

Middleware to Support Group-to-Group Collaboration

Rick Stevens,^{1,2} Justin Binns,¹ Terry Disz,¹ Mark Hereld,^{1,2} Ivan Judson,¹
Susanne Lefvert,² Ti Leggett,¹ Eric Olson,¹ Robert Olson,¹
Michael E. Papka,^{1,2} and Thomas Uram¹

¹Argonne National Laboratory ²University of Chicago

Summary

The Middleware to Support Group-to-Group Collaboration effort continues to build on the tremendous success of the Access Grid project. The major goal is to establish the foundation that other groups can use to build technology for a given domain. This work includes development and support of Virtual Venue technology, integration of security, and management of Access Grid nodes. In addition, this work looks at ways to incorporate asynchronous collaboration, to integrate new and legacy applications, and to use new display technology. The results are used daily by numerous groups; for example, a General Atomics led an experiment over the Access Grid at the Joint European Torus facility in Culham, UK.

1. Introduction

In the past year, a large part of the Access Grid (AG) was newly architected, designed, implemented, and released. The new software uses Web services to communicate among its components: from the venue server to the venue clients, and from the venue client into the hierarchy of machines and services aggregated by node management. These transactions occur over Globus Toolkit-secured communications channels.

In 2003, we made two major releases of the Access Grid Toolkit 2.0 (AG2), including documentation for the user-level components. The software maximizes portability; currently delivered on two platforms, it can support additional platforms, with minimal effort required only for platform-specific aspects.

The community has been migrating nodes to the new software at a regular pace. Adoption of the new version is aided by its ability to run on a single machine; hence, users can install and become familiar with the

software before installing it on their production nodes. Moreover, the new software can be installed without disrupting an older version of the software on the same machines. To promote community adoption of the AG2 software, we hosted the 3rd Annual Access Grid Retreat, gave tutorials during the year, ran weekly testing meetings, and led monthly AG town hall meetings.

2. Research Progress

Research has progressed in four distinct areas: scalable venue server, venue client, node management, and security.

The architecture and design of the *virtual venue* server build on the concept that succeeded so well in Access Grid 1.0 software. In particular, the venue server now supports user identification through X509 certificates, data sharing, and application sharing. Running a venue server is sufficiently easy that multiple venue servers are now being run persistently at ANL and other institutions.

The *venue client* software was developed as the client-side application to the venue

server. It enables users to communicate through text and to share data and applications. The software includes an API for creating new shared applications to register with the venue client. Several such applications have already been developed demonstrating this feature: a shared Web browser, a shared presentation viewer, and a shared movie viewer.

The venue client also provides facilities to register arbitrary Web- and Grid service clients to coordinate with Web and Grid services available within venues. The Futures Lab group has provided several examples of Web service integration and demonstrated the integration of a Globus Toolkit 3.0 service at Supercomputing 2003. In a separate demonstration, a venue service was used to submit jobs to a Condor-managed compute cluster, with the resulting output written to the venue.

Unicast bridging was integrated with the venue server and venue client software, to overcome instances in which multicast connectivity is unavailable or unstable. This technology is used regularly in meetings on AG2 venue servers and was used to support the SCGlobal portion of SC03.

The *node management* software also underwent a rigorous architecture and design cycle before being constructed. Node management provides the mechanism by which audio and video are exchanged between a node and the network. Both multiple node and dynamic node configurations are supported. Also included is a tool to configure the node automatically.

Node management also enables extension services (e.g., core media services) to be developed and added dynamically. The pluggability of the architecture was demonstrated with the integration of two

prototypes: positional audio developed by Boston University, in which a user's audio sounds as if it is coming from the user's window, and camera control software from Lawrence Berkeley National Laboratory. This work lays the foundation for exploring formats such as high-bandwidth video.

Access Grid communications are, now by default, *secure*. Users are identified with X509 identity certificates, which the venue server uses to authorize entry to private venues and to designate venue administrators. Certificates support asymmetric encryption of the communications channels between the venue server, venue client, and node management software. Media streams are encrypted to prevent unwelcome eavesdropping on audio and video communications. Users can have multiple certificates to select from when using the Access Grid, and newly issued certificates are automatically imported. Through this tool, the AG team has issued certificates to all users of the new software.

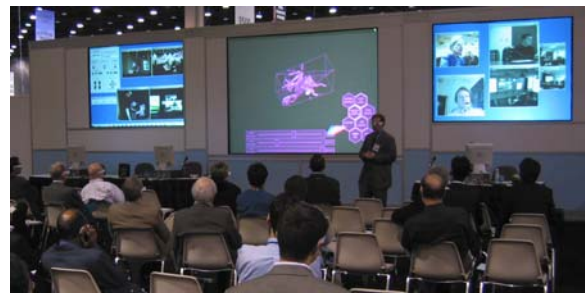


Figure 1: Dr. Jonathan Silverstein (UC) presents results of work to RSNA audience and remote participants via the Access Grid.

For further information on this subject, contact:

Rick Stevens
Mathematics and Computer Science Division
Argonne National Laboratory
Argonne, IL 60439

Phone: (630) 252-3378
E-mail: stevens@mcs.anl.gov