



White Paper

Levels of Linux Operating System Security

Owl Approach to the Hardening of Linux

Abstract

Cross Domain Solutions produced by Owl Computing Technologies, Inc., running on Security Enhanced (SE) Linux operating systems may be hardened to varying degrees, depending on site-specific security requirements. Hardening is achieved by configuring the SELinux package suite and SELinux security policies. SELinux methods enhance Mandatory Access Controls (MAC) and Role Based Access Controls (RBAC) already implemented in Owl CDS systems to enforce integrity and availability security. When combined with Owl DualDiode® one-way data transfer hardware technology, software hardening methods described in this paper satisfy the most stringent security requirements of the U.S. Intelligence community and Department of Defense.

This paper describes three levels of hardening, including the advantages and disadvantages of each. The minimal level of hardening satisfies DISA STIG requirements for Unix operating systems, and also satisfies PL2/3 levels of hardening required for dedicated servers under DCID 6/3. This same level of hardening provides a cost-effective degree of security for most industrial consumers of network security equipment.

The maximum level of hardening, when integrated with DualDiode hardware technology, satisfies risk mitigation requirements under both SABI RDAC and DCID 6/3 PL5 security controls that are particularly stringent.

Reuse of specific SELinux configurations and security policies can accelerate the accreditation process for new CDS systems based on the existing bodies of test evidence for CDS systems already tested and deployed. Staged deployment of increasingly restrictive OS configurations can shorten development time for new CDS systems by allowing functional testing and advanced security policy development to proceed concurrently.

The paper shows that OS hardening always requires a compromise between configurability and security of the system.

Introduction

Typical Owl CDS systems are designed for machine-to-machine communications and are only accessed directly by privileged (human) users who are tasked with CDS maintenance. Recent trends in OS development favor the use of SELinux in CDS systems.

Defense Information Systems Agency (DISA) publishes guidelines for hardening Unix operating systems (including Linux) called Security Technical Information Guidance (STIG) documents. STIG publications may be downloaded from the DISA website. More guidance for hardening Unix operating systems is available from the National Security Agency (NSA).

A hardened version of Linux provides a Certifiable Linux Integration Platform (CLIP). CLIP comprises a limited suite of Linux packages that may be further hardened with the application of Security Enhanced policies that constrain operation of the OS and software applications running in the OS environment.

CLIP is designed to provide a high level of STIG compliance with minimal modification, and an environment for robust implementation of Mandatory Access Controls (MAC). CLIP also augments the security of Role Based Access Controls (RBAC) implemented in Owl CDS systems, using a combination of Unix best practices, sudo methods, and text-based user interface menus designed to minimize command line access.

By creating a tailored version of CLIP and using software scripts to load the OS and CDS software applications, STIG compliance, configuration repeatability, and disaster recovery requirements are satisfied simultaneously.

Additional levels of hardening are achieved by enforcement of SELinux security policies that may be configured to different levels of software constraint, as described below. SELinux security policies are loaded concurrently with the base OS and software applications. The OS and SELinux security policies may be configured in a manner that enforces all security policies and prevents CDS configuration changes after initial installation.

Use and reuse of specific OS package configurations and SELinux security policies can accelerate the regulatory approval process based on existing bodies of test evidence for CDS systems already tested and deployed. Scheduled deployment of increasingly restrictive SELinux security policies can also shorten development time for new systems. Delivering a STIG-compliant CDS version early in the program with augmented security patches later allows all CDS Use Cases to be tested -- and personnel trained -- while more stringent SELinux security policies are still under development. With development so scheduled, the customer also has the option of halting further security policy development while knowing the CDS is fully functional.

In most cases, it is not necessary to harden the CDS to the full extent that is technically feasible. Rather, it is possible to achieve an appropriate level of CDS security that is cost-effective and satisfies requirements for mitigating anticipated risks.

Showing a time-line for the two methods of when the program can begin testing use cases and operation would tell the tale.

Levels of Hardening

Cross Domain Solutions operating at Top Secret And Below (TSABI) Confidentiality levels are typically subject to security controls defined by the DCID 6/3 document used in the U.S. Intelligence Community. For typical Owl CDS systems operating under the DCID 6/3 rule set, the minimal acceptable level of hardening satisfies DISA STIG requirements for Unix operating systems, and also satisfies PL2/3 levels of hardening required for dedicated servers as described in DCID 6/3 Section 9.2.G. For typical Owl CDS systems in TSABI environments, superuser access is permissible, and a degree of CDS configurability is desired.

Owl CDS systems that transfer files from NIPRnet to SIPRnet are governed by a security control rule set for Secret and Below Interoperability (SABI) as defined by the Risk Decision Authority Criteria (RDAC) version 2.2. RDAC provides a formal analytical process for assessing risk and for making risk acceptance decisions. SABI CDS systems require approval from the Defense Information Assurance Security Accreditation Working Group (DSAWG), whose security requirements are among the most stringent within the U.S. Department of Defense.

For typical Owl CDS systems in SABI environments, the highest levels of hardening are required. Superuser access is disabled, command-line access is severely restricted for privileged users, and changes to CDS configuration are disallowed. Typical Owl CDS systems operating in SABI environments are configured like specialized appliances that operate with minimal maintenance by privileged users.

As described above, TSABI and SABI environments require different levels of OS hardening for CDS systems that operate in them. These two environments provide examples of two extremes. Intermediate levels of OS hardening are also possible. It is assumed that all CDS Use Cases associated with normal operation and routine maintenance are fully determined, documented, and implemented in terms of user interface menus and command-line restrictions for privileged users.

