IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5143

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour.

Issues and Challenges for Secured Ad Hoc Collaboration

Kristie Kosaka and Samir Chatterjee
Claremont Graduate University, USA, kristie.kosaka@cgu.edu

INTRODUCTION

Advances in science and engineering are driven by collaborative efforts focused on sharing ideas, data and accessing computing resources and experimental facilities. Teams of researchers from various parts of the world communicate with each other using various modalities that include messaging, email, telephone, voice over IP and video-conferencing. Securing such communications poses some difficulties. Recent advances in middleware have led to widely available collaboration tools that are used today by disparate research teams. Although minimal security in terms of authentication and privacy is available, it is clear that such security is only available when using similar tools in a carefully configured environment. In a mobile world where people are often traveling while working, it is quite evident there is no support for ad hoc collaboration. Ad hoc collaboration is defined as environments that 1) support "spontaneous" collaboration, where two or more people have an unplanned interaction or 2) enable participants to create collaboration groups "on the fly" with little involvement from an administrator. Securing such interaction is very challenging. [1]

CHALLENGES

Securing collaborative environments is complicated because of the need to integrate heterogeneous applications and data hosted on dissimilar platforms. Ad hoc collaboration is unique in that provisioning of collaboration membership and privileges is done immediately by the participants, without administrative involvement.

These scenarios help further describe ad hoc collaboration.

- *Scenario 1:* Professor John of Claremont is working on his desktop PC inside his office. He receives a message from Professor Larry at Caltech inviting him to join a video conference call using Virtual Rooms Video Conferencing System (VRVS) VRVS was developed by Cal Tech to extend research collaboration globally. John has a SIP Client and connects to Larry using it. SIP, the Session Initiation Protocol, is a signaling protocol for Internet conferencing, telephony, presence, events notification and instant messaging. They use their respective preferred video clients to connect using all the trust and authentication servers that are supporting their applications. However, the reason for this conference is to bring Mary into the call to discuss a startup opportunity. Larry escorts Mary into the secured conference. The system does not trust Mary yet since she is a new system entity without prior arrangements. This requires a private session between three individuals located in federated campus networks using trust and security mechanisms that are available and appropriate.
- *Scenario 2:* Engineer Eric of Company A is collaborating with Engineer Sam of Company B on a proposal. They need to coordinate with Sue, a supplier, who works in Purchasing. Eric has his Blackberry and is at the airport. Sam has his laptop in the office and Sue has her PDA out in the field. They need a secure, encrypted, "on the fly" network set up to quickly review pricing and parts information needed in the proposal.

We can categorize the major challenges into five areas: authentication, authorization, trust management, incremental modalities and federated resource sharing.

- *Authentication:* Several authentications are available today. They range from simple schemes such as username/password or Kerberos tickets to more sophisticated techniques such as X.509 certificates to even more secured mechanisms such as biometrics. In a mobile ad hoc virtual collaboration, participants may be precluded from providing the necessary credentials because of location, lack of trust or simply limited constraint connections. Existing authentication models do not work well in ad hoc scenarios. New authentication models that allow for a combination of less secured to more secured techniques are needed.
- *Authorization:* Once an authentication token is established, authorization is typically done by checking some access control list or a server that has some policies in place. Such mechanisms work well for preset environments but do not perform well in the ad hoc context. Existing techniques work without intervention of an administrator and are based on gaining confidence in the identity of the user. Ad hoc scenarios typically build trusts incrementally and hence require support for adding dynamic authorization rules.
- *Trust management:* Establishing trust in fixed preset environments and between organizations that participate in virtual collaboration is challenging. The complexity increases when trust needs to be established in an ad hoc collaboration environment. We believe that new models are needed. Today's systems establish rules and policies for access and trust on *a priori* basis up front. Ad hoc collaboration requires the addition of new users with little initial trust placed into their identity and must support the incremental building of trust relationships through endorsements from established collaborators. Trust typically refers to systems that manage the access rights of users (trusted entities) to resources. Trust management systems traditionally encompass both authentication and authorization. The more intuitive meaning of trust is a relationship between two parties with the expectation of a good outcome from the interaction. In an access control system, trust is meaningful as it allows user specific rights to resources and is a pre-requisite of authentication.

