A Model to Partially Outsourcing Access Control for Databases

Amril Syalim† Toshihiro Tabata‡ Kouichi Sakurai††

†Graduate School of Information Science and Electrical Engineering, Kyushu University
6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581, Japan

amril@itslab.csce.kyushu-u.ac.jp

‡Graduate School of Natural Science and Technology, Okayama University
3-1-1 Tsushima-naka, Okayama 700-8530, Japan

tabata@it.okayama-u.ac.jp

††Faculty of Information Science and Electrical Engineering, Kyushu University
6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581, Japan

sakurai@csce.kyushu-u.ac.jp

Abstract There are many situations where users of databases cannot fully trust the administrators of databases where they store their data. In this paper we propose a partially outsourced access control model for such databases. In this model, access control to databases is partially outsourced to third parties. The tasks of the third parties are: partially mediates access control to databases and partially stores and manages policies for controlling access to databases.

1 Introduction

There are many situations where users of databases cannot fully trust the administrators of databases where they store their data. An example is in a database service provider (DSP) model [7]. In a DSP model, users of databases outsource management of their data to a not fully trusted provider in the Internet. Another example is in large collaborated organizations (enterprises or governments) where there is no one trusted authority for managing the shared data of the organizations [2].

In [6] we showed an access control model for conflicting interests between users and administrators in a Database Management System (DBMS) by using separation of duty feature of Role-based Access Control (RBAC) model. In [7], we proposed access control model for database service provider by separating control domain in a Usage Control (UCON) model. In this paper we propose a partially outsourced access control model for conflicting interests between users and administrators of databases or the situations where users of databases cannot fully trust the administrators of databases where they store their data. In this model, access control to databases is partially outsourced to third parties. The tasks of the third parties are: partially mediates access control to databases and partially stores and manages policies for controlling access to databases.

Partially outsourcing paradigm for access controls is discussed in [1]. The authors of [1] believe that with the increasing complexity of security policy, specification and the resulting decrease in usability of security mechanisms, outsourcing paradigm will become next shift in access control.

The idea of our model is by using a multi-policy system [4] to divide the access control authority in databases into domains of the administrators, users and the trusted third parties. Conflict resolutions and data sharing between users, administrators and the third parties are resolved by secure domain interactions using *policy groups* [5].

Organization of this paper: in section 2 we briefly discuss partial outsourcing paradigm for access controls. Section 3 discuses our proposed model to partially outsourcing access control for databases. Section 4 is conclusion.

2 Outsourcing Paradigm for Access Controls

With the increasing complexity of security policy, specification and the resulting decrease in usability of security mechanisms, outsourcing paradigm will become next shift in access control. There are four different classes of outsourcing models for access controls identified in [1]. Partial oursourcing is the fourth model. This section briefly discusses these classes.

2.1 Class α: Single Administration, Internal

In this class no outsourcing takes place and both administration and the protected objects belong to the same domain. Figure 1 shows this scenario.

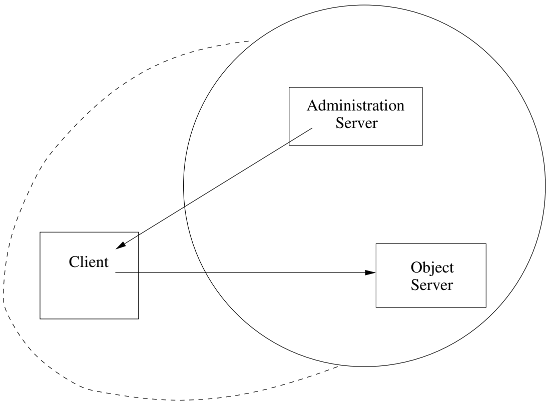

Figure 1: Class α: No Outsourcing, Single Administration

2.2 Class β: Single Administration, External

Figure 2 shows the second class: administration is fully outsourced. Security depends fully on the behaviour of the external administration.

2.3 Class γ: Outsourcing via External Security Server

In this class, as shown in Figure 3, administration is done by the system itself. However, policies require the client to retrieve a credential of the external security server.

