White Paper

SGI® Altix® Security

November, 2004

Table of Contents

1.0 Abstract

SGI has recognized the need for operating system security for many years. SGI was the first company to support Multi-level Security (MLS) for computer data by achieving certifications for Common Criteria for IT Security Evaluation (ISO Standard 15408) for both Controlled Access Protection Profile (CAPP) and Labeled Security Protection Profile (LSPP) for SGI® IRIX® and SGI® Trusted IRIX™, respectively. SGI follows standard operating procedures to ensure timely and orderly service for security issues to our customers. SGI is a member of FIRST, a coalition of individual response teams around the world, and other industry-wide security organizations. SGI tracks security issues, alerts, advisories and updates, and rapidly addresses software breaches with immediate patches and longer-term solutions as soon as possible.

In addition, SGI has closely followed the industry standards for computer security and has incorporated the functionality into SGI IRIX as they have become available. With arrival of Linux® in corporate computer use, SGI continues to leverage our experience and incorporate computer security as a required feature for SGI Altix systems.

Computer security has become even more important and essential to organizations following 9/11 and the increasing virus and hacker attacks to computer networks. Unfortunately, most computers are subject to lapses in security. However, years of research in computer security have resulted in many solutions that make a computer system more secure in small to large computer networks.

2.0 What is Computer Security?

Computer security can be segmented into three areas:

- Network Security
- Trusted Environments
- User and Application Security

With the spread of computer networks worldwide, many industry standards have been developed to manage firewalls, virtual private networks, and higher levels of encryption in order to ensure data integrity and to prevent network intrusion, denial of access, data theft, and other attacks. Many of the technologies which started as proprietary are now Open Source software which has been incorporated in all the operating systems both proprietary and community developed. For example, OpenSSL secure sockets layer and strong cryptography library are used by OpenSSH for encrypting network traffic and by OpenLDAP for directory services. Networking hardware and software and network security has become a standard part of a computer system.

Trusted environments are operating systems that attempt to provide a secure environment for the development and storage of sensitive information. In reality, no system is perfectly secure from harm, so the term trusted is used instead of secure. Trusted environments have gone beyond securing the physical disk device with a lock and key or storing the system in a locked room with an armed guard. As you may know, with computer networks, almost anyone can access unprotected data. In many corporations, government organizations, universities and research facilities, it is a requirement to log accesses to certain data or restrict access to data by types of users. The results are operating system features like access control lists, auditing, authentication, and discretionary and mandatory access control.

In addition, industry certifications have been created to maintain the same level of trusted quality worldwide. The Common Criteria for IT Security Evaluation provides worldwide recognition for evaluations and certifications of IT security products and their levels of trust. IT security products can range from computer operating systems, computer systems, to peripherals. Each country has their own Common Criteria organization to evaluate and certify products. It does not matter where the evaluations and certifications are done, all the countries follow the same guidelines and recognize each other's evaluations and certifications. Two of the certifications, that apply to operating systems and their associated hardware systems, are Common Criteria for IT Security Evaluation (ISO Standard 15408) Controlled Access Protection Profile (CAPP) and Labeled Security Protection Profile (LSPP). Some projects require Multi-Level Security (MLS) support whose functionality is defined by LSPP and mandatory access control.

User and application security applies to how applications are managed on a user's system. Many different types of tools are available for protecting the user and their applications. Software licensing was developed to protect intellectual property for Independent Software Vendors by preventing software pirating. Password management tools prevent hackers from breaking into systems. Some functions of password management tools are encrypting the passwords, monitoring the age of passwords, and keeping a history of previously used passwords. Pluggable Authentication Modules were developed to provide user authentication for applications. Over the years, these features have become ubiquitous to all operating systems including Microsoft® Windows®, UNIX®, and Linux®.

3.0 Security Features for SGI Altix

Security features for SGI Altix systems are provided by the underlying Linux operating system. Today, users have the choice of SGI Advanced Linux™ Environment, based on Red Hat® Enterprise Linux (RHEL), or Novell's SUSE Linux Enterprise Server (SLES).

Network Security for SGI Altix:

Network security for SGI Altix systems is supported by the foundation Linux operating system. With SGI Altix, you have the choice of SGI Advanced Linux Environment or Novell® SLES. The Linux community has incorporated the industry standard network security interfaces into its kernel, these include support for:

- 128-bit encryption
- OpenSSH Secure Shell
- OpenSSL Secure Sockets Layer & Strong Cryptographic Library
- IPsec Virtual Private Network support
- Ipchains Firewall
- TCP Wrappers

Trusted Environment for SGI Altix:

The Linux community has embarked on The Common Criteria (CC) Controlled Access Protection Profile (CAPP) evaluations. This protection profile is based on the C2 class of the "Department of Defense Trusted Computer System Evaluation Criteria" (DOD 5200.28-STD).The Common Criteria Controlled Access Protection Profile specifies a set of security functional and assurance requirements for Information Technology (IT) products. CAPP-conformant products support access controls that are capable of enforcing access limitations on individual users and data objects. They also provide an auditing functionality which records the security-relevant events which occur within the system.

Recent announcements have been made for Linux systems achieving or planning CAPP evaluations with both Red Hat Enterprise Linux Advanced Server 3 and Novell® SUSE Linux Enterprise Server 8, SP3. SGI is pursuing The CAPP with SUSE Linux Enterprise Server with SGI ProPack™ and expects to achieve CAPP at EAL/3+ by Q3 CY 2005. The Common Criteria certification process is not new to SGI. SGI was the first company to certify MIPS® and IRIX® systems at Common Criteria CAPP EAL3 and LSPP EAL3.

