Confidentiality Policy: The Bell-La Padula Model

by

Amit Konar

Dept. of Math and CS, UMSL

What is a confidentiality policy?

A **confidentiality policy**, also called an **information flow policy** prevents the unauthorized disclosure of information.

Example: The navy must keep confidential the date on which a troop ship will sail. If the enemy knows the date of sailing, the ship could be sunk.

Recapitulation: Military/Governmental Security Policy

A **security policy** is a statement that partitions the states of the system into a set of authorized or secure states and a set of unauthorized or non-secure states.

A **military/governmental security policy** is a security policy developed primarily to provide confidentiality.

The Bell-La Padula Model

The **Bell-La Padula model** corresponds to military style classification model **to segregate the secure and non-secure states**.

It combines **mandatory** (system based compulsory) and **discretionary** (user-set) access controls. **S has discretionary read/write access to O means were the mandatory control not existent, S would be able to read/write O.**

Characteristics of the Model

1. The model provides a set of security clearance levels of subject set S and security classification for Object set O.
2. Let L(s) =l_s be the security clearance level of subject s and L(O) = l_o be the security classification for object o, then

   s can read o if and only if $l_o <= l_s$ and s has discretionary read access to o. (simple security condition)

Characteristics (Contd.)

3. S can write o if and only if l_s <= l_o, and s has discretionary write access to o. (*-property)
4. Let ∑ be a system with a secure initial state Q_o, and T be a set of transformations. If every element of T preserves the simple security condition and the *-property, then every state Q_i is secure.

Example: Illustrating characteristics

Top Secret (TS)	Tamara,Thomas	Personnel Files
Secret(S)	Sally, samuel	E-mail files
Confidential (C)	Claire, Clarence	Activity Log files
Unclassified(UC)	Ulaley,Ursula	Telephone list files

Claire/Clarence cannot read personnel files;
Tamara/Thomas cannot write on E-mail files.

Extension of the Bell-LaPadula Model

Why Extension is needed?

Since all information is not meant for all people, we need to classify the information too into categories. Suppose, for instance, we have three categories of information:

Nuclear Defence (abbreviated: **NUC**)
European Politics (**EUR**)
US Governmental issues (**US**)

But how these categories can go with security classification levels: Top Secret (TS), Secret (S), Confidential (c) and Unclassified (UC)

Attaching Category with i) User and ii) Info. Security Levels

Example: William may be cleared into the level: (SECRET, {EUR}) and

George into the level (TOP SECRET,{NUC,US}).

A document may be classified as (CONFIDENTIAL, {EUR}).

How can we compare the security levels of user with that of documents? This is needed to satisfy the Bell-LaPadula model.

Comparing Security Levels of Subject with that of Objects

To compare the security levels of subjects with that of objects, we define a relation, called **dominance**.

Defn.: The Security level (L, C) **dominates** security level (L$^{/}$, C$^{/}$) if and only if L$^{/}$ <= L and C$^{/}$<=C.

How to test dominance?

Example 1: Given George is cleared into security level: (SECRET, {NUC}).

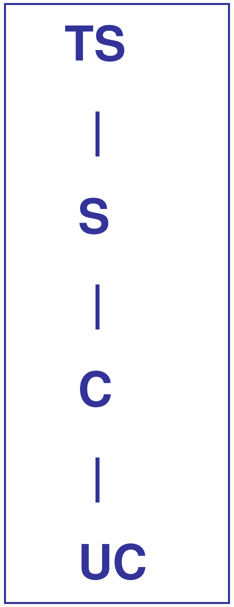
Doc A is classified as (CONFI.,{NUC}).

Here, $(L, C) = (S, \{NUC\})$

$(L', C') = (C, \{NUC\})$

$L' <= L$ and $C' \subseteq C$.

Therefore, George *dom* Doc A.



More Examples on Dominance

Suppose, George has a security level: (SECRET, {NUC, EUR}), and

Doc. B has a security level: (SECRET, {EUR, US}).

