# A Dynamic Security Mechanism Based on a Decentralized Authorization Model

4R−3

Idunn Weidemann Løvseth Hanne Linaae Yahiko Kambayashi

Faculty of Engineering, KYOTO UNIVERSITY

## 1 Introduction

In this paper we will discuss key security and authorization mechanisms in Virtual Office. In [LiLoKa93] the concepts will be developed further.

Authorization features in Virtual Office are based on a fully decentralized model and are connected to the concepts of **Files**, **Keys**, and **Groups**. So far, few commercial information or database systems have been made using a decentralized authorization mechanism. However, in 1970, IBM made such a database system called System R. We will show how the System R method for access-control can be generalized so that it can be used in an office information system, and in Virtual Office in particular.

## 2 The Virtual Office Concept

Virtual Office is an information system made to support ordinary office work in a distributed computer system. It is named **Virtual** because the office in the computer system is virtual in a way that users can construct their own office space to work in. The main objective of Virtual Office is to make life in the office easier by integrating all parts of the office environment and thus give a total solution to support usual office work. The following issues are focused on:

**User friendly interface.** When working with different tools and communication equipment, the user should face an easy-to-use graphical interface, and not be confronted with a different user-interface for each new tool she uses.

**Integration with communication equipment.** Virtual Office also integrates means of communication which not usually are supported by computers (telephone, fax, etc.). All communication equipment will be modeled on the screen using icons.

**Communication among multiple users.** Virtual Office will focus on support of co-operative work, with various communication functions among multiple users. This includes advanced mail, conference, and conversation functions, and the possibility of propagating work to other people.

**Construction of personal office space.** In a real office, people can arrange their own work space. This is also possible in Virtual Office by a graphic model of the actual physical layout of the office space. It is possible to virtualize office space and in this way be able to designate several desks to each user.

**Security.** When using computer networks, data-sharing becomes very easy. However, not all data should be shared. Security management becomes extremely important in order to handle classified information and individual's privacy.

A prototype of Virtual Office is developed using GAIN (a tool for developing interactive software with a graphical user-interface). See [TaTaKa92] and [TaKa92].

分散認証モデルによる動的セキュリティ機構
イードゥン ロブセト、ハンネ リノー, 上林弥彦
京都大学工学部

## 3 Authorization in Virtual Office

Authorization mechanisms in Virtual Office are connected to the concepts of Files, Keys, and Groups. Most information systems today have authorization mechanisms connected to File-access. In Virtual Office, however, we want the access-control to be fully decentralized. Also we want the authorization mechanisms to include Keys and Groups. A Key is introduced to lock areas in the personal office space, and a Group is introduced to enable co-operative work.

### 3.1 Files

A decentralized authorization model implies that there is no central "security manager" to distribute file access to various users. Instead, we wish to have a model where each user automatically has access to all her files, and is permitted to propagate this access-right to other users. An access-right can be given with or without a **Grant option**. If an access-right is given with a Grant option, this implies that the new user is permitted to give the access-right to yet other users.

This model could be extended with possibilities to e.g. specify different kinds of access (e.g. write, read, run, index, – depending on the nature of the file), give time-limited access-rights, revoke access-rights already given, or give common access-rights to a group of users.

#### 3.1.1 Keys

The office environment in Virtual Office is modeled as a picture on the screen with different rooms, equipment, desks, shelves, drawers, etc. In a real office a person is able to hide away things, put them in a locked room, box or drawer so that nobody else has access to these objects without possessing a key to them. This feature is also necessary in Virtual Office, and therefore the Key-notation is introduced.

A Key can be used to handle classified information, e.g. by making a lock on a desk that is assigned to a certain project. The Key is also important to protect individual's privacy. In order for people to trust the system, they have to be sure that no intruders are able to read their personal information.

A Key can be assigned to all of the objects modeled in the workspace. Keys can be given to other users, in a similar way the access-rights on files are distributed. A Key can also be given with or without a Grant option. A Key with a Grant option is like a physical key that may be copied.

This model could be extended by e.g. having a single Key that goes to several different rooms, or assigning a Key to a whole Group of users (and not only to individuals). It is also desirable to have the possibility of giving time-limited Keys or revoking Keys which already are assigned to users.

### 3.2 Groups

The Group-concept is introduced to support co-operative work. A Group can be functional (like a department or lab.), or founded on demand (like project-groups). A Group in Virtual Office is defined to be a collection of users. In a simple model a Group can be founded by anyone, and the founder can include any other user she feels like including. Similar to the fashion in which access-rights to Files and Keys are distributed, a user can become a member of a Group with or without a Grant option. A membership with a Grant option gives the member right to include other users into the group.

These basic features are not enough, – we need a model that is even more flexible and powerful. A user should be

asked and **agree** prior to being included in a group. Within the Group, there is a need for a more democratic decision-making process. In small groups it may be efficient that individual group-members make decisions on behalf of the whole group, but when the group becomes large it is intolerable not to have other options for decision-making.

While a group is working, many issues have to be decided upon: Which new group members should be included, whether the group should to grant file-access to other users, how to edit common files, what kind of work is to be performed within the group, which rules should apply to the group in general, etc. To achieve a more democratic decision-making process, it can be required that a certain percentage of the group-members have to agree on a decision before it is put into effect. To model a real-life situation in an office, it should be possible to assign roles to group-members. Each user should be given rights and responsibilities according to the role she has.

### 3.3 Combination

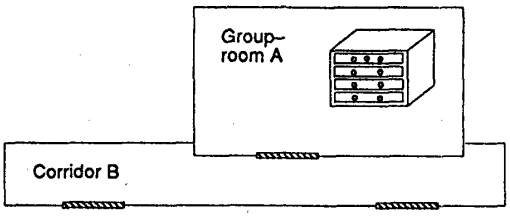


Figure 1: Floor Plan in Virtual Office

Virtual Office takes the whole office into consideration, and unlike other database and information systems, also physical aspects can be modeled. The concepts of Files, Keys, and Groups can be combined to make a **Floor-plan** (see fig. 1). A Floor-plan is a model of the office environment where physical hindrances also are included. We can attach Keys to all the objects in the Floor-plan (doors, drawers, etc.), specify where documents are stored, and assign a Group of users as owner of certain objects. By combining the objects in a Floor-plan with the authorization mechanisms of File, Group, and Key, the authorization-scheme for a real-life office can be modeled. E.g. in figure 1 one can specify that the doors to "Corridor B" always are locked, that the "Group-room A" only is accessible to people in "Project A", the chest of drawers inside "Group-room A" has the top drawer locked, and that "Report 1" is inside that drawer. So, for a user to access "Report 1" she needs to have the right keys, be in "Project A", and have file access to "Report 1". Authorization limits are specified for each object, and there is no need to supply the full (combined) rule for all the objects as a whole. The user can "walk" through the office environment (Floor-plan), and access-rights are checked for each object as she proceeds.

## 4 Theoretical model

In this section we will explain System R's method for access-control, and show that this serves as a suitable framework for the distributed access-control needed in Virtual Office. For a thorough discussion of the method, see [GriWad76], [Fagin78] and [Kamb80].

The term **distributed** or **decentralized** access control refers to the way the authorization function is divided among a number of administrators. System R, an IBM database system, has distributed access control, where an owner of a table may grant various access rights to other users. The owner also has the option of permitting the grantee to further grant the acquired rights to other users. For example, if owner Ann wishes to grant user Susan the SELECT and INSERT rights to the STUDENT relation and to allow these rights to be passed on (Grant option), Ann enters the following statement:

```
GRANT SELECT, INSERT ON STUDENT TO Susan WITH
GRANT OPTION;
```

Any user who has granted a privilege may subsequently REVOKE it. The state of the system after the revocation is as if the grant had never been made.

