

ECS 235B Module 33

Chinese Wall Model

Chinese Wall Model

Problem:

- Tony advises American Bank about investments
- He is asked to advise Toyland Bank about investments
- Conflict of interest to accept, because his advice for either bank would affect his advice to the other bank

Organization

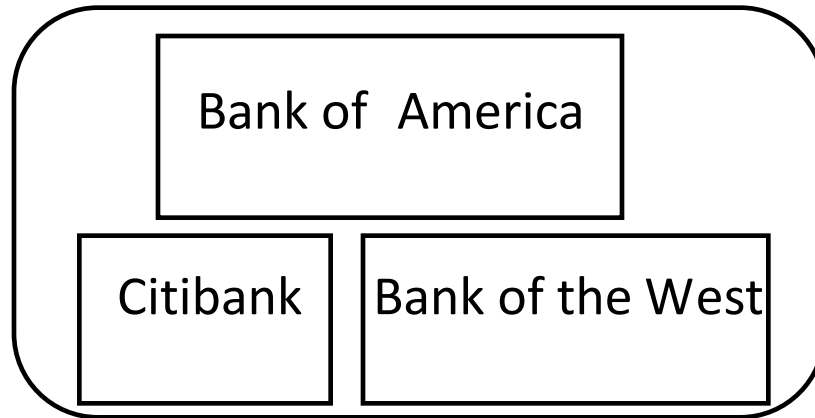
- Organize entities into “conflict of interest” classes
- Control subject accesses to each class
- Control writing to all classes to ensure information is not passed along in violation of rules
- Allow sanitized data to be viewed by everyone

Definitions

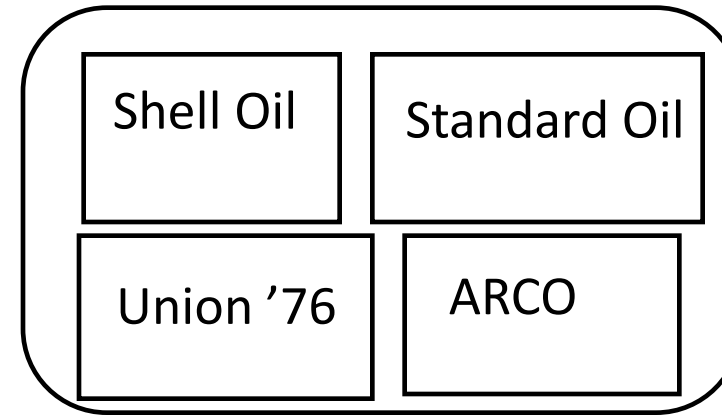
- *Objects*: items of information related to a company
- *Company dataset (CD)*: contains objects related to a single company
 - Written $CD(O)$
- *Conflict of interest class (COI)*: contains datasets of companies in competition
 - Written $COI(O)$
 - Assume: each object belongs to exactly one *COI* class

Example

Bank COI Class



Gasoline Company COI Class



Temporal Element

- If Anthony reads any CD in a COI, he can *never* read another CD in that COI
 - Possible that information learned earlier may allow him to make decisions later
 - Let $PR(S)$ be set of objects that S has already read

CW-Simple Security Condition

- s can read o iff either condition holds:
 1. There is an o' such that s has accessed o' and $CD(o') = CD(o)$
 - Meaning s has read something in o 's dataset
 2. For all $o' \in O$, $o' \in PR(s) \Rightarrow COI(o') \neq COI(o)$
 - Meaning s has not read any objects in o 's conflict of interest class
- Ignores sanitized data (see below)
- Initially, $PR(s) = \emptyset$, so initial read request granted

Sanitization

- Public information may belong to a CD
 - As is publicly available, no conflicts of interest arise
 - So, should not affect ability of analysts to read
 - Typically, all sensitive data removed from such information before it is released publicly (called *sanitization*)
- Add third condition to CW-Simple Security Condition:
 - 3. o is a sanitized object

Writing

- Anthony, Susan work in same trading house
- Anthony can read Bank 1's CD, Gas' CD
- Susan can read Bank 2's CD, Gas' CD
- If Anthony could write to Gas' CD, Susan can read it
 - Hence, indirectly, she can read information from Bank 1's CD, a clear conflict of interest

