Proceedings of Thirteenth Annual Computer Security Applications Conference,
San Deigo, California, December 8-12, 1997

Lattice-Based Models for Controlled Sharing of Confidential Information in The Saudi Hajj System

Tarik F. Himdi Ravi S. Sandhu
Laboratory for Information Security Technology
Department of Information and Software Systems Engineering
George Mason University, Fairfax, VA 22030, USA
{thimdi,sandhu}@ isse.gmu.edu

Abstract

The pilgrimage (Hajj) is an annual event that takes place in Saudi Arabia. Three major government ministries (Foreign, Internal, and Hajj) create and process Hajj data separately in their systems. Currently all data sharing between these ministries regarding Hajj is done manually. Benefits from sharing data electronically are obvious. But due to the sensitivity of some data and the common requirement of not sharing everything, a trusted environment which provides interoperability between these systems while ensuring confidentiality of shared data is needed.

In order to study the possibility of establishing such an environment, data was collected regarding the security requirements of the three Saudi ministries directly from the source through interviews. There are three increasingly sophisticated security requirements: No obligation access security, Multi-level security, and Chinese Wall security. This paper analyzes each security requirement, builds a lattice model for it, and uses these models to specify the information flow policy for each system.

1. Introduction

Every year a large number of Muslims come from all over the world to Saudi Arabia to perform pilgrimage (Hajj) in certain places during certain times. The government of Saudi Arabia annually spends millions of dollars to ensure the safety and comfort of pilgrims. Three major government ministries (Foreign (F), Internal (I), and Hajj (H)) create and process Hajj data separately in their systems. Data sharing between these ministries regarding Hajj is currently done manually. There are many benefits from sharing data electronically. For example currently each system enters the personal data of every pilgrim, while this data could be captured once at the F-system (when a pilgrim applies for Hajj-visa) and transferred later to I and H systems. But due to the sensitivity of some data and the common requirement from officials in these ministries of not sharing everything, there is a need for a trusted environment which provides interoperability between these systems while ensuring confidentiality of shared data. To study the feasibility of establishing such an environment, the first author collected data regarding the security requirements of the three Saudi ministries directly from the sources through interviews. Analysis of this information showed that the three ministries require three increasingly sophisticated security requirements: No obligation access security, Multi-level security, and Chinese Wall security.

In this paper we show that all three requirements can be enforced using the Lattice-based access control model with MAC (Mandatory Access Control) in the classic BLP (Bell-LaPadula framework) [1,10] which was developed to deal with information flow in computer systems. Information flow policy in a lattice-based access control model is concerned with flow of information from one security class to another. The concept of such policy was defined by Denning [5] and has received much attention in the security community. This paper analyzes each security requirement, builds a lattice model for each requirement, and uses these models to specify information flow policy for each system (F, I and H).

Lessons learned from this case study can be applied to a large number of organizations with similar security requirements. In general our analysis is applicable to any Multi-Domain Organization (MDO). We define an MDO as any organization that has two or more sub-organizations, each performing specific tasks using separate systems, with the need to share data in a controlled manner. Each sub-organization is usually distributed over multiple locations. Governments and large corporations are examples of MDOs.

The paper is organized as follows. Section 2 introduces Hajj case study, and how the three systems interact with Hajj data. Then Section 3 considers the Saudi government as an MDO, and presents the security requirements of such systems. Section 4 introduces the lattice-based models for each of the three requirements, while Section 5 presents the information flow policy for the system's network. Section 6 concludes the paper.

2. Hajj case study

The Hajj, or pilgrimage, is the fifth task in ISLAM which all adult Muslims must perform at least once in their lifetime [12]. For the past 13 centuries pilgrims came to Saudi Arabia every year during Hajj month with no restrictions or visa or any kind of permit. Their total number averaged between 20,000 to 30,000 annually. Most came in convoys which spent months on sea and land. As the number of Muslims increased and methods of transportation made it easier and affordable to travel, the total number of pilgrims increased 40 times. Currently it averages between 1 million to 1.2 million per year [9]. Figure 1 shows this growth and the percentage of pilgrims by region.

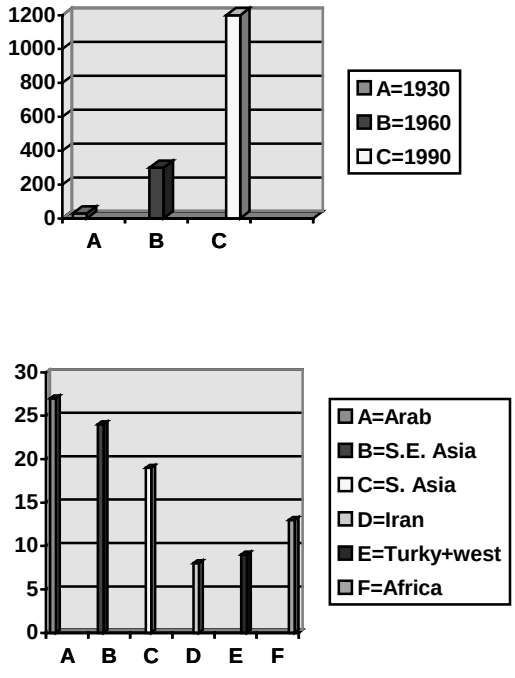


Figure 1. Pilgrims total (by 1000) for the past 60 years and the percentage of their geographical distribution

Three heterogeneous systems (Foreign or F, Internal or I, and Hajj or H ministries) separately create and process Hajj data (summarized in Table 1), and need to share this data continuously to provide services and security to pilgrims during this annual event.

2.1. The Foreign ministry's system (F)

Currently the system administrators of the F-system are working to connect it via modems with every Saudi embassy's system (E) all over the world. The F-system (which is located in Riyadh) is applying multi-level security policy for access control. Figure 3 shows the plan for F-system's architecture.

