INNOVATION
FOR RESULTS™

White Paper

SGI® Linux® Security

Abstract

SGI has long recognized the need for improved operating system security. SGI is participating in the widespread adoption of Linux and its penetration into markets where security is critical and mandated. This white paper provides an overview of computer security, discusses security standards, and describes the efforts that SGI has made to certify standard Linux distributions running on SGI platforms.

Table of Contents

1 Introduction

SGI has been pursuing enhancements to operating system security for many years. SGI was the first system provider to support Multi-level Security (MLS) for computer data through 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™.

With the widespread adoption of Linux and its penetration into markets such as government and defense where security is critical and mandated, SGI is taking steps to ensure that security improvements are available on SGI Linux platforms. At the same time, SGI is pursuing an aggressive certification strategy to attain security certifications for SGI hardware running the standard Linux releases.

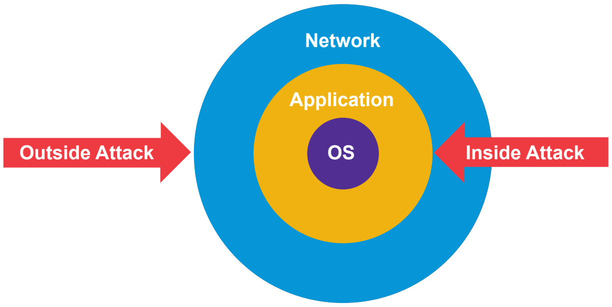
This white paper reviews SGI Linux security efforts and ongoing security certification program.

2.0 What is Computer Security?

Computer security can be segmented into three areas:

- Network Security
- User and Application Security
- Operating System Security/Trusted Environments

Network security using firewalls is typically the first line of defense against outside attack for most organizations. Secure network protocols also prevent data from being compromised as it traverses internal or external networks. User and application security provides the next line of defense, and the first line of defense against security breaches from inside the organization. The operating system is the last line of defense. A significant security breach of an operating system offers the most opportunity to access sensitive data and/or disrupt critical services.



For **network security**, industry standards have been developed for firewalls, virtual private networks, and network encryption in order to ensure data integrity and to prevent network intrusion, denial of access, data theft, and other attacks. Networking hardware and software and network security have become a standard part of a computer system.

Many technologies which were initially proprietary are now Open Source software, and have been incorporated in both proprietary and community-developed operating systems. For example, OpenSSL secure sockets layer and strong cryptography library are used by OpenSSH for encrypting network traffic and by OpenLDAP for directory services. IPsec (IP security) is a suite of protocols that secure communication through authentication and/or encryption of each IP packet. IPsec is optional for use in IPv4 (the current version of the Internet Protocol) but will be mandatory in IPv6. It is already available in standard Linux distributions.

User and application security applies to how applications and user data are managed on a computer system. Many different tools are available to protect user information and applications. 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. Encryption tools and libraries keep sensitive data encrypted within a system. Over the years, these features have become ubiquitous to all operating systems including Microsoft® Windows®, UNIX®, and Linux®.

Trusted environments utilize operating systems that provide a secure environment for the processing and storage of sensitive information. In reality, no system is perfectly secure from intrusion, 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. On computer networks, almost anyone can potentially 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 user type. Operating system features such as access control lists, auditing, authentication, and discretionary and mandatory access control have been developed to address such requirements.

How do you know how secure your operating environment is? Industry certifications have been created to define security criteria and ensure the same standards of security are followed worldwide. The Common Criteria for IT Security Evaluation provides worldwide certifications of IT security products (including computer operating systems, computer systems, and peripherals) at clearly defined levels of trust. The standard has been in place since 1999. The Common Criteria organization includes 16 member countries worldwide, with testing laboratories in several of those countries to evaluate and certify products. Two 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).

3.0 Security Standards

Over the years, a number of security standards has emerged. This white paper discusses the Common Criteria standards, particularly CAPP, LSPP, and RBAC which have been derived from earlier standards.

CAPP conformant products support access controls that are capable of enforcing access limitations on individual users and data objects. CAPP-conformant products also provide an audit capability which records the security-relevant events which occur within the system. The CAPP provides for a level of protection which is appropriate for an assumed non-hostile and well managed user community requiring protection against threats of inadvertent or casual attempts to breach the system security. The profile is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well funded attackers to breach system security. CAPP was derived from the requirements of the C2 class of the U.S. Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC).

LSPP conformant products support access controls that are capable of enforcing access limitations on individual users and data objects. Specifically, two classes of access control mechanisms are provided: those that allow individual users to specify how resources (e.g., files, directories) under their control are to be shared; and those that enforce limitations on sharing among users. The latter is implemented by the use of security markings (i.e., “labels”). LSPP-conformant products also provide an audit capability which records the security-relevant events which occur within the system. The LSPP was derived from the requirements of the B1 class of the U.S. Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC),Projects that require Multi-Level Security (MLS) support can achieve that functionality through LSPP and mandatory access control.