Ad Hoc collaborations need different levels of trust depending on what is being done and the size and permanency of the collaboration; ideally they should be able to support more than one method of authentication. Authentication tokens can be shared secrets *(something you remember)*, asymmetric keys *(something you carry)* or biometrics *(something you are)*. Each has its own pros and cons. Trust could be expressed as a level, or as set of access privileges, defined by each member who provides resources. Incremental trust means levels of trust are associated with different methods of authentication for the same individual. An individual's level of trust may vary over time or context and should be easily modifiable by trusting party.

- *Incremental modalities:* A unique aspect of ad hoc collaboration environments is to use the communication modality that is best for the purpose or task at hand. Secured video-conferencing may not be the best mechanism to use from an untrusted café in a foreign country. Hence, one needs to incrementally ramp up from simple text messaging to audio and video while the system is building confidence and trust.
- *Federated Resource Sharing:* Grid middleware has provided resource sharing tools and software. However, they need to be

significantly changed to address ad hoc collaboration. In an ad hoc scenario where users are joining using different clients, how can an MCU (for SIP) and reflector (for VRVS) be made available to new users? If such collaboration is to be managed by a trust management server, where is this located and how can it be accessed by participants or administrators?

Some resources are owned by everyone and need to have a common authorization policy (e.g., chat room); this requires procedures for combining individual trust decisions. An appropriate balance must be established between securing and sharing information. The owners of the data must be confident that access is granted to the appropriate organizations with the proper level of authorization based upon the type of data, roles an organization is assigned, and level of trust. From the user perspective, collaborators must be made aware of what data and information is at their disposal, how to access that information, and know when new data of interest has been posted. The objective of secure collaboration is to ensure that only authorized people/organizations have access to the appropriate data, and the data is properly protected (users have read-only access). The data owners/custodians want to retain the right to control access to their data, yet not be encumbered by daily security administration. In order to develop a process to define, design and administer a secure, collaborative environment, researchers must learn from past efforts as well as solicit new collaboration requirements.

In almost all computer mediated ad hoc environments, it is necessary to have a system that is easy to set up initially, and can be scaled up to something more robust and secured over time. The cost of travel to send people to meet can be expensive, which results in the need for technologies that facilitate "virtual work groups". To ensure a company stays competitive and operates at optimum production levels, it is important that efficient collaboration between business processes and organizations not only exists, but increases [2]. Shared and coordinated use of resources within large, dynamic multi-organizational communities is becoming a key component within a range of computer systems including scientific collaboratories and healthcare [3]. Trust is at the core of how data sharing is established. Achieving an acceptable degree of trust becomes increasingly complicated as the collaborative environment grows larger. The more people and organizations involved, the more involved it becomes to manage and administer the various security policies [4]. Expensive resources (data & equipment) must be used efficiently. Sharing reduces costs and can optimize the benefits through increased usage. For example, scientific bio-medical data may take years to accumulate; the value of this information is high. The data mining of such information is of interest to biologists, data analysts, pharmacists and other researchers looking to understand the results and extend the knowledge through further research endeavors and collaboration.

Sound collaborative security to prevent the undesired "leaking" of information to anyone unauthorized to receive it is crucial [5]. Accurately establishing the boundaries of collaboration is one way to reduce information "leakage" [6]. Reports on security vulnerabilities indicate that many short-comings still exist in the development of secure application systems [7]; ad hoc collaboration via the Internet has exacerbated this risk. Sound security programs should include policies, standards and guidelines. Security policies serve as "blueprints" that help implement the "specific controls, processes and awareness programs necessary," elevating both security awareness and security program strength for an organization [8].

