Secure Presence-based Services

A. Ghavam[1], R. Liscano[2], M. Barbeau[3], T. Gray[2], N. D. Georganas[1]

Amir@discover.uottawa.ca, Ramiro_Liscano@mitel.com, Barbeau@scs.carleton.ca, Tom_Gray@mitel.com, Georgana@discover.uottawa.ca

[1] School of Information Technology and Eng., University of Ottawa, Ottawa, ON, CANADA, K1N 6N5
[2] Strategic Technology, Mitel Networks, Kanata, ON, CANADA, K2K 2W7
[3] School of Computer Science, Carleton University, Ottawa, ON, CANADA, K1S 5B6

ABSTRACT

Ad hoc communication applications like 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 *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

INTRODUCTION

The Modern communication features have been transformed radically in the past 15 years with the advent of affordable wireless communications and the adoption of the Internet as a communication network.

The driving factor in investigating presence as a mechanism to facilitate ad hoc communications is bolstered by the results of the pioneering series of studies by Thomas J. Allen. These results were reported in his book *Managing the Flow of Technology* [1] on the factors that predict the success of research projects and the promotion of innovation within an organization. Allen found that informal communication was the prime means by which useful information flowed both into and within an organization. Whittaker et al. [2] also stressed the importance of opportunistic informal communication within an organization as a means to provide for effective collaboration. Hillier in his book *Space is the machine* [3], demonstrates in his studies of Lab X and Lab Y, that informal interactive activity is encouraged by the ability to view each other's activities by happenstance. He remarks that this explains the cultural difference between Lab X and Lab Y. Lab Y with better visibility has a more entrepreneurial and initiating culture. Lab Y is recognized as being more innovative and successful. Penn, a colleague of Hillier, has extended this work. In his paper [4], Penn demonstrates that useful contacts generated by this form of visibility can be greatly facilitated by office layout. Greater visibility within and between offices encourages informal interaction and more creativity.

We also note that workers in distributed groups miss out on these face-to-face interactions since they rely on mediated communications with limited projection of a person's mannerisms. With the infiltration of Instant Messaging (IM) into the workforce and household there has been a renewed interest in investigating how that technology increases user co-presence across physical distances. A recent paper by Nardi et al. [5] studied the use of IM in communities and reported on the fact that people have experienced a strong sense of being aware of the presence of others and that this resulted in the creation of effective communication zones. This evidence points towards the importance of projecting user presence among persons that come together in an ad hoc fashion.

In a similar manner effective access to services and resources is facilitated by their projection using presence. With the advent of wireless networking technology like the IEEE 802.11 WLAN specification, 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 physically 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. The truth is that many corporations restrict access to the corporate networks and make it difficult to facilitate ad hoc network connections. It is therefore crucial to develop mechanisms that support the creation of secure and private

communications among members of a[1] group or between people and resources available to be used through the network. This in our view is a major impediment to the adoption of ad hoc communications in or across enterprises.

In this paper, we present a framework that integrates secure group communication and presence by developing a group management entity that we define as *Association Management Service*. These association services manage access to corporate resources, support data confidentiality, and project availability among a community of members. This type of service is crucial in an enterprise so that nomadic employees feel comfortable in communicating using a corporate infrastructure as well as the enterprise is comfortable that the security of their resources has not been compromised.

Related Work

The goal of the presented framework in this paper is to enable and manage the automatic and pervasive access to a set of secure communication services among the users. To do this, our design incorporates the following technologies:

- A presence service as the basis infrastructure to connect users to members of the association and to resources that the association manages.

- Common Open Policy Service (COPS) as the protocol for initializing or updating the secure services with the policies and security associations (SA).

- Session Initiation Protocol (SIP) to initialize and manage the services in a unified way

- Transport Layer Security (TLS) as security protocol for bi-directional authentication, and data confidentiality and integrity.

