Enhancing Privacy Protection in Distributed Environments through Identification and Authentication-Based Secure Data-Level Access Control

Nisreen Aldeen, Gerald Quirchmayr

Enhancing Privacy Protection in Distributed Environments through Identification and Authentication-Based Secure Data-Level Access Control

Nisreen Alam Aldeen & Gerald Quirchmayr

University of Vienna
Faculty of Computer Science
Research Group Multimedia Information Systems
Währinger Straße 29, 1090 Wien, Austria
a0948830@unet.univie.ac.at, gerald.quirchmayr@univie.ac.at

Abstract. System-level access control methodologies depending on Perimeter Protection proofed their efficiency in the past, but the appearance of many new significant developments in digital communications highlighted the limitations of this approach. Increased concerns about the compatibility of system-level access control mechanism with new distributed and ubiquitous environments are turning aspirations towards de-perimeterisation protection and data level access control as solutions. This research does therefore try to make a contribution to privacy protection based on already advanced data-level access control work, such as the SPIDER project. The solution developed in this research suggests an X.509 certification extension to fit the data-level access control requirements, and proposes a new design for application structure in order to improve the identification and authentication-based secure data-level access control process.

Keywords: Privacy Protection, De-perimeterisation (De-P), Data-level Access Control, Self-Protecting Data, X.509 certification.

1 Introduction

Perimeter protection represented by system-level access control was the earliest framework to provide and support privacy protection and handle control. Despite the great implementation features of system-level access control there are various limitations helped to raise awareness related to the problems of perimeter protection, and to promote De-perimeterisation (De-p) protection [6]. The main purpose of De-p protection is to attain continuous and modifiable access control to the information shared beyond the system's boundaries [3]. Digital rights management (DRM) with its security processes can be considered as a non- perimeter security model, where the control can be applied to the resource outside the system's boundaries. DRM access control still is static, not modifiable, and a fine-grained classification scheme is missing [1]. The JISC funded SPIDER project (Self-Protecting Information for De-Perimeterised Electronic Relationships) [2] is one of the currently very promising solutions based on

adfa, p. 1, 2011.

the De-p principle. It aims to provide a set of tools including classification scheme, persistent and modifiable access control and enforcement mechanisms for information shared in collaborative distributed work environments. However, there are specific limitations, related to identification and authentication issues, which restrict its efficiency and put a stop to its reliability.

The aim of this paper is to attempt to bridge the gap between the SPIDER project and DRM techniques, using modifiable digital certification construction. More specifically, in this paper we suggest an extended X.509 certificate [10] to be compatible with modifiable and continuous data level access control in distributed environments, in addition to a modified SPIDER application that allows shifting the emphasis from system as controller to user-definable policies. Starting with an overview of existing technologies the paper identifies the most interesting gaps and then explains the own research approach, its expected benefits and limitations, it concludes with a reflection of the current state of the work and outlook to future work.

2 Existing Access Control Technologies

System- level access control is the traditional strategy of existing access control systems. The central theme of this strategy is perimeter protection which means the application of control to information access requests within the system's boundaries using previously assigned access rights. System-level access control provides a sufficient access control and authentication infrastructure for entities. However, it has various limitations [1] such as a lack of information classification schemes, and a Lack of continuous and modifiable control behind the secure network boundaries.
Furthermore, the emergence of many new variables and environments in the context of digital communication (e.g., global corporate, cloud computing, and online business) highlighted the problem of system-level access control, and showed the inability of the perimeter protection to be compatible with the new environments [4]. Growing problems of level access control associated with disappearing boundaries between networks have raised an important question: What is the alternative? And how can we extend the control on our data beyond the system's boundaries?

2.1 De-perimeterisation Protection as a Key

The first description of the De-p protection was in the Jericho forum [5] [7]. It suggests shifting from protecting data from the outside (system and applications) to protecting data from within. Mainly it aims to apply continuous control to data outside the system’s boundaries using data-level access control (i.e., Information-centric security) and including some access control policies into the information itself [3].

2.2 Some Existing Approaches for De-perimeterisation Protection

Many methods have been presented in order to solve the problems of perimeter protection, and they can be viewed as partial solutions towards de-p achievement. Partly

we can look at digital rights management DRM as non- perimeter security model as it provides a continuous control beyond the system's boundaries. However DRM access control is static, not modifiable and doesn't provide a fine grained classification scheme. In 2001 and 2002, two selective access approaches for information sharing in distributed environments via the Web have been presented [8] [9]. These two approaches aim to protect information using XML's Properties to allow the fragmentation of content, and to apply different controls to the same resources. The major drawback of these approaches is the lack of persistent and modifiable access controls. The SPIDER project [1] [2] being led by Cardiff University combines the advantages of previous methods. It provides a practical way to modify the existing models of information classification based on access control requirements, with a live URL link which allows the possibility to enforce and modify the access control policy beyond the system boundaries. The SPIDER Project represents a valuable approach towards solving the Perimeter protection problems, certainly, the problem of non-continuous and non-modifiable control. However, a few aspects of SPIDER are still under development, and there are considerable gaps effect on SPIDER performance and efficacy.

