exe-GUARD

A whitelist malware protection solution to protect control systems at the device level

Background

Malware is an ever increasing threat to the safe and reliable operation of our power systems. Companies must balance security safeguards with operational costs and technical capabilities. Devices can become infected with malware when vulnerable devices are exposed or when operators unintentionally install infected files or connect infected storage devices.

In traditional information technology environments, blacklist antivirus software has effectively been used to protect devices against compromise. However, blacklist antivirus software requires recurrent system scans, regular decommissioning to perform updates and careful configuration, which can negatively impact the performance of control systems. It is also vulnerable to zero-day exploits that have not yet been incorporated into updates. Many asset owners have not employed device level malware protection due to these drawbacks.

Barriers

- Blacklist antivirus software causes performance losses and is vulnerable to zero-day exploits
- Blacklist antivirus requires signature updates
- Blacklist antivirus requires ongoing maintenance or subscription costs to receive future updates

Project Description

The exe-Guard project focuses on developing malware protection technology that takes advantage of the low amount of change required for control system devices after deployment to baseline and whitelist executing code and guard that it doesn't change. Whitelist antivirus methods establish a security baseline and automatically search for and deny deviations from that baseline, including attempts to inject malicious code or alter settings without proper authentication. The whitelist process also eliminates the need for frequent decommissioning to install security patches and signature updates in order to keep up with newly released malware. Instead, updates are only needed when firmware updates are performed, allowing for the security baseline to be determined before the system returns to service.

Benefits

- Establishes a known, good security baseline
- Eliminates frequent antivirus signature patches
- Addresses North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirement CIP-007-R4, which requires asset owners to employ malicious software prevention tools
- Minimizes the CIP-007-R3 requirement for security patch management
- Provides an upgrade solution for deployed systems
- Protects against malware at the device level

Partners

- Schweitzer Engineering Laboratories
- Sandia National Laboratories

Technical Objectives

This project will develop whitelist malware protection technology and commercially release it as an integrated part Schweitzer Engineering Laboratories' SEL-3620 Ethernet Security Gateway, also developed under the DOE project, Lemnos. The solution will be developed in two phases.

Phase 1: Research and Development

- Research and develop for commercialization a whitelist malware protection solution on the SEL-3620, demonstrating the capabilities for Linux embedded products

Phase 2: Testing and Demonstration

- Laboratory test, field test and demonstrate the technology and prepare best practice guides for testing, deployment and long-term management of the technology

End Results

Project results will include:

- A whitelist malware protection solution that establishes baseline system security and provides automated, device level protection against firmware changes
- Cost-effective malware protection for maintaining system integrity and reliability
- An upgrade solution for deployed systems
- Technical controls addressing NERC CIP-007-R3 and R4 requirements
- Device integrity at firmware upgrade with digital signatures
- Device operating system integrity with root kit prevention technology
- Device functional integrity with application whitelisting
- Device memory protection with mandatory access controls

Content last updated: August 2012

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Chris Ewing
Lead Product Engineer
Schweitzer Engineering Laboratories
509-334-8032
chris_ewing@selinc.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov