Secure PVM

DICCE Proposal
March 17, 1995

Abstract

Funds would be used to extend the distributed computing facility PVM (Parallel Virtual Machine) developed at ORNL to operate in an authenticated and secure mode. PVM would be extended to include multi-realm Kerberos support over wide area networks. PVM would incorporate Kerberos authentication services, optional application encryption, and DCE DFS/AFS file support among ESnet sites, coupling DOE's massively parallel and supercomputing facilities.

Principal Investigators:

Al Geist *gst@ornl.gov*
MS 6367 Bldg. 6012
Oak Ridge National Lab
Oak Ridge, TN 37831
615-574-3153 Fax: 615-574-0680

Tom Dunigan *thd@ornl.gov*
MS 6367 Bldg. 6012
Oak Ridge National Lab
Oak Ridge, TN 37831
615-576-2522 Fax: 615-574-0680

Proposed Research

PVM (Parallel Virtual Machine) is a programming library and collection of utilities that allow an ensemble of heterogeneous computers on a network to work in parallel in solving both scientific and commercial applications. PVM was developed at ORNL in collaboration with the University of Tennessee, Emory University, and Carnegie Mellon. PVM is freely available, deployed world wide, and is the *de facto* standard in distributed computing. PVM can couple workstations, vector super computers, and massively parallel computers together to provide a virtual parallel computer with potentially teraflop performance.

The proposed research would add security extensions to PVM. First, PVM's remote task initiation would be extended to support Kerberos. The user could require that the set of PVM machines used in his application use Kerberos for user authentication and for *rsh* services used in spawning remote PVM demons and applications. For intersite PVM computing over the ESnet, inter-realm Kerberos would be required, and we would draw on the work of the DCCC authentication task force. Second, PVM would use Kerberos-authenticated access to distributed file systems (DFS or AFS). Distributed file systems could be used to distribute copies of the execution images as well as application data. PVM already utilizes weakly authenticated NFS distributed file system. Finally, PVM would be extended to permit the programmer to request that PVM messages (both control and user) be either checked for data integrity (encrypted checksum) or fully encrypted (for sensitive data).

Research issues include key distribution and using a single key for many-to-many communication. Data integrity signature and full encryption will degrade communication performance, so the impact of these options will be measured and reported.

The proposed research meets the DICCE 1995-96 goal of creating the basis for a "distributed tera/petaflop computing environment." The research includes both local and wide area network components, key distribution, authentication, and encryption services over wide area networks, and utilization of a distributed file system (AFS/DFS). Intersite collaboration in developing and testing the secure PVM will require both signed and encrypted electronic mail using PGP as well as inter-realm Kerberos. Making the proposed security extensions to PVM at ORNL would leverage the OSC funding by utilizing the PVM development staff and ORNL HPCC computing resources.

Schedule

A tentative set of schedule milestones would be:

Milestones

- **Jun '95** Funds awarded
- **Sep '95** Upgrade local Kerberos and AFS servers to support inter-realm authentication services with the collaborating sites (PVM:ORNL, University of Tennessee, Emory University, and Carnegie Mellon; and DOE high performance computing facilities)
- **Dec '95** Beta test of Kerberized PVM
- **Feb '96** Performance analysis of Kerberized PVM
- **May '96** Wide-area tests of Kerberized PVM
- **Aug '96** Secure PVM demonstrations utilizing AFS/DFS
- **Sep '96** Formal reports on performance and utility of secure PVM

Deliverables

The research project will produce both technical reports and journal articles describing the steps required to produce a secure PVM and the performance implications. As has always been the case for PVM, source code and documentation for these extensions to PVM will be available via electronic mail (*netlib*) and the WWW (*http://www.epm.ornl.gov/pvm*).

Budget

The following table summarizes fiscal year funding requirements. Funds will be used to support research personnel.

FY95	FY96	Total
\$30K	\$120K	\$150K

Table 1: Programmatic costs.