In this section we address these technologies

Presence

A presence service allows users of the service to "Subscribe" to another person's availability. Users that view another person's availability are called "Watchers". The user that projects their availability is called a "Presentity". This is in conformance with the definitions used the IETF RFC 2778 on the Common Profile for Instant Messaging [6]. A Presence service should offer two types of information:

- *Projection Of Availability*. This is the traditional user's availability information. It is an indication of the person's desire or willingness for immediate communication. The availability information is projected to other users. If people are willing to communicate they will appear available, otherwise they appear unavailable.

- *Communication Contact Information*. This second type of information reflects how the person is available for immediate communication. The contact information describes different media that the person is currently available on – the devices, software applications, etc. Examples of such would be – a telephone, an Instant Messaging via a certain provider, chat, video conferencing application etc.

Availability can also be extended to resource services like room projectors and printers. In this work we are extending presence to support secure group associations and secure conference services.

COPS

COPS is a client/server protocol for distributing policy information from a centralized Policy Decision Point (PDP) to a set of Policy Enforcement Points (PEP). COPS has been originally proposed to IETF by the Resource Allocation Protocol (RAP) Working Group [7] for controlling the allocation of network resources. It was originally designed to work over TCP. However using COPS for distributing security policies requires additional security measures. For such applications like in our case, using of COPS over TLS has been proposed [8].

SIP

SIP is a language and protocol for initiating, modifying and terminating interactive sessions. It supports discovery of entities so that descriptions of sessions can be delivered. It is explicitly designed for distributed systems and it is ideal for managing multiple communications sessions. Of particular interest to our work is the capability of SIP to support user agent authentication when negotiating communications between entities [9]. The proposed framework leverages SIP authentication in order to set up secure communication among users of an association or among users and resources of an association.

TLS

Secure communication protocols have a crucial role in our system and are used in the following places:

- Between the Association-enabled Presence server and its clients to provide both user authentication and data confidentiality and integrity.

- Between the server and the provided services. As the management and configuration of these services needs to communicate security parameters, it needs to happen over secure channels.

- Inside every secure service for data confidentiality and integrity perhaps user authentication.

For the first two cases our system utilizes TLS as the secure protocol. TLS is the IETF standardized version of SSL [10]. It provides secure end-to-end channels and can be used in any connection-oriented communication. TLS provides mechanisms for authentication, dynamic session keying, and data confidentiality and integrity.

The third case is very specific to the service and we will be looking at adopting existing approaches. Some of these

secure group communications efforts are Secure Group Layer (SGL) [11] and InterGroup Protocols [11], and the IETF Multicast Security Working Group [12]. Current SGL implementations do not address user authentication and policy management for ad hoc interactions.

AD HOC INTERACTIONS

Ad hoc interaction systems have well-known issues in the vein of security and privacy. To be useful they must also have knowledge of both the user and enterprise context. In principle, this means that they will only be found useful in an enterprise if they create a controlled domain that is knowledgeable of the intent of the users and the constraints of the enterprise. What is required is a new set of communication features that can to be tuned to the working area. These features require knowledge of the context of users and their availability to communicate.

Interaction Scenarios

We present 3 scenarios to strengthen this claim. These scenarios are presented as different types of meetings. They are the hallway meeting, the room meeting, and the conferencing meeting. Table 1 is a chart that summarizes some of the attributes of these 3 types of common interactions.

We have primarily come about these rather subjectively, from experience and numerous discussions. Five characteristics were chosen that reflect the uniqueness of each type of interaction. These characteristics are Scheduling Type, Number of Participants, Networking Type, Method of Authentication, and Type of Information Exchanged.

Scheduling type means was the meeting previously scheduled? A scheduled meeting includes ad hoc statements like "Let's meet in my office" or could include meetings pencilled in a calendar. Hallway-interactions, unlike room- and conference-interactions, occur by being interrupted on the way to perform some task. Most hallway interactions are comprised of a very small number of persons, primarily 2, and are ideal for creation of private networks in order to share data. In reality, we have witnessed very few situations where data sharing is desired during such casual primarily verbal meetings. For this particular reason, we are more interested in addressing room and conferencing interactions rather than hallway interactions. Room and conferencing interactions leverage the use of electronic networking to a greater extent than hallway interactions. For these interactions there is more demand for access to local and distant resources especially for data sharing.

