U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Firmware Indicator Translation (FIT)

Idaho National Laboratory

Scalable binary firmware analysis using advanced machine learning, graph theoretics, and visualization to identify vulnerable ubiquitous libraries for big data analytics

Today's most advanced and capable adversaries exploit a lack of awareness within operational technology (OT) and deploy malware to the lowest levels of firmware in embedded systems. Advanced integrity checking of firmware libraries and functions are needed to determine security baselines and create indicators for detection of commonly used libraries with identified vulnerabilities. This project provides firmware code inspection and analysis for insight into previously hidden firmware. FIT operationalizes three tools for firmware vulnerability identification: WiiBin provides initial library triage, Annotated Translated Disassembled Code (@DisCo) enables reverse engineering of the libraries at scale and translates the results into graph databases for machine learning and visualization, and DISCOverFlow visualizes firmware to detect anomalies and understand code behavior. The FIT big data analytics method aggregates a large spectrum of data alerts filtered for embedded OT applicability and searchable through a database and delivers feedback into information technology (IT) threat indicators for maximum application across systems.

KEY TAKEAWAYS

- Conducts firmware analysis at scale to establish baseline code libraries prior to installation, enabling ongoing trend analysis of firmware changes
- Translates indicators of firmware-level vulnerabilities across the energy sector using big data
- Visualizes firmware and vulnerability detection within commonly used libraries to enable better cyber defenses

OUTCOME

This project develops three tools for advanced firmware analysis to decrease the time required to detect and identify previously hidden firmware from years to days and deploys big data analytics methods for sharing indicators between IT and OT environments. The big data analytics methodology demonstrates how indicators can be harvested and represented to provide sharable, actionable, and implementable threat intelligence to be shared across OT/IT domains.

PARTICIPANTS	ROLE
Idaho National Laboratory	Leads laboratory development of three FIT products: WiiBin, @DisCo, and DISCOverFlow
NEW CONTEXT	Technology partner for indicator sharing from multiple sources including network traffic; big data analytic methodology development
Southern California Edison – Energy for What's Ahead	Asset owner, test bed provider, and advisor
Schneider Electric	Equipment provider to asset owner and test beds
Idaho State University	Provides interns for firmware testing
BYU Brigham Young University	Provides interns for machine learning testing
SIEMENS	Equipment provider to augment test beds and advisor
EATON	Industry advisor
PG&E	Asset owner, advisor
HITACHI Inspire the Next	Industry advisor
DTE	Asset owner, test bed equipment provider, and advisor

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Rita Foster
Principal Investigator
Idaho National Laboratory
208-526-3179
Rita.Foster@inl.gov

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: October 2017 – December 2020

Total Award Value: $2,400,144
DOE Share: $2,400,144
Cost Share: $0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021