Consider the grants of a specific privilege on a specific table. The grants may be represented by the sequence:

$$G_1 \ldots G_i \ldots G_j \ldots G_n$$

where $i < j$ implies that $G_i$ was granted at an earlier time than $G_j$. If $G_i$ later is revoked by the command $R_i$ then:

$$G_1 \ldots G_{i-1},\ G_i,\ G_{i+1} \ldots G_n,\ R_i$$

is formally identical to:

$$G_1 \ldots G_{i-1},\ G_{i+1} \ldots G_n.$$

That is, the revoked grant appears never to have occurred. (See [FeSuWo81])

System R's method for access control is transferable to Virtual Office. The owner of a File or a Key can distribute her access-right by granting privileges to other users. In a similar manner to that used in System R, the access-right might be granted with or without a Grant option. A founder of a Group can include other members by granting membership-rights with or without a Grant option.

As an example of how this is done in a office information system, consider the following sequence of grants to a File (Letter21) by user **Jane**, **Eiko**, **Yumi**, and **Tom**:(Virtual Office has a graphical user-interface so commands will not be *written* like shown in the example, but the essence is still the same. In Virtual office the commands will be given by selecting menu-items.)

**Jane:**
```
GRANT EXECUTE, WRITE ON FILE Letter21 TO Eiko
WITH GRANT OPTION;
```
**Jane:**
```
GRANT EXECUTE ON FILE Letter21 TO Yumi;
```
**Eiko:**
```
GRANT ALL PRIVILEGES ON FILE Letter21 TO Tom;
```
**Jane:**
```
REVOKE ALL PRIVILEGES ON FILE Letter21 FROM Eiko;
```

This sequence is formally equivalent to removing the first grant from the sequence. Then one of the remaining grants

**Eiko:**
```
GRANT ALL PRIVILEGES ON FILE Letter21 TO Tom;
```

is not valid since Eiko has no right to access Letter21. Hence the effect of the revocation is to withdraw rights not only from Eiko but also from Tom.

## 5 Conclusion

In this article we have discussed security mechanisms in the office information system Virtual Office. We have focused the attention on authorization. System R's method for access-right checking serves as a suitable framework and theoretical foundation for authorization in Virtual Office. In Virtual Office, authorization is connected to the concepts of Files, Keys, and Groups, and works in a fully decentralized fashion. Physical hindrances can be modeled using a Floor-plan. This gives us a chance to model real-world situations in a better way than done in most information systems available today.

## References

[LiLoKa93] Hanne Linaae, Idunn Weidemann Løvseth, and Yahiko Kambayashi *An Authorization Mechanism Utilizing Functional Dependencies for Distributed Dynamic Security Management* 1993

[TaTaKa92] Hideyuki Takada, Naoki Tanaka, and Yahiko Kambayashi *VIRTUAL OFFICE: Computer Supported Office Work System* IMEL, Faculty of Engineering, Kyoto University, 1992

[TaKa92] Hideyuki Takada and Yahiko Kambayashi *Office Space Description Language for Computer Supported Office Work System* IMEL, Faculty of Engineering, Kyoto University, 1992

[GriWad76] Patricia P. Griffiths and Bradford W. Wade *An Authorization Mechanism for a Relational Database System* ACM Transactions Database Systems 1.3, Sept. 1976, p.p. 242-255

[FeSuWo81] Eduardo B. Fernandez, Rita C. Summers, and Christopher Wood *Database Security and Integrity* Addison-Wesley Publ. Comp. 1981

[Fagin78] Ronald Fagin *On an Authorization Mechanism* ACM Transactions on Database Systems, Vol. 3, No. 3, Sept. 1978, p.p. 310-319

[Kamb80] Yahiko Kambayashi *Generalized Dynamic Authorization Mechanisms* Operating Systems Engineering, p.p. 63-77, Proceedings of the IBM Computer Science Symposium, Amagi, Japan, Oct. 1980