Multilevel Security in UNICOS/mk

Roman Saucedo, *Eric Lund*, and *Jim Grindle*, Cray Research, A Silicon Graphics Company, Eagan, Minnesota, USA

ABSTRACT: *This paper describes the Multilevel Security (MLS) functionality to be available in a future release of UNICOS/mk. Every effort has been made to provide MLS feature compatibility between the UNICOS and UNICOS/mk operating systems. Yet, because of architectural and operational differences between the two systems, some aspects of MLS differ between them. Factors that have affected those MLS feature differences are described.*

Introduction

This paper describes Multilevel Security (MLS) functionality to be available in a future release of the UNICOS/mk operating system. It presents the goals for introducing MLS features into UNICOS/mk, and describes MLS interface differences between UNICOS and UNICOS/mk systems.

Architectural differences between UNICOS and UNICOS/mk require the low-level implementation of MLS features to differ between the systems. However, every effort is being made to provide MLS compatibility between UNICOS and UCNIOS/mk at the system call and library interface layers. Minor modification to some MLS administrative procedures will be necessary to provide consistency with broader UNICOS/mk operational procedures. However, virtually all UNICOS MLS command interfaces will be preserved in UNICOS/mk.

Questions regarding the content of this paper should be addressed to the authors.

Goals for UNICOS/mk Multilevel Security (MLS)

Objectives for implementing MLS features in UNICOS/mk include:

- Preserve MLS functionality as available in UNICOS 9.2.
- Provide MLS compatibility with UNICOS at the operating system (OS) system call and library interface layers.
- Preserve UNICOS MLS administrative and user command interfaces.
- Enhance MLS feature configuration
- Improve security auditing resiliency

In pursuing the above goals, we recognize the opportunity for migrating away from obsolete and/or unnecessary MLS interfaces. As such, compatibility with some MLS interfaces will not be preserved from UNICOS to UNICOS/mk.

UNICOS 9.2 MLS Functionality in UNICOS/mk

There are currently no plans to introduce additional MLS features into UNICOS beyond UNICOS 9.2. All MLS feature development resources are currently being applied to UNICOS/mk. MLS functionality in UNICOS/mk is based on the MLS functionality available in UNICOS 9.2. MLS features will be included in the UNICOS/mk base configuration, as with UNICOS 9.2.

MLS features available in a future release of UNICOS/mk include:

- Access Control Lists (ACLs)
- Security Auditing
- Privilege Assignment Lists (PALs)
- Mandatory Access Control (MAC) Policy Enforcement
- Network Security Enhancements

Support for the PRIV_TFM security policy will not be provided in UNICOS/mk.

System Call and Library Interface Compatibility

UNICOS/mk will provide MLS compatibility at the OS system call and library interface layers. However, compatibility will not be preserved for system calls that were used only to support the obsolete PRIV_TFM security policy. Those system calls are:

- setfcls(2)
- setucls(2)
- setfcat(2)
- settfm(2)

Source code that references the above system calls will receive a compilation error. Attempted use of each system call within existing binaries will result in the error return code ENOSYS.

Additionally, some MLS system calls will be replaced with new system calls, or functionality will be limited because of obsolescence. Affected system calls are:

- setsysv(2)
- getusrv(2)
- setusrv(2)
- secstat(2), lsecstat(2), fsecstat(2)

Support for the setsysv(2) system call will be eliminated in UNICOS/mk. Source code that references the setsysv(2) system call will receive a compilation error. Attempted use of that system call within existing binaries will result in the error return code ENOSYS.

The setsysv(2) system call permits dynamically setting the system security label range. That functionality has proven incompatible with the UNICOS security model. The system security label range can be configured only across UNICOS/mk system boots.

Also, the setsysv(2) system call permits security auditing configuration. The new system call audctl(2) will be introduced in UNICOS/mk to replace and enhance the audit control functionality provided by setsysv(2).

The getusrv(2) system call will automatically return zero (0) values for the active class, maximum class, saved level, and saved compartments user attributes. Those values were used only to support the obsolete PRIV_TFM security policy.

