Trust Anchor Lifecycle Attack Protection

Cryptographically secure software providing independent testing, monitoring, and control of energy control system component operation

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

Cyber Security for Energy Delivery Systems

Trust Anchor Lifecycle Attack Protection

Project Lead:
Sandia National Laboratories

The Concept

Commercial-off-the-shelf energy control systems and components are primarily designed, produced, and maintained by foreign companies. With control of commercial hardware and software supply chains and routine access through configuration and updates, foreign developers have an unprecedented opportunity to compromise a system by inserting malicious code.

Trust anchors are independent monitoring and control devices that have access to the inner workings of system components . Trust anchors will give operators unbiased measurements at the lowest levels of a system that independently verify system function, reveal deceptive malicious function, independently attest to system state, and verify the correctness of system tests.

Trust anchors also will give operators unimpeded control capabilities that make it possible to implement trusted control functions, remove discovered malicious content, execute system tests, and analyze and experiment on suspected system compromise.

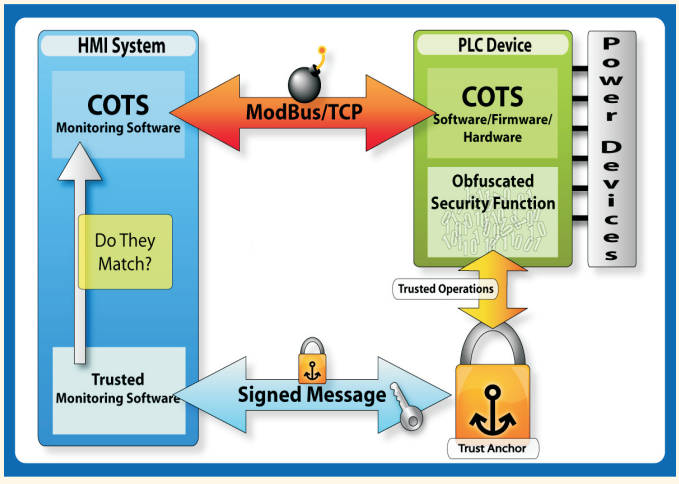
The Approach

Trust anchors use obfuscation technology to ensure that they can operate without being detected by adversaries. Obfuscation cryptographically hides the trust anchors' functions, enabling them to test a system in an unpredictable manner—which greatly increases an adversary's risk of detection when inserting malicious code.

The technology has been implemented and tested using a variety of programming languages. The team is now enhancing it to support Turing Machine (a machine that can simulate the logic of any computer algorithm) obfuscation. This will enable the team to obsfucate more powerful functions, a capability not possible with previous R&D.

Trust anchors verify system function at the lowest level to ensure proper behavior and secure communications between two untrustworthy system components.

In this example, trust anchors are incorporated into a commercial off-the-shelf (COTS) human-machine interface (HMI) system and a programmable logic controller (PLC) to validate that commands to the PLC originated from the HMI and were not injected in the communication stream.



Next Steps

In 2009, a successful laboratory demonstration proved trust anchors' ability to protect a programmable logic controller running on an Intel computer. Next, the team will move trust anchors closer to commercialization by pursuing three goals:

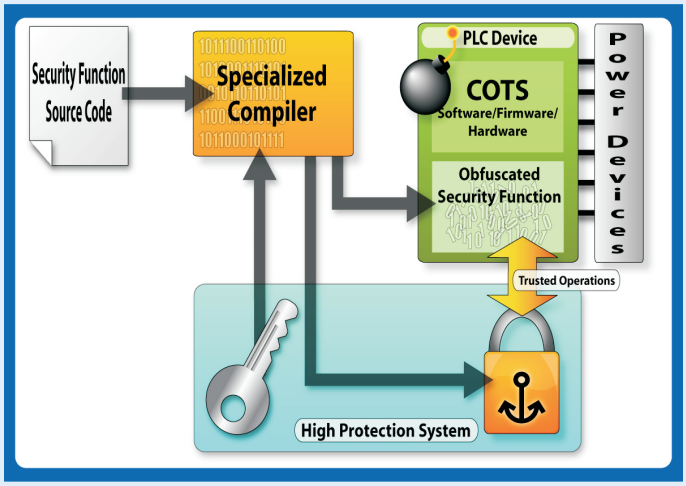
1. Expand functionality to allow trust anchors to run Turing machine logic written in a common programming language
2. Improve performance to ensure acceptable execution speed
3. Port trust anchor functionality to new hardware platforms and operating systems that are more relevant to process control systems

Ultimately, the project will deliver secure, reliable trust anchors that operate without detection by or interference from adversaries.

Benefits

- Provides a higher level of confidence in the correct operation of a system developed using untrusted components
- Offer operators unimpeded control capabilities to ensure correct operation
- Executes tests in an unpredictable manner, greatly increasing risk to adversaries
- Provides tamper-proof security
- Offers protective functions that make the process control system lifecycle harder to compromise

In this scenario, a trust anchor is integrated into a PLC to provide added security against possible lifecycle attacks existing in the COTS software/firmware/hardware residing on the PLC. The trust anchor can be applied to monitor, implement, and authenticate the functions executed within the COTS software/firmware/hardware.



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

Bob Pollack
Sandia National Laboratory
505-844-4442
rdpollo@sandia.gov

Current Contact as of Aug. 2020

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