available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Enable delegation for RBAC with Secure Authorization Certificate

GuangXu Zhou[a], *Murat Demirer*[a,c], *Coskun Bayrak*[a,*], *Licheng Wang*[b]

[a] *University of Arkansas at Little Rock, 2801 S. University Ave, Little Rock, AR 72204, USA*
[b] *Beijing University of Posts and Telecommunications, 10 Xitucheng Rd Beijing, PR China*
[c] *Istanbul Kultur University, Istanbul, Turkey*

ARTICLE INFO

Article history:
Received 6 October 2010
Received in revised form
12 May 2011
Accepted 17 June 2011

Keywords:
Access Control
Computer Network Security
Random Number Generator
Secure Authorization
Secure Delegation
Quasirandom Structures
k-Uniform Hypergraph

ABSTRACT

Our motivation in this paper is to explore a Secure Delegation Scheme that could keep access control information hidden through network transmission. This approach introduces the quasirandom structure, 3-Uniform Hypergraph, as the representation structure for authorization information. It generates a Secure Authorization Certificate (SAC) in place of an Attribute Certificate (AC) to enable both Role-based Access Control (RBAC) and a delegation process for hiding authorization information. We have two contributions in this regard: (1) a value-based delegation scheme and (2) a pattern-based RBAC. A Secure Delegation Scheme is based on the hashing values generated with the quasirandom structure. With this scheme, the delegation process will greatly reduce the risk of sensitive authorization information leakage for applications. In the case of pattern-based access, we introduce a new hash function using quasirandom structure to make a fingerprint[1] for RBAC. The quasirandom structure derived from k-Uniform Hypergraph has measurable uniformity, which is an advantage over traditional hash functions. Another advantage is that it does not need to access the entire message context to generate the fingerprint which is essential for traditional hash functions such as MD5, SHA-1, etc.

1. Introduction

Delegation service is a common requirement in Role-Based Access Control (RBAC) (Ferraiolo et al., 2001) systems. With the delegation process, there are no well-accepted models addressed in the literature. The concept of delegation in access control is not clearly defined and the basic principles for delegation are not well-identified yet. The confinement problem, for example, cannot be demonstrated as being resolved in current delegation applications. Particularly for RBAC model, delegation is demanding more while the Public Key Certificate (PKC)-based delegation process has several defects: first, inordinate use of the private key increases the risk of compromise; second, the approach usually combines the authentication and authorization tightly, and the extensions embedded into the certificate overloads the semantics of the authentication certificate; third, the lifetime difference between the authentication and authorization attributes may increase the cost and complexity of managing the underlying Public Key Infrastructure (PKI) (Benantar, 2006); fourth, the cross-domain problems with RBAC could not be easily resolved.

In this paper, we present a Secure Delegation Scheme that could enhance the security of the transmission with Role-based Access Control information through network. First, with respect to the original work on quasirandomness with 3-Uniform Hypergraphs appeared in (Gowers, 2006a), we

[*] *Corresponding author*. Tel.: +1 501 569 8137; fax: +1 501 569 8144.
[1] The term fingerprint is used to refer to a unique pattern.

0167-4048/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2011.06.005

introduced the quasirandom structure, 3-Uniform Hypergraph, as the representation structure for RBAC information. Based on this structure, we defined a hash function which generates a quasirandom sequence as the fingerprint of RBAC information. Each element of the quasirandom sequence is called Secure Authorization Token (SAT). With a set of SATs, a Secure Authorization Certificate can be compiled as the authorization certificate in place of Attribute Certificate to facilitate delegation process for RBAC with hiding authorization information.

The rest of this paper is organized as follows: Section 2 discusses the related work; Section 3 reviews the authorization scheme and presents the argument in Secure Authorization Scheme; in Section 4 the definition of Secure Delegation Scheme is introduced; Section 5 describes the system design and architecture of the secure delegation prototype introduced; Section 6 presents the use of quasirandom approach to generate the fingerprint for RBAC; Section 7 contains an intellectual discussion of the model; Section 8 provides a conclusion of the study; and finally Section 9 presents the relevant future work to be considered.

