A new Chinese Wall Security Policy Model Based On the Subject’s Wall and Object’s Wall

Mr. Saad Fehis  
National School of Computer 
www.esi.dz 
Algiers, Algeria 
Email: s_fehis@esi.dz

Dr. Omar Nouali  
Research Center on Scientific and Technical Information 
www.cerist.dz 
Algiers, Algeria 
Email: onouali@cerist.dz

Pr. Tahar Kechadi  
University College Dublin 
School of Computer Science and Informatics 
Dublin, Ireland 
Email: tahar.kechadi@ucd.ie

Abstract—To controlling the information flows between the competing companies (CC) in the cloud computing (Multi-tenancy) or in the social network, the Chinese wall security policy (CWSP) is very interesting solution. Its rule is the building of the walls between the CC. The CWSPs idea, is the building of impenetrable wall among subject, and this to controlling the information flow between the CC, caused by the subjects. However, the preview proposed models [1-6]; they have a set of errors and they can’t fix the composite information flows (CIF) problem between the CC (a malicious Trojan horses problem).

In this article; we will propose a new approach based on the access query type of the subject to the objects and the philosophy of the CWSP. In our model we have two types walls placement, the first are built around the subject, and the second around the object; which, we can’t find inside each once wall two competing objects data.

Keywords—Security Policy, Chinese Wall, Information flow, Access Control.

I. INTRODUCTION

To control information flow between the competing companies in the cloud computing (Multi-tenancy) or in the social network (facebook, twitter ), the Chinese wall security policy (CWSP) is very interesting solution. The CWSP arises in the UK's financial sector that provides consulting services to other companies. Consultants naturally have to deal with confidential company information for their clients. The objective of the CWSP is to prevent information flows which cause conflict of interest for individual consultants.

The CWSP was identified and so named by Brewer and Nash (BN-model); where they developed a mathematical model for this policy [1]. Their idea is the grouped of the dataset of companies in conflict of interest classes (COI), so a set of partitions and applying to subjects a mandatory ruling, where all subjects are allowed access to at most one dataset belonging to each such conflict of interest class (simple security rule). Where, the access is only granted if the object requested:

(a) Is in the same Company Dataset as an object already accessed by that subject, or,

(b) Belongs to an entirely different Conflict of Interest Class. Access means read or write.

So, this to answer that no direct information flow (DIF) between CC. And also they prevents the CIF by the application of the start-property rule to write access, where is only permitted if, the:

(a) Access is permitted by the simple security rule, and

(b) No object can be read which is in a different Company Dataset to the one for which write access is requested and contains un-sanitized information.

The proposal was a great idea; unfortunately, BN’s model was based on incorrect assumption that corporate data can be partitioned (decomposed) into mutually disjoint conflict of interest classes (CIR-classes); such a disjoint collection is called a partition in mathematics. CIR-classes seldom disjoint; they do overlap, and hence BN theory collapses. Also, the authors did not distinguish between human users and subjects that are processes running on behalf of users. Consequently, the model proposed is very restrictive as it allows a consultant to work for one company only. Sandhu [7] improves upon this model by making a clear distinction between users, principals, and subjects, defines a lattice-based security structure, and shows how the CWP complies with the Bell-Lapadula model [10].

In the same year, Lin [2] announces a new model (ACWSPM) to fix the errors of BN. The error is that the conflict of interest is a binary relation CIR, and not equivalence class (partitions). The CIR is non-reflexive, symmetric and anti-transitive. The Lin’s idea is the construction of a partition, where they were based on the idea of each binary relation induced equivalence relation [2-6]. The induced equivalence relation named by IAR In allied with relation used by Lin is the complement of CIR.

We observing that, Lin in [2-6] fix the problem of the CIF by the using of the same idea of BN [1], un-sanitized/sanitized information and also the read/write access type; where: in BN the un-sanitized information is confined to its self-company but in Lin to allied dataset. However, in Lin; they make stronger it, by the idea of the anti-transitive; and their CIR theorem (Theorem CIR is a symmetric and anti-reflexive and anti-transitive binary relation. Its complement IAR is an equivalence relation).
We observed that the induced equivalence relation of CIR is composed just by two partitions, so all the companies are grouped into two allied partitions. And this caused by the constraint of the anti-transitivity of CIR. And this hardly exists in the real word (just in cold war, example of Lin). We will give following in appendix a new proposition with demonstration about the number of the partitions related to the induced equivalence relation.

