

Securing Dynamic Collaborations

Karlo Berket, Abdelilah Essiari and Mary Thompson
Lawrence Berkeley National Laboratory

Collaborative applications, such as video conferencing, collaborative editing, chat applications, shared workspaces and file sharing, support human-to human interactions in synchronous and asynchronous modes. These applications provide users with a highly flexible environment where they meet, exchange information, and work toward a common goal. These collaboration environments are often times dynamic, in the sense that collaborators frequently enter and exit the environment. In addition, the membership of the collaboration is dynamic.

Providing security for dynamic collaborations is difficult due to the dynamic nature of the collaboration groups and the distributed and autonomous nature of the participants. It is important that security should not in any way undermine the very properties that make collaborative applications attractive. A secure collaboration environment should thus make it easy to join a collaboration, create and share out resources, interact with other people, and access resources.

Our experience in applying traditional security solutions to collaborative applications has led us to identify the following issues with existing security solutions in dynamic collaborative environments:

- 1) There exists a large startup cost for new collaborators.
- 2) The policies for accessing resources within the collaboration are static and determined by a central authority.
- 3) There is a single, static level of trust for each user.
- 4) There is no way to make group access decisions.
- 5) Lack of efficient means to secure group communication.

Large startup cost for new collaborators

Traditional security solutions have focused on protecting fairly static resources from use by unauthorized users. Normally the user must get an authentication token and some access rights assigned before any access is allowed, causing some delay between the time that a user wants start work and when he can. However, in most collaborative applications, spontaneity is highly desired. Users should be able to set up a collaboration or invite guests into an established collaboration in a matter of minutes if not seconds. Contacting central authorities and setting up the guests is a process that was designed to be anything but quick.

Static and central access control policies for resources

Standard security systems tend to treat all objects in a domain as requiring the same level of security, causing all items to be handled in the same manner as the most valuable. As a result the security requirements tend to get rather extreme. In collaboration environments most of the resources need some protection but not to the point where they become too difficult to use. For example, a group of users wants to have a secure video conference. At its extreme, a security model would have each of the participants build a soundproof room, physically secure access to that room, create a secure network between these rooms, and fill it with the appropriate equipment before they can start. Of course, things are not so extreme, but it often feels that way to the users of secure collaborative tools.

We believe that users should be given more control over the security of the collaboration environment. Users need to be able to easily create and share resources and to easily create and update the policies for those resources. Since humans are involved in the application there should be interfaces into the security system for them to change access policy as a result of knowledge they may have from out-of-band means. For example, in a video conference, a participant may be lacking a credential, but the other members can recognize him. They should be able to tell the authentication system to accept him. The human model also allows for a more trusted user to invite or escort a less trusted user into a collaborative space as long as the other members of that space agree. The ideal collaborative security system will provide interfaces for inviting or escorting a user into a protected space as well as rejecting an untrusted user.

Single static level of trust for each user

Another situation that commonly occurs in collaborations is that a trusted member needs to connect from a totally untrusted site, such as an Internet café, or from a moderately trusted site, say a colleague's workstation, but does not have his cryptographic credentials. This requires authentication and authorization models that can accommodate different session-based levels of trust for the same individual. Ideally, it will also allow a more trusted user to vouch for a user who has insecurely connected, but has communicated him identity by some off-line means.

In addition to session-based trust levels, the overall trust level of an individual should be able to evolve. In a collaboration, one normally builds trust incrementally through interactions with the other collaborators. Thus, the underlying system should also support incrementally building trust in the individuals who are members of the collaboration

No way to make group access decisions

Access to most resources, e.g. files, only requires a single access decision. The access control policy to access these resources may be distributed, but only one access decision is required. In collaborative environments, some resources, such as a chat room, may require a group access decision. In the case of a chat room owned by a number of users, every one of these users would want to contribute to the authorization decisions that allow other users access to the room.

Lack of efficient means to secure group communication

Collaborative applications use a combination of point-to-point and group communication channels to enable users to interact with each other and to access resources. Secure group communication is most efficient if the group members have a common, shared key for securing the communication. Centralized solutions to distribute such keys do not adapt well to the collaborations we have described. And only a couple of systems are currently working on providing decentralized key-agreement and key-distribution protocols (e.g. Secure Spread[1], SGL[2]). In any case, there is no dominant TLS-like technology to secure group communication. A lot of work is being done in providing security at the message level, but it is not quite clear how these new technologies would benefit dynamic collaborations

Conclusion

As a result of these requirements and the fact that the participants should be allowed to take part in trust decisions we believe that dynamic collaborations require authentication and authorization systems that are fundamentally different from those used by computer mediated access to static resources. These ideas should be applied to specific applications in order to gauge their effectiveness and we have already begun this process [3]. This should then lead to a security toolkit that can be used to enable security in collaborative applications.

References

- [1] Y. Amir, G. Ateniese, D. Hasse, Y. Kim, C. Nita-Rotaru, T. Schlossnagle, J. Schultz, J. Stanton, and G. Tsudik, "Secure group communication in asynchronous networks with failures: integration and experiments," in Proceedings of the 20th IEEE International Conference on Distributed Computing Systems, April 2000, pp. 330–343.
- [2] D. A. Agarwal, O. Chevassut, M. R. Thompson and G. Tsudik, "An Integrated Solution for Secure Group Communication in Wide-Area Networks," in Proceedings of the 6th IEEE Symposium on Computers and Communications, Hammamet, Tunisia, July 3-5, 2001, pp 22-28. Also, LBNL report number LBNL-47158.
- [3] K. Berket, A. Essiari and A. Muratas, "PKI-Based Security for Peer-to-Peer Information Sharing," to appear in Proceedings of the Fourth IEEE International Conference on Peer-to-Peer Computing, Zurich, Switzerland, Aug 25-27, 2004. Also, LBNL report number LBNL-54975.