During cooperative endeavors, the participating organizations engage in some form of distributed collaborative planning and information sharing. Such ad hoc, impromptu collaborations might occur after a natural disaster or to support other crisis management collaboration [9]. Secure collaborative environments must be formed quickly, be cost effective and ensure appropriate levels of security. It is vital that recipients of messages be able to confirm or authenticate the sender, that the recipient be confident that the message has not been modified during transmission, and that the sender is not able to later deny having sent the message. One area requiring further research involves removing the need for a server and central administration; this is particularly important for supporting wireless ad hoc collaborative environments. Many collaborative groups are dynamic, with frequently changing membership and levels of trust changing the level of security, highlighting the need for low-cost, easy-to-maintain collaboration groups. Increasingly, collaboration work is being performed on mobile machines, frequently connected by ad hoc unsecured or minimally secured wireless networks, not via established network infrastructures. A security system should adequately address several concerns: authentication, authorization, data confidentiality, non-repudiation and privacy. Authentication involves validating the identity of the user based upon either something one knows, one has, or an attribute of the person. Examples of these various authentication types are: user id/password, secure token, and fingerprint. Security authorization concerns what a person is permitted to do (e.g., just read some data, edit, author, and/or run selected programs).

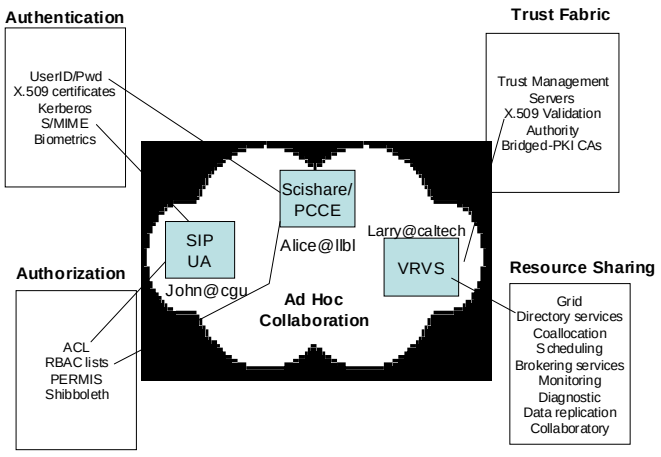
Collaboration may involve a few people or a few hundred people. People need to connect using devices that they have at hand, a varied collection of telephones, PDAs, laptops, desktops, etc. Collaboration among customers, partners, suppliers, and employees spanning the globe requires secure integration across diverse heterogeneous systems owned or operated by a variety of organizations. This environment must be easy to use, hide the complexities from the end-users and be based upon open source standards. Increasingly, people need a method to quickly establish a secure ad hoc collaboration session that is low cost and ensures appropriate security based on confidence in the user identity. Privileges should be dynamic, and change as the roles and relationships, as well as levels of trust, change [1].

RESEARCH PROTOTYPE EXAMPLES

Some recent research addressing secure collaboration shows promise. The Community Authorization Service (CAS) was developed to address three major authorization problems that occur in distributed virtual organizations: scalability, flexibility, and the need for policy hierarchies. A major component of their proposal is that it enables resource providers to delegate some of the authority for maintaining fine-grained access control policies to communities, while still retaining final control over their resources [3]. Their initial efforts show promise, yet further research, especially related to ad hoc collaborative environments is needed.

A Secure Virtual Enclave (SVE) facilitates sharing of distributed objects while still respecting organizational autonomy through use of middleware. An enclave is a collection of computers and networks managed by the same organization and subject to the same security policy. Within an SVE, collaboration occurs when principals in partner enclaves are permitted access to selected local resources. The SVE architecture is

Figure 1. Secure Ad Hoc Collaboration



based upon an infrastructure where the components create, distribute and enforce security policy [9]. Ellison and Dohrmann have developed a Next Generation Collaboration (NGC) research prototype to address many of the security needs of collaboration through a design that blends both computers and humans. They refer to their mixed protocol as a "ceremony", "enabling the designer to identify decisions being made and the data upon which they are based – and to verify that the ceremony provides all that data in a secure manner." [10].

