Issues in High Performance Computing Security
-A Panel Discussion-

Panel Chair:
Rayford B. Vaughn, Jr., Mississippi State University

Panel Members:
Yvo Desmedt, Florida State University
Douglas Engert, Argonne National Laboratory
Jesse Pollard, DOD Major Shared Resource Center, Stennis Space Center

Session Abstract
This panel is composed of researchers and practitioners in the area of high performance computing (HPC) security and its purpose is to address whether or not HPC represents new security issues or whether traditional solutions apply. This topic has been addressed at the NISSC for the past two years in the form of technical papers - but the opportunity has not yet been presented for a panel discussion on the topic. This panel seeks to close that gap and to describe not only positions associated with this interesting topic, but to also describe current research in the field.

The panel will address the following issues:

- High performance computing in today's world represents new architectures, which include networks of high-end workstations, clusters, and very high-speed networks. Do these architectures represent a different security challenge?
- How does distributed high-speed computing differ from traditional network security.
- What currently available tools and techniques can we apply successfully to the HPC environment?
- What new science (or tools) needs to be advanced.
- What (if anything) makes HPC different from traditional computing.

The panel will be composed of a mix of researchers in this area. Specifically – two presentations from academic and two from practitioners will be offered. The intent of the panel is to review the HPC security problem, the challenge it represents, discuss some of the current research activity in this area, and outline some practical aspects of trading off speed of computation for security improvement.

High Performance Computing Security Research at Mississippi State University

Rayford B. Vaughn, Jr.
Associate Professor, Computer Science
PO Box 9637
Mississippi State, MS 39367
(662) 325-7450
vaughn@cs.msstate.edu

Mississippi State University is conveniently located in a high performance computing rich state. Mississippi is one of the top ten states in the U.S. in HPC computing power – largely due to the Department of Defense having located two of its Major Shared Resource Centers in the state – one in Vicksburg and one at Stennis Space Center. This, coupled with the highly successful NSF Engineering Research Center for Computational Engineering at MSU, has created the opportunity for an excellent HPC research focus – and a current thrust area within the MSU Computer Science Department. Over the past two years, we have coupled the existing HPC research with information security research in an effort to look at vulnerabilities in such architectures and possible counter measures.

Our research has been successful in certain areas. We have presented an analysis of vulnerabilities in PacketWay and Myrinet. We have pointed out some protocol changes that offer more assurance in HPC systems – all of which have been presented for the past two years at the National Information Systems Security Conference and are recorded in the proceeding for 1998 and 1999. This year, we have begun a project to look at how one might instrument a cluster-computing environment for intrusion detection. A separate paper presented by MSU at this NISSC 2000 conference discusses the results we have achieved with an intrusion detection system we developed and applied to an typical distributed system. This system employees some unique artificial intelligence techniques and has achieved lower false positive and false negative rates than one normally expects to achieve. We have begun to move this system to a cluster environment and will modify its architecture over the next year to accommodate the HPC processing needs – yet still alert when an intrusion is discovered.

This presentation will outline our HPC research to date and our future plans. It is designed to give the audience a sense of what research is being accomplished, why it is of interest, and expected results.

Statement on:
Issues in High Performance Computing Security

Yvo Desmedt
Department of Computer Science, Florida State University
Tallahassee, FL 32306-4530
desmedt@cs.fsu.edu http://www.cs.fsu.edu/~desmedt

The allegations against a Los Alamos computer expert have confirmed, once more, that not only outsiders, but also insiders, can be a threat. So, only a very limited security can be achieved by not connecting high performance computers to the internet. However, the need for high performance computers, and their price, make sharing such resources attractive. Moreover, the work on Internet2 has demonstrated that Gbit/sec. Wide Area computer Networks are feasible. This makes the sharing of high performance computers even more attractive. Although the speeds of computer networks is increasing enormously, the difference in delay in internal communication and in external communication will remain (or even increase). The delay in external communications makes it much easier to deal with protecting the network security aspects of high performance computers against outsiders than to address the internal security problems. We therefore focus on the latter.

High performance computers have to deal with, not only, the same security problems as other computers have, but have also to deal with special security concerns. However, addressing and implementing solutions to the traditional security problems on high performance computers is harder, since the steps taking to address these problems should not decrease the performance of these computers. For example, separation, whether achieved, e.g., by time scheduling different jobs, or using cryptography, needs a special design, which may reduce the sharing flexibility, the security, or the performance. We now discuss some of these security concerns typical for high speed computers.