Room and conference interactions share similar behaviors. The most significant difference is the location component. Room interactions are single location interactions, while conferencing ones are distributed across several locations. The distributed nature of conferencing introduces new cross enterprise challenges that include user and resource authentication.

Security is always a concern when persons come together and need access to local and distributed resources. It is necessary to protect both the enterprise's and the user's resources, as well as to offer a secure communication channel among participants of a meeting. The challenge is in the creation of a framework that supports ad hoc interactions while offering enough security that is satisfactory to the users and IT managers in an enterprise. This paper presents a preliminary framework that integrates secure association managers with a presence service in an attempt to achieve secure ad hoc communications.

ASSOCIATION MANAGER

An association is a software entity that manages presence and resource access for a group of persons that share a common context. It can be viewed as a manager that maintains a common set of presence and resource access policies for its members. We would primarily like to keep an open communication policy among members of the association as well as between members and resources that are managed by the association. The association can also contain restriction policies but it is important to consider the association as one entity rather than a group of members.

One of the first types of associations we envisioned is location-based association. For example room associations. These associations would be persistent objects with the resources of that room already registered with that particular association. 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. We will come to that later.

Features	Hallway	Room	Conference
Scheduled	NO	YES	YES
# of Participants	2 or 3	2 – 7	2 – 10
Networking Type	Personal (IRDA / Bluetooth)	Enterprise LAN / WLAN	Enterprise LAN / WLAN
Electronic Resources	PDAs	PDAs / Laptops / Projectors	Phones / Laptops / PDAs / Projectors
Method of Authentication	Facial	Facial / Electronic	Verbal / Facial / Electronic
Type of Information Exchanged	Verbal / Small Data	Documents / Verbal / Presentations	Documents / Verbal / Presentations

Table 1: A categorization of different types of personal interactions and their corresponding features.

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. Of interest to this paper is the creation of a room meeting association that inherits from a particular room location association the access policies to the rooms resources. This room meeting association needs to be created by a user after which it is possible for all other users to register with the association. The process of creating an association results in a particular URL being created for that association. We see a user creating an association using a particular client represented as item 1 in the figure below. The dashed line between the Association and User Client signifies that the creator of the association may also be a member of the association.
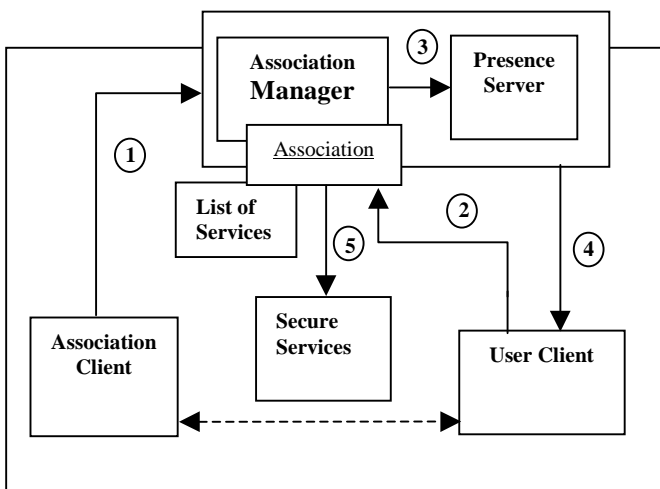

Figure 1. System components and interaction diagram for association access model.

When a user registers to the association, step 2 in figure 1, it first of all identifies its node address and secondly supplies a list of services that it supports. For this procedure

we can leverage the SIP Registration method that allows SIP User Agents to register their address as well as a list of contact services like Instant Messaging (IM), voice, and video.

At this point we come to the first set of policies the association manages, *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. This is not that difficult for meetings where all the members are co-located or small conference meetings where each other knows each of the participants.

An association maintains a list of services that belong to resources available for its member's use. 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, items 3 & 4 in figure 1. The association is a special group-based component of the presence service. It is an extension of other presence group-based such as private groups and role-based groups [13].