2.3 Building on Existing Work

With the SPIDER project [2] already covering the core functionalities, we can focus on closing the following interesting gaps:

- Trusted computing: With the application of SPIDER, the entire resource is encrypted with the same key for all security levels; then the whole resource in memory is open to attack in case of key disclosure. In addition, a trusted computing module to ensure confidentiality during decryption encryption is required.
- Identity management is still under development, there is a trend to use a digital certificate (not yet defined).

Our previous description of the SPIDER limitations highlights the need for confidentiality, authentication and identity management mechanisms.

3 Towards a Solution Model

Following on from this, a set of requirements based on the drawbacks of the previously mentioned methods will be derived, then used to implement a solution that considers these requirements using a modified application of SPIDER [1], in order to provide a solution that enhances the access control process in widely distributed and expanding collaborative working environments, and to improve the information exchange privacy by providing X.509 extension to allow fine grained access controls.
Taking advantage of the X.509 standard certificate [10] which can be viewed as one of the DRM processes, and taking into account the requirements of data-level access control architecture such as SPIDER project [2], using X.509 certificate to enhance the confidentiality and authentication is not sufficient. Despite the high level of confidentiality achieved by X.509 there are significant drawbacks affecting X.509 adoption in distributed structures:

- The user is not a controller; everything is done by a trusted third party.
- Doesn't provide a classification scheme for access control
- The access control depends on previously assigned rights; thus, it is not modifiable.

On the other hand, SPIDER doesn't provide authorization credentials or authentication mechanisms. In addition, we still have to deal with the crisis of using one key to encrypt the entire resource. Therefore, in order to enhance access control process reusing the De-p structure of the SPIDER, we suggest a new vision as follows:

- Combining the advantages of digital certification and the SPIDER project.
- Mixing a centralized strict hierarchical structure with a stand-alone structure.
- Using various keys to encrypt the resource for different levels of security.
- Suggesting a modified X.509 digital certificate ISAC (Identification and Secure Access Control Certificate) for the purpose of identification, authentication and secure data-level access control.

3.1 Suggested Digital Certificate

The suggested certificate is generated centrally by a trust authority and contains the original structure of the X.509 [10], in addition to a new annex contains compatible fields for secure data-level access control process (as figure.1 shows). At the time of issuing an extended X.509 certificate, the center applies its electronic signature on the main part of the X.509. The special annex should later be signed by the resource's owner if he wishes to grant access privileges without referring to the authority center.

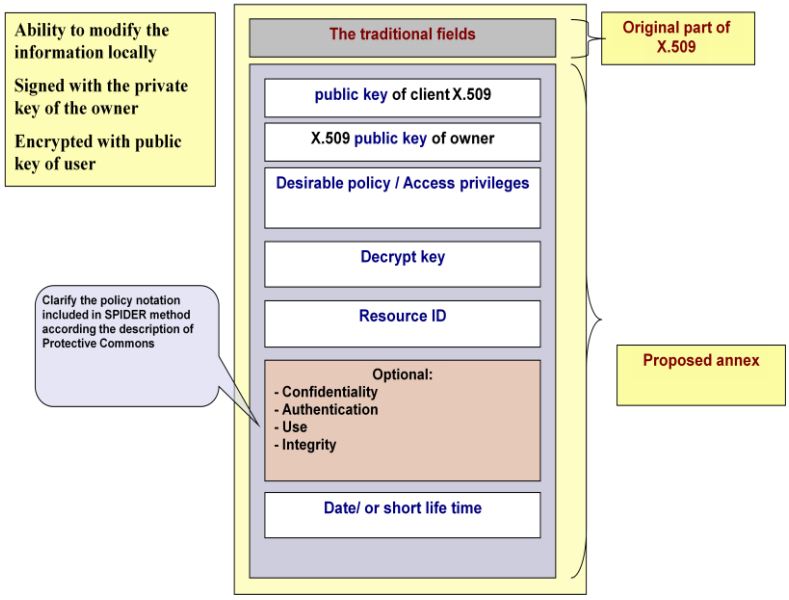

Fig. 1. The essential fields of the suggested annex

3.2 Basic Structure of the Process

The underlying idea for a process is illustrated in figure.2, when the user wishes to access the resource; he will send an access request including his certificate. The owner side will check the identity and connect the database to extract the policies and keys which match this identity; then it will fill the fields of the annex with the required information, sign it with the private key of the owner and encrypt it using the public key of the user before sending it back to the user. The SPIDER application in the user side will verify the access control annex, parse the resources for the classifications labels that match the security label returned for the user and generate a dynamic subset of the original resource in unencrypted form for the user to access.

