Resilient Energy Systems
Mission Campaign

HALLUCINATING CANARIES: INSTRUMENTED FIRMWARE RE-HOSTING FOR CYBER RESILIENCE IN ENERGY SYSTEMS

Hallucinating Canaries creates cyber-redundant systems that detect cyber-attacks on field devices, at the point of the attack, and capture artifacts to understand attack mechanisms and impacts.

THE CHALLENGE

Field devices and other intelligent electronic devices (IED) enable automated and remote-control of the electric grid; their correct functionality is critical to the operation of the U.S. electric grid. These systems are often embedded systems running custom firmware. Today, there is a severe gap in our ability to detect and defend embedded systems from cyber threats. Hallucinating Canaries aims to create digital twins to detect cyber-attacks. Digital twins act as virtual models that reflect physical devices. Successful completion of this project will enhance our ability to detect zero-day attacks, detect entire classes of cyber-attacks, and pave a path forward to enabling continuous upgrading of defenses on legacy field devices. Ultimately, this will transform field devices to become some of the best protected components in energy systems.

APPROACH

Hallucinating Canaries will utilize HALucinator, an open source firmware re-hosting capability developed at Sandia to create digital twins of select field devices. The twins will then be instrumented with detectors for various classes of cyber-attacks. These instrumented twins become the canaries. The canaries will process the same network inputs as the physical device enabling them to detect attacks on the physical device. The canaries will alert when they detect undesired behaviour. This project proposes to demonstrate the Hallucinating Canaries concept in a laboratory environment through re-hosting firmware from a Remote Terminal Unit and detectors for two or three classes of attacks and use proof-of-concept attacks to demonstrate their effectiveness.

EXPECTED RESULTS

Successful completion of this project will enable early detection of cyber-attacks on field devices at the point of vulnerability, without requiring knowledge of the attacker's tools, techniques or practices. This will enable detection of "zero-day attacks". By running multiple canaries, it will be possible to completely eliminate classes of cyber-attacks on field devices. In addition, Hallucinating Canaries will have transformative impact by decoupling cyber protection from physcial devices. This will enable the continous upgrading of defenses at the pace of attackers' capabilites and addresses challenges with legacy systems that have plagued systems.

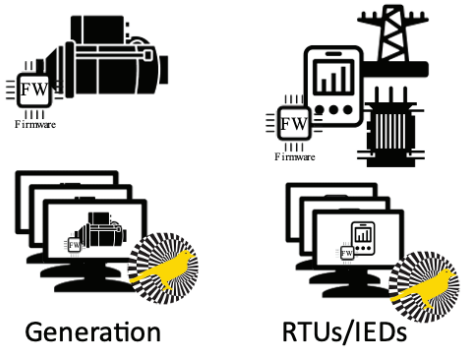

Image Credits: Generator Amethyst Studio, RTU verry poernomo, Transformer Motion Videos UK, Transmission Lines Creative Stall, Computer Monitor Markus

EXPECTED IMPACT OF THIS RESEARCH

Research from this project will enable detection of unknown cyber-threats on field devices integrated in energy systems, control systems, and other embedded devices used in our modern way of life. It uncovers a way to continuously update legacy field devices that evolve with attackers' capabilities enabling resilient energy sytems that are central to DOE's and DHS-CISA missions. Their missions are to ensure the security of the United States energy systems and infrastructure. This impact also answers CISA and NSA's call for immediate actions to reduce the exposure of these systems to cyber-attacks.

RESILIENT ENERGY SYSTEMS

Sandia's investment in this project is part of its Resilient Energy Systems portfolio of projects, coordinated R&D that addresses the resiliency of the nation's energy systems. Hallucinating Canaries will enable protection of embeded systems used in SCADA and other industrial controls system's central energy systems using the Resilient Energy Systems Testbed as a demonstrator platform.

CONTACT:

resilience@sandia.gov

U.S. DEPARTMENT OF ENERGY | NNSA National Nuclear Security Administration

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2022-0376 O

Sandia National Laboratories