Integrated Security Services for Dynamic Coalitions

Himanshu Khurana[1], Serban Gavrila[1], Rakeshbabu Bobba, Radostina Koleva,
Anuja Sonalker, Emilian Dinu, Virgil Gligor, and John Baras
Electrical and Computer Engineering Department, University of Maryland, College Park, MD
[1]Institute for Systems Research, University of Maryland, College Park, MD
hkhurana@umd.edu, sgavrila@starpower.net, {bobba, radost}@eng.umd.edu
{aasonalk, edinu, gligor, baras}@eng.umd.edu

Abstract

Coalitions are collaborative networks of autonomous domains where resource sharing is achieved by the distribution of access permissions to coalition members based on negotiated resource-sharing agreements. The focus of our research is on dynamic coalitions, namely, coalitions where member domains may leave or new domains may join during the life of the coalition. We have developed a set of tools that integrate security services for dynamic coalitions, namely, services for (1) private and shared resource management, (2) identity and attribute certificate management, (3) secure group communication, and (4) joint administration for enforcing joint-action policies on shared critical resources. In this extended abstract we give an overview of the architecture and implementation of our tools.

1. Introduction

In various collaborative environments such as alliances for research and development, health care, airline route management, public emergency response, and military joint task forces, autonomous domains form coalitions to achieve common objectives by sharing resources (e.g., objects and applications). These coalitions can be dynamic in that member domains may leave or new domains may join after coalition establishment. Resource sharing is achieved by the distribution of permissions for coalition resources to coalition members based on negotiated resource-sharing agreements, or *common access states*, which ensure that all domains can have a common view of coalition operations, can execute shared applications, and access shared objects. Shared resources are either privately administered by individual domains or jointly administered by multiple domains. Jointly administered resources are typically critical to coalition objectives and remain with the coalition even after the departure of member domains. Access to jointly administered resources is one of the benefits individual domains derive from their membership in the coalition.

As an example of a dynamic coalition, consider a genetics research firm that discovers a gene sequence associated with a disease and establishes a coalition with a pharmaceutical company, two research hospitals and a Food and Drug Administration review board (FDA board) to find a cure using the gene sequence. Each domain shares some of its local resources with the coalition partners to achieve the coalition objective; e.g. the genetics firm contributes its gene sequence database, the pharmaceutical company provides a drug composition tool, the hospitals support clinical trials and give access to their patient databases (while preserving patient privacy by withholding sensitive patient information such as name, social security number, etc.), and the FDA review board shares a database of safety regulations. Given the impact of finding a cure, the coalition decides to jointly administer an application for remote consultation and drug analysis. This remote consultation and drug analysis application relies on a jointly administered secure group communication service. As coalition operations proceed, one of the member hospitals leaves the coalition while another joins the coalition. Other examples of dynamic coalitions can be found in Gligor *et al*. [3] and Khurana *et al*. [4].

We have developed a set of tools that provide integrated security services for dynamic coalitions, namely, services for resource management, certificate management, secure group communication, and joint access policy administration. These tools have been implemented in the Windows 2000 Server environment using Java. Extensions to RCC (Role Control Center), a RBAC (Role Based Access Control) tool developed at VDG Inc., along with Windows IIS web servers provides services for resource management. Windows 2000

Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03)
0-7695-1897-4/03 $17.00 © 2003 IEEE

Certificate Services provide identity certificate management. OpenSSL CA utility provides attribute certificate management. A group key management tool and a Windows IIS web-based group communication server integrated with SPREAD [8] provide secure group communication services. A threshold CA using shared public-key cryptosystems [2, 5] integrated with RCC provides joint administration services. These integrated security services enable management of coalition resources with easy-to-use graphical interfaces and support coalition dynamics efficiently.

Section 2 gives an overview of the architecture and Section 3 provides some implementation details. Section 4 briefly discusses coalition dynamics and Section 5 summarizes our work.

2. Architecture Overview

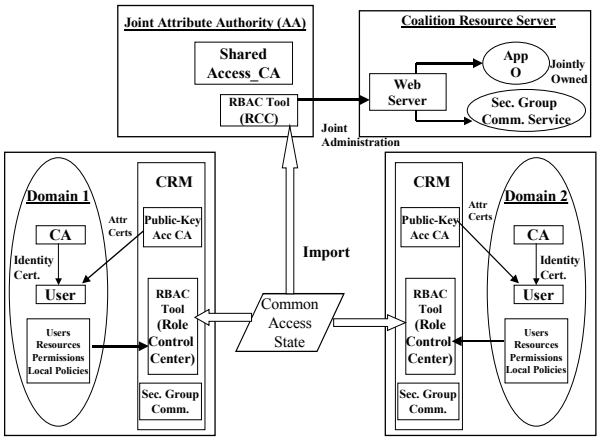

Figure 1: Architecture for Administration of Integrated Security Services

In Figure 1 above, we outline the architecture for administration of integrated security services in dynamic coalitions comprising of two domains – a scenario that can easily be extended to *n* domains. We assume that each autonomous domain has its own Identity Certificate Authority (CA) that distributes identity certificates to users registered in that domain, and a database of users, resources (objects, applications), permissions, and local access policies. Each domain installs one Coalition Resource Management (CRM) toolkit that consists of a public-key Access CA, Role Control Center (RCC – a RBAC Tool), and a Secure Group Communication (SGC) service. The public-key Access CA distributes attribute certificates to both local and foreign domain users authorizing access to local domain resources. RCC administers the access policies of local domain resources via the container of users, resources, permissions, and local policies. The SGC service initially allows domains to communicate and commit a common access state (after it has been negotiated) and then allows domain users to join groups for secure group communication.