The association interacts with the presence service to create a presence group by the same name as the association and create presence agents for each of the members of the association. Each presence agent contains a set of notification and subscription policies that are used to determine which users and under what context the users can see the availability of other users. The association maintains a second set of policies, *the presence policies*, that it asserts into each presence agent that is part of the association. In a similar fashion, the association also creates presence agents for the resources that it manages. These also will appear in the member's presence clients. We see such a view in figure 2 for a presence client displaying users that are part of a private group. The association component is an extension of the private group formalism.. We are just commencing to develop the Presence Agents for services.
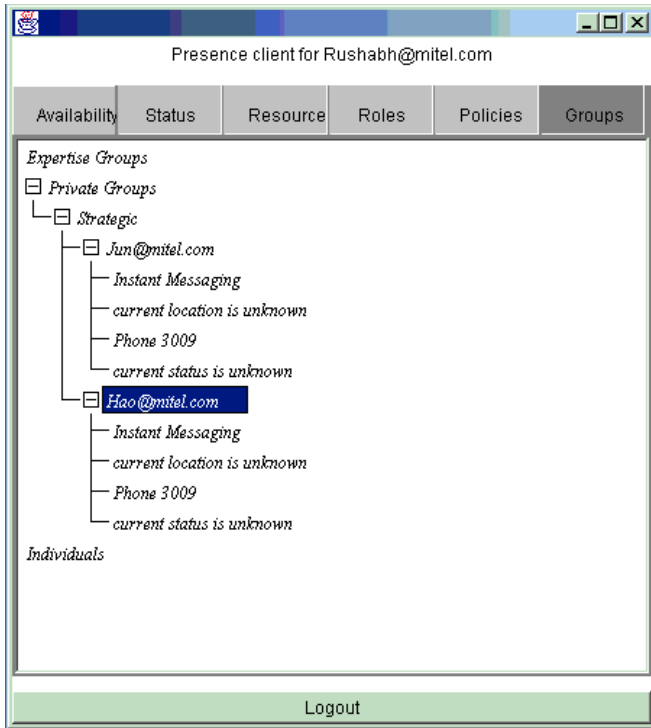
Figure 2. Screen shot of a presence client showing private group functionality.

In this configuration the presence service manages the distribution of service contact information among all the members of the association. The presence service can also monitor the availability of resources through the user of Presence User Agents located with the service manager of the resources. The presence service uses the SIP SIMPLE protocol for communication with the presence clients.

An association must also maintain a third set of policies, *the resource access policies* that are placed in the resource manager, item 5 in figure 1, in order to control access to those resources. This is important since other users on the network can physically access networked resources so it is necessary to prevent access to these resources when in use by members of the association. We have been investigating the use of the COPS protocol for this functionality.

SECURE ASSOCIATIONS
In the previous sections we have presented 3 access types of policies that the associations manage, *association membership, presence, and resource access policies*. In this section, we will present a framework for how the associations along with the presence framework manage authentication and secure connections. Figure 3 is a similar figure to the one shown in figure 1 with the exception of the user creating the association. We will present the method by which the association manages to properly secure the communication channels used by the association members.
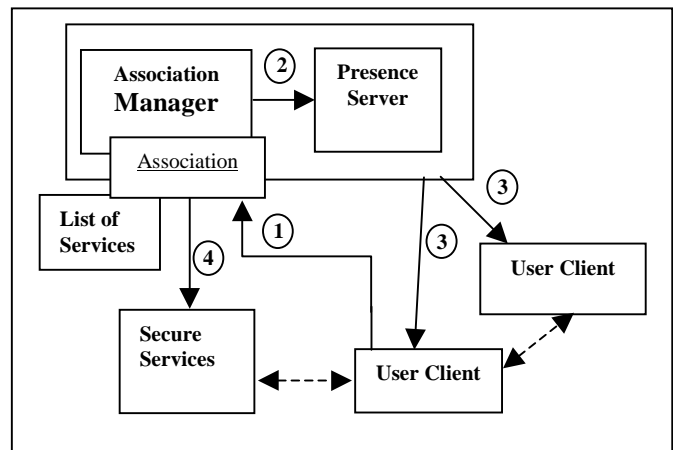

Figure 3. System components and interaction diagram for association security model.