In our article, and to fix those errors, we keep just the non-reflexive; and the symmetric of CIR and we will propose a new CWSP mode. In our model, we are giving a real interpretation of the access queries type by the subject to the object. In the real word they are two accesses type: Reading or Writing queries.

The reading queries is a reading by the subject from the object, so the moving of the data from the object into inside of the subject. The subject can’t read information from two competing objects (rules of the CWSP [1]). The idea is too attached to subject a security label composed by two elements, the granted and the denied access right; where:

- The Granted: Contains a set of all objects identification (or company identification) who theirs data inside the subject wall (read by the subject).
- The Denied: Contains the set of all denied objects identification (or the companies identifications) where they can’t read it in the future by the subject.

The granted and denied access can be represented by an access matrix between Subjects and Objects, and this can be interpreted by the building of a wall around the subject and we call this by the subject’s wall.

The writing queries is made by the subject to write any information from the side of its self to the object (inside the object), let the name of the object is Ob1 and the subject name is Sub1. It’s easy, to induced that this information related to the previews reading queries from many objects made by the subject. So, this query is permitted if and only if this information isn’t in competing of the data stored inside the object. So, our second type of the wall is built around the object.

And we can’t find inside the same wall, datas related to competing objects. To modeling this: the idea (as a same to the subject), is too attached to each object a security label composed by two elements, the IAR (allied with) and the CIN (conflict of interest); where:

- The IAR: Contains a set of all objects identification (or companies identifications) who theirs data inside the object wall (data stored inside the object).
- The CIN: Contains the set of all competing objects identification (or the companies identifications) where they cant write it inside the object, or there is a related competing data stored inside this object.

The IAR and CIN can be viewed as binary relation between objects, and represented by matrix between Objects to Objects, and this can be interpreted by the building of a wall around the object and we call this by the Object’s wall. By this approach, we will assuring that not just any DIF between competing companies but also no CIF between them; so the fixing of the malicious Trojan horse’s problem.

The remainder of the paper is organized as follows. In section 2, we present the previews proposed CWSP models and our motivation. In section 3, we will present our new model, idea, illustration by an example, the formal model, and information flow. In section 4 provides conclusions and future research directions, than an appendix related to the binary relation and our observation related to the number of the partitions. And finally, a list of references used in our article.

II. RELATED WORK AND MOTIVATION

Firstly, our main objective is the application of the CWSP in the Cloud Computing, and the social network and not the proposition of a new model for the CWSP. However, and after analyze of the previews proposed models [1-9] and theirs applications [12-19], we are surprising by many errors. For example the problem of the Conflict of interest (COI) is a set of disjoint class disjoint or a binary relation (CIR), the error was fixed in 1989 by Lin [2-6], but to our days there are many applications based on COI classes and not a CIR binary relation.

Some work subsequent to BN [1] has pointed out that their enforcement mechanism can be highly restrictive. Specifically, in [7-9] they establish the following two properties: (P1): A subject that has read objects from two or more Company Datasets cannot write to any object. And (P2): A subject that has read objects from exactly one Company Dataset can write to that Dataset only.

There is a recent and interested work proposed by [11], where they proposed a Least-Restrictive Enforcement of the CWSP based on graph representation, where, their enforcement mechanism mediates read attempts only to prevent subject-violations, and write attempts only to prevent object-violations. However, in his article there is a strong mathematical confusion between the notion of the class, partition, equivalence binary relation and the transitivity property (page 3). Also, their graph representation is very complex for the implementation.

III. OUR CWSP-MODEL BASED ON THE PLACEMENT WALL, AROUND SUBJECT OR OBJECT:

In our model; we constructed our idea on the access query type of the subject to the objects and the philosophy of the Chinese wall security policy CWSP. Thiers rule is the building of the walls between the competing companies. In our model we have two types walls placement, the first are built around the subject, and the second around the object; which, we can’t find inside the once wall two data related to two competing objects. So, we start by these analyses:

A. Idea Analyses:

The subject firstly, is freely to choose to access to any object; at this step its important to known the nature of this access reading or writing access, as in the following:
1) Reading Queries: If the access is Reading query; this induced us to read from the object by the subject, and we can interpret this by the moving of the data from the object inside the wall rounded this subject. So, there is a related data (information) of the object inside this wall. Also, the access is denied of this subject to the competing objects with our object (inside the wall rounded this subject). So, there is a related data induced to read from the object by the subject, and we can interpret this type of query by the writing of related information of the set off all subject has the security label, composed by two components:

- The granted objects (Granted): That represents the set of all objects where their related data inside the subject wall.
- Denied objects (Denied): That represents the set of all objects denied to moving them into the inside of this subject wall.

