IRIX™ Security - Present and Future

Jay McCauley, Silicon Graphics Computer Systems, Inc.,
Mt. View, California

ABSTRACT: *This paper discusses the current state of security related products for the IRIX™ operating system, and how future products will combine the best security features from the IRIX and Unicos® operating system environments. All of the products mentioned here are more completely described in available product literature and in most cases, web pages at http://www.sgi.com.*

Background

Silicon Graphics® systems serve a wide breadth of markets with radically different security needs. A significant portion of the customer base works in isolated, collaborative environments in which ease of use is of paramount importance. To support these users, the concentration has been on improving the ease of system administration from the desktop. In the middle of the security spectrum are customers in less benign environments which must be protected from the outside Internet community and must provide credible mechanisms for the protection of intellectual property. We address this market segment with system features such as auditing of security relevant events, and with add on products such as the Gauntlet™ firewall. At the far end of this spectrum are the military and intelligence community customers who need systems compliant with the requirements for processing classified information in a multi-level security setting. These customers are served with the Trusted IRIX™/CMW offering. The remainder of this talk will expand upon these products and features. I will conclude with a discussion of how these products and features will be combined with similar developments from the Unicos environment to produce a "best in breed" security environment for the future SN1 family.

Desktop Administration Enhancements for Security

The model for the administration of personal workstations is to provide a rich GUI which makes it easy to setup the system and administer it. In the recently introduced O2™ system, new features have been added to the desktop to allow control over the system security setup. These features permit the user to exert fine grained control over such aspects of the system as network accessibility, NFS export and password control. The goal is to make it easy for a relatively unsophisticated user to setup the system in a secure way, while preserving the flexibility that collaborative workgroups require.

The Indigo Magic™ desktop environment includes a flexible, real time monitor for the System Log, *sysmon*. The alerter scripts can be locally customized to provide indication of security relevant events, and invoke arbitrary programs in response. A similar capability has been developed for the security audit log in Trusted IRIX. This is an area of active academic research, and we expect to see more sophisticated intrusion detection systems incorporating the fruits of this research.

C2 Security Features

The system software originally developed in the Trusted IRIX/B 4.0.x systems was incorporated into the main source tree for IRIX. This gives the current commercial versions of IRIX the features necessary to meet the C2 requirements of the Orange Book. Because SGI had a B1 system in formal evaluation, we elected not to seek formal evaluation of these features by the National Computer Security Center. Thus, the system is "designed to meet" the C2 requirements but has not been formally evaluated. The primary C2 features are the security audit trail mechanism and the implementation of shadow passwords.

The security audit trail machinery consists of the generation of binary coded audit records at each point that a security decision is made in the IRIX kernel and in trusted applications (e.g. login). These records are then written to audit trail files by a daemon. There is a surprisingly large volume of audit records

generated if all decisions are recorded. For example two security decisions were made on every packet transmitted or received by the networking software in Trusted IRIX/B. The high volumes of audit records expected in the largest configurations of the new Origin 2000™ or the SN1 systems in the future are the focus of significant collaborative design efforts between the security software teams at Silicon Graphics and Cray Research.

Commercial Security Pak™

The Trusted IRIX team has recognized that the military security model ("Mandatory Access Control", MAC) is inappropriate for most commercial organizations. However, there are a number of features developed in Trusted IRIX that are applicable to the commercial world. We are in the process of packaging these into an add on product for the IRIX operating system, the Commercial Security Pak. The major features planned for this product are:

- Access Control Lists (ACLs) compliant with the POSIX P1003.1e/.2c Draft 16 specifications
- Capabilities (Least Privilege) also compliant with P1003.1e/.2c
- Kerberos V5 integration

ACLs provide the system with much finer control over the access to files. Associated with a file or directory is an optional ACL which specifies per user or per group permissions for the file. These may extend or restrict access to the file. Directories have a second, default ACL (also optional) which is applied to a newly created files or subordinate directories, similarly to the functions of *umask.*

Capabilities allow precise definitions of exactly what a privileged program can do. Briefly, the classic binary privilege scheme (root Vs everybody else) is replaced by a fine grained scheme with approximately 45 distinct privileges. These are initialized on a per user basis, allowing the use of "roles". Privileges are also associated with files analogously to the setuid bits. Well written trusted programs raise a specific set of privileges around a trusted system call, and lower them after the call, a structure called "privilege bracketing". Surprisingly few system programs in Trusted IRIX need privileges, only around 100 programs there are privileged. Commercial systems may have functions which are not supported in Trusted IRIX, but the number of privileged programs should be small. The number of programs needing powerful privileges (e.g. override the system access control rules) is extremely small. It is possible to configure a system with the Commercial Security Pak in a way that UID 0 does not convey special privilege, which is the way Trusted IRIX is shipped.