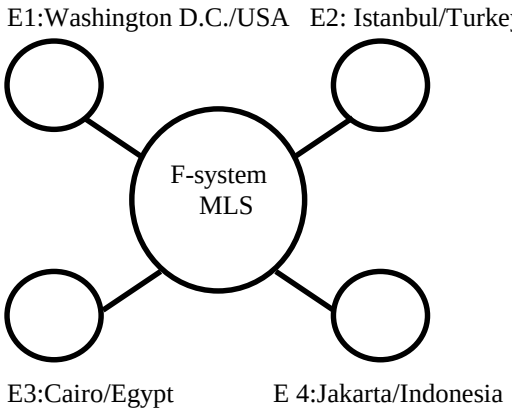


Figure 2. F-system

2.2. The Internal ministry's system (I)

The Internal ministry is the largest ministry in the Saudi government. The responsibilities and services of this ministry include: police force, fire and rescue, intelligence services, secret services, immigration and naturalization, passports and citizenship, traffic control, vehicle registration and ownership, civil rights and disputes, and foreign labor permits. Figure 3 shows some departments of the Internal ministry.

The Internal ministry's main system is currently at the National Data Center in Riyadh, connected to every department of the Internal ministry in every city via modems. The main system is applying multi-level security policy for access control. Figure 4 shows the I-system's architecture.

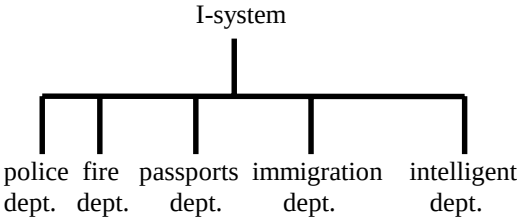


Figure 3. Some Internal ministry departments

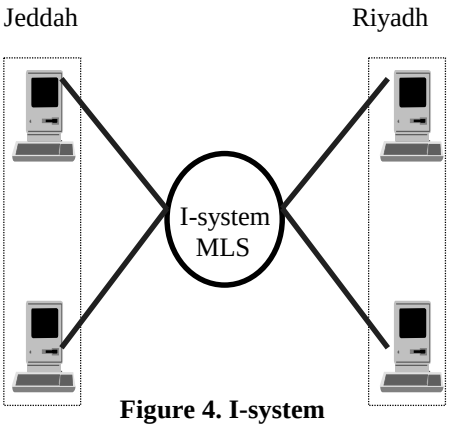


Figure 4. I-system

2.3. The Hajj ministry's system (H)

The Hajj ministry has many sub-organizations. Each sub-organization has a different system. Some of these are located in Jeddah, while the rest are located in Makkah and Madenah. The central computer of the H-system is located in Jeddah, and it is applying multi-level security policy. The system administrators in the Hajj ministry are working to connect the central computer with the other sub-organizations' systems via modems. Some of these sub-organizations are [8]: One Guide Establishment (Adela) in Madenah, six Guide Establishments (Mutauf) in Makkah, Registration (United Agents Office), and Transportation (Public Vehicle Union) in Jeddah. Figure 5 shows the plan for H-system's architecture, while Figure 6 shows the six guide establishments in Makkah which serve pilgrims according to the geographical areas of their nations:

- Arab Hajj-guide Establishment: serving pilgrims from Middle East countries.
- South-East Asia Hajj-guide Establishment: serving pilgrims from: Indonesia, Malaysia, China, etc.
- South Asia Hajj-guide Establishment: serving pilgrims from: India, Pakistan, Bangladesh, etc.
- Iran Hajj-guide Establishment: serving pilgrims from Iran only.
- Turkey and West Hajj-guide Establishment : serving pilgrims from Turkey, Europe, North and South America.
- Africa Hajj-guide Establishment: serving pilgrims from the rest of Africa excluding Middle East countries, Nigeria, South Africa, etc.

Each establishment has many service offices. Each office serves 2000-3000 pilgrims. All guides in each office have been approved and selected by the Operation department in the headquarter of the establishment. Not any one can be a guide, only those who inherit this job from their ancestors can be chosen to practice it [8].

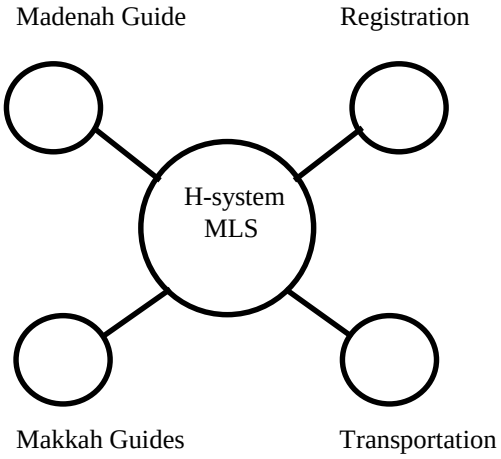


Figure 5. H-system

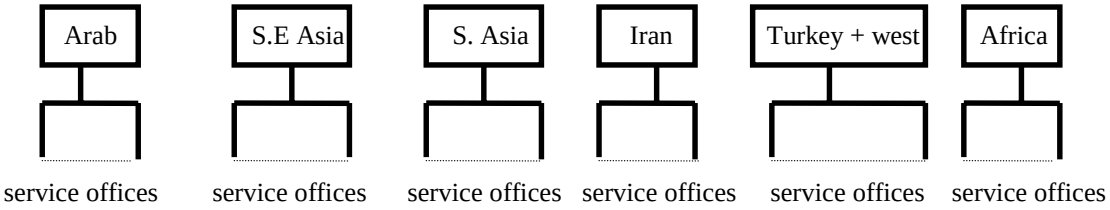


Figure 6. The six guide establishments in Makkah

3. Multiple security requirement of Hajj

By considering the Saudi government as an MDO with three sub-organizations (F, I, H), we can analyze the security requirements of the over-all system as the combination of the security requirements needed by F, I, and H systems.