The setusrv(2) system call will continue to accept, but will ignore supplied values for the active class, maximum class, saved level and saved compartment values.

The secstat(2), lsecstat(2), and fsecstat(2) system calls will automatically return zero (0) values for the class and category file attributes.

Command Interface Compatibility

Virtually all MLS administrator and user commands that were available in UNICOS 9.2 will also be available in UNICOS/mk. However, MLS compatibility will be eliminated or limited for the following commands:

- setucls(1)
- setusrv(1)
- spget(1)
- spset(1)

Support for the setucls(1) command will be eliminated in UNICOS/mk. That command is used only to support the obsolete PRIV_TFM security policy. Attempted use of the setucls(2) command will result in a command “not found” error.

The setusrv(1) command will no longer recognize the -i option. That option is used to set the maximum class user attribute in support of the obsolete PRIV_TFM security policy.

The spget(1) command with no options specified will display zero (0) values for the class and maximum class user attributes. The spget(1) command with the -f option will display zero (0) values for the class and category file attributes.

The spset(1) command will no longer recognize the -i and -j options. Those options are used to set the class and category file attributes

The spset(1) command will no longer recognize the -s option. That option is used to dynamically set the system security label range. That functionality has proven unnecessary. The system security label range will be configurable across UNICOS/mk system boots.

MLS Configuration

MLS configuration parameters will be centralized, and configuration capabilities will be expanded in UNICOS/mk. The UNICOS/mk param file will provide a central location for UNICOS/mk MLS system configuration parameters. Those configuration parameters will include the traditional UNICOS config.h file parameters to control security auditing and privilege configurations. In addition, the param file will include boot-time definitions for security labels and administrative roles.

As with UNICOS 9.2, UNICOS/mk will support only two privilege configurations:

- PRIV_SU with Privilege Assignment Lists (PALs)
- PAL-only

Assignment of PALs will be required on all UNICOS/mk systems. We recognize that most customers require the traditional superuser privilege model. Those customers should enable the PRIV_SU system configuration option. We also recognize that some site security policies do not permit the existence of a superuser. For those sites we provide the more constrained PAL-only privilege configuration.

Security Auditing

Resiliency of the security auditing feature will be improved by replacing the security auditing daemon (slogdemon) with the Audit Log Manager (ALM) server in UNICOS/mk. Traditionally, UNICOS formats and buffers audit data that is subsequently managed and written to file by a user-level audit daemon. UNICOS valiantly attempts to manage the system complexities, especially when audit data is rapidly generated. The ALM in UNICOS/mk avoids many complexities by eliminating the need for a user-level daemon to manage audit data. Rather, the ALM handles all managing and writing of audit data.

Installation and Upgrade Procedures

As with UNICOS 9.2, UNICOS/mk MLS features will be included in the base configuration. Procedures for installing and upgrading UNICOS/mk MLS systems will be identical to those of the base UNICOS/mk system.

Other Issues

We are in the process of implementing the policy to charge for use of Mandatory Access Control (MAC). This means that a license will be required to configure the UNICOS/mk system such that the user community is divided using MAC security labels. The spnet(8) command will enforce license requirements.

We are aware that some customer sites use the Network Access List (NAL) to control access by hosts, but are not interested in using Mandatory Access Control (MAC). The NAL is intended for use with MAC. We are investigating ways to resolve this issue.

We are investigating the ability to set MAC attributes on symbolic links. Interfaces affected in providing this functionality are as yet undetermined.

Conclusion

Every effort is being made to maintain MLS feature compatibility between UNICOS 9.2 and UNICOS/mk. Customers should see no change in MLS feature availability, except more limited support of the obsolete PRIV_TFM security policy. Customers should see positive improvements in MLS configuration and security auditing resiliency.

We continue to strive to improve the MLS product, and encourage hearing about your experiences. We welcome your suggestions. You may reach us by e-mail or post at the address in the Attendee List.