SCI-FI: Supply Chain Integration for Integrity

Integrated, open source tools to evaluate hardware and software integrity

Background

The equipment and systems involved in electric power grid operation use an array of software and hardware components. These can range from processor code embedded in the custom automation equipment of generation plants, transmission substations, and smart power meters, to supervisory control and data acquisition (SCADA) systems, and even to standard commercial off-the-shelf (COTS) operating systems that collect, process, and display large amounts of operational data. The ability to analyze system subcomponents, including embedded code, firmware, hardware, and application software, for potential security vulnerabilities can improve supply chain integrity for the electric power industry and provide an increased degree of assurance in product selection and implementation.

Barriers

- A large percentage of subcomponents are manufactured overseas, creating difficulty in managing supply chains.
- There are few practical methods of determining whether approved designs are actually implemented in subcomponents.
- The reverse engineering of subcomponents to determine malicious intent can be expensive and/or destructive.

Project Description

This project is developing a suite of open source tools and technologies to address supply chain integrity needs for end utilities, vendors, and chipset manufacturers. The suite ranges from stand-alone tools that can be run locally to provide hardware supply chain assurances, to large-scale high-performance computing services that can statistically analyze systems of systems to identify potential concerns in critical infrastructure supply chains.

To address supply chain challenges in an integrated manner, Pacific Northwest National Laboratory and its partners are taking a three-part approach: addressing policy and architecture for the built-in supply chain integrity of trusted components, analyzing software and firmware, and evaluating hardware supply chain concerns. Although the effort will address supply chain integrity for energy delivery systems, the work will also be broadly relevant to other industries.

Benefits

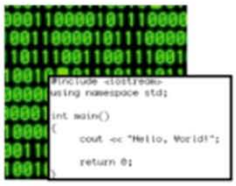
- Enhances the integrity of energy system infrastructure through integrated supply chain evaluation tools
- Reinforces trusted computer system security policies
- Supports custom forms of analysis for both embedded field device firmware and energy management system application software
- Mitigates systemic vulnerabilities through improved software and hardware verification

Partners

- Pacific Northwest National Laboratory (PNNL)
- Lawrence Livermore National Laboratory (LLNL)
- Oak Ridge National Laboratory (ORNL)
- Digital Management, Inc.
- Pacific Gas and Electric (PG&E)

Lawrence Livermore National Laboratory

LLNL will develop the analysis capabilities for both embedded field device firmware and energy management system application software.



Software and Firmware

Pacific Northwest NATIONAL LABORATORY

PNNL will develop the tools and the techniques needed to reverse-engineer, identify, and attribute the components of the state machines that integrated circuits are built upon to ensure the accuracy and integrity of the hardware.

Hardware

OAK RIDGE National Laboratory

ORNL will develop the policy and processes needed to implement the hardware and software/firmware analysis tools and techniques created by PNNL and ORNL.

Policy and Architecture

Technical Objectives

This project will use a three-part approach to develop a suite of tools that can be used to ensure the supply chain integrity of hardware and software components.

1: Policy and Architecture

This work is developing tools and techniques to address static and dynamic discovery in the supply chain architecture.

Static discovery identifies the compromise of digital assets after they are manufactured but before they are commissioned into service, while *dynamic discovery* detects the compromise of digital assets during their period of service.

2: Software and Firmware

This work is developing custom analysis tools and capabilities for different types of embedded and application software. The tools and techniques will span both source code and binary executables.

3: Hardware

This work is developing tools and techniques to perform intelligent, brute-force exploration of hardware:

- Develop tools for querying and analyzing unknown integrated circuits (ICs).
- Develop techniques to compare reverse-engineered components with intended design to improve the understanding of the components' functionality.

End Results

The project will produce an integrated suite of open source tools that can be used to ensure the supply chain integrity of hardware and software components. The suite will include the following:

- A trust model and trust architecture for the secure development and delivery of products in the electric power industry supply chain
- Tools for analyzing firmware releases and SCADA application software for electric power industry field devices
- Tools for analyzing hardware with formal methods approaches

Content last updated: September 2013

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

David Manz
Senior Cyber Security Scientist
Pacific Northwest National Laboratory
509-372-5995
david.manz@pnnl.gov

Current Contact as of Aug. 2020

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