Three levels of OS hardening are described below, each of which provides a different balance among conflicting requirements for cost, security, configurability, and ease of use.

Level 1 – STIG Compliance

A cost-effective degree of OS and software application hardening is achieved by creating a software-scripted (and thus repeatable) loading of the CLIP OS that is tailored to satisfy STIG security requirements. The OS, privileged user role types, and all CDS software applications are loaded together.

This level of hardening provides the following desirable security features:

- Minimal suite of Linux packages necessary to perform all CDS tasks
- Non-root internal Linux process owner for all CDS software applications
- Preconfigured privileged user role types -- all non-root
- CDS data transfer software applications
- CDS data filter software applications
- CDS self-protection software applications
- CDS privileged user interface software applications
- CDS remote monitoring software applications (if specified)
- Full audit logging of materially significant data filter and data transfer events

Note that Level 1 hardening does not enforce SELinux security policies. The SELinux clipuser role type is enabled, and superuser privilege may be accessed from the command line. Level 1 hardening provides a cost-effective degree of security for most industrial consumers of network security equipment.

Level 2 – SE Policy Enforced

Additional hardening of OS and software applications (beyond Level 1) is achieved by creating SELinux security policies (Type Enforcement) for each CDS software application, and maintaining enforcement at all times.

Level 2 hardening protects the CDS from reconfiguration by all privileged user role types associated with normal operation and routine maintenance. With SELinux security policies enforced at Level 2, privileged users can only execute software applications and OS commands already installed.

This level of hardening provides these additionally desirable security features (beyond Level 1):

- Only CDS software applications of known types are allowed to operate
- CDS software applications of unknown type are not allowed to operate
- Attempts to invoke unauthorized applications are audited (logged) and may trigger alarms

Note that Level 2 hardening typically includes enabled SELinux clipuser role type, which has sufficient privilege to alter the SELinux security policy configuration. Superuser privilege may be accessed from the command line. A Level 2 enforced version allows sufficient protection for many programs and allows for regression testing of individual confined policies as they are developed.

Level 3 – SE Policy Enforced with Confined Applications

The highest level of hardening is achieved by creating additional SELinux security policies for each CDS software application that also confines the software application and restricts its access to system resources. Level 3 confinement prevents software applications of known types from "going rogue" and performing functions that are unexpected and/or unauthorized. At Level 3, confinement of all software applications is enforced at all times.

At Level 3, the SELinux clipuser role type is disabled, which prevents alteration of the SELinux security policies and denies all access to superuser privilege. The CDS operates like an appliance; CDS configuration cannot be modified by any privileged user role type. Level 3 hardening includes protection against changes to SELinux configuration files. If changes to SELinux security policy configuration files are detected, the host computer shuts down and all data flow is stopped.

This level of hardening provides the following desirable security features (beyond Level 1):

- CDS software applications are allowed to perform authorized tasks and access authorized system resources
- CDS software applications are not allowed to perform any tasks or access system resources beyond those already approved
- Attempts by CDS software applications to perform unauthorized tasks or access unauthorized system resources are audited (logged) and may trigger alarms
- Any attempt to change SELinux security policy configuration files triggers kernel panic and host shutdown

Conclusion

Cross Domain Solutions produced by Owl Computing running the SELinux operating system may be hardened to varying degrees, depending on site-specific security requirements. SELinux methods enhance Mandatory Access Controls (MAC) and Role Based Access Controls (RBAC) already implemented in Owl CDS systems to enforce integrity and availability security. When combined with Owl DualDiode one-way data transfer hardware technology, software hardening methods described in this paper satisfy the most stringent security requirements of the U.S. Intelligence community and Department of Defense.

Even at minimal level of hardening, the CLIP operating system provides cost-effective levels of hardening; satisfying DISA STIG requirements for Unix operating systems, and PL2/3 levels of hardening required for dedicated servers under DCID 6/3. This same level of hardening provides a cost-effective degree of security for most industrial consumers of network security equipment.

If higher levels of hardening are required, SELinux security policies may be crafted to confine OS functions and software applications to the degree necessary. The maximum level of hardening, when integrated with DualDiode hardware technology, satisfies risk mitigation requirements under both SABI RDAC and DCID 6/3 PL5 security controls that are particularly stringent.

Reuse of specific SELinux configurations and security policies can accelerate the accreditation process for new CDS systems based on bodies of test evidence for CDS systems already tested and deployed. Staged deployment of increasingly restrictive OS configurations can shorten development time for new CDS systems by allowing functional testing and advanced security policy development to proceed concurrently.

About Owl Computing Technologies, Inc.

Owl Computing Technologies, Inc. is a privately owned and funded U.S. company. Owl delivers NIAP Common Criteria EAL-4 certified one-way cross domain systems & electronic perimeter defense solutions to transport and protect an organization's most sensitive data between discrete domains of varying security levels and policies. Information sharing Secured by Owl® is enforced with Owl Computing proprietary DualDiode® technology. DualDiode one-way transfer systems guards against data leakage and protects networks from unauthorized access. Owl systems meet the highest levels of information protection within the U.S. Department of Defense, the Intelligence community, & the Power Generation industry, delivering secure, reliable, information transfer of multiple data sources and types across single DualDiode systems -- any file size or data type. www.owlcti.com