2) Writing Queries: If the access is writing query by the subject Sub1 to the object Ob1; we can interpret this type of query by the writing of related information of the set off all objects inside the wall rounded our subject (Sub1) into the object Ob1. So, our second type wall is building around the object, and this object wall can’t contain the competing object’s data. So, we induced, that the object’s wall has two securities labels:

- The allied objects (IAR): That represents the set of all objects where their related data inside the object wall or in allied with the object.
- Conflict of interest objects (CIN): That represents the set of all objects in conflict of interest with the objects stored inside our object wall, so they denied to moving them into the inside of the object wall.

3) Illustration by an example: If we have two subjects Sub1 and Sub2, and five objects Ob1, Ob2, Ob3, Ob4 and Ob5, where Ob1 in competition with Ob2, Ob3 in competition with Ob4 but Ob5 neuter with the others objects. And we have this queries sequence in our system:

   Q1: Subject Sub1 reading access from the object Ob1; so there is a related data of Ob1 inside the subject wall of Sub1.

   Q2: Subject Sub1 reading access from the object Ob2; this access is denied, because there is inside of its wall a data related to the object Ob1, which is in competition with the object Ob2 (Rules of Chinese wall security policy [1]).

   Q3: Subject Sub2 reading access from the object Ob2; so there is a data inside the subject wall of Sub2.

   Q4: Subject Sub1 reading access from the object Ob5; we have inside the subject wall a data related to the object Ob1 and this object isn’t in conflict of interest with the object Ob5, so the access is granted and also the moving of the data from Ob5 to the subject Sub1, inside of its wall.

   Q5: Subject Sub1 writing access to the object Ob5; so write information from the inside subject wall (data related to Ob1 and Ob3) into the object Ob5, so the object wall of Ob5 contain a data related to the objects Ob1 and Ob3.

Q6: Subject Sub2 writing access to the object Ob5; so write information from its inside subject wall (Ob2) into the object Ob5, but, the object wall of Ob5 contain a data related to the object Ob1 who it is in competition with Ob2. However, this is in contradiction with the Chinese wall security policy. So this query is denied and not permitted.

Let now, if we have a third subject Sub3, where he need to read a data from the object Ob5 and then write it to the Ob2. So, the problem is that our malicious subject (Sub3) need to create a CIF between competing object Ob1 and Ob2!

Firstly; the subject Sub3, read data from the object Ob5. However, Ob5, contains a related data of the two objects Ob1 and Ob3 (from Q5) and also the object have two sets information the CIN and the IAR. So, we have the two following steps:

The first step is the reading: After the reading access, we have inside the subject Sub3 a data related to three objects Ob1, Ob3 and Ob5. So, the Sub3’s Granted contains the IAR of Ob5 and his Denied contains the CIN of Ob5 (that contains the Ob2).

The second step is the writing: the writing access to the object Ob2, this, is not permitted, because the object is in the Denied set of the subject. So, the access is denied. So, we conclude, that our malicious subject can’t create a CIF between competing objects.

In end we can view in table I and II, the end stat of the Subjects’ wall and Object’s wall.

4) Queries’ running conditions: Let the subject Sub1 has the two sets object: Grantedi and Deniedi, and the object Obj has the two objects set: IARj and CINj

After, the previous interpretation of the query access type (Reading / Writing), we can induced the necessary condition to running the query of the access of the subject Sub1 to the object Ob2 is:

\[ \text{Granted}_i \cap \text{CIN}_j = \emptyset \lor \text{Denied}_i \cap \text{IAR}_j = \emptyset \]

If this condition is verified, we need to update the labels as following:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sub1</td>
<td>Granted = {Ob1, Ob2}; Denied = {Ob2, Ob4}</td>
</tr>
<tr>
<td>Sub2</td>
<td>Granted = {Ob2}; Denied = {Ob3}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Object</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ob1</td>
<td>IAR = {Ob1}; CIN = {Ob2}</td>
</tr>
<tr>
<td>Ob2</td>
<td>IAR = {Ob2}; CIN = {Ob1}</td>
</tr>
<tr>
<td>Ob3</td>
<td>IAR = {Ob3}; CIN = {Ob4}</td>
</tr>
<tr>
<td>Ob4</td>
<td>IAR = {Ob4}; CIN = {Ob1}</td>
</tr>
<tr>
<td>Ob5</td>
<td>IAR = {Ob1, Ob3, Ob5}; CIN = {Ob2, Ob4}</td>
</tr>
</tbody>
</table>
B. Formal Model:

Let \( OB \) denote the set of all objects, \( OB = \{obj_1, .. , obj_n\}, \) \( SU \) denote the set of subjects, \( SU = \{s_1, .. , s_m\}, \) and \( Comp(\text{obj}_j) \) or simply \( Comp_i \) be the company dataset \( [1] \).