Here, (L,C) = (S, {NUC, EUR}), and

$(L^{/}, C^{/})$= (S, {EUR, US}).

So, $\mathbf{L^{/} <= L}$, but $\mathbf{C^{/}}$ ={EUR, US} **not** $\subseteq$ {NUC,EUR} = **C**. So, George ¬dom Doc B.

Revised Characteristics of the Bell-LaPadula Model

To take into account of categories in comparison of security levels between subjects and objects, the following revised characteristics are suggested:

1. **Simple Security Condition:** S can read O if and only of S *dom* O, and S has discretionary read access to O.

Revised Characteristics (Contd.)

2. **The *-Property:** S can write to O if and only if O *dom* S, and S has discretionary write access to O.

3. **Basic Security Theorem:** Let ∑ be a system with a secure initial state Q_0, and let T be a set of transformations. If every element of T preserves the simple security condition and the *-property, then every Q_i , i>0, is **secure**.

Why a Colonel cannot write on a Major's file?

A Colonel with (SECRET,{NUC,EUR}) clearance needs to send a Major with (SECRET,{EUR}). Here,

$(L,C)=$ (SECRET,{NUC,EUR}), and

$(L^{/}, C^{/})=$ (SECRET,{EUR}).

Since $L^{/} <= L$ and $C^{/} \subseteq C$, Colonel *dom* Major.

So, Colonel cannot write in major's file following the *-property, which states that Colonel can write on major's file if Major dom Colonel. This is not the case here.

Bypass Strategy to allow Colonel to write on Major's File

The Colonel can go down to his desired security level to enable him to write on Major's file by satisfying the *-property.

Colonel's maximum security level is (SECRET, {NUC, EUR}), but he can **go down** to his **current level: (SECRET,{EUR})** to be able to write message to Major's file, whose security level too is (SECRET, {EUR}).

Hybrid Policy: The Chinese Wall Model

What is a hybrid policy?

A hybrid policy is a security policy that refers equally to confidentiality and integrity.

The **Chinese Wall Model** ensures both confidentiality and integrity, and therefore it is a model of a **hybrid security policy**.

Where can we employ the Chinese Wall Model?

Consider the database of an investment house. It consists of companies’ records about investment and other data that investors are likely to request.

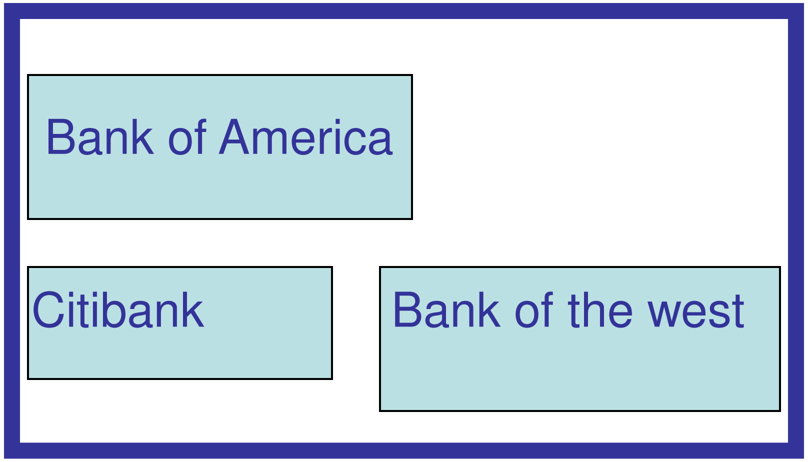
Analysts use these records to guide the companies’ investments, as well as those of individuals. If Anthony counsels Bank of America, he cannot counsel Citibank, as the two banks’ investments may come into **conflict.**