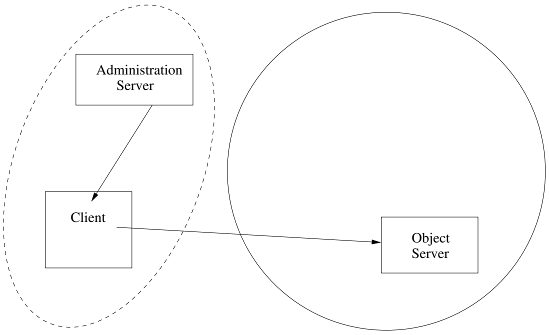

Figure 2: Class β: Fully Administrated by External Administration

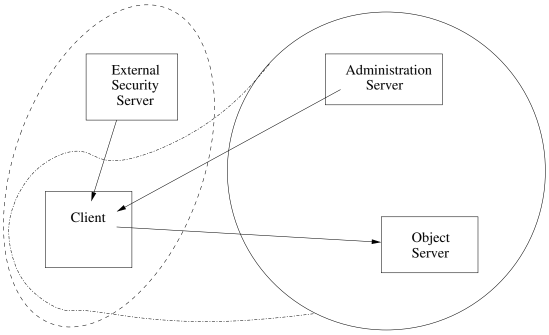

Figure 3: Class γ: Outsourcing Using External Security Server Approach

2.4 Class δ: Partial Outsourcing Using External Rule Servers

Figure 4 shows the final possibility. The external rule server delivers rule implementations to the local administration server. The administration server combines different rule implementations (here, Rule X+Rule Y) to policy objects. The local administration has the full control over which rule implementations are used. Because the external rule implementations are not the only ones included, the external rule server cannot arbitrarily permit access.

3 A Model to Partially Outsourcing Access Control for Databases

In this section, we describe our model to partially outsourcing access control for databases. The idea is by using a multipolicy system [4] to divide the access control authority in databases

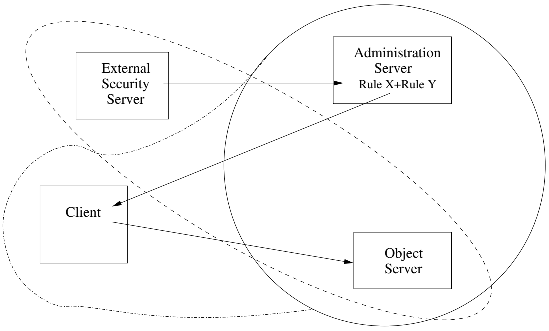

Figure 4: Class δ: Partial Outsourcing Using External Rule Server

into domains which represent the authorities in the system (the administrators, users and the trusted third parties). Conflict resolutions and data sharing between users, administrators and the third parties are resolved by secure domain interactions using *policy groups* [5].

3.1 Basic Model

Multipolicy system is a system that support multitude of independent security domains in which an individual security policy is enforced on the applications [5]. Several components that are required to handle multiple policies [3]:

1. Multiple security policies
2. Multiple security policy enforcers
3. Multiple policy coordinators (metapolicies)
4. Assignments to specify which policies apply to which subjects and objects

Figure 5 shows these components in our model. The circles represent the domains in the system. There are administrators domains, users domains and trusted third parties domains.

3.1.1 Multiple security policies

Security policies are policies in administrators domains, users domains and trusted third parties domains.

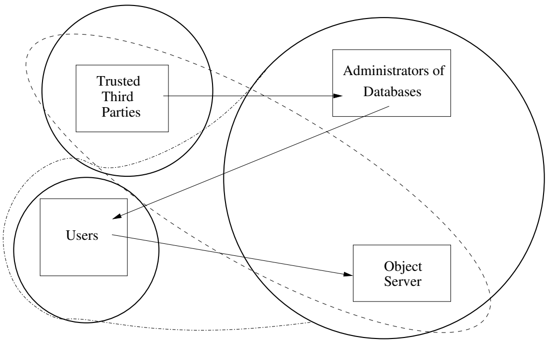

Figure 5: Basic Model

3.1.2 Multiple security policy enforcers

The enforcers are enforcers in administrators domains, users domains and trusted third parties domains.

