Watchdog

A managed switch with integrated deny by default all-layer firewall and network access control

Background

Local area networks (LANs) connect electronic devices within small geographic areas, such as office networks, in order to enable communication and transfer of data between devices. Control system protocols are designed with inherent trust. Gateways and firewalls protect devices on a LAN from communications attempting access from outside the LAN. There is a need to protect devices on the same LAN from each other and from new untrusted devices being plugged into the local LAN.

Network switches are used to connect each device to the LAN and are an ideal appliance to use as the inspection and filter point for all traffic on the LAN. Traditional switches operate at layer 2 of the Open Systems Interconnection (OSI) model. Layer 2 is the data link layer and the only traditional filter points are media access control (MAC) addresses and virtual LANs.

Barriers

- Communications on a single LAN have limited filter options and lack data inspection capabilities
- Control system protocols are designed with inherent trust and owners have few options for how to protect communication on a LAN
- Most control system products lack host-based firewall functionality and rely on network filters
- Control systems require high reliability and deterministic communications making it attractive to create large LANs that have many hosts and are geographically distributed

Project Description

The Watchdog project will develop a managed switch that performs deep packet inspection using a whitelist configuration approach to establish a set of known, allowed communications. A switch is an ideal solution to integrate deep packet inspection technology because it sits in the center of the LAN and controls all traffic paths for equipment on the network.

Watchdog will start at layer 1, the physical layer, of the OSI model and provide "all-layer" inspection by monitoring all layers of network traffic through layer 7, the application layer. It will quarantine devices that are not authorized to join the network or exhibit unusual or threatening behavior until they can be cleaned and redeployed, as well as provide administrative visibility to the network behavior to validate performance and reliability metrics.

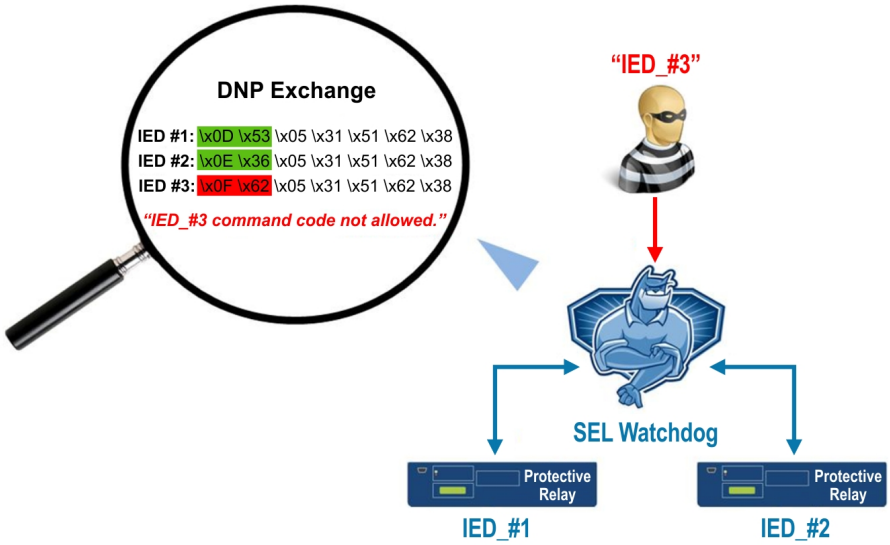
Benefits

- Provides needed filter and inspection capabilities on the LAN
- Deny by default and whitelisted approach makes the technology scalable and manageable in larger systems
- Offers a cost-effective alternative to traditional intrusion detection systems with less administration and eliminates continuous signature updates
- Quarantines malicious traffic and unregistered devices
- Logs and reports events and actions on all layers of the network
- Works with both new and existing control system networks

Partners

- Schweitzer Engineering Laboratories
- Centerpoint Energy Houston Electric
- Pacific Northwest National Laboratory

Deep packet inspection protection



Technical Objectives

The Watchdog project will build upon the perimeter defensive solutions designed under the Lemnos project and provide the next layer of defense on the local network itself. The Watchdog project will also integrate with the Padlock project and identify physical tamper detections on field equipment outside the substation control house. This project balances the operational and security requirements of control system communications between end devices. The project will consist of two phases.

Phase 1: Research and Development

- Research local network communication load needs and develop filter and inspection use cases for Watchdog technology
- Develop the commercial managed switch with deep packet inspection

Phase 2: Testing and Demonstration

- Laboratory test, field test and demonstrate the technology in real-world control system installations and prepare best practice guides for testing, deployment and long-term management of the technology

End Results

Project results will include:

- A managed switch with integrated application-layer firewall providing filter and inspection functionality on all traffic on a LAN
- Solution providing a countermeasure for newly discovered security vulnerabilities until end devices can safely be upgraded or patched
- Control system network access control and defense solutions
- Automated LAN resiliency through identification and reaction to unauthorized traffic
- A cost-effective alternative to traditional intrusion detection systems with reduced operational management overhead and elimination of signature updates

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

Rhett Smith
Development Manager
Schweitzer Engineering Laboratories
509-336-7939
rhett_smith@selinc.com

Current Contact as of Aug. 2020

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