Role Based Access Control (RBAC) is an alternative method of restricting computer system access. With RBAC, the ability to perform certain functions is restricted based on a user’s assigned role or roles. Users acquire permission to perform certain actions through the assignment of a specific role or roles to their accounts rather than the creation of specific permissions or ACLs on files. When a user changes job functions with an organization, his or her account is simply re-assigned to the appropriate roles to grant permission to perform the new functions (and revoke permission to perform old functions if appropriate).

4.0 SGI Linux Security

SGI Altix and Altix XE platforms are able to execute the following standard Linux distributions:

- Red Hat Enterprise Linux
- Novell SUSE Linux Enterprise Server

As a result, SGI Linux platforms deliver the standard network, application, and OS security features of the particular operating system chosen.

To provide forthe security of each operating environment running on SGI hardware, SGI has also undertaken Common Criteria for Information Security Evaluation and Validation testing on each operating system running on SGI hardware. When a Common Criteria Evaluation is carried out, that evaluation pertains to a specified set of hardware and software, referred to as the Target of Evaluation (TOE).. The security of the operating software is evaluated when running on the specified hardware and the hardware itself is evaluated to correct design flaws that can facilitate non-secure access through back doors, etc.

The following sections describe current and ongoing security evaluations on SGI Linux hardware.

5.0 Current SGI Linux Security Certifications

SGI has current security certifications on both Red Hat Enterprise Linux 4 and SUSE Linux Enterprise Server 9.

5.1 Red Hat Enterprise Linux Version 4

Date of Completion: September 15, 2006.
Operating System: Red Hat Enterprise Linux AS Version 4 Update 4
Hardware: SGI Altix 4000 and 400 systems
Validated encryption methods: TDES, AES, SHS, RSA
Certification: CAPP EAL3+
Strength of Function: Medium

Security Features Validated:

- **Identification and Authentication:** The TOE provides identification and authentication using pluggable authentication modules (PAM) based upon user passwords.
- **Audit:** The TOE provides the capability to audit a large number of events including individual system calls as well as events generated by trusted processes.
- **Discretionary Access Control:** Discretionary Access Control (DAC) restricts access to file system objects based on Access Control Lists (ACLs) that include the standard UNIX permissions for user, group and others.
- **Object Reuse:** File system objects as well as memory and

IPC objects will be cleared before they can be reused by a process belonging to a different user.
- **Security Management:** The management of the security critical parameters of the TOE is performed by administrative users.
- **Secure Communication:** The TOE supports the definition of trusted channels using either the SSH v2 or the SSL v3 protocol.
- **TSF Protection:** While in operation, the kernel software and data are protected by the hardware memory protection mechanisms. The memory and process management components of the kernel ensure a user process cannot access kernel storage or storage belonging to other processes.

In essence this certification means that the operating system running on the target SGI hardware has been validated and found to conform to Evaluation Assurance Level 3 and that it exceeds this level in some areas (EAL3+). EAL3 is applicable where a moderate level of security is required. In general, EAL definitions provide for levels 1-7. Levels 5-7 are typically restricted to specially engineered secure systems. Levels 1 through 4 are generally applicable to more widely available commercial hardware and software. For those who are more familiar with the older security standards, CAPP EAL3 certification is equivalent to the Trusted Computer System Evaluation Criteria (TCSEC) C2 class of the US Department of Defense (The Orange Book).

5.2 SLES9

Date of Completion: October, 2005
Operating System: SUSE Linux Enterprise Server 9 with Service Pack 2
Hardware: SGI Altix Bx2 and A350 systems
Validated encryption methods: None
Certification: CAPP EAL3+
Strength of Function: Medium

Security Features Validated:
- Identification and Authentication using pluggable authentication modules (PAM) and a password-based authentication mechanism.
- Audit using the LAuS system with associated administrative interfaces.
- Discretionary Access Control (DAC) providing the standard UNIX permission bit mechanism and access control lists (ACLs) on the ext3 and XFS file system
- Object reuse functionality to clear file system and memory objects before re-use
- Security Management performed by administrative users
- Secure communication is provided with applications implementing the SSHv2 and SSLv3 cryptographic protocols when communicating over insecure networks
- TSF Protection: TSF data is protected by the DAC mechanism. Kernel software and data are protected by hardware protection mechanisms provided through the TOE environment.

In essence this certification means that the operating system running on the target SGI hardware has been validated and found to conform to Evaluation Assurance Level 3 and that it exceeds this level in some areas (EAL3+). EAL3 is applicable where a moderate level of security is required and is equivalent to the Trusted Computer System Evaluation Criteria (TCSEC) C2 class of the US Department of Defense.

The strength of function claim applies to the password based user authentication function only. No strength of function claim was made for the cryptographic functions provided by the TOE or related functions such as key generation functions and cryptographic hash functions.

