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

SEL recognizes the need to protect embedded devices from the threat of malicious software, otherwise known as malware. 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 that they can do so.

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. Each malware can infect only a host that uses that particular operating system or application. Depending upon the goals of an attacker, malware can target such widely used operating systems as Microsoft® Windows®, popular applications such as word processors, or uncommon software applications used only in a specific industry. Malware can come in many forms, including viruses, worms, and Trojan horses.

Embedded products, including SEL products, are inherently immune to most malware targeted at personal computer (PC) systems because they contain no operating system or application code common to the PC. To compromise an embedded product, malware would have to 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. SEL devices, for example, are unlike PCs in that they do not permit installation of additional software. In addition, SEL devices continuously check their read-only memory (ROM)-based code for corruption and continuously compare any code executing from random-access memory (RAM) against the reference ROM code. This process detects any corruption in ROM or RAM.

SEL features that mitigate malware threats to our embedded devices 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. Furthermore, these devices run memory integrity checks to ensure against any alteration of embedded software.
- **Verification of software stored in permanent memory.** When the device starts, it performs a detailed checksum of the contents of permanent memory and compares the checksum value against an SEL factory value.
- **Continuous verification of executing software.** This verification compares the firmware byte-codes in memory to their original values in permanent storage on the device. The comparison detects any modification of the executing software.
- **White-listing.** Certain SEL devices that use an embedded Linux® operating system incorporate SEL exe-GUARD®, which uses kernel-level application white-listing and mandatory access controls to prevent malware installation on or modification of the system.

SEL devices incorporate features to prevent intrusion of malicious code. Our devices are designed to detect program corruption and to disable 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 such events, but they do not specifically identify malicious code and so do not log malicious code events.

Summary

We are dedicated to providing our customers with high quality, reliable, and secure products and will continue to include effective safeguards in our embedded device platforms. Informational documents such as this are part of our commitment to delivering products that make electric power safer, more reliable, and more economical.

Contact Information

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