Member domains establish a Joint Attribute Authority (AA) that consists of a RCC module and a shared Access CA, that is, a CA whose private key is shared among the member domains. Coalition domains also establish a coalition web server that manages jointly administered applications such as App O and a Secure Group Communication service.

In order to establish a coalition, Domain 1 and Domain 2 install the CRM toolkit and setup the joint AA and the coalition web server. They then create a shared public-key using the algorithm of Malkin *et al*. [5] as illustrated in Khurana *et al*. [4]. The domains then specify a common access state (by using tools and techniques [1] that are currently being developed by our research group) and sign it using their private key shares. The common access state, representing the sharing agreement of the member domains for access to privately and jointly administered coalition resources, is imported by the RCC tools in all domains and at the joint AA. The RCC at the joint AA then instantiates the jointly administered resources along with their access policies at the web server as specified in the common access state and authorizes the shared Access CA to distribute attribute certificates to coalition users for access to these jointly administered resources. These attribute certificates are jointly signed by all coalition domains using their private key shares. The RCCs at the domains authorize their local domain Access CAs to distribute attribute certificates to foreign users for access to local domain resources as specified in the common access state. Coalition users can then access jointly administered resources at the coalition web server or privately administered resources at domain web servers using their attribute certificates. Furthermore, RCC administrators can modify the access policies of resources they administer after commitment of the common access state; e.g., add or remove users from roles.

3. Implementation

RCC is implemented in Java and is integrated with Active Directory of Windows 2000 server. It uses the database of the active directory to manage local roles and resources, and both local and foreign domains users. The tool has a well-developed graphical interface, which allows administrators to manage coalition resources with an intuitive feel.

Web servers implemented on windows IIS using ASP host the shared resources in each domain and at the Joint Attribute Authority. The access policies of the shared resources, however, are administered by RCC based on the *common access state* specification.

Windows 2000 certificate services are used to set up an Identity CA in each domain. Identity CAs issue identity certificates to the users registered in their respective domains. The OpenSSL CA utility is used to set up an Attribute CA at each domain. The Attribute CA policy module is modified to issue attribute certificates to only those local and foreign domain users authorized by RCC (via the common access state).

A threshold CA using a shared public-key cryptosystem [5] implemented in Java [2] is modified and integrated with RCC to function as a shared Access CA. It consists of signature servers residing in member domains each of which has a share of the private-key. A CA server at the Joint Attribute Authority composes certificates and CRLs at the request of RCC (at the Joint Attribute Authority) and sends them to the signature servers for a signature. It then composes the partial signatures obtained from each signature server to obtain a valid signature. The signature servers and the CA server communicate via RMI over SSL.

The secure group communication service is developed using key-management techniques of [11] and SPREAD for reliable multicast. It consists of group communication server and client modules. The group communication server is used for authenticating group members, defining group membership and assisting group key generation as required by the scheme. Users authenticate members via a web interface, implemented on windows IIS (ASP), using their identity certificates. Group managers, who are authorized jointly by the member domains, define communication groups via the same web interface. The client modules interact with each other and the group communication server to generate group keys. We have implemented a "chat" application to illustrate secure group communication.

4. Supporting Coalition Dynamics

The important characteristic of dynamic coalition is that member domains may leave or new ones may join during the life of the coalition. When a domain leaves the coalition it withdraws its private resources. However, it must not be able to withdraw jointly administered resources as per prior agreement. The remaining member domains exclude the departing domain from joint administration and revoke the accesses of its users. When a new domain joins the coalition, it shares some of its private resources with the existing coalition members and joins them in administration of shared resources. Our infrastructure supports these dynamic events efficiently. A full-length paper describing the techniques employed will be available in the near future.

5. Summary

We have described a set of tools that provide integrated security services for dynamic coalitions. We are currently developing tools for common access state negotiation. We will integrate our security services with negotiation tools to enable domains to set up, manage, sustain joins and leaves, and break down the coalition in a seamless manner with ease and efficiency.

Acknowledgements

This work is supported by the Defense Advanced Research Projects Agency and managed by the U.S. Air Force Research Laboratory under contract F30602-00-2-0510. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Defense Advanced Research Projects Agency, U.S. Air Force Research Laboratory, or the United States Government.

References

1. V. Bharadwaj and J.S. Baras, "A Framework for Automated Negotiation of Access Control Policies", To appear in proceedings of the third DARPA Information Survivability Conference and Exposition, Washington D.C., April 2003.
2. G. T. Byrd, F. Gong, C. Sargor T. J. Smith, "Yalta: A Collaborative Space for Secure Dynamic Coalitions", IEEE 2nd SMC Information Assurance Workshop, West Point, New York, 2001.
3. V.D.Gligor, H. Khurana, R. Koleva, V. Bharadwaj, and J. Baras, "On the Negotiation of Access Control Policies", Proceedings of the 9th Security Protocols Workshop, LNCS vol. 2467, Springer-Verlag, pp 188-201, April 2001.
4. H. Khurana, V.D. Gligor and J.Linn, "Reasoning about Joint Administration of Coalition Resources", Proceedings of the International Conference on Distributed Computing Systems, Vienna, Austria, July 2002.
5. M. Malkin, T. Wu and D. Boneh, "Experimenting with Shared Generation of RSA keys", Proceedings of the Internet Society's Symposium on Network and Distributed System Security, Feb. 1999, pp. 43—56.
6. C. Phillips, T.C. Ting, S. Demurjian, "Information Sharing in Dynamic Coalitions", Proc. of 7th ACM Symposium on Access Control Models and Technologies (SACMAT 2002), Monterey, CA, June 2002.
7. R. Poovendran, "Key Management for Secure Multicast Communications", Ph.D. Dissertation, University of Maryland, College Park, MD, 1999.
8. SPREAD, http://www.spread.org, Johns Hopkins University.