Currently each system is using Multi-Level Security (MLS) locally, with the four classical hierarchical security levels: unclassified (U), confidential (C), secret (S), and top secret (TS).

Based on data collected by the first author from Saudi officials, we present three increasingly sophisticated security requirements: No obligation access security, Multi-level security, and Chinese Wall security. These requirements are explained, somewhat informally and intuitively, in the rest of this section. A formal statement of each requirement in terms of a lattice model is given in Section 3. The three system's administrators should agree on a security architecture that is capable of using different types of access control models to meet these security requirements.

3.1. First requirement: No obligation access security

The First requirement deals with sharing files that do not contain sensitive information, but only certain systems can access them. It is defined as follows:

A user's subject can access a remote unclassified file provided :

a) the user is assigned to access the remote system which has that file,

b) the user's local system has permission to access that remote file,

c) unclassified subjects can have Read/Write access to that file but Confidential (and higher) subjects can only have Read access.

We call this the **No obligation requirement** because there is no obligation which requires the subject's security level to be upgraded if two or more files are accessed simultaneously by that subject (see below).

For example, say Fu-10 is an unclassified user from F-system who is assigned to access H-system (condition a). This means he can invoke unclassified subjects only. The H-system has two unclassified files (Haj-Missions, and Housing) as shown in Table 1(a) column I. The F-system has permission to access the Haj-Missions file but cannot access the Housing file (condition b). Therefore, Fu-10 can access Haj-Missions file with Read/Write rights when he invoked his unclassified subject. Now if Fc-20 is a confidential user from F-system who is also assigned to access H-system, then he may invoke unclassified as well as confidential subjects. If he invoked his confidential subject, he can access the Haj-Missions file with only Read right (due to star-property).

In addition, an access to more than one unclassified file is done with no obligation to upgrade the security level of the user (i.e., unclassified + unclassified = unclassified). For example, if the unclassified user Iu-40 from the I-system is authorized to access H-system (condition a), and since H-system has two unclassified files Haj-Missions and Housing both of which are accessible to I-system's users as shown in Table 1(a) column I (condition b), then Iu-40 can access both files with Read/Write rights with no obligation to upgrade his subject's security level to confidential for instance (condition c). In other words any combination of unclassified files will have the security level as unclassified. As we will see this is not true for confidential or secret files where the combination may have a higher security level.

Column I of Table 1 (a) represents the unclassified files for the first requirement, and the systems that can access them. For example F-system has two unclassified files Haj-Attaché and Haj-Tourist each of which can be accessed by users from F, I, and H systems. Access by F-system users is implied and not shown explicitly in the Table, whereas access by I and H systems is shown by the tag [I,H] attached to each file. The I-system has a single unclassified file Haj-Plan which can be accessed by I and H systems but not the F-system. As discussed above, the H-system has two unclassified files: Haj-Missions which can be accessed by users from H, F, and I systems, and Housing which can be accessed by users from H and I systems only. The tokens such as "*atc*" and "*tor*" attached to the respective files will be used as abbreviations later in this paper. This notation also applies to columns II and III. Note that access by a system to its own files is implied and not shown explicitly in Table 1(a). Table 1(b) gives a brief description of the contents of each file.

3.2. Second requirement: Multi-level security

The second requirement deals with sharing sensitive files, where confidentiality and multi-level security are the major concerns. These files are shown in column II of Table 1(a). Each of these files is individually labeled as Confidential (C). The "+" sign between any two confidential files indicates that the combination of those two files will be Secret (S). Similarly a combination of Secret files from two or more different systems will be Top Secret. For example, the combination of the confidential files Haj-Visas and Gov-Guest is Secret. The combination of the two secret files "Haj-Visas + Gov-Guest" and "Haj-In + Haj-Out" is labeled Top Secret because each one belongs to a different system.

	I	II	III
	No obligation/Unclassified	Multi-level / C,S,TS	Chinese Wall
F-System	Haj-Attaché "*atc*"[I,H] Haj-Tourist "*tor*"[I,H]	Haj-Visas"*vis*"[I,H]+ Gov-Guest"*gus*" [I,H]	Haj- Deplom*"dpl"* [I,H] Secret-Comm *"scm"* [I,H]
I-system	Haj-Plan *"pln*"[H]	Haj-In *"hji"* [F,H]+ Haj-Out *"hjo"* [F,H]	Black List "*bkl*" [F] Non-Saudi in List *"nsl"* [F]
H-system	Haj-Missions *"mis"* [F,I] Housing "*hos*" [I]	Guide-Est "*gde*" [I] + Arrival&depature*"a&d"*[F,I]	Haj-Registration"*rgs*"[F,I] Transport *"trn"* [I]

at H-system "file" [F,I] = from H to F, and I (a)

File Name	File Description: each includes *
Haj-Attaché	reports about agreements between Saudi officials and other Governments' officials about co-operation in organizing their pilgrims
Haj-Tourist	data about tourist groups who organize journeys for Hajj
Haj-Plan	data about plans for traffic control, and fire fighting
Haj-Mission	data about every nation's pilgrimage mission in Saudi Arabia
Housing	data about houses rented to accommodate pilgrims in Makkah, and Madenah
Haj-Visas	personal data of a pilgrim granted Hajj visa
Gov-guest	the names, nationality, and all necessary arrangements of government's guests who will perform Hajj
Haj-In	data about a pilgrim's arrival flight, date and port
Haj-Out	data about a pilgrim's departure flight, date and port
Guide-Est	data about each establishment and its services offices, including the names of pilgrims in each office
Arrival&depature	personal data about each pilgrim arrived and denatured to Makkah and Madenah
Haj-Deplom	reports about senior government staff and VIP from other nations who wish to perform Hajj
Secret-Comm	reports of confidential letters between F central system and its sub-systems regarding Hajj
Black-List	data from intelligence resources about non-Saudi citizens who should not enter or leave Saudi Arabia
Non-Saudi in List	personal data about every non-Saudi citizen who live inside Saudi Arabia and information about his sponsor
Haj-Registration	type and amount of payment received from each pilgrim, this database summarize total revenue for each session.
Transport	data about number of pilgrims who used Hajj transportation system and financial reports about this system

