Proceedings of Ad Hoc Networks and Wireless (ADHOC-NOW), Toronto, September 2002.

Enabling Secure Ad hoc Communications in the Enterprise*

A. GHAVAM
University of Ottawa, Canada

R. LISCANO
Mitel Networks, Canada

M. BARBEAU
Carleton University, Canada

T.A. GRAY
Mitel Networks, Canada

N.D. GEORGANAS
University of Ottawa, Canada

Abstract

Ad hoc communication applications, such as computer-facilitated collaboration, have become possible with the rapid advancements in portable computing and ad hoc wireless networking. Ad hoc communication solutions require a balance between private communications and access to corporate networked services in order to succeed. In this paper, we discuss and offer some approaches in integrating ad hoc communications into an enterprise framework through the use of secure group services and presence. We believe that the projection of presence and availability are crucial in facilitating spontaneous and ad hoc communication sessions, but argue that the challenges lie in the proper manipulation of user and enterprise policies to allow these sessions to occur in a manner acceptable to the enterprise. We present concepts that focus on the use of presence and group-based policies which we call Presence Associations, that we hope will encourage communications and collaboration among users as well as protect their privacy.

Keywords

Secure Ad hoc Collaboration, Secure Group Management, Pervasive Collaborative Environments, Presence, Policy-based Management.

*This work has been supported in part by Communications and Information Technology Ontario (CITO) and Mitel Networks

1 Introduction

With the advent of wireless networking technologies, it has become easier to establish ad hoc connections to existing networks and therefore network resources. At the same time network administrators must tighten security around these networks due to their accessibility outside of the physical boundaries of an organization. The result is that this ease of connection only exists either in public locations or places where network security is not enforced. It is therefore crucial to develop mechanisms that support the creation of secure ad hoc communications among members of a group or between people and available resources in a network inside an enterprise. In this paper, we present a framework that integrates secure group communication by developing a group management entity that we define as Association Manager.

2 Related Work

Our framework incorporates the following technologies:

- A Presence service based on SIP [1] as the basic infrastructure to connect users to members of the association and to resources that the association manages. This service allows users to observe each other's availability.
- Common Open Policy Service (COPS)[2] as the protocol for initializing or updating the secure services with the policies and security associations (SA).
- Session Initiation Protocol (SIP) [3] to initialize and manage the services in a unified way.
- Transport Layer Security (TLS) [4] as security protocol for bi-directional authentication, and data confidentiality and integrity.

3 The Role of Presence Associations

A presence association is an entity that manages presence and resource access for a group of people who share a similar context. The behaviour among the members of the association is based on a set of common policies. Although the association can contain policies that restrict communication among members, we primarily would like to keep an open communication policy among association members and resources. One of the first types of associations we envisioned is location-based associations, for example room associations. A room association is a persistent object with the resources of the room already registered with it. This is not an unreasonable assumption, since many resources in meeting rooms

are generally stationary. Mobile resources most often belong to users and need to be dynamically registered with the association. Location associations will most likely be the primary association that users will indirectly interact with. They behave as a first entry point for users to a corporate network. All users in a particular location will be subjected to a particular set of policies for network and resource access.

4 The Framework

The basic components of our framework are shown in Figure 1 and consist of an Association Manager, Presence Associations, a Presence Service, Secure Services, Association Clients and Presence Clients.

The *Association Manager* is the entity that creates and manages the associations.

Each *Association* manages 3 different types of policies. These are membership, presence, and service access policies. The membership policies which will accept or reject a registration request to the association. An example of a membership policy might be that the creator must confirm each new member. The second set of policies, the presence policies controls the projection of availability among members and services of an association. The third set of policies, the resource access policies control the access to those services shared among the members. Since other users on the network can physically access networked resources, it is necessary to prevent access to these resources when in use by members of the association. We use the COPS protocol for this functionality.

The *Presence Service* projects the properties of associations like the availability of their members and services. The projection is done according to a set of notification policies that determine for example which members and under what context the member sees the availability of other members.The presence service uses the SIP SIMPLE protocol [5] for communication with the presence clients.