Novell SLES supports the basic components required for CAPP certification including access control lists (ACLs), capabilities, and auditing via Linux Audit System. Novell has already achieved CAPP at EAL/3+ with IBM and is working toward EAL/4+ level. Support for CAPP from a variety of hardware vendors ensures users of the highest security attainable today with Linux.

For the SGI Advanced Linux Environment, SGI supports SNARE for auditing. SNARE is Open Source software from Intersect Alliance (www.intersectalliance.com). SNARE has been ported and extended to support multiprocessor systems and runs on the SGI Advanced Linux Environment. SNARE for Altix is available today to all SGI Altix customers requiring RHEL.

Today, Linux systems are not certified for LSPP. Mandatory Access Control is the missing feature* in Linux required for LSPP. The Linux community is working today to provide the functionality to meet the Common Criteria LSPP evaluation requirement and expects to achieve LSPP evaluation in late 2005. SGI and Novell expect to leverage the NSA's SELinux project, which provides a Mandatory Access Control implementation for Linux. SGI will be pursuing LSPP with Novell SLES with SGI ProPack as soon as LSPP is achievable.

Multi-Level Security (MLS) is defined as the ability to compartmentalize user interactions according to specific security labels as defined by the site administrator. For example, a two security level environment can be defined as unclassified and classified or many levels of security can be defined. For implementing Multi-level Security environments today with your SGI® systems, a guard box configuration may work for your environment. As the guard box, a SGI® Origin® 350 system runs Trusted IRIX and manages systems across your network that will each have its own classification level. In this configuration, SGI Altix systems run at a single classification level alongside other systems running at the same or different classification levels. In the future, SGI expects to have SGI Altix systems capable of supporting MLS once the Common Criteria Security LSPP certification is complete.

User and Application Security for SGI Altix:

The Linux community has incorporated the industry standard interfaces for user and application security. In addition, there are third-party solutions to provide tools for system management areas.

SGI Advanced Linux Environment and Novell SLES both support SGI Altix. The user and application security features include:

- 128-bit encryption
- Pluggable Authentication Modules

* SLES9 provides SELinux as an unsupported feature
Fedora 3 (FC3) provides SELinux as a beta feature.

- Kerberos
- RSA Authentication
- Secure Key Generation
- Password Management
- Secure E-mail, DNS

4.0 Security Standards

Over the years, industry standards have emerged for computer security. Besides Common Criteria Security CAPP and LSPP, there are US government-mandated requirements that can be called “standards”. Of note, there is the DISA Common Operating Environment (COE), which requires security features such as auditing. SGI supports COE Version 4.2p6 for SGI systems with MIPS processors and SGI IRIX and intends to certify SGI Altix systems in the near future. Also, the US government NISPOM Chapter 8 regulation is supported in SGI Advanced Linux Environment for SGI Altix systems and in SGI IRIX for SGI systems with MIPS processors.

5.0 Conclusion

SGI understands your need of computer security for your systems. We are actively monitoring the latest developments in computer security for Linux. We are working with our Linux operating system partners and customers to improve computer security for SGI Altix systems. We welcome your feedback and suggestions for future security feature improvements.

6.0 References and Resources

See SGI Technical Documentation at www.techpubs.sgi.com for:

- Trusted IRIX/CMW Security Administration Guide (document number: 007-3299-009 / published: 2003-12-04)
- Trusted IRIX/CMW Security Features User's Guide (document number 007-3300-005 / published: 2003-12-04

White Papers:
Trusted Computing, the SGI Solution (www.sgi.com/pdfs/3185.pdf)
Multilevel Security (MLS) by Trusted IRIX white paper (www.sgi.com/pdfs/3241.pdf)
SGI Support and Value Add to the Common Operating Environment (www.sgi.com/pdfs/3174.pdf)

Web Pages:
Online SGI Security Support (www.sgi.com/support/security/)
SNARE (www.intersectalliance.com/snareserver/index.html)

Corporate Office
1500 Crittenden Lane
Mountain View, CA 94043
(650) 960-1980
www.sgi.com

North America +1 800.800.7441
Latin America +55 11.5509.1455
Europe +44 118.925.7500
Japan +81 3.5488.1811
Asia Pacific +1 650.933.3000

©2004 Silicon Graphics, Inc. All rights reserved. Silicon Graphics, SGI, IRIX, Altix, Origin, the SGI logo and the SGI cube are registered trademarks and Trusted IRIX, SGI Advanced Linux, SGI ProPack and The Source of Innovation and Discovery are trademarks of Silicon Graphics, Inc., in the U.S. and/or other countries worldwide. Linux is a registered trademark of Linus Torvalds in several countries used with permission by Silicon Graphics, Inc. MIPS is a registered trademark of MIPS Technologies, Inc. UNIX is a registered trademark of The Open Group in the U.S. and other countries. Microsoft, and Windows are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat and all Red Hat-based trademarks are trademarks or registered trademarks of Red Hat, Inc. in the United States and other countries. All other trademarks mentioned herein are the property of their respective owners. “Product plans, descriptions, and dates are estimates only and subject to change without notice.” This articlecontains forward-looking statements regarding SGI technologies and third-party technologies that are subject to risks and uncertainties. These risks and uncertainties could cause actual results to differ materially from those described in such statements. The reader is cautioned not to rely unduly on these forward-looking statements, which are not a guarantee of future or current performance. Such risks and uncertainties include long-term program commitments, the performance of third parties, the sustained performance of current and future products, financing risks, the ability to integrate and support a complex technology solution involving multiple providers and users, and other risks detailed from time to time in the company's most recent SEC reports, including its reports on Form 10-K and Form 10-Q.

3719 [11.03.2004]

J14747