***** Files' names used are not the original ones (b)

Table 1. Security requirement-data table

The second requirement is defined as follows:

A user's subject can access a remote confidential / secret / top secret file provided:

a) the user is assigned to access the remote systems which has that file,

b) the user's local system has permission to access that remote file,

c) the subject and file labels must satisfy the standard simple-security and star properties (with write-up allowed), except that combinations of files may have higher security level than their individual constituents as per the following rules

I. a combination of two Confidential files from a single system is Secret

II. a combination of Secret files from two or more systems is Top Secret

Note that conditions a and b are identical to conditions a and b of the first requirement. Condition c is different and stipulates that confidential + confidential may equal secret and secret + secret may equal top secret. The reason for these rules is to prevent aggregation of sensitive information. Without such aggregation controls the

individual systems are not willing to share their data. Fortunately, the system administrators of the three systems will agree on this above uniform requirement.

For example in column II of Table 1(a), the I-system requires that only secret users from I, F, and H systems can access its secret file "Haj-In+Haj-Out" with Read/Write rights used by a secret subject labeled "Haj-In+Haj-Out". Confidential users from those systems may access one of the confidential files "Haj-In" or "Haj-Out" with Read/Write rights used by a confidential subject labeled "Haj-In" or "Haj-Out" respectively.

3.3. Third requirement: Chinese Wall security

The third requirement deals with sharing special and sensitive files by special users, such that a user can access only one file from each system. Moreover these special users are not allowed to access files under the first or second requirements. Furthermore top secret users are exempted from this rule, because they are sufficiently trusted.

The third requirement is defined as follows:

A user's subject can access a remote Chinese Wall file provided:

a) The user is assigned to access the remote systems which has that file,

b) The user's local system has permission to access that remote file,

c) The subject is limited to a maximum access of one Chinese Wall file from each system, and the user cannot access any non-Chinese Wall file (under the first two requirements). Top secret users are exempted from condition c.

Again note that conditions a and b are identical to conditions a and b of the previous two requirements, but condition c is very different.

For example in column III of Table 1(a), the I-system requires that any special user (non-TS) from the F-System (or I-System) who has access to the "Black-List" file of the I-System, should not have access to the I-system's file "Non-Saudi in List". This requirement is motivated by the Chinese Wall Model [2] to prevent aggregation of information. Such a requirement is very strong and important to prevent leakage and misuse of sensitive data. Otherwise, users (lower than Top Secret) who access the "Black-List" file might modify records in the "Non-Saudi in List" file which have data about a black listed person. Column III of Table 1 (a) represents the special files (Chinese Wall files) for the third requirement, and the systems that can access them. Each system has two Chinese Wall files such that a non-TS user can access only one of them.

4. Lattice Based Models

In this section we construct lattice based models for each of the requirements discussed above. The first requirement may not appear to require a lattice model, but as we will see it is needed to prevent illegal information flow by Trojan Horses. The second requirement explicitly requires the use of MAC and is therefore well suited for a lattice model. A general lattice model allows information flow upward in the lattice from low to high and does not allow information flow from high to low or between incomparable security classes. By using MAC with such a lattice, the first and second requirements can be enforced.

For the Chinese Wall policy it was shown in [11] how to use a lattice. In our construction we distinguish two disjoint types of users:

Type A users [Multi]: deal with categories of a lattice used by the first or the second requirement, where [U,C,S TS] users access (U) files for the first requirement, and (C,S,TS) files for the second requirement.

Type B users [Chin]: deal with categories of a lattice used by the third requirement, where special users access Chinese Wall files only (except for top secret users who can access files of all three requirements).

4.1. The No obligation Lattice Model

In order for a user to access certain remote unclassified files, under the No obligation requirement, two conditions must be met:

a) The user must obtain access right to the remote system which has these files.

b) The user's system must have permission to access these files.

The major problem with this requirement is the Trojan horse problem. For example, an unclassified user from I-system such as Iu-1 may access the H-system's files "*hos*" and "*mis*" with Read/Write right, where he can read "*hos*" file and write its contents to "*mis*" file. Now when an unclassified user from F-system such as Fu-10 accesses the H-system's "*mis*" file, he will have access to data from "*hos*" too, in violation to the access control requirements.

In order to allow a user to access more than one unclassified file simultaneously, without the Trojan horse problem, we define the No obligation lattice shown in Figure 7. This is a standard subset lattice on five compartments (with no system low). Figure 7 omits the dominance relationships in the lattice to avoid cluttering the diagram. (Dominance relationships are similarly omitted in Figures 8 and 9.) The five compartments correspond to the five unclassified files in column I of Table 1(a). They appear as singleton categories in the bottom row of Figure 7. Categories above these