The users register themselves with an association over a secure channel, step 1 in figure 3. One challenge that we face is that there is no standard for secure communications among services. For that particular reason the association maintains a separate Service Security Profile (SSP) for each service. A SSP contains information about the supported security communication protocol for the service. For example, for a video service this could be secure RTP. Furthermore a SSP contains a list of supported security algorithms, the required passwords or certificates to access it and the current session keys. A SSP is generated for every registered service in an association, and gets updated with every change in the association. For example the arrival of a new member leads in the change of session key.

After each new member has joined the association, the association enables the access to the available services to the new member. The procedure depends on the type of the authentication for each service and can include sending the member's authentication information (like the certificate) to the service, step 2 in figure 3. The presence service projects to all members the SSP information for each service, so that a secure communication channel can be established with it, steps 3 & 4. Secure sessions can now be established between members of the association and services managed by the association.

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. This will form the basis of the Association Manager. We have investigated the use of SGL as a secure group service and have concluded that it needs to be extended to support authentication. We believe that a good model for this is to implement a secure session using SIP above any secure group services. This offers a uniform way to manage

5

authentication and the dynamic a hoc nature of users joining and leaving sessions.

CONCLUSION

In this paper, we presented our system as a framework for secure ad hoc communications. We introduced the concept of association that supports 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. We believe that introducing a SSP for each available service contributes to the ease of use of such services and reduces the required setup and configuration steps by the users.

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. A concrete example would be the modeling of the SSP concept and developing a protocol for exchanging security profiles. Another milestone would be incorporating different types of secure group-based services in our system, like chat, audio and video. For this task, we will need to implement prototype services or extend the existing ones to integrate them in our system.

REFERENCES

1. Allen, Thomas J., Managing the Flow of Technology, MIT Press, 1984
2. Whittaker S, Frolich David, Daly-Jones Owen, *Informal Workplace Communication What Is It and How Might We Support It?*, Human Factors in Computing Systems, Boston, April 24-28, 1994
3. Hillier B, *Space is the machine*, Cambridge University Press, 1996
4. Penn A, Desyllas J, Vaughan L (1999) *The Space of Innovation: interaction and communication in the work environment'* Environment and Planning B: Planning and Design, Theme Issue on Space Syntax, 26(2), 1999, pp 193-218
5. Nardi, B., Whittaker, S., and Bradner, E. *Interaction and Outeraction: Instant Messaging in Action*, Proc. from the Conf. on Computer Supported Cooperative Work, Philadelphia, PA, Dec. 2-6 2000.
6. Day M., Rosenberg, J., and Sugano, H., A Model for Presence and Instant Messaging, IETF RFC 2778, February 2000.
7. Durham D. et al, The COPS (Common Open Policy Service) Protocol, IETF RFC 2748, January 2000
8. Walker J., Kulkarni A., COPS over TLS, Internet Draft, April 2001
9. Rosenberg J., Schulzrinne, H. , Camarilli, G., Johnston, A., Peterson, J., Sparks, R. ,Handley, M., and Schooler, E., SIP: Session Initiation Protocol, IETF RFC 2543 Draft #9, February 2002.
10. Dierks T. et al, The TLS Protocol Version 1.0, IETF RFC2246, January 1999.
11. Agarwal D., Berket K. et. Al, Reliable and Secure Group Communication, Lawrence Berkeley National Laboratory, http://www-itg.lbl.gov/CIF/GroupComm/homepage.html.
12. IETF Multicast Security (msec), March 2002, http://www.ietf.org/html.charters/msec-charter.html
13. Liscano, R., Baker, K., Balaba, N., and Zhao, J. Role-based Presence, Mitel Patent Submission, Patent Pending, 2002.