3.1.3 Multiple policy coordinators (metapolicies)

The coordinators are the trusted third parties.

3.1.4 Assignments to specify which policies apply to which subjects and objects

These assignments are managed by the trusted third parties.

3.2 Conflict Resolutions and Data Sharing

Conflict resolutions and data sharing between users, administrators and the third parties are resolved by secure domain interactions using policy groups [5]. Policy group is a set of regular security policies together with a set of policies that control interdomain actions, and a classification function that for any given interdomain action select the right policy from the sets.

3.2.1 Classification of Interdomain Actions

There are three classes of interdomain actions [5]:

1. **Class 1**: $|\prod_s| = |\prod_o| = 1 \wedge \prod_s = \prod_o$
Action of class one are characterized by

the situation that subject and object are members of the same domain and are not member of any other domain. Actions within this class do not cross domain borders, and consequently, a single policy is both capable and authorized to make the access decision.

2. **Class 2**: $|\prod_s \cap \prod_o| = 0$
   This access class is characterized by the situation that no security policy exists that has both subject and object in its domain. Especially, there is no security policy that is capable of providing a rule for this particular access.

3. **Class 3**: $|\prod_s \cap \prod_o| \geq 1 \wedge \exists e \in \{s, o\} : |\prod_e| > 1$
   This access class is characterized by the situation that on the one hand there is (at least) one policy that might provide a rule for the access; nevertheless, on the other hand (at least) one of the entities is a member of more that one domain

3.2.2 Policy Group Definition

Let I be a finite index set and $\{P_i\}_{i \in I}$ the set of regular security policies of a given multipolicy system. A *policy group* G is a tuple $G = (\{P_i\}_{i \in I}, T, F, c)$, consisting of [5]

- a finite set of regular security policies $\{P_i\}_{i \in I}$, implementing the security requirements for class 1 accesses
- a completeness policy T, implementing the security requirements for class 2 accesses
- a conflict mediation policy F, implementing the security requirements for class 3 accesses
- a classification function c that for each access of subject s to object o: $(s, o), s, o \in \bigcup_{i \in I} Dom_{p_i}$, yields the class of (s, o).

4 Conclusion

In this paper we described a model to partially outsourcing access control for databases. The idea of our model is by using a multipolicy system to divide the access control authority in databases into domains which represent the authorities in the system. We also described conflict resolutions and data sharing using *policy groups.*

5 Acknowledgment

This research was partly supported by Joint Forum for Strategic Software Research (SSR) of International Information Science foundation.

References

[1] Joerg Abendroth and Christian D. Jensen. *Partial Outsourcing: A New Paradigm for Access Control.* SACMAT'03, 2003.

[2] Thomas Hildmann and Jorg Bartholdt. *Managing Trust between collaborating Companies using outsourced Role Based Access Control.* RBAC'99 Fairfax, VA, USA, 1999.

[3] Hilary H. Hosmer. *The Multipolicy Paradigm for Trusted Systems.* Proceedings on the 1992-1993 workshop on New security paradigms.1993.

[4] Winfried E. Kühnhauser. *A Classification of Interdomain Actions.* Operating Systems Review, 32(4):47-61, October 1998.

[5] Winfried E. Kühnhauser. *Policy Groups.* Computers & Security, Volume 18, Issue 4, 1999, Pages 351-363.

[6] Amril Syalim, Toshihiro Tabata and Kouchi Sakurai. *Access Control Model for a Secure Enhanced Database Management System.* Computer Security Symposium (CSS) 2004.

[7] Amril Syalim, Toshihiro Tabata and Kouchi Sakurai. *Usage Control Model and Architecture for Data Confidentiality in Database Service Provider.* Indonesia Cryptology and Information Security Conference (INACISC2005), Jakarta, Indonesia, May 2005.