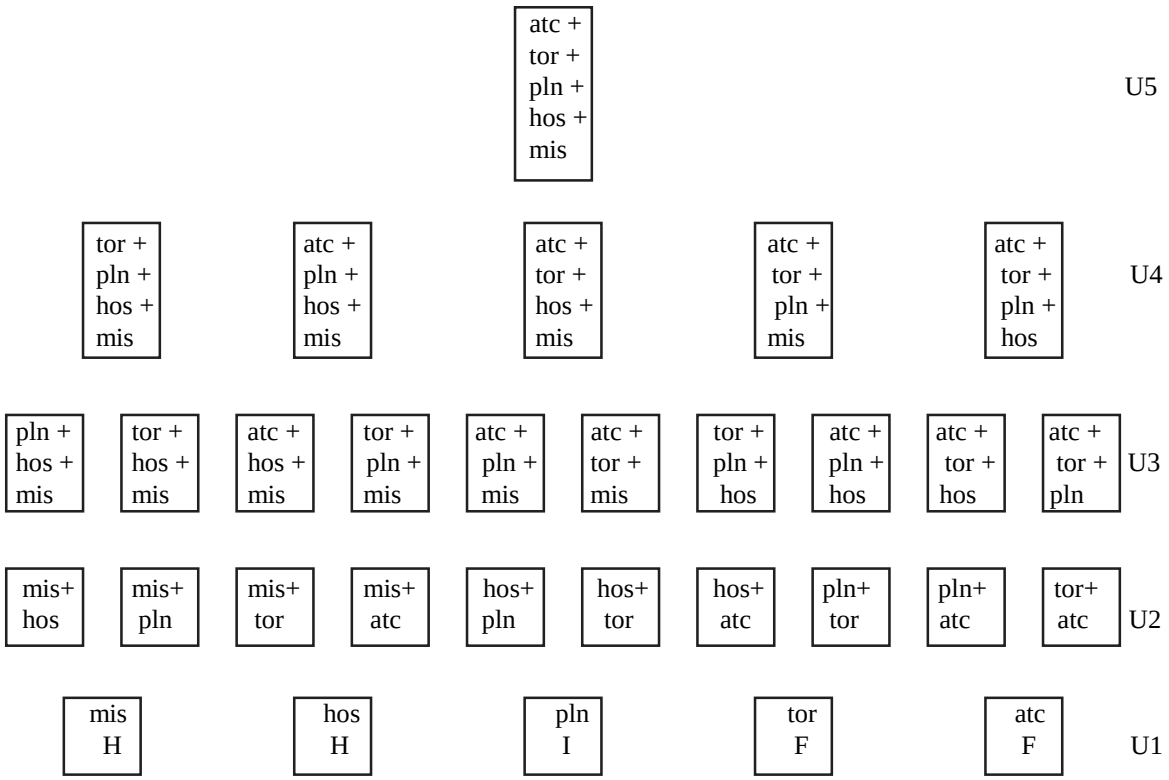


Figure 7. No obligation lattice model

correspond to simultaneous access to multiples files as indicated. A category dominates another if compartments of the former are a superset of the latter. The No obligation requirement is enforced by the following rules in context of the No obligation lattice.

1) *As in the usual practice in multi-level systems a user is allowed to have subjects at any label dominated by the user's clearance.*
2) *A user can only have those subjects allowed by conditions a and b of the No obligation requirement.*

Now if the unclassified user Iu-1 wants to Read/Write to "*mis*" file only, he must invoke his unclassified subject **mis** (since he can invoke unclassified subjects only), where he can access "*mis*" category in level U1 with Read/Write rights, and access with Write right all other categories in level U2 and above that have "*mis*" as part of their labels. Similarly, in order for Iu-1 to Read/Write to "*mis*" and "*hos*" files simultaneously, he must invoke his unclassified subject **mis+hos** to access "*mis+hos*" category which holds the combination of these two files. In this case Iu-1 can Read/Write "*mis+hos*", Read only "*mis*" and "*hos*", and Write only to categories that have any file(s) in addition to "*mis+hos*" file, such as "*pln+mis+hos*", "*tor+mis+hos*", ect. Thus when Fu-10 access *"mis"* category by invoking his **mis** subject, he can Read/Write to it where he will not access any data from *"hos"* file now.

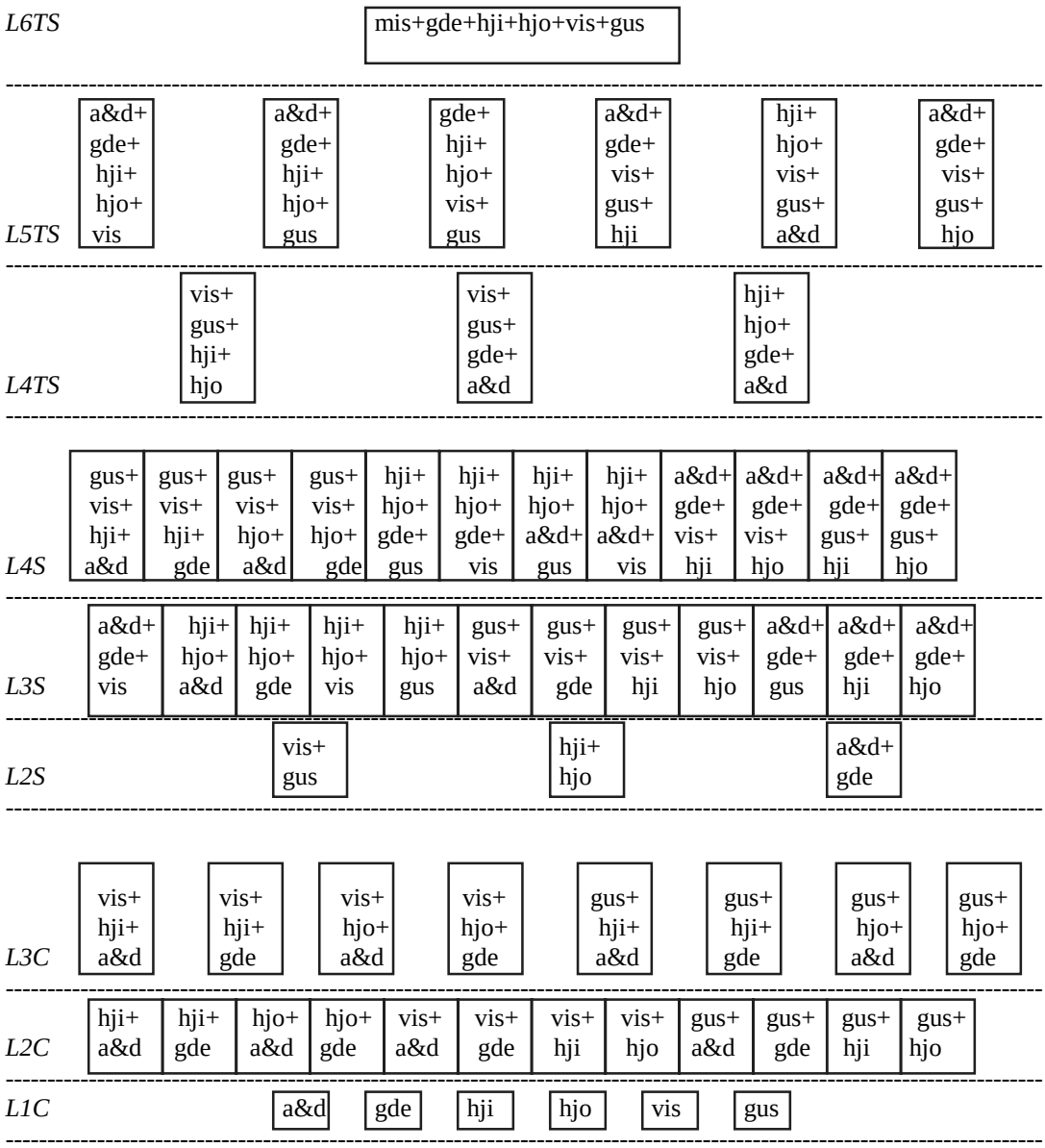
In the other hand, the confidential user Fc-20 may access *"mis"* category by invoking his unclassified subject **mis**, where he can Read/Write to it too, or by invoking his confidential subject (say **a&d**), where he can Read only to the unclassified categories:

"atc", *"tor"*, *"mis"*, and their combinations, Read/Write to the confidential category which its label is equivalent to the subject's label (*a&d*), and Write to secret and top secret categories (which hold *a&d*).

Notice that all F-system users can not Read only or Read/Write to categories which hold *"hos"* file from H-system or *"pln"* file from I-system since their system (F) does not have permission to access these files. But they may Write only to those categories which hold any one of those files with *"atc"*or *"tor"* file from F-system or *"mis"* file from H-system.

4.2. The Multi-level Lattice Model

For the multi-level security requirement with respect to column II of Table 1(a) we have six confidential files. Similar to section 3.1 we could take each of these to be a



LN: level no. C: confidential S: secret TS: top secret

Figure 8. The lattice model for MLS

separate compartment to satisfy the second requirement. However, certain combinations of confidential files need to be labeled Secret as discussed in section 3.2. Likewise combinations of certain Secret files need to be labeled Top Secret. Figure 8 presents a lattice for the second requirement. It is very similar to a subset lattice on six compartments. There are 2^6-1=63 categories (omitting empty one). The major difference is that some of these categories (marked L1C, L2CandL3C) are Confidential, others (marked L2S, L3S and L4S) are Secret, while the rest (marked L4TS, L5TS and L6TS) are Top Secret. This follows from condition c of the second requirement that certain combinations of files have higher security level than their individual constituents as per the following rules:

I. a combination of two Confidential files from a single system is Secret

II. a combination of two Secret files from two or more system is Top Secret

Information flow and category dominance is the same as the previous lattice of Figure 7, that is, a category

dominates another if compartments of the former are a superset of the latter. To emphasize the labeling rule for combinations of compartments we have shown the lattice going up from C to S to TS categories. Note that all categories of size four are S or TS, and all of size 5 or 6 are TS. Categories of size 2 or 3 can be S or C. Nevertheless the information flow is exactly that determined by the superset relationship. For example, if Fc-30 is a confidential user from F-system who is selected to access I-system's confidential file *"hji"* with Read/ Write rights, then he must have a confidential subject labeled **hji** that will allow him to Read/Write to *"hji"* category. Now if Fc-30 wants to access the secret category *"hji+hjo"* with Read/Write rights, he cannot have a secret subject labeled **hji+hjo** because his security level is confidential which prevents him from having a subject with higher security level than his. Fc-30 can only have subjects which are unclassified and confidential.

4.3. The Chinese Wall Lattice Model

The lattice model for Chinese Wall indicates the categories which represent the Chinese Wall files and their combinations as follows from Table 1. The Chinese Wall lattice is shown in Figure 9. This lattice will satisfy the third requirement, since categories from "CHN1" level to "CHN3" level can have at most one file from each system. For example, as discussed in [7,11], the lattice's category labeled *[dpl,bkl,ϕ]* is the category that contains *"dpl"* file from F-system, *"bkl"* file from I-system, and Null from H-system.