CW-* -Property

- s can write to o iff both of the following hold:
 1. The CW-simple security condition permits s to read o ; and
 2. For all *unsanitized* objects o' , if s can read o' , then $CD(o') = CD(o)$
- Says that s can write to an object if all the (unsanitized) objects it can read are in the same dataset

Formalism

- Goal: figure out how information flows around system
- S set of subjects, O set of objects, $L = C \times D$ set of labels
- $I_1: O \rightarrow C$ maps objects to their COI classes
- $I_2: O \rightarrow D$ maps objects to their CDs
- $H(s, o)$ true iff s has *or had* read access to o
- $R(s, o)$: s 's request to read o

Axioms

- Axiom 8-1. For all $o, o' \in O$, if $l_2(o) = l_2(o')$, then $l_1(o) = l_1(o')$
 - CDs do not span COIs.
- Axiom 8-2. $s \in S$ can read $o \in O$ iff, for all $o' \in O$ such that $H(s, o')$, either $l_1(o') \neq l_1(o)$ or $l_2(o') = l_2(o)$
 - s can read o iff o is either in a different COI than every other o' that s has read, or in the same CD as o .

More Axioms

- Axiom 8-3. $\neg H(s, o)$ for all $s \in S$ and $o \in O$ is an initially secure state
 - Description of the initial state, assumed secure
- Axiom 8-4. If for some $s \in S$ and for all $o \in O$, $\neg H(s, o)$, then any request $R(s, o)$ is granted
 - If s has read no object, it can read any object

Which Objects Can Be Read?

Theorem 8-1: Suppose $s \in S$ has read $o \in O$. If s can read $o' \in O$, $o' \neq o$, then $l_1(o') \neq l_1(o)$ or $l_2(o') = l_2(o)$.

- Says s can read only the objects in a single CD within any COI

Proof

Assume false. Then

$$H(s, o) \wedge H(s, o') \wedge I_1(o') = I_1(o) \wedge I_2(o') \neq I_2(o)$$

Assume s read o first. Then $H(s, o)$ when s read o , so by Axiom 8-2, $I_1(o') \neq I_1(o)$ or $I_2(o') = I_2(o)$, so

$$(I_1(o') \neq I_1(o) \vee I_2(o') = I_2(o)) \wedge (I_1(o') = I_1(o) \wedge I_2(o') \neq I_2(o))$$

Rearranging terms,

$$(I_1(o') \neq I_1(o) \wedge I_2(o') \neq I_2(o) \wedge I_1(o') = I_1(o)) \vee (I_2(o') = I_2(o) \wedge I_2(o') \neq I_2(o) \wedge I_1(o') = I_1(o))$$

which is obviously false, contradiction.

Lemma

Lemma 8-2: Suppose a subject $s \in S$ can read an object $o \in O$. Then s can read no o' for which $l_1(o') = l_1(o)$ and $l_2(o') \neq l_2(o)$.

- So a subject can access at most one CD in each COI class
- Sketch of proof: Initial case follows from Axioms 8-3, 8-4. If $o' \neq o$, theorem immediately gives lemma.

COIs and Subjects

Theorem 8-2: Let $c \in C$. Suppose there are n objects $o_i \in O$, $1 \leq i \leq n$, such that $l_1(o_i) = c$ for $1 \leq i \leq n$, and $l_2(o_i) \neq l_2(o_j)$, for $1 \leq i, j \leq n, i \neq j$. Then for all such o , there is an $s \in S$ that can read o iff $n \leq |S|$.

- If a COI has n CDs, you need at least n subjects to access every object
- Proof sketch: If s can read o , it cannot read any o' in another CD in that COI (Axiom 8-2). As there are n such CDs, there must be at least n subjects to meet the conditions of the theorem.

Sanitized Data

- $v(o)$: sanitized version of object o
 - For purposes of analysis, place them all in a special CD in a COI containing no other CDs
- Axiom 8-5. $I_1(o) = I_1(v(o))$ iff $I_2(o) = I_2(v(o))$

Which Objects Can Be Written?

Axiom 8-6. $s \in S$ can write to $o \in O$ iff the following hold simultaneously

1. $H(s, o)$
 2. There is no $o' \in O$ with $H(s, o')$, $I_2(o) \neq I_2(o')$, $I_2(o) \neq I_2(v(o))$, $I_2(o') = I_2(v(o))$.
- Allow writing iff information cannot leak from one subject to another through a mailbox
 - Note handling for sanitized objects

How Information Flows

Definition: information may flow from o to o' if there is a subject such that $H(s, o)$ and $H(s, o')$.

