SAND2023-00544C

Proceedings of the 2023
30th International Conference on Nuclear Engineering
ICONE30
May 21-26, 2023, Kyoto, Japan

ICONE30-1673

APPLICATION OF SECURE ELEMENTS TO ENHANCE REAL-TIME CONTINUOUS MONITORING AND CONFIGURATION

Michael T. Rowland
Sandia National Laboratories
Albuquerque, NM

Benjamin R. Karch
Sandia National Laboratories
Albuquerque, NM

Lee T. Maccarone
Sandia National Laboratories
Albuquerque, NM

ABSTRACT

The research investigates novel techniques to enhance supply chain security via addition of configuration management controls to protect Instrumentation and Control (I&C) systems of a Nuclear Power Plant (NPP). A secure element (SE) is integrated into a proof-of-concept testbed by means of a commercially available smart card, which provides tamper resistant key storage and a cryptographic coprocessor. The secure element simplifies setup and establishment of a secure communications channel between the configuration manager and verification system and the I&C system (running OpenPLC). This secure channel can be used to provide copies of commands and configuration changes of the I&C system for analysis.

Keywords: Instrumentation, Control, Supply Chain, Cybersecurity, Hardware, Root of Trust, Nuclear Power Plants.

1. INTRODUCTION

Supply Chain attacks are of increasing concern. A European Union Agency for Cybersecurity (ENISA) report titled "ENISA Threat Landscape for Supply Chain attacks" noted that "supply chain attacks increased in number and sophistication in the year 2020 and this trend is continuing in 2021, posing an increasing risk for organizations. It is estimated that there will be four times more supply chain attacks in 2021 than in 2020." [1].

The ENISA report lists several publicly disclosed supply chain attacks for which hardware roots of trust are expected to provide varied levels of protection. For example, consider counterfeit of a Hardware Wallet for cryptocurrency. Attackers have demonstrated a capability to provide consumers with counterfeit hardware (USB) based cryptocurrency wallets. Upon the user's insertion of the wallet into a computer, the private keys are then exfiltrated back to the attackers. A hardware root of trust (HROT) would be able to prevent this attack because the counterfeit devices would not have an embedded root of trust capable of providing signed and verifiable information by a trusted public/private key pair.

This paper summarizes research [3] that seeks to evaluate the protections provided by tamper-resistant smart cards and determine whether they are a suitable candidate to provide a HROT within a digital instrumentation and control (I&C) device or platform operated or relied upon by Nuclear Power Plant (NPP) licensees (i.e., critical digital asset (CDA)). This effort leverages the previous report, "A Review of Technologies that can Provide a 'Root of Trust' for Operational Technologies" [2], combined with a reporting mechanism to uncover malicious changes made to the device after the design phase. The findings in [2] indicate that smart cards are particularly well-posed to act as an HROT that provides supply chain protections, as they can be bound to the device at an early stage in the supply chain.

2. BACKGROUND

The Supply Chain Attack Surface (SCAS) [4] is a concept developed by Dr. Shannon Eggers to provide a conceptual overview of the entry points for attacks aimed at compromising Operational Technology (OT) systems within NPP supply chains. The SCAS also identifies the organizations and entry points for these attacks.

The SCAS, depicted in Figure 1, provides the stages and flow between stages in the supply chain for nuclear I&C devices. Additionally, the stages (and the time in between each stage) are labeled with the class of cybersecurity relevant attacks that may occur during that portion of the supply chain. For example, during Factory Acceptance Testing (FAT), the device is under supervision, but could still be vulnerable to Theft of IP or malicious manipulation to configuration data. However, during the custody change between FAT and Installation, malicious personnel could attempt a wider range of attacks, including malicious substitution or insertion of the device or its subcomponents.

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.

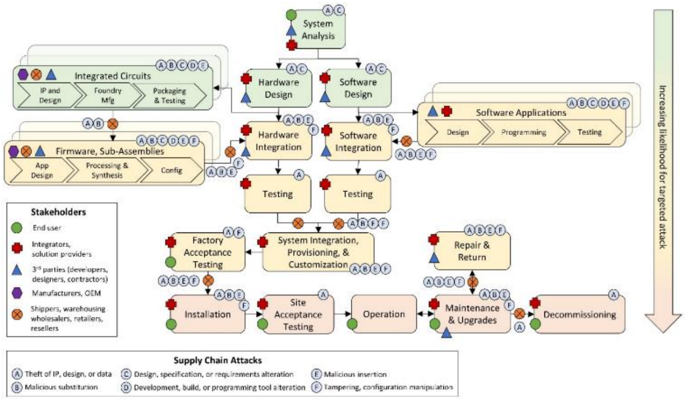

FIGURE 1: SUPPLY CHAIN ATTACK SURFACE [4]

For this research, the attack types from SCAS and the accompanying further analysis in [4] were used to evaluate the protections of HROT. The summary of this analysis [2,4] is captured below with the corresponding confidence in HROT to protect or detect the attack. The confidence ratings include "low", "medium", and "high".

2.1 Theft of IP, Design, or Data

These attacks aim to achieve unauthorized disclosure of information from a stakeholder who has a trust relationship with the end target, enabling future attacks and/or causing economic loss. This information may include but is not limited to intellectual property (IP), design information, operational / configuration data, or stored secrets (i.e., private key, digital certificates).

The HROT Protection confidence against these attacks was evaluated as "low". HROT integration may provide some useful tools that can be used to prevent unauthorized disclosure of sensitive information from a system. These include storage of such information on the HROT, and a lower attack surface on the device containing the HROT due to measures such as a trusted boot. However, a HROT will not prevent an authorized user from maliciously leveraging their authorized access.