Deb Agarwal, from Lawrence Berkeley National Laboratory, shared her experience building a secure ad hoc collaboration environment at the Internet2 2004 member meeting [1]. Her work involved developing and supporting collaboration tools for use by distributed science teams, concentrating on supporting the day-to-day work environment. Figure 1 depicts an example of one of the secure ad hoc collaborative environments explored by Agarwal. She started with traditional kerberos-based and X.509-based solutions for securing collaborative environments. Elements included: shared experiment control, instant messaging (e.g., IRC, Jabber), and peer-to-peer file sharing (e.g. SciShare). Agarwal's requirements were to provide: 1) the ability to participate from anywhere with a low threshold for entry into the system (incorporates new users easily with no waiting for authorization to enter the system), 2) support for identifying trusted users, 3) the ability to specify the type of authentication and authorization needed. The architectural approach consisted of a peer-to-peer system, with each site able to act as client, server or both. Added value is provided by specialized servers that handle archiving, certificate authority, user registry and connection points. Registration can be by oneself, a trusted user or an administrator. This research identified some issues including: where users are registered, who controls/administers the registry, who decides the list of trusted users and how identities can be verified. Users can authorize both pseudo certificates and trust CA signed certificates for access to resources. Jabber instant messaging requires more research effort to support 1) running servers where required, 2) enabling specification of authentication level for chat room entry, and 3) providing the ability to augment the definition of trust groups [1].

SUMMARY

Research integrating security issues, with ad hoc collaboration issues has not been heavily explored. Increased globalization has resulted in greater reliance upon the internet to foster collaboration, and heightening the importance of secure ad hoc collaboration research. What's needed are: tools to manage trust, policies and identities in ad hoc settings, software that can adapt to environmental constraints and choose proper modalities and implementation and testing of new open source security models that apply to ad hoc requirements. We need to have authentication and authorization policy easily set by the owner of the node that is providing resources. What is needed: 1) a quick way to set up a user and define his trust level, 2) a map trust level to authorization rights, 3) a simple way to both statically and dynamically set access policy for users, 4) procedures and tools to coordinate node policy into a shared collaboration policy.

REFERENCES

1. Chatterjee, S, Agarwal, D., Thompson, M, Kosaka, K., and J. Miller, *Internet2 2004 Meeting*, Austin Texas, September 27, 2004, "Ad Hoc Collaboration: Technology, Applications, and Security"
2. Srikanth, Anjana, (2004), Collaboration Toolkit, http://web-enable.com/industry/collabarativetools.asp
3. Pearlman, Laura, Foster, Ian, Welch, Von, Kesselman, Carl, Tuecke, Steven, (2002), *A Community Authorization Group for Collaboration*, www.globus.org/research/papers/CAS_2002_Revised.pdf.
4. Alijareh, S. and N. Rossiter, (2002) , In *SAC 2002* ACM, Madrid, Spain, pp. 744-749.
5. Stallings, W. (2003) *Network Security Essentials Applications and Standards*, Prentice Hall, Pearson Education, Upper Saddle River, New Jersey.
6. Urcuyo, C. E. and Kunnathur, A. (2002), *Knowledge Sharing Strategy: The Significance of Security and Collaboration*, Eighth Americas Conference on Information Systems, pp. 1922-1939.
7. Steffan, J. and Schumacher M. (2002) In *SAC 2002*ACM, Madrid, Spain, pp. 253-259.
8. King, C. M., Dalton, C.E. and Osmanoglu, T. E. (2001) *Security Architecture: Design, Deployment & Operations*, Osborne/McGraw-Hill.
9. Shands, D., Yee, R. and Sebes, E. (2001) *ACM Transactions on Information and System Security, 4, 103-133.*
10. Ellison, C. and Dohrmann, S. (2003) *ACM Transactions on Information and System Security*, 6, pp. 547-565.
11. Agarwal, D.A., Chevassut, O., Thompson, M.R., Tsudik, G. "An Integrated Solution for Secure Group Communication in Wide-Area Networks", *Proceedings of the 6th IEEE Symposium on Computers and Communications*, Hammamet, Tunisia, July 3-5, 2001, pp 22-28.