

# *Reliable and Secure Group Communication*

<http://www-itg.lbl.gov/CIF/GroupComm/>

PI: Deb Agarwal ([DAAgarwal@lbl.gov](mailto:DAAgarwal@lbl.gov))

*Executive Summary*

*September 2001*

## **Vision:**

The goal of this project is to develop the components necessary to support a peer-to-peer group communication infrastructure that provides reliability, security, and fault-tolerance while enabling scalability. Applications such as shared remote visualization, shared virtual reality, and collaborative remote control of instruments require reliable and secure distributed information sharing and coordination capabilities. The collaborations using these applications are usually built in an incremental and ad hoc manner. This incremental and dynamic growth pattern is not well supported by a rigid server-based structure. Thus, the natural alternative to a server-based model is to provide a reliable and secure group communication infrastructure to support a dynamic and scalable peer-to-peer model.

There have been several systems that have addressed individual aspects of building a reliable and secure group communication capability, however, few have come close to providing a complete solution to the problem. This project is developing the components necessary to provide reliable and secure group communication mechanisms that scale to the Internet. The InterGroup protocols will be used to provide the reliable group communication services. These properties include reliable delivery of messages, ordered delivery of messages, and membership services. The Secure Group Layer will provide the secure group communication services including authorization and access control, key management, authenticity, integrity and/or confidentiality.

## **Major Goals and Technical Challenges:**

Collaborative applications need to support dynamic groups that can scale to large numbers of users. A peer-to-peer model inherently makes these applications easier to design and to operate for groups. Since there are no servers, groups can form ad hoc and there is no setup or scheduling with a centralized authority required. There are many DOE applications that can benefit from the use of a peer-to-peer group communication model. For example, this group communication model has already been used in a collaborative electronic notebook to provide distributed event notification services. With the advent of the DOE Science Grid and the availability of distributed resources, comes the need to provide distributed information sharing and coordination capabilities. As the DOE Science Grid begins to deploy, there will likely be a need for support of replicated services. A server can be a performance bottleneck, a single point of failure, and require significant administration. Group communication provides a natural mechanism for helping to maintain consistent state among a set of replicated servers. The group communication service provides group membership services, reliable ordered message delivery, and allows the system to make progress in the presence of process and network faults. In this model, users do not send traffic to other users but instead elect to receive traffic from a multicast group. This means that at any time a user may join a group, receive its traffic, and leave a group. Thus controlling access to a multicast group and establishing a secret session key for the group present a complicated set of problems.

There are two primary components to a reliable and secure group communication system. These components are a reliable group communication protocol and a Secure Group Layer. A peer-to-peer reliable multicast protocol combined with group security services can provide a secure scalable communication infrastructure in the Grid and the Internet. It is important that this service allow the group members to act as peers, trust the group to be secure and trust the delivery guarantees. This service must also scale to the Internet. InterGroup is a new group communication protocol under development at LBNL that is designed to be scalable to the Internet and provide a very flexible service model. The Secure Group Layer, also currently under development, is designed to provide security services for the InterGroup protocols. The InterGroup protocols will be developed in this project to provide the reliable group communication services. These properties include reliable delivery of application messages, ordered delivery of application messages, and membership services. The Secure Group Layer will provide the secure group

communication mechanisms: authorization and access control, establishing session key, authenticity, integrity and/or confidentiality. We will develop, disseminate and support the InterGroup protocols and the Secure Group Layer for a select group of application developers, with the long-term goal of integrating these components into the DOE Science Grid infrastructure.

An initial proof of concept implementation of the InterGroup protocols and the Secure Group Layer have been completed, there are still many features of the system that are missing. The algorithms and the models that the prototype system is based on still need further development. The delivery model and performance need to be investigated more completely. The group security modules need to be formally analyzed individually and as a whole. The Secure Group Layer also needs to be converted to work on top of the InterGroup protocols. A robust implementation of the system needs to be completed and the performance of the combined system must be investigated and verified.

### **Major Milestones and Activities:**

#### **Year 1:**

- ?? InterGroup Alpha release testing and improvements identified during deployment
- ?? Begin development of example applications
- ?? Publish proof of security for Secure Group Layer key exchange algorithms.
- ?? Limited prototype implementation of the Secure Group Layer using the InterGroup protocols.

#### **Year 2:**

- ?? Beta release of InterGroup implementation
- ?? Support of alpha and beta adopters
- ?? Improvements to InterGroup membership and message delivery protocols
- ?? Publish an informal security analysis of the Secure Group Layer as a whole
- ?? Release the Secure Group Layer using InterGroup protocols (sender group mode).

#### **Year 3:**

- ?? Support InterGroup beta adopters and continued releases of new functionality as available
- ?? Add asymmetric protocols to membership and delivery protocols
- ?? Implement the full Secure Group Layer on top of the InterGroup protocols.

#### **Year 4:**

- ?? Further enhancements to scalability of InterGroup membership and message delivery protocols
- ?? Release the Secure Group Layer using InterGroup protocols
- ?? Publish a review of experience with the Secure Group Layer using InterGroup protocols and an application like group chat, MUDs or teleconferencing.

#### **Year 5:**

- ?? Support of InterGroup and Secure Group Layer adopters
- ?? Implement improvements to congestion control
- ?? Investigate cryptographic mechanisms to support open groups.

### **Current Connections with Other SciDAC Projects:**

Pervasive Collaborative Computing Environment, DOE Science Grid, and Self-Configuring Network Monitor