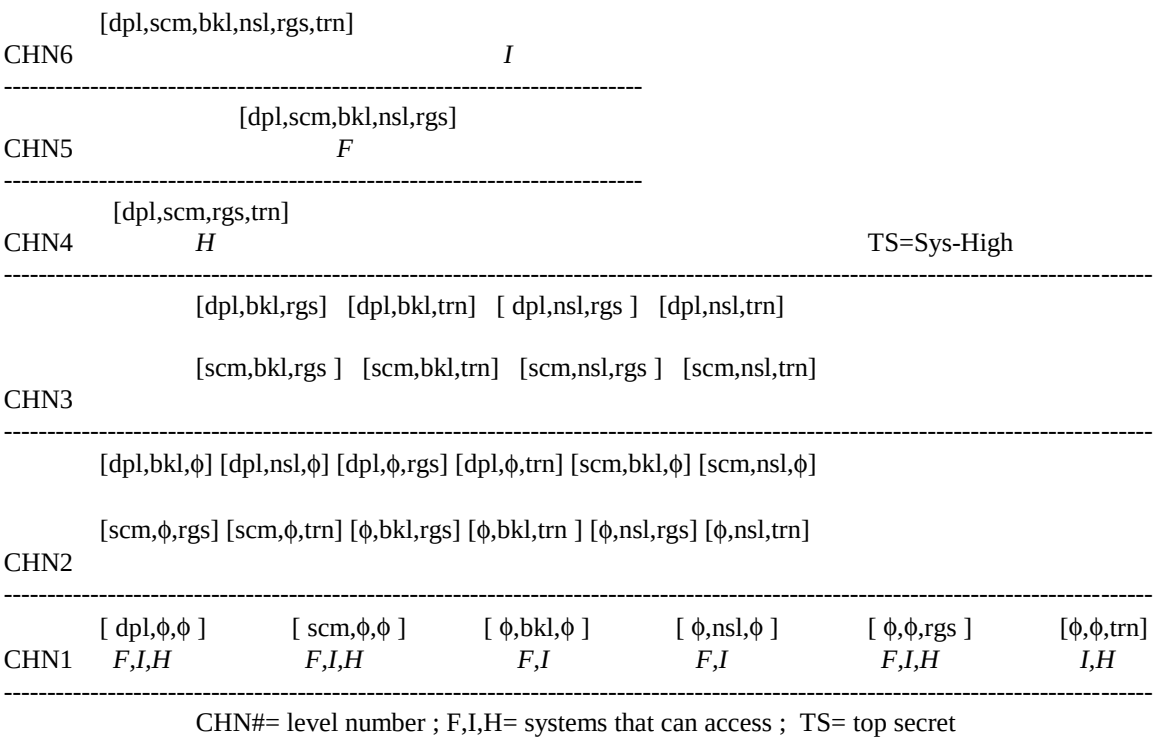
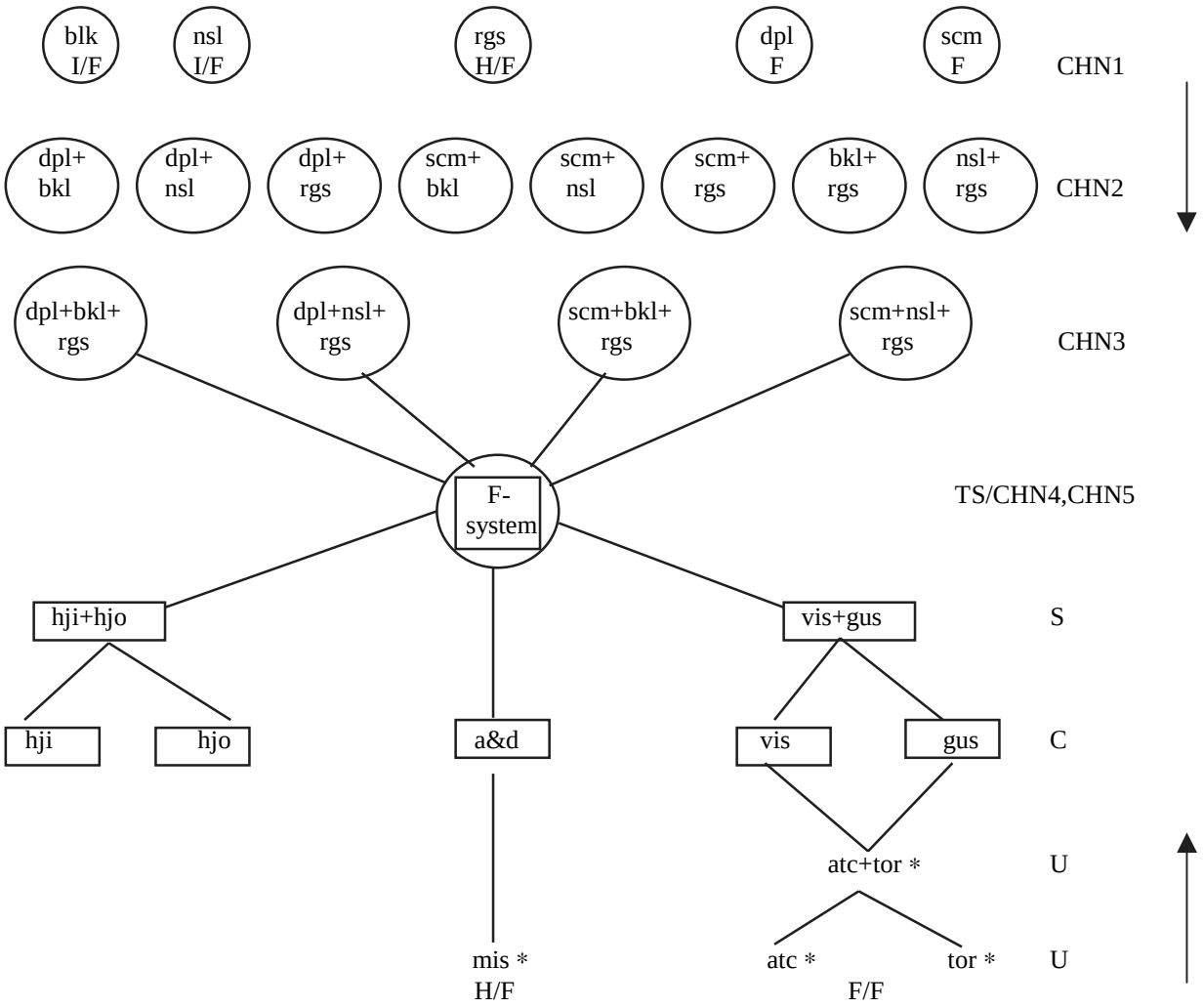


Figure 9. The lattice model for Chines Wall

Now a subject whose label is **[dpl,bkl,ϕ]** may Read/Write to the category whose label is *[dpl,bkl,ϕ]* in "CHN2" level, Read the categories whose labels are *[dpl,ϕ ,ϕ]* and *[ϕ ,bkl,ϕ]* in "CHN1" level, and Write to the categories whose labels are *[dpl,blk,rgs], [dpl,bkl,trn]* in "CHN3" level, and to all categories in "CHN4", "CHN5, and "CHN6" which contain both *"dpl"* and *"bkl"* files. CHN1, CHN2 and CHN3 labels can only be applied to special users and their subjects. Special users are disjoint from multi users as discussed earlier.

