SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Phone: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com

The SEL Process for Mitigating Malware Risk to Embedded Devices

At SEL, we have made security a top priority for over 30 years and protecting embedded devices from the threat of malware is a central part of that effort. Moreover, North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards require owners of high or medium impact Bulk Electric System Cyber Systems and their associated access control systems to use methods that prevent malware from entering a system, detect and mitigate malware threats, and maintain the most recent signature-based detection methods. The standards also require that devices log detection of malware at the system level to the extent possible.

Malware targets a specific operating system or application and attempts to find and use a security vulnerability to provide the entry point it needs to infect a host. Depending upon the goals of an attacker, malware may be designed to target commodity operating systems and applications, or uncommon software applications used only in a specific industry. Malware comes in many forms, including viruses and worms, or malicious applications such as ransomware.

Embedded products, including SEL products, are inherently immune to most malware targeted at commodity operating systems because they contain no operating system or application code common to personal computers and consumer devices. To compromise an embedded product, malware must specifically target the embedded device by exploiting a vulnerability in the product. SEL is unaware of any instances of malware infection of an SEL embedded device.

Although the risk associated with malware attacks to SEL embedded devices is low, the potential consequences of a successful attack are severe. The following process outlines the protective measures we have incorporated into our embedded devices to protect against malware.

The SEL Process

SEL provides safeguards in its embedded device platforms to prevent malware infection. Unlike most consumer devices, SEL devices do not permit installation of additional software. In addition, SEL devices continuously check their stored software (firmware) code for corruption and continuously compare any code executing from memory against the firmware. This process detects any corruption of the program.

SEL features that mitigate malware threats to our embedded devices, which includes all hardware products except SEL Rugged Computers include the following:

- **Use of an embedded environment that allows neither installation nor execution of new programs.** SEL embedded devices cannot load or run new programs. These devices also run memory integrity checks to ensure that the running program has not been altered.
- **Verification of software stored in permanent memory.** When the device starts, it performs a detailed checksum of the contents of permanent memory and verifies the checksum value to verify integrity.
- **Continuous verification of executing software.** This verification compares the firmware in memory to the factory-installed firmware on the device. The comparison detects any modification of the executing software.

- **Whitelisting.** Certain SEL devices use an embedded Linux® operating system that incorporates SEL exe-GUARD™ with kernel-level application whitelisting and mandatory access controls to prevent malware installation on or modification of the system.
- **Signed Firmware.** Most SEL devices use digitally signed firmware files, and the device checks the digital signature when a new firmware version is loaded. An altered or unsigned firmware file cannot be loaded and executed. Verification of the integrity of unsigned firmware can be done by using hash values published on the SEL website.

SEL devices incorporate features to prevent intrusion of malicious code. Our devices are designed to detect program corruption and to disable and activate an alarm contact if corruption occurs. In addition to preventing malware intrusion, some SEL devices provide features to detect and log conditions that may indicate malware intrusion. Devices with exe-GUARD detect whitelist and program violations that may indicate malicious code and log those events. Other SEL devices may retain diagnostic information for use in analyzing these types of events.

Summary

We provide our customers with high quality, reliable, and secure products that outpace ever-evolving threat actors. We understand that effective safeguards in our embedded device platforms are essential to our mission to make electric power safer, more reliable, and more economical.

Contact

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 USA
Telephone: +1.509.332.1890
Fax: +1.509.332.7990
Internet: www.selinc.com
Email: security@selinc.com