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. Malware is malicious code targeted to a specific operating system or application that attempts to find and use a vulnerability. Malware can come in many forms, including viruses, worms, and Trojan horses.

Malware usually exploits a vulnerability within a specific system to provide the entry point it needs to infect a host. Each malware release targets a specific operating system or application and only infects that particular operating system or application. Therefore, most malware targets widely used operating systems such as Microsoft® Windows® or popular applications such as Microsoft Word, which are running on computer desktops around the world.

Embedded products, including SEL products, are inherently immune to the malware targeted to these applications because they do not contain 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.

The *SEL Process* outlines the measures SEL has incorporated into our embedded devices to protect against malware. We recognize that the risk associated with malware attacks is very low, but the potential consequences of a successful attack are severe. Therefore, we have incorporated protection measures in our embedded devices.

NERC CIP

NERC has implemented reliability standards that require responsible entities to define methods, processes, and procedures for securing cybersecurity assets within the respective organization's electronic security perimeter(s).

NERC CIP-007-1 addresses Systems Security Management and outlines the following requirements for Malicious Software Prevention:

> **R4.** Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> > **R4.1.** The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

SEL Process

SEL provides safeguards in its embedded device platforms to mitigate the risk of malware infection. SEL devices continuously check their ROM-based code for corruption, as well as continuously compare any code executing from RAM with the reference ROM code. This process detects any corruption in ROM or RAM.

Other SEL solutions for mitigating malware threats to our embedded devices consist primarily of the following:

- **Continuous verification of the 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.
- **Verification of the software stored in permanent memory.** When the device is started, a detailed checksum of the contents of permanent memory is performed and compared against the value created at the SEL factory.
- **Use of an embedded operating system that is designed to prevent installation and execution of new programs.** The operating systems of SEL embedded devices are not designed to load or run new programs. Furthermore, memory integrity checks are run to ensure that the embedded operating system has not been altered in an unintended or unauthorized manner.

Summary

SEL will continue to include effective safeguards in our embedded device platforms. We are dedicated to providing our customers with high quality products that are reliable and secure. Process documents like this one 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