2. Related work

Most of the current authorization mechanisms do not hide the access control information in transmission. For example, in PMI (Iso, 2005) infrastructure, the Attribute Certificate (Farrell and Housley, 2002) is transferred through the network, including authorization information of users such as roles, permissions, etc. With the revelation of such information, it is possible for the adversary to recover the authorization map of an organization, which is risky in many cases (i.e., in the military field or in commercial competition). Recently, people have been aware of this defect on information leakage (Holt et al., 2003; Li and Tripunitara, 2006; Seitz et al., 2005). Li et al. developed a system that enables the hiding of policy information for access control (Li and Li, 2005); Calvert et al. introduced a model to enforce information-hiding policies for network management (Calvert and Griffioen, 2006); Frikken et al. presented how to protect both sensitive credentials and sensitive policies by the set of protocols they designed (Frikken et al., 2006).

Especially for the delegation process and regardless of the delegation type (Role-based (Wang and Osborn, 2006; Zhang et al., 2003, 2002; Joshi and Bertino, 2006; Na and Cheon, 2000) or Attribute-based delegation (Frikken et al., 2006; Zhou and Meinel, 2004; Kakizaki and Tsuji, 2007; Xie et al., 2004; Chadwick et al., 2003)), the problem of information authorization may be revealed by the delegated certificates when transferring through network. Therefore, all of these delegation solutions should focus on the properties of unforgability or undeniability issues.

Our work is related to trust negotiation with hidden credentials and hidden policies as well as role-based delegation. Most of the early research with trust negotiation focuses on protecting resources and credentials (Winsborough et al., 2000; Winsborough and Li, 2002, 2004; Winslett et al., 2002). Later on, some research work considered policies as sensitive information (Bonatti and Samarati, 2000; Yu et al., 2003; Yu and Winslett, 2003). Li (Li and Li, 2005; Li et al., 2005), Frikken (Frikken et al., 2006, 2004), and Brickell (Brickell and Li, 2007) contributed accumulated work on the hidden credentials and hidden policies to incorporate them into trust negotiation and trust management systems.

Concerning the delegation process, MyProxy (Novotny et al., 2001) is the most popular Credential Repository which serves as user credential management and delegation proxy server for grid environments. Other delegation models include role-based delegation (Wang and Osborn, 2006; Zhang et al., 2003, 2002; Joshi and Bertino, 2006; Na and Cheon, 2000) and attribute-based, or X.509-based delegation (Zhou and Meinel, 2004; Kakizaki and Tsuji, 2007; Xie et al., 2004; Chadwick et al., 2003). However, all of these delegation models do not use hidden credentials or hidden policies because they accept the assumption that authorization information or policies are not sensitive. Later, in Li and Tripunitara (2006), the use of security analysis techniques to maintain desirable security properties while delegating administrative privileges was introduced; and a precise definition of a family of security analysis problems in RBAC (which is more general than safety analysis that is studied in the literature) was given.

Our goal in this work is to present a theoretical framework of a prototype implementation for encoding RBAC authorization information into a X.509 certificate to facilitate secure delegation process.

3. Secure Authorization Scheme

Before giving the definition of Secure Delegation Scheme, it is necessary to clarify the definition of Secure Authorization Scheme (SAS). Our perception of SAS is nothing more than a authentication feature which performs the access control as described in Example 1.

Example 1. Bob wants to operate on a PC in the lab. So, he inquires the administrator to grant the permission for him. The administrator distributes a token to Bob. With this token, Bob can open the PC and operate on it. Neither Bob nor the PC can understand what the token means. Here Bob's concern is that he can do what he wants to do on the PC. Similarly, the PC's concern is that Bob's operation is granted by the administrator. The administrator is responsible for the validity of Bob's operation and handles the process it works.

RBAC is the model to handle authorization for the User through the permission with respect to Role. User, Role, Object, and Permission are essential components for RBAC. Here, Bob is the user, and PC is the Object.

AA (Authorization Authority) is the subsystem to grant, revoke, modify, and retrieve authorization clearance. Here, the administrator is the Authorization Authority (AA). Based on the structure illustrated in Fig. 1, the following four cases should be considered, in order to define a secure authorization model:

- **Case 1:** User, Object, and AA hold the authorization information,
- **Case 2:** User and AA hold the authorization information,
- **Case 3:** Object and AA hold the authorization information,
- **Case 4:** Only AA holds the authorization information, where Object is the resource that the User wants to access.