In a traditional computer, software should be protected against copyright violations. Seeing the nature of several applications that need high performance computers, the software should remain secret. Encrypting the data on the buses is not enough to achieve such a property. An insider having physical access to the machine can still observe when a loop takes place, which memory addresses are being used, how often, etc. However, addressing this issue successfully opens another problem: the one of covert computation.

The problem of covert computation is not limited to the case the software being used as cover is secret, but also when the latter is public. For example, can the software used to factor a large integer, be used covertly to compute problems related to the design of a nuclear weapon?

Issues in High Performance Computing Security

Security in a Computational Grid Environment

Douglas E. Engert
DEEngert@anl.gov
Argonne National Laboratory

Increasingly, independent institutions with similar goals and interests are forming loosely coupled virtual organizations for collaboration and resource sharing. The construction of virtual organizations is hampered, however, by two conflicting goals: all members of the organization should have access to a resource as if it was their own, but participating institutions must not be required to change local security mechanisms or surrender control over their access control policies.

Users themselves can form their own virtual computing environments, when they have resources allocated to them by different organizations. This is very common in the research environment, where a researcher has multiple grants.

A distributed application may then be run across multiple systems at multiple organizations, where there may be many communication channels setup between all the processes comprising the application. The user may have initiated all of this from some other site as well.

This environment goes far beyond the simple client server security model. Not only is security needed for the initial invocation of the application at each site, but communication channels between processes also need security.

The Globus Project, http://www.globus.org, has developed the Grid Security Infrastructure (GSI), an authentication and authorization infrastructure that meets these requirements. GSI capabilities include single sign-on, no plaintext passwords, proxy credentials, mapping to local security mechanisms (including Kerberos, DCE/DFS and AFS), site control over access control policies, and user controlled delegation. The GSI is a set of libraries and tools which implements a GSS-API using the SSL protocols with X.509 certificates.

GSS delegation is accomplished by the use of "proxy" certificates, certificates signed by the user or previous "proxy". These can then be used in an SSL certificate chain. Process to process authentication can be accomplished using these "proxy" certificates. "Limited proxy" certificates and also be issued which can not be delegated, and only used for the process to process authentication. Work is under way to improve the methods used to limit the authority of the proxy certificates.

Since the GSI implements GSS, a number of other applications have been extended to include GSSAPI, including SSH and a number of different versions of FTP clients and servers. GSI supports smart cards via PKCS#11.

Security in Depth

Mr. Jesse Pollard
DOD Major Shared Resource Center (MSRC)
Naval Oceanographic Office
Stennis Space Center, MS
(228) 688-5308

High performance computing needs a high level of assurance that its resources, and information, are secure. A problem with obtaining this high assurance is the need for user cooperation along with security policies. This cooperation is not always available. The user may be running insecure applications or the overhead of using security practices may be considered too onerous. It appears that much of "security" has become "network security" - ignoring the fact that "network security" really depends on "host security." This is primarily due to the difficulty of enforcing security policies at the host, and getting users to practice good security procedures.

Using routers and firewalls to implement "network security" is exceptionally difficult because they do not have enough context for many security decisions. They can, however, support reliable and effective communication control. They can also enforce some facility level of control (based strictly on the host/port addressing). Routers and firewalls may not make communication decisions other than those established by address/port/protocol lookup tables. Additional decisions are prevented since the necessary context is not available.

The additional context needed for security decisions is based on the user identification and classification. For example, is the user allowed to communicate with the remote host/port or allowed to use the local port number or to establish a communication link using the current data classification? The target host also has to make decisions. For example, is the remote user (from the view of the target host) allowed to communicate with the local host/port or use the facilities attached to the port (e.g., daemon services, such as telnetd), or establish communication at the requested security classification? In both situations (local and remote hosts), is encryption required?

Most of these situations can be handled by a complete implementation of the IPSec specification. A complete implementation must include the ability to pass identification and security classification of the user on the local host. This ability can be used by the remote system to complete the security decisions needed to establish communications.

After a secure communication path is established, it is still necessary to protect the local host. This capability is best done with the use of multi-level security (MLS). MLS can be used to protect the host from internal attack, and not just to protect information. Mandatory controls can be used to prevent the possibility of modifying system code or configuration. It can also be used to provide the security classifications needed for decisions allowing remote connections. The accompanying presentation addresses these issues and others in managing a High Performance Computer System from a system administration point of view.