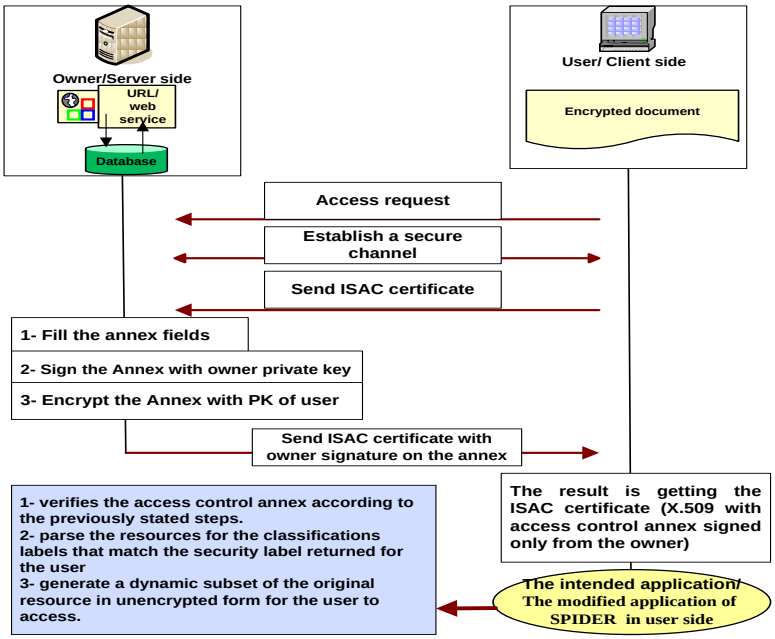

Fig. 2. Basic structure of the process

3.3 Advantages and Limitations of the Suggested Solution

The suggested solution exploits the high level of security in X.509, gaining the advantages of the hierarchical structure in confidentiality and authentication. Including access rights in the extended certificate enables the use of classification methods and partial access rights, these rights are continuous and modifiable by drilling down to the level of data using SPIDER project. The suggested X.509 extension allows this certificate to be used in distributed environments and paves the way for building a standards-based for de-p approach in the future. Furthermore, the use of different keys for encrypting the resource protects the encrypted resource existing in memory in case of key disclosure. The suggested solution has some well-known limitations, including limiting data-level access control operations to X.509 holders, and using various keys

to encrypt the resource, which takes us back to the key management problem, for which we should measure the efficiency of our suggestion in reality.

4 Conclusions and Future Work

The inability of perimeter protection and system-level access control mechanism to match new significant developments in digital communications made it a must to come up with a new flexible and secure access control method. In this paper we have provided a brief description of the SPIDER project as the currently most advanced and practical method based on De-perimeterisation protection and data-level access control. We have investigated the X.509 standard certification and highlighted its disadvantages focusing on the difficulties of applying this standard to distributed environments to be completed in our current research. Later in the paper we have introduced our suggestion aiming at two improvements:

- Strengthening the authentication and identification mechanism of SPIDER project
- Making the X.509 standard certificate applicable and more efficient in a distributed environment by adding a data-level access control annex.

A deeper security analysis of this extended certificate is planned and experiments will be conducted to test the viability of this approach in realistic settings.

5 References

1. Pete Burnap and Jeremy Hilton, Self Protecting Data for De-perimeterised Information Sharing, Cardiff School of Computer Science, Cardiff University, Third International Conference on Digital Society, 2009
2. Pete Burnap, Jeremy Hilton, Anas Tawileh, Self-Protecting Information for De-perimeterised Electronic Relationships (SPIDER), Final Report, 30th July 2009
3. Andre van Clee, Roel Wieringa _, De-perimeterisation as a cycle: tearing down and rebuilding security perimeters, December 5, 2008.
4. Tomas Olovsson, CTO, The Road to Jericho and the myth of Fortress Applications, AppGate Network Security, appgate, 2007
5. Tomas Olovsson, Surviving in a hostile world, The myth of fortress applications, CTO, Appgate, Jericho Forum, Professor at Goteborg University, 2007
6. Graham Palmer, De-Perimeterisation: Benefits and limitations, Network and Security, Siebel Systems Ltd., Siebel Centre, The Glanty, Egham, Surrey TW20 9DW, United Kingdom, 2005
7. Paul Simmonds, Architectures for a Jericho Environment, Global Information Security Director, ICI Information Security, 2004
8. Ernesto Damiana, Sabrina De Cabitani Di Vimercati, Stefano Paraboschi and Pierangela Samarati, A Fine-Grained Access Control System for XML Documents, ACM Transactions on Information and System Security, Vol. 5, No.2, May 2002, Pages 169–202.
9. Elisa Bertino, Silvana Castano, On Specifying Security Policies for Web Documents with an XML-based Language, 2001.
10. ITU-T Recommendation X.509, ISO/IEC 9594-8, Information Technology – Open Systems Interconnection- The Directory: Authentication Framework, 1997 Edition.