RedHawk

An Overview of RedHawk Linux Security Features

Kernel- and User-level Security Features Join to Harden RedHawk to Military-grade Standards

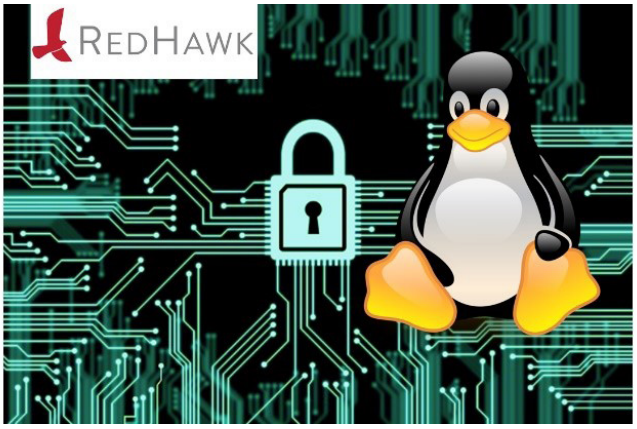
Info@concurrent-rt.com
www.concurrent-rt.com
(800) 666.4544 or (954) 974-1700

RedHawk

An Overview of RedHawk Linux Security Features

Kernel- and User-level Security Features Join to Harden RedHawk to Military-grade Standards

Overview



RedHawk Linux provides several kernel-level and user-level security features that together can provide powerful levels of security capable of hardening RedHawk systems to military-grade standards. This document discusses several main RedHawk security features including SELinux, Secure Boot, FIPS, STIG, LUKS and TPM.

SELinux

Security-Enhanced Linux (SELinux) is a set of kernel modifications and user-space tools that have been developed by the National Security Agency (NSA) and Red Hat. All RedHawk kernels include the SELinux security module, and SELinux user-space tools are installed as part of a standard RedHawk Linux product installation. RedHawk also provides a default set of security policy configuration files designed to meet general-purpose security goals, and these policies can be tailored for site-specific security requirements

The SELinux kernel security module implements a powerful and flexible Mandatory Access Control (MAC) architecture on top of each major subsystem of the Linux kernel. MAC enforces the separation of information into different security levels based on confidentiality and integrity; blocks all attempts to tamper with or bypass security mechanisms; and significantly contains and controls any damage that may be caused by malicious or flawed applications.

Secure Boot

Secure boot is a security standard agreed upon by members of the PC industry/Original Equipment Manufacturers (OEMs) to validate software through the entire boot cycle. Validation of software starts at the hardware level and continues up the stack through UEFI firmware drivers (ROMs), EFI bootloaders, kernels, and finally to drivers. All Redhawk kernels are signed by a secure, Certificate Authority (CA)-based key that is validated by a secure EFI bootloader. RedHawk provides tools for creating and signing custom RedHawk kernels and drivers for use with secure boot systems.

Secure boot relies on closely guarded private keys that are used to sign all software involved with the boot process. Only signed, trusted software may be loaded onto a system. This prevents a bad actor from adding untrusted software or malicious malware such as rootkits to a system. Any unsigned software is immediately rejected by the system when there is no trusted signature associated with the binaries. Thus, the firmware, kernel and all underlying drivers always maintain a high degree of integrity.