- Intuition: if s can read 2 objects, it can act on that knowledge; so information flows between the objects through the nexus of the subject
- Write the information flow between o and o' as (o, o')

Key Result

Theorem 8-3: Set of all information flows is

$$\{ (o, o') \mid o \in O \wedge o' \in O \wedge I_2(o) = I_2(o') \vee I_2(o) = I_2(v(o)) \}$$

Sketch of proof: Definition gives set of flows:

$$F = \{ (o, o') \mid o \in O \wedge o' \in O \wedge \exists s \in S \text{ such that } H(s, o) \wedge H(s, o') \}$$

Axiom 8-6 excludes the following flows:

$$X = \{ (o, o') \mid o \in O \wedge o' \in O \wedge I_2(o) \neq I_2(o') \wedge I_2(o) \neq I_2(v(o)) \}$$

So, letting F^* be transitive closure of F ,

$$F^* - X = \{ (o, o') \mid o \in O \wedge o' \in O \wedge \neg(I_2(o) \neq I_2(o') \wedge I_2(o) \neq I_2(v(o))) \}$$

which is equivalent to the claim.

Aggressive Chinese Wall Model

- Assumption of Chinese Wall Model: COI classes are actually related to business, and those are partitions
 - Continuing bank and oil company example, the latter may invest in some companies, placing them in competition with banks
 - One bank may only handle savings, and another a brokerage house, so they are not in competition
- More formally: Chinese Wall model assumes the elements of O can be partitioned into COIs, and thence into CDs
 - Define CIR to be the conflict of interest relation induced by a COI
 - For $o, o' \in O$, if o, o' are in the same COI, then $(o, o') \in CIR$

The Problem

- Not true in practice!
 - That is, in practice CIR does not partition the objects, and so not an equivalence class
 - Example: a company is not in conflict with itself, so $(o, o) \notin CIR$
 - Example: company c has its own private savings unit; b bank that does both savings and investments; oil company g does investments. So $(c, b) \in CIR$ and $(b, g) \in CIR$, but clearly $(c, g) \notin CIR$

The Solution

- Generalize *CIR* to define COIs not based on business classes, so *GCIR* is the reflexive, transitive closure of *CIR*
- To create it:
 - For all $o \in O$, add (o, o) to *CIR*
 - Take the transitive closure of this
- Then $(o, o') \in GCIR$ iff there is an indirect information flow path between o and o'
 - Recall $(o, o') \in CIR$ iff there is a direct information flow path between o, o'
- Now replace the COIs induced by *CIR* with generalized COIs induced by *GCIR*

Compare to Bell-LaPadula

- Fundamentally different
 - CW has no security labels, Bell-LaPadula does
 - CW has notion of past accesses, Bell-LaPadula does not
- Bell-LaPadula can capture state at any time
 - Each (COI, CD) pair gets security category
 - Two clearances, S (sanitized) and U (unsanitized)
 - $S \text{ dom } U$
 - Subjects assigned clearance for compartments without multiple categories corresponding to CDs in same COI class

Compare to Bell-LaPadula

- Bell-LaPadula cannot track changes over time
 - Susan becomes ill, Anna needs to take over
 - C-W history lets Anna know if she can
 - No way for Bell-LaPadula to capture this
- Access constraints change over time
 - Initially, subjects in C-W can read any object
 - Bell-LaPadula constrains set of objects that a subject can access
 - Can't clear all subjects for all categories, because this violates CW-simple security condition

Compare to Clark-Wilson

- Clark-Wilson Model covers integrity, so consider only access control aspects
- If “subjects” and “processes” are interchangeable, a single person could use multiple processes to violate CW-simple security condition
 - Would still comply with Clark-Wilson Model
- If “subject” is a specific person and includes all processes the subject executes, then consistent with Clark-Wilson Model

Quiz

Why are sanitized documents put into their own COI with one CD that holds them all?

1. It's really not necessary, but organizationally, it's easier to keep them separate from the sensitive documents.
2. It's necessary because otherwise two entities with access to different COIs could not access sanitized documents.
3. Mathematically, it's simpler to work with the sanitized documents in a separate COI.
4. The sanitized documents must be in the same COI but also should be in separate CDs corresponding to the CDs in which the unsanitized documents reside.