The "CHN4", "CHN5", and "CHN6" levels are exempted from the Chinese Wall policy. They consist of three system-high labels, one each for H, F and I systems respectively. Since I-system Chinese Wall files are not available to H-system users, the H-system TS users can access *"dpl", "scm", "rgs",* and *"trn"* files.



*=Unclassified file, = Confidential, Secret, Top Secret file, O = Chinese Wall file, ↑ = information can flow, I/F = I-system file accessed by F-system users.

Figure 10. F-system's information flow policy

Similarly, F-system TS users can access all except *"trn"* file, while I-system TS can access all Chinese Wall files.

5. Information flow policies for each system

By analyzing each system according to Table 1 and the lattice based models, it is possible to create the information flow policy for each system. For example, Figure 10 shows F-system's information flow policy with the access to its users/ subjects to the following local/remote categories with Read/Write as follow:

1- All subjects that belong to Multi users: U,C,S,TS have access to the following unclassified files and their combinations with different rights depending on the subject's security class and its label: *"atc"* and *"tor"* (from F-system), and *"mis"* (from H-system).

2- A confidential subject that belongs to a Multi user: C, or S, or TS may access one or null local confidential category: *"vis"* or *"gus"* (from F-system). It may also access the single confidential category *"a&d"* (from H system) and one of *"hji"* or *"hjo"* (from I-system).

3- A secret subject that belongs to a Multi user: S, or TS may access one secret category from each system. In this case we have *"vis+gus"* from F-system, and *"hji+hjo"* from I-system, while there is no secret category from H-system.

4- A Chinese Wall subject that belongs to a special user may access Chinese Wall categories according to the subject's label.

5- A top secret subject that belongs to a Multi user: TS may access all secret categories and below, as well as the Chinese Wall files: *"bkl", "nsl", "rgs", "dpl", "scm"* and all combinations.

In Figure 10 the system high Top Secret class is shown in the center of the diagram to make the diagram clearer. As before we have omitted the dominance lines in the Chinese Wall categories from CHN1 through CHN3 to simplify the figure. Similarly, I, and H systems' policies could be specified.

6. Conclusion

In this paper we considered the Saudi Arabian government as an MDO with three sub-organizations (F, I, and H) who need to share Hajj data. The first author collected data regarding the security requirements of the three Saudi ministries directly from the sources through interviews. Analysis of this information showed that the three ministries require three increasingly sophisticated security requirements: No obligation access security, Multi-level security, and Chinese Wall security.

The first requirement (No obligation) deals with how a user's subject can access **unclassified** files, while the second requirement (Multi-level) deals with how it can access **confidential, secret, and top secret** files, and the third requirement (Chinese Walls) deals with how it can access **Chinese Wall** files.

Due to the difference between each requirement's rules, two types of users are identified: one [Multi] = {U,C,S,TS} for the first and second requirement, and the other [Chin] for the third requirement (except top secret who can access all three requirements' files). The paper analyzed each security requirement, built a lattice model for it, and showed how to use these models to specify information flow policy for each system. Our case study demonstrates that the lattice model is very useful for analyzing multiple security requirements for confidentiality in MDOs. Although the details of the policy will differ for other MDOs, similar analysis of security requirements based on No obligation, Multilevel and Chinese Wall considerations can be applied.

In this paper we presented multiple requirements in an MDO (the Saudi Government), but implementations were not discussed. For implementations, we are studying the Department of Defense Goal Security Architecture (DGSA) [3] toward these requirements. Although pure DGSA does not support these requirements, or any lattice-based model requirement, there are various extensions to DGSA that will result in different schemes which can achieve these goals.

Another existing architecture is Secure Information Through the Replicated Architecture (SINTRA) [4,6] which could be applied to MLS or any lattice-based requirement.

Acknowledgment

We would like to thank all Saudi officials who support us in conducting this study especially Dr. Nabel Bukary director of computer department in the Foreign ministry, Eng. Mohammed Tabi Alkalbi Networks and Data Communications department in National Data Center, and Dr. Essa Rawas project manger in the Hajj ministry. In addition we would to thank the anonymous reviewers for their comments and supports.

Reference:

[1] Bell, D.E. and LaPadula, L.J. Secure Computer Systems: Mathematical Foundations and Model. M74-244, Mitre Corporation, Bedford, Massachusetts (1975).

[2] Brewer, D.F.C. and Nash, M.J. The Chinese Wall security Policy. Proceedings IEEE Symposium on Security and Privacy, 215-228, (1989).

[3] Center for Information System Security Program. Department of Defense (DOD) Goal Security Architecture (DGSA). Version 1.0, 1 August 1993.

[4] Costich, O., McLean, J., and McDermott, J. Confidentiality in a Replicated Architecture Trusted Database System: A Formal Model. Proceeding of the Computer Security Foundations Workshop VIII, pages 60-65, IEEE Computer Society, 1994.

[5] Denning, D.E. A lattice Model of Secure Information Flow. Communication of ACM 19(5):236-243, (1976).

[6] Kang, M.H., and Peyton, R. Design documentation for the SINTRA global scheduler. Naval Research Laboratory Memo Report 5542- 93-7362 (1993).

[7] Meadows, C. Extending the Brewer-Nash Model to a Multilevel Context. Proceedings IEEE Computer Society Symposium on Research In Security and Privacy, Oakland, California, May 7- 9-1990.

[8] Ministry of Hajj. Pilgrimage Organizing Instructions. Office of the Minister, Special Publication (1994).

[9] Ministry of Information. At the Service of Allah's Guest. Information Affairs, Special Publication (1993).

[10] Sandhu, R.S. Lattice-Based access Control Models. IEEE Computer, November -1993.

[11] Sandhu, R.S. Lattice-based Enforcement of Chinese Walls. Computer & Security, 753-763, November -1992.

[12] Zani, M.H. Hajj in Islam. Al-Manhel Magazine, May-1995.