday you were asked to write your entry date. What if you were the only person in the room who entered at that date?

Enforcement Principle: Computer systems that handle personal health information shall have a subsystem that enforces the above principles in an effective way. Its effectiveness shall be subject to evaluation by independent experts. (assurance)

- "The system should be able to be managed by a clinician whose computer literacy and administrative tidiness are less than average" (psychological acceptability)

Main Point

2. Confidentiality of medical records is very important. It is important to prevent unauthorized access to patient information and to maintain the integrity of the records. Ayurveda is also interested in prevention and integrity. Its goal is to detect disease at an early stage and treat it by restoring the balance (integrity) of the physiology.

Originator Controlled Access Control

Chapter 7.3

Originator Controlled Access Control

- There are situations where the originators of documents retain control over them even after those documents are disseminated.
- In ORCON ("Originator Controlled"), a subject can give another subject rights to an object but only with the approval of the creator of that object.

Originator Controlled Access Control

Combines features of mandatory and discretionary access controls:

1. (Mandatory) The owner of an object cannot change the access controls of the object
2. (Mandatory) When an object is copied, the access control restrictions of that source are copied and bound to the target of the copy
3. (Discretionary) The creator (originator) can alter the access control restrictions on a per-subject and per-object basis

Copyright Protection

- **Thin copyright** - enough protection to encourage creativity but not restricting too strongly the availability of the works to the public
- **Thick copyright** - maximize profits
- **Digital Rights Management** (DRM) - use of technological controls to protect digital works

Copying

Copying a book is prohibited by copyright law but that just makes people feel guilty.

The reason books aren't copied is because it is inconvenient and costs money.

However, it's easy to make multiple copies of a digital book at no cost.

Encryption prevents access, not copying

Encryption Options

1. Encrypt and give purchaser the key. Hah!

2. Use a voucher. When digital media is downloaded, an encrypted key is also downloaded and stored as a hidden file on the computer. The program that reads the media knows how to find the encrypted key and use it to decipher the media. May work with naive users but not with users who know about the two files. This violates the principle of open design.

3. Have voucher contain unique information about the machine that is used to download the media. Media player reads the voucher and compares information about machine with the actual machine information. If different then don't play file. What if user gets new machine? This violates the principle of psychological acceptability.

Rights Expression Language

- Digital Rights Management is a form of ORCON that is attracting a lot of attention today (Steve Jobs)
- Renato Lanella's Open Digital Rights Language (ODRL) is an example

Rights	Constraints	Payments
display	fixedamount	feeType
excerpt	hardware	payment
execute	interval	postpay
give	network	prepay
install	percentage	transaction
lease	peruse	
lend	range	
modify	screen	
move	uid	
play	version	
print	unit	
printer		
remark		
restore		
sell		
transferPerm		
uninstall		

Renato Lanella's Open Digital Rights Language

ORDL is rendered in XML

```
<permission>
 <display>
  <constraint>
   <unit type="NumberOfPages">
    <constraint>
     <range>
      <min>1</min>
      <max>5<p;/max>
     </range>
    </constraint>
   </unit>
  </constraint>
  </display>
</permission>
```

Can Systems be Trusted?

- A rights expression language just expresses, it has no enforcement abilities of its own.
- How can seller of digital media trust that your computer will not circumvent controls.
  - E.G. if you rent a book with the agreement that you have two weeks to read it (like renting a DVD) and you can reset your clock, then your computer is not trusted.
  - OS has to get involved.
  - Microsoft is working on this.
- "Trusted computing means that content owners can trust that the computer will obey the DRM instead of you, the computer's owner."
- The above is excerpted from
  http://www.kcoyle.net/drm_basics1.html

- Some more links on DRM are found in the lecture 5 notes on the course web page

Main Point

3. Originator Controlled Access Control lets the originator of a document control its dissemination. Pure consciousness is the source of all manifest creation and controls it using the laws of nature.

Role-Based Access Control

Chapter 7.4

Role-Based Access Control (RBAC)

- Users cannot pass access permissions on to other users at their discretion.
- This is a fundamental difference between Discretionary Access Control and RBAC
- RBAC is a form of MAC, but it is not based on multilevel security requirements.
- Role-Based access control in many applications is concerned more with access to functions and information rather than just access to information.

For example,

```
<os>
  <roles>
    <role name='student'>
      <operation object='file1' rights='r'/>
      <operation object='file2' rights='a'/>
      <operation object='file4' rights='rw'/>
    </role>

    <role name='intern'/>
      <operation object='file1' rights='w'/>
      <operation object='file3' rights='rwe'/>
    </role>
  </roles>
```

```
  <users>
    <user subject='joe'>
      <role>student</role>
      <role>intern</role>
    </user>
    <user subject='jack'>
      <role>student</role>
    </user>
    <user subject='pat'>
      <role>student</role>
    </user>
    <user subject='kathy'>
      <role>student</role>
    </user>
    <user subject='rene'>
      <role>student</role>
    </user>
  </users>
</os>
```

Role-Based Access Control

- Within a role-based system, the principle concern is with protecting the integrity of information, "who can perform what acts on what information".
- The ability or need, to access information may depend on one's job function

Definition 7-7. A *role* is a collection of job functions. Each role r is authorized to perform one or more transactions (actions in support of a job function). The set of authorized transactions for r is written *trans(r)*.

Definition 7-8. The *active role of a subject s*, written *actr(s)*, is the role that s is currently performing.

Role-Based Access Control

Definition 7-9. The *authorized roles of a subject s*, written *authr(s)*, is the set of roles that s is authorized to assume.

Definition 7-10. The predicate *canexec(s, t)* is true if and only if the subject s can execute the transaction t at the current time.

Definition 7-11. Let r be a role, and let s be a subject such that r is in authr(s). Then the predicate *mutex(r)* is the set of roles that s cannot assume because of the separation of duty requirement. This restricts authr(s).

Three Rules

Three rules (derived from Axioms 7-1, 7-2, and 7-3) reflect the ability of a subject to execute a transaction

1. If a subject can execute any transaction, then the subject has an active role
2. The subject must be authorized to assume its active role
3. A subject cannot execute a transaction for which its current role is not authorized.

- These rules indicate that RBAC is a form of mandatory access control.
- DAC may further restrict transactions.
- This is richer than using groups in Windows XP

- An introduction to Role-Based Access Control is also found at URL

  http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm

Main Point

4. Role-Based Access Control only allows subjects to execute transactions for which their current role is authorized. All activity of manifest creation is controlled by the laws of nature.

Summary

- Policies typically combine features of both integrity and confidentiality policies
- Chinese Wall Model captures the requirements of a particular business (brokering under British Law)
- Similarly for the Clinical Information Systems Model for medical records
- ORCON and RBAC take a different approach
  - Focus on which entities will access data
  - ORCON allows the author to control access to the document
  - RBAC restricts access to individuals performing specific functions (this can be applied to previous models)

CONNECTING THE PARTS OF KNOWLEDGE WITH THE WHOLENESS OF KNOWLEDGE

1. Interactions of a person with their doctor should be confidential.
2. Thorough auditing is one way to assure the integrity and confidentiality of medical records.
3. Transcendental Consciousness is the source of all the laws of nature that govern the universe.
4. Wholeness moving within itself: in Unity Consciousness one has total knowledge of natural law lively in one's own Self.