FIPS

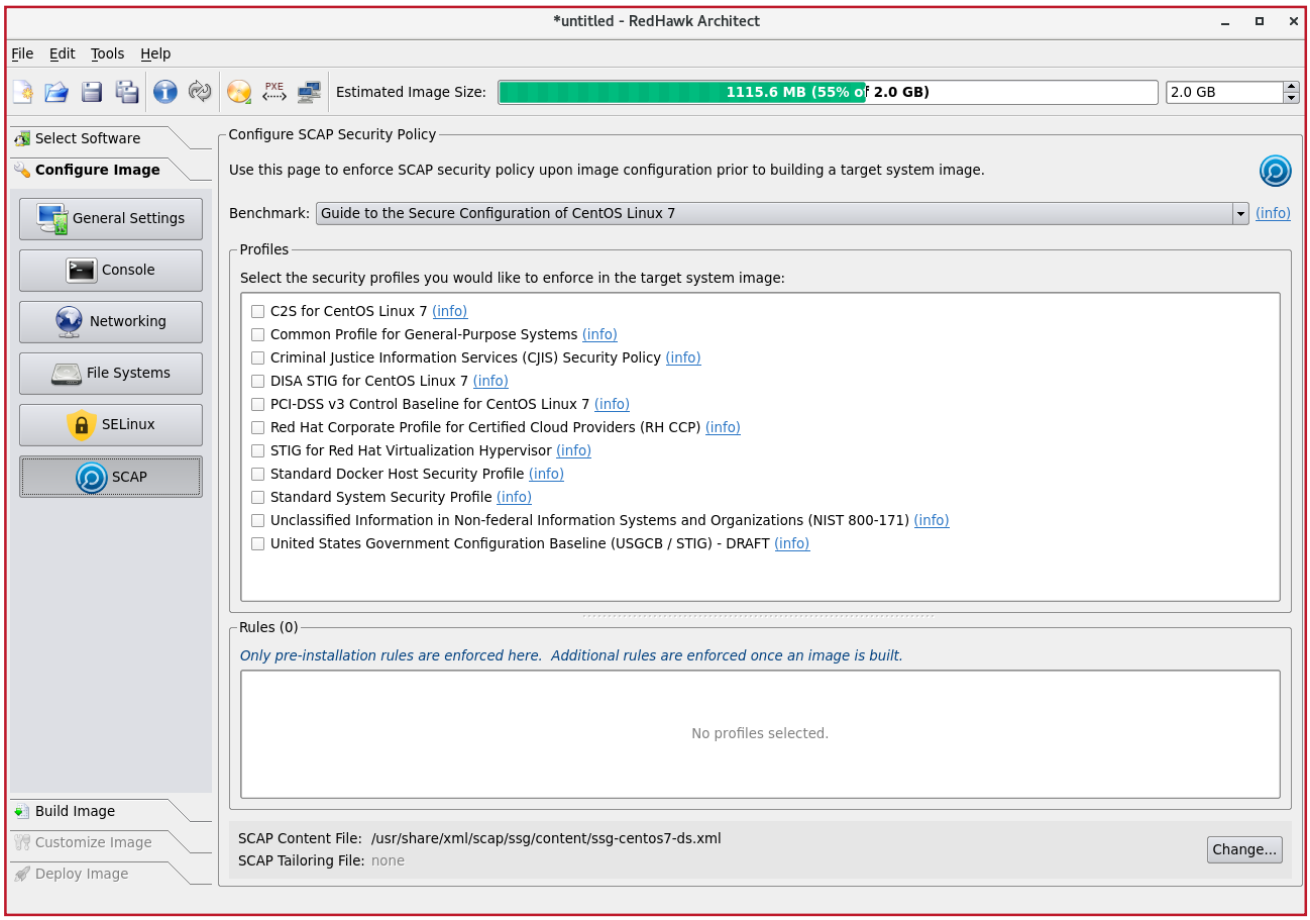
The Federal Information Processing Standard (FIPS) publication is a security standard that certifies cryptographic modules. FIPS defines critical encryption standards for protecting sensitive data. RedHawk supports all encryption methods used within FIPS protocols. RedHawk kernels support booting in FIPS compliant mode where all encryption is based on the FIPS security level required. The FIPS standard provides four security levels that cover different industry, security, and administration needs. The RedHawk kernel is fully compatible with RHEL/CentOS software which maintains FIPS-related packages.

FIPS is enabled at boot time, which loads the required cryptographic modules into the RedHawk kernel. These modules are responsible for cryptographic key generation for ciphers and Message Authentication Codes. FIPS algorithms rely on hardware-based entropy within the system to generate encryption keys. By enforcing FIPS, RedHawk systems can enforce cryptographic standards used by government agencies and third-party vendors.

STIG

Security Technical Implementation Guide (STIG) is a cybersecurity methodology for standardizing security protocols with logical designs, networks, servers and computers to enhance overall security. STIG protocols are developed and published by the Department of Defense (DoD). STIGs are defining protocols that encompass the totality of a RedHawk system from defining file system types and encryption to network security protocols. STIG rules enforce compliance of RedHawk user-level packages to meet stringent security standards.

RedHawk offers STIG compliance via the RedHawk Architect tool. Architect is a powerful tool that can be used to configure an entire RedHawk system for compliance with various STIG protocols. You can choose from several different STIG protocols and Architect will prepare the system and begin running STIG compliance tests to validate system integrity. The DoD releases STIG guidelines in machine readable XML files that can be directly passed to Architect to create highly secure RedHawk systems.



LUKS And TPM

RedHawk provides full support for hard disk encryption through the Linux Unified Key Setup (LUKS) standards. LUKS provides secure management of passphrases by storing encrypted keys in partition headers, and LUKS prevents a user from unlocking partitions and booting the system without first manually supplying a correct passphrase.

In addition, RedHawk provides full support for the hardware Trusted Platform Module (TPM) standards. The TPM can be securely configured to automatically unlock LUKS partitions at boot time for situations where manually entering a passphrase is not practical. Even when the TPM is used, LUKS encryption remains strong and any attempt to remove the hard disk and boot it in another system will fail unless a user manually enters a correct passphrase.

Summary

RedHawk maintains a high degree of compliance with security protocols recommended by the Department of Defense, the National Security Agency and the National Institute for Standards and Technology. This high degree of compliance allows RedHawk to meet the strictest requirements of government agencies and their third-party vendors. These features improve the IT infrastructure by reducing the attack surface of critical RedHawk systems.

RedHawk is fully compatible with Red Hat Enterprise Linux (RHEL) Software which maintains Common Criteria standards (EAL3 and EAL4) and FIPS security certifications. While RHEL certifications are not automatically inherited by RedHawk, its close compatibility with RHEL enables RedHawk to be certified to the same standards. Please contact us to learn more.

About Concurrent Real-Time

Headquartered in Pompano Beach, FL, Concurrent Real-Time is the industry's foremost provider of high-performance real-time computer systems, solutions and software for commercial and government markets worldwide. Its real-time Linux solutions deliver hard real-time performance in support of the world's most sophisticated hardware in-the-loop and man-in-the-loop simulation, high-speed data acquisition, process control and low-latency transaction processing applications. With over 50 years of experience in real-time solutions, Concurrent Real-Time provides sales and support from offices throughout North America, Europe and Asia.

More Information

Concurrent Real-Time
Info@concurrent-rt.com
www.concurrent-rt.com
(800) 666.4544 or (954) 974-1700

concurrent REAL-TIME