The Commercial Security Pak 1.0 also will provide the first steps towards an eventual goal of strong authentication support throughout the system. The initial version will provide integration of the Kerberos V5 environment with the IRIX Identification and Authentication utilities. With help from the Cray team in Eagan, we have demonstrated a single signon capability between IRIX and Unicos in a laboratory setting.

Internet Security Products

SGI has placed a major emphasis on providing Internet servers, particularly WWW servers. On systems exposed to the "raw" Internet, it is common to include Internet firewall services on these systems. Working with the leading Internet firewall provider, Trusted Information Systems, Inc., SGI has ported the TIS Gauntlet product into the IRIX environment. This port utilizes the basic IP filtering capabilities that have been available in IRIX for some time. In addition, Gauntlet provides:

- proxy services which allow users inside the firewall to reach sites on the outside in a transparent, safe manner
- Virtual Private Network services which let two systems communicate securely (using cryptographic techniques) over an insecure Internet
- authentication device support for popular devices which eliminates the transmission of passwords over the net "in the clear"

Internet commerce is an area of intense activity and great promise. SGI has formed strategic partnerships with many of the industry leaders in the field. Some of the hottest sites on the web are "Powered by SGI" systems. True commerce requires secure transaction services for the protection of the customer and the vendor. Products such as the Netscape Commerce Server®, available on IRIX, allow secure transactions using cryptographic techniques. Web serving poses new challenges for the system as it has a much different activity profile than other networking activity. The challenge for the system is how to support high volumes of secure transactions.

Support for Security Issues

The World Wide Customer Support organization has several individuals dedicated to system security issues. This includes monitoring network news groups and other information sources for new threats to the system. Customer support works closely with engineering for assessment of the threat and for responses to real problems. Patches are generated as necessary, and the appropriate alerting information is forwarded to customers and reporting organizations like CERT. Like many other parts of our business, we have web pages for security. This allows very rapid access to the data from anywhere around the world. Go to:
http://www.sgi.com/Support/Secur/security.html
for the latest information.

Trusted IRIX

Trusted IRIX is now an add-on package for the base IRIX environment. It is integrated with the main source tree and will be released with a few months of major OS releases. The major components that are added by Trusted IRIX are:

- MAC support, and the enforcement of the system's MAC policy

- Mandatory Integrity (MINT). Mathematically the dual of the MAC mechanisms, MINT provides protection of the Trusted Computing Base (TCB).
- Multi-level directories
- Security event auditing
- Trusted Networking. Systems inform each other about the MAC labeling and other information about the connection endpoints, allowing security policy to be enforced on network applications.
- Labeled printing and tape support. Provides MAC/MINT labels on input and output.
- Trusted windowing. Allows windows (and other X objects) to have labels and enforces system security policy on access to them.
- Access Control Lists
- Capabilities
- Audit Alerter

A key element of trusted systems work is the evaluation of the system security properties. The National Computer Security Center (NCSC) has formally evaluated Trusted IRIX/B 4.0.5 EPL at the B1 level, and placed it on their Evaluated Products List in March, 1995. SGI and NSA are working together on the formal evaluation of Trusted IRIX/CMW as a joint B1/C2 Orange Book/Red Book/Common Criteria environment. One of the important aspects of this evaluation is the use of WWW technology for the management of the highly complex submittal package. This has the promise of making the evaluation both more timely and more complete, as well as being much easier to create and access. Separately, SGI is pursuing and ITSEC evaluation of Trusted IRIX/CMW in the United Kingdom. Since the security architecture of the system changes very slowly, we anticipate that much of the evaluation will be directly relevant to future versions of the system for the SN1 family and beyond.

For the SN1 system, the plans are to incorporate the best features from the security products for IRIX and Unicos. The teams are already working closely together, as evidenced by the joint development of single signon support for IRIX and Unicos. The Unicos team will be hitting some of the toughest problems slightly before the IRIX team. For example, there are some novel ideas for handling the volume of audit records in T3E that will blaze the trail for the auditing in SN1. The Program Access List feature in Unicos has some interesting potential and is planned for future incorporation into IRIX.

Visions for the Future

The marketplace is placing increasing demands on the security features of the system. While it is not possible to make formal commitments for future products, some trends and goals are fairly clear.

First, there is an undeniable increase in the importance of system security features. As functions such as Internet commerce take off, security features are a crucial, integral part of the product. These products are based on cryptographic techniques which are quite CPU intensive in high volume applications. This places a priority on providing hardware assistance for those cases. The reliable use of client/server environments will require improved authentication techniques and their integration with common services such as the RPC libraries and NFS. Since a no clear winner has emerged in the authentication space, these techniques must be flexible enough to accommodate a variety of techniques and devices. These client/server structures are also vulnerable to denial of service attacks, such as the recently publicized SYN attacks on Internet Service Providers. In the future, the system must provide either credible, strong authentication or rate limiting on un-authenticated services. These issues will, I believe, accelerate the pressure on IPSEC and IP V6 availability, as these new protocols address many of these issues.

Trademarks