Definitions to capture the above problem

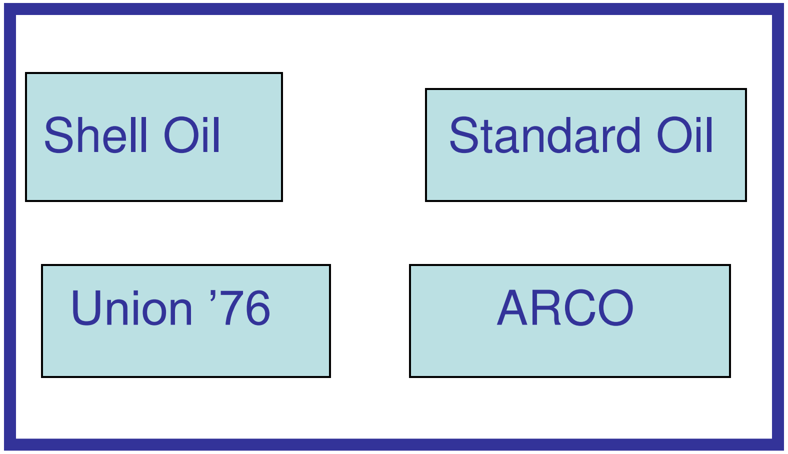
1. The **objects** of the database are items of information related to a company.
2. A **company dataset** (**CD**) contains objects related to a single company.
3. A **conflict of interest** (**COI**) class contains the datasets of companies in competition.

Example: The Chinese Wall Model database

Bank COI Calss



Gasoline Company COI Class



The model database has two COI classes: Bank class and gasoline class. The Bank class includes 3 CDs, whereas the Gasoline class includes 4 CDs. Susan may have access to one CD in each COI class.

A Big Problem

Suppose, Anthony first worked on Bank of America’s portfolio, and was then transferred to Citibank portfolio.

Even though he is working only on one CD in the bank COI class at a time, much of the information he learned from Bank of America’s portfolio will be current. Hence, he can guide Citibank’s investments using information about Bank of America, **which falls in the same COI class.** How can we overcome this problem?

Formalization of Rules to handle the said problem

CW-Simple Security Condition: 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 $O^{/}$, $O^{/} \varepsilon PR(S)$ implies $COI(O^{/}) \neq COI(O)$, where PR(S) is the set of objects that s has already read.

Problems that arise to enforce the second rule

1. Suppose, Susan accesses some information in in Citibank’s CD, she cannot access information in Bank of America’s CD.
2. Minimum no. of subjects needed to access every object in a COI class is the same as the no. of CDs in that COI class.

We accept both.

But what happens when the companies released data publicly?

Companies sometimes release data such as annual stockholders' report and filings before government commissions. The Chinese Wall Model should not consider this information restricted, because it is available to all. Hence, the model distinguishes between sanitized data and unsanitized data. We **modify** the **CW-Simple Security Condition** to take into account of **sanitized data only**.

Modified CW-Simple Security Condition

S can read O if and only if any one 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 $O^{/}$, $O^{/} \varepsilon PR(S)$ implies $COI(O) \neq COI(O)$.

3. **O is a sanitized object.**

One More Problem!

Suppose Anthony and Susan work in the same trading house. Anthony can read objects in Bank of America’s CD, and Susan can read objects in Citibank’s CD. Both can read objects in ARCO’s CD.

If Anthony can also write to objects in ARCO’s CD, then he can read information from Bank of America’s CD and write to objects in ARCO’s CD. Susan can read that information. So, Susan can indirectly obtain information from Bank of America’s CD, **causing a conflict of interest**.

A solution to the problem

CW-*-Property: A subject S may write to an 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 $O^{/}$, S can read $O^{/}$ implies CD($O^{/}$) = CD(O).

Assuming that **Bank of America's CD contains un-sanitized objects**, **condition 2 is false**, and Anthony cannot write in to objects in ARCO's CD.

Why Role-based Access Control?

Example: Alison is responsible for keeping track of all accounting for the CS dept. Now, alison moves to university's office of Admission. Sally is a new book-keeper of the CS dept. She will acquire full access to all those accounts.

Access to A/C is a function of the job: book-keeper, and is not tied to any particular individual. Here is the need for a role-based access control.