The *Secure Services* can be any form services that support access control policies and secure communication

The *Association Client* serves as an interface to the Association Manager.

The *Presence Client* serves as an interface to the Presence Service.

For both the Association and Presence Clients, TLS is used to provide secure communications.

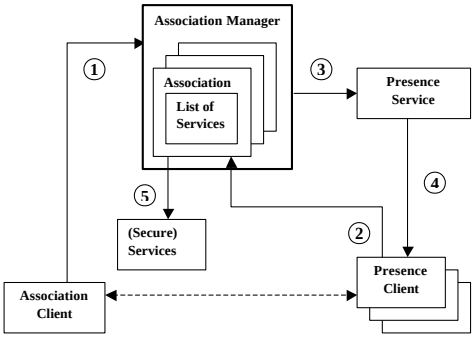

Figure 1 - Association access model

5 Example Scenario: Creating an Association

The numbered lines represent the scenario of creating an association by a user. Line 1 in Figure 1 shows that a user creates an association using the Association Client. The dashed line between the Association Manager and User Client signifies that the creator of the association may also be a member of the association. When a user registers to the association, Line 2 in Figure 1, it provides its identity and a list of services that it supports. For this procedure we can leverage the SIP Registration method [3] that allows SIP User Agents to register their address as well as a list of contact services like Instant Messaging (IM), voice, and video. An association maintains a list of services that belong to resources available to its members. These services along with any other communication services that users bring into the association are projected among members of the association using a presence service, Lines 3 and 4 in Figure 1. Each Association configures its services with access policies and appropriate security parameters (Line 5).

6 Implementation

Even though we are in the early design and implementation stages, there has been much work in group-based presence that forms the basis for association-based presence. We have already developed a Presence service that supports the creation of private groups, and are in the process of extending the role of private groups to support associations. A private group is a group in which membership is reciprocal. All members in such a group will be managed with the same set of policies. This will form the basis of the Association Manager. At this time, we are developing a SIP-based secure session layer above the available group services in our system. This offers a uniform way to manage authentication and the dynamic a hoc nature of users joining and leaving sessions.

7 Conclusion

We presented our system as a framework for secure ad hoc communications. We introduced the concept of association that supports and enables pervasive collaborations by providing seamless setup and maintenance of connectivity among a selected group of people. Our model introduces one point of entry with known set of behaviors exemplified by the associations. In general, there is a need for balance between security and ease of use. To support pervasive collaborations, this has to be all done with minimal user interactions. In our system, we showed that the associations manage user authentication and projection of contact information so that from a user's perspective they simply have to register once. The future work on our system includes in first place the completion and refinement of the system model. Implementing incomplete or missing components especially for policy and security management inside the association would be the main focus of our work.. Another milestone would be incorporating different types of secure group-based services in our system, like chat, audio and video. This requires incorporating new prototype services or extending the existing ones in our system.

References

[1] M. Day, J. Rosenberg, and H. Sugano, H. A Model for Presence and Instant Messaging. *IETF RFC 2778*, February 2000.

[2] D. Durham et al. The COPS (Common Open Policy Service) Protocol. *IETF RFC 2748*, January 2000.

[3] J. Rosenberg et al. SIP: Session Initiation Protocol. *IETF RFC 2543 Draft #9*, February 2002.

[4] T. Dierks et al. The TLS Protocol Version 1.0. *IETF RFC2246*, January 1999.

[5] http://www.ietf.org/html.charters/simple-charter.html *IETF, SIMPLE Working Group*, 2002 2002.

Amir Ghavam and Nicolas Georganas are with the DISCOVER Lab, School of Information Technology and Engineering, University of Ottawa, Ottawa, ON, Canada, K1N 6N5. E-mails: amir@discover.uottawa.ca and georgana@discover.uottawa.ca

Ramiro Liscano and Tom Gray are with the StraTech group, Mitel Networks, Kanata, ON, Canada, K2K 2W7. E-mails: Ramiro_Liscano@mitel.com and Tom_Gray@mitel.com

Michel Barbeau is with the School of Computing Science, Carleton University, Ottawa, ON, Canada K1S 5B6. E-mail: barbeau@scs.carleton.ca