1) Dataset organization: In our model we keep the dataset proposed by Lin [2-6], where:

(1) At the Lowest Level, we consider individual items of information, each concerning a single corporation. We will refer to the files in which such information is stored as objects [1].

(2) At the intermediate level, we group all objects which concern the same corporation together into what we call a company dataset [1].

(3) At the highest level we associate with each company dataset, say X, a Frechet neighborhood, denoted by CIN(X) Conflict of Interest Neighborhood of X, where CIN(X) is the set of all company datasets that are in conflict of interest to X.

2) Conflict of interest relation CIR: Let \( CIR \subseteq OB \times OB \) as a binary relation, satisfies the following properties.

- CIR-1: CIR is symmetric.
- CIR-2: CIR is anti-reflexive.

It should be clear CIR-2 is necessary; a company cannot conflict to itself. If company A is in conflicts with B, B is certainly in conflicts with A, so CIR-1 is valid.

3) Model: Our model is 5 tuples:

\( (SU, OB, IAR, ACC, Query) \) where:

1) \( OB \): Denote the set of all objects,
2) \( SU \): Denote the set of all subjects
3) \( IAR \): Be a matrix with element \( IAR(i,j) \) corresponding to the members of \( OB \times OB \), where the value of \( IAR(i,j) \) is:

- 1: That the object \( O_i \) contain (or stored inside itself) a related information about the object \( O_j \);
- 0: That the object \( O_i \) can’t will contain any related information of the object \( O_j \). Or the object \( O_j \) has information in the conflict of interest with the object \( O_i \);
- -1: there isn’t any information related to the object \( O_i \) stored inside the object \( O_j \);

Initially, \( IAR(i,j) = 1 \) if \( i = j \); 0 if \( (O_i, O_j) \in CIR \); Otherwise -1. And we can define also two subsets of \( OB \):

- \( IAR(O_i) = \{O_j \in OB | IAR(i,j) = 1 \} \) the set of all objects inside of the object \( O_i \);
- \( CIN(O_i) = \{O_j \in OB | IAR(i,j) = 0 \} \) the set of all objects denied to be stored inside of the object \( O_i \);

4) \( ACC \): Is an access matrix with elements \( ACC(i,j) \) corresponding to the members of the \( SU \times OB \), where the value of \( ACC(i,j) \) is:

- 1: That the subject \( S_i \) contain related information of the object \( O_j \).
- 0: That the subject \( S_i \) can’t will contain any related information of the object \( O_j \).

Initially, \( ACC(i,j) = -1 \) for all \( (i,j) \). And From this matrix, we can also define two subsets of:

- \( Granted(S_i) = \{O_j \in OB | ACC(i,j) = 1 \} \) the set of the objects inside of the subject wall of \( S_i \);
- \( Denied(S_i) = \{O_j \in OB | ACC(i,j) = 0 \} \) the set of the objects denied to the subject \( S_i \);

5) \( Query(S_i, O_j, mode) \): Any query made by a subject \( S_i \) to access to the object \( O_j \) with the mode equal to:

- \( read \): to reading from the object
- \( write \): to writing into the object

The access is authorized, if and only if; this condition is verified:

\( Granted_i \cap CIN_j = \emptyset \) OR \( Denied_i \cap IAR_j = \emptyset \)

And in the same time:

If the mode is Reading Query (Writing in the subject side, inside the wall that rounded the subject):

- \( ACC(i,h) = 1 \) where \( O_h \in IAR_j \); (or \( Granted_i = Granted_i \cup IAR_j \))
- \( ACC(i,h) = 0 \) where \( O_h \in CIN_j \); (or \( Denied_i = Denied_i \cup CIN_j \))

If the mode is Writing Query (In Object side, inside the wall that rounded the object):

- \( IAR(j,h) = 1 \) where \( O_h \in Granted_i \); (or \( IAR_j = Granted_i \cup IAR_j \))
- \( IAR(j,h) = 0 \) where \( O_h \in Denied_i \); (or \( CIN_j = Denied_i \cup CIN_j \))

Otherwise, the access is denied, and in the same times:

- \( ACC[i,j] = 0 \)

C. Information flows, Objects, Companies and their Allies:

In our model we were focalize on the relations between objects and the information flows between them. However; what about of the flow between the object in the same company or in allies? The answer is the information flows is
freely between them. So, we build the object wall around of
the allied objects (allied companies).