6.0 Security Certifications in Progress

The existing security certifications described above are suitable for environments that require moderate security, but don’t meet the requirements of many government and defense applications. For that reason, SGI is undertaking an additional security certification during 2007 using Red Hat Enterprise Linux 5 (RHEL5) running on currently available Altix and Altix XE platforms.

RHEL5 is currently in evaluation by the National Information Assurance Partnership (NIAP) for three protection profiles. The three protection profiles are:
- Controlled Access Protection Profile, Version 1.d
- Labeled Security Protection Profile, Version 1.b
- Role Based Access Control (RBAC) Protection Profile Version 1.0

SGI will seek certification for all three of these profiles.

The new LSPP and RBAC functionality has been co-developed by the NSA for security enhanced Linux (SELinux) in conjunction with IBM, HP and Red Hat and accepted into the community Linux source tree. This level of functionality is considered suitable for Department of Defense and other secure sites, providing the equivalent of B1 security or greater with Multi Level Security (MLS). MLS ensures that users with different security clearances can only access information they are cleared to view.

7.0 Conclusion

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

8.0 References

- **NSA Information Assurance:** http://www.nsa.gov/ia/industry/niap.cfm
- **Cryptographic Standard Validation lists:** http://csrc.nist.gov/cryptval/140-1/avallists.htm
- **Security Enhanced Linux:** http://www.nsa.gov/selinux/
- **RedHat Security:** http://www.redhat.com/security/
- **Novell SUSE Security:** http://www.novell.com/linux/security/mission.html

9.0 Glossary

ALC_FLR.3. Flaw remediation practices. The “+” in designations such as EAL3+ refer to this capability.

AUDITING. An audit subsystem allows a system administrator to keep a detailed and precise log of all system activity.

Common Criteria (CC). An international standard derived from the US Orange Book and Europe’s ITSEC. This standard is recognized by 16 countries and administered in the United Kingdom by a GCHQ division called the Communications-Electronics Security Group (CESG), which grades products based not only on their security and reliability but also on the development and support processes that ensure quick responses to problems.

SGI provides Common Criteria security certified solutions, including:

- 2002 LSPP, Trusted IRIX/CMW on Origin/Mips platforms (NIAP)
- 2002 CAPP, IRIX version 6.5.13 on Origin/Mips platforms (NIAP)
- 2005 CAPP, SLES9 SP2 on Altix/ia64 platforms (BSI)
- 2006 CAPP, RHEL4 U4 on Altix/ia64 platforms (NIAP)

CC CAPP. Controlled Access Protection Profile. Roughly equivalent to the Orange Book C2-level.

CC LSPP. Labeled Security Protection Profile. Roughly equivalent to Orange Book B1-level.

CC RBAC. Role Based Access Control Protection Profile. From the NIST Role Based Access Control web page:

One of the most challenging problems in managing large networks is the complexity of security administration. Role based access control (also called role based security), as formalized in 1992 by David Ferraiolo and Rick Kuhn, has become the predominant model for advanced access control because it reduces the complexity and cost of security administration in large networked applications. Most information technology vendors have incorporated RBAC into their product line, and the technology is finding applications in areas ranging from health care to defense, in addition to the mainstream commerce systems for which it was designed.

EAL1-EAL7. Evaluation Assurance Levels:

- EAL1 - functionally tested.
- EAL2 - structurally tested.
- EAL3 - methodically tested and checked.
- EAL4 - methodically designed, tested and reviewed.
- EAL5 - semiformally designed and tested.
- EAL6 - semiformally verified design and tested.
- EAL7 - formally verified design and tested.

MAC. Mandatory access control. This mechanism allows the system administrator to assign security classification labels to files and directories and security clearance labels to users.

Multi-Level Security (MLS). MLS operating systems compartmentalize user interactions according to specific Mandatory Access Control (MAC) labels. This allows the administrators to set up policies and accounts that will allow each user to have full access to the files and resources he or she needs, but not to information and resources not necessary to perform the assigned task.

NIAP. The National Information Assurance Partnership (NIAP) is a U.S. Government initiative that originated to meet the security testing needs of both information technology (IT) consumers and producers. It is operated by the National Security Agency (NSA).

TCSEC. US Department of Defense Trusted Computer Systems Evaluation Criteria, otherwise commonly known as Orange Book. Trusted IRIX 4.0.5 was evaluated and achieved Orange Book B1-level security certification. This is an older standard that has now been largely superseded.

TOE. Target of Evaluation

TSF.TOE security functions. These are the functions that enforce the security policy as defined in the Security Target. These can be either software or hardware.

Corporate Office
SGI
1140 East Arques Avenue
Sunnyvale, CA 94085-4602
650.960.1980

North America +1 800.800.7441
Latin America +55 11.5185.2860
Europe +44 118.912.7500
Japan +81 3.5488.1811
Asia Pacific +1 650.933.3000

4004 [5.2007]

J15286