However, in our proposed model the update of the matrix
IAR is focalized on the object and not on the companies or
their allied. So, to fix this problem, the solution is the mapping
of IAR from of $OB \times OB$ to $Comp \times Comp$. By this mapping;
we will assure that, we can’t find the data of two competing
companies stored inside the same company (in different objects
of the same company).

IV. CONCLUSION

In this article, we based our idea by the applying by
symmetry of the building of the wall around the object a same
rule as the subject; and this by the starting from these points:
From BN in [1]:

(a) The basis of the Chinese wall policy is that people
are only allowed access to information which is not
held to conflict with any other information that they
already possess.

(b) Chinese wall is created for that user around that
dataset and we can think of “the wrong side of this
Wall” as being any dataset within the same conflict of
interest class as that dataset within the Wall.

And the third point from [11]:

(c) Information can flow between two objects only via
a subject, and information can flow between two
subjects only via an object (malicious Trojan horses
problem)

Also, in this article we based our model on the mathematical
model, where the Conflict of interest is a binary relation and
not a set of partitions (Class) [2-6]. And, by the interpretation
gave of the two kinds of the queries (Reading / Writing).Our
model assured that can’t find any information flow between
competing companies (DIF or CIF).

Our model, can it is the starting point of application the
distributed Chinese Wall security policy. And, in the futures
works we believe to applying our model in the Cloud Computing,
workflow or any previews application of the Chinese
wall in the past based on the wrong models.

APPENDIX

Binary Relation Property:

Let $V$ a set of objects (or elements), and we recall some
definitions:
A binary relation is a subset, $B \subseteq V \times V$ for each object
$p \in V$, we associate a set $B_p$ defined by:

$$B_p = \{v \in V \mid pBv\} \text{ or } B_p = \{v \in V \mid (p, v) \in B\}$$

That consists of all elements $v$ that are related to $p$ by $B$. $B_p$
is called a binary neighborhood.

If the binary relation is an equivalence relation, then $B_p$ is the equivalence class containing $p$.

A symmetric binary relation $B$ is a binary relation such
that for every $(u, v) \in B$ implies $(v, u) \in B$.

A binary relation $B$ is anti-reflexive; if $B$ is non-empty
and no pair $(v, v)$ is in $B$. That is, $B \cap \Delta = \emptyset$, where
$\Delta = \{(v, v)\mid v \in V\}$ is called diagonal set.

A binary relation $B$ is anti-transitive; if $B$ is non-empty and
if $(u, v)$ belongs to $B$ implies that for all $w$ either $(u, w)$ or
$(w, v)$ belongs to $B$.

Let the complement, $B' = V \times V \sim B$, is called the
complement binary relation (CBR) of $B$.

Proposition: if $B$ is symmetric, anti-reflexive and anti-
transitive, then $B'$ is an equivalence relation [6].

Our Proposition: if $B$ is symmetric, anti-reflexive and
anti-transitive, then the number of $B$’s partitions are two.

Proof:
Let $(u, v)$ belongs to $B$, so by the definition of the anti-
transitive; implies that for all $w$ either $(u, w)$ or $(w, v)$
belongs to $B$, so:

$$B_u = \{w \mid (u, w) \in B\}, B_v = \{w \mid (w, v) \in B\} \text{ and } B_u \cap B_v = \emptyset.$$ 

$$B'_u = \{w \mid (u, w) \notin B\} = \{w \mid (w, v) \in B\} \text{ this is the first partition.}$$ 

$$B'_v = \{w \mid (v, w) \notin B\} = \{w \mid (u, w) \in B\} \text{ this is the second partition.}$$

Let $H \neq \emptyset$ the third partition, so $H = \{h \mid (u, h) \notin B \text{ and } (v, h) \notin B\}$, this is in contradiction with the ant-transitivity
of $B$, QED.

REFERENCES

Policy, in Proceedings of the IEEE Symposium on Security and Privacy,
ings of the Fifth Aerospace Computer Security Application Conference,
December 4-8, 1989, pp. 286-293.
- Analysis of Symmetric Binary Relations. COMPSAC 2002: 966-974
SMC 2007: 3027-3028
European Symposium on Research in Computer Security (ESORICS 92).


[17] Xing Xie, Indrakshi Ray, Raman Adaikkalavan, Rose Gamble: Information flow control for stream processing in clouds. SACMAT 2013: 89-100