2.2 Malicious Substitution

These attacks aim to achieve complete replacement of digital technology, including hardware, firmware, and/or software. Hardware clones or counterfeits may not impact all end users depending on the distribution, whereas a substituted software package may compromise all end users even if only a few were targeted.

The HROT Protection confidence against these attacks was evaluated as "high" as a HROT will be able to provide real time trusted information on the device hardware, firmware and software. This will provide an indicator for an NPP operator to detect the unauthorized substitutions.

2.3 Design, Specification, or Requirements Alteration

These attacks aim to accomplish unauthorized modification of design, specifications, or requirements that compromise the design stages and result in the purposeful inclusion of latent design deficiencies (e.g., requirements that result in vulnerabilities) or built-in backdoors.

The HROT Protection confidence against these attacks was evaluated as "low" as the design specifications and their implementation are authorized and therefore will be certified by the supplier as authorized and valid.

2.4 Development, Build, or Programming Tool Alteration

These attacks are aimed at unauthorized modification of the development environment, including platform, build and programming tools, with the intent to corrupt the device under development.

The HROT Protection confidence against these attacks was evaluated as "medium" as the software and tools/programs should be signed by the supplier allowing for subsequent attempts to alter this signed software as being detectable.

2.5 Malicious Insertion

These attacks aim to achieve an addition or modification of information, code, or functionality directly into a device to cause malicious intent, such as impairing or altering device operation or function.

The HROT Protection confidence against these attacks was evaluated as "high" as these attacks are similar to malicious substitution (see Section 2.2). A malicious insertion during the logistics and ICT transfer to the customer or during operation would be detected by system.

2.6 Tampering and Configuration Manipulation

These attacks aim to unauthorized alteration or fabrication of configuration, non-executable data, or sending of unauthorized commands with the goal of impacting device operation or function.

The HROT Protection confidence against these attacks was evaluated as "medium to high" because changes to non-executable data for which known good/authorized values or ranges are known can be detected. However, not all non-executable data will be known to the level of detail required to not produce false positives. It is infeasible given current I&C systems to enumerate all possible malicious or benign configurations. However, a system with an integrated HROT can provide high reliability reporting of its configuration for record keeping or real time review by trained personnel. Record keeping improves the ability of personnel to attribute a successful attack.

3. RESEARCH METHODOLOGY

The research efforts developed test scenarios to verify that the protections can be implemented using a smart card based HROT. The test results and analysis provide evidence supporting the hypothesis that an integrated HROT significantly lowers the probability (or makes impossible) certain types of attack (See Section 2) that may occur in the supply chain for a digital I&C device.

3.1 Environment

A representative environment was established using single-board computers (i.e., Raspberry Pi 4) that are often used in Internet-of-Things (IoT) implementations, coupled with a commercially available and programmable smart card. This environment, depicted in Figure 2, represents a Programmable Logic Controller (PLC), an HROT, and a Configuration Manager and Verifier (CMV). This environment aligns strongly with how a smart phone, its Subscriber Identity Module (SIM), and a cellular tower confirm a subscriber's (i.e., smart phone) identity and configuration.

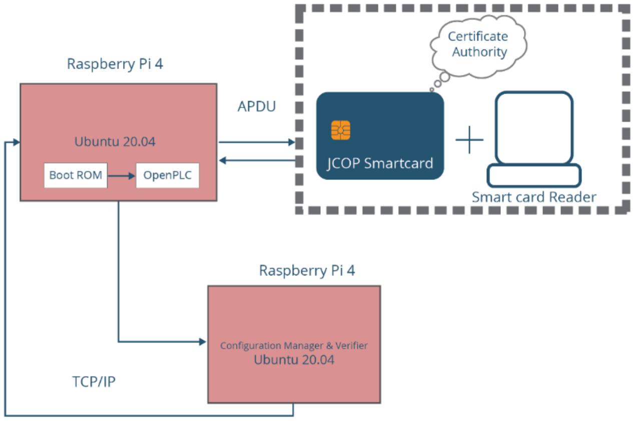

FIGURE 2: ENVIRONMENT ARCHITECTURE [3]

The environment consists of the following major components:

1. The "PLC" – a Raspberry Pi 4 with an Ubuntu 20.04 Long Time Support (LTS) Advanced Reduced Instruction Set Computer Machine (ARM) version running a custom Boot ROM and OpenPLC;
2. Configuration Manager and Verifier – a second Raspberry Pi 4 with an Ubuntu 20.04 LTS ARM version; and
3. The HROT – Implemented using a Java Card Open Platform (JCOP) smart card.

The HROT is integrated with the PLC via a USB card reader. OpenPLC is implemented as a service that begins on the startup of the PLC. The startup script for OpenPLC serves the role of an ad-hoc Boot Read Only Memory (ROM) for the PLC, as it is the first executed file for commencing PLC related functions. The startup script is standard within an OpenPLC installation but has been edited to include routines that interact with the HROT to ensure and report on the trustworthiness of code that is executed subsequently in the greater OpenPLC program. The CMV receives reports from the PLC and uses these reports to make determinations about the PLC's state. The CMV (i) verifies the signature and message data, (ii) maintains the records of state information and allowed configurations, and (iii) tracks reported nonces. There are two possible outcomes from the CMV:

1. The CMV receives information from the PLC that indicates the PLC is outside of its expected state or that it has been altered or replaced; it detects this variation and raises an alarm condition. This is an abnormal condition but may be the result of an authorized change to the PLC, such as maintenance personnel changing PLC firmware to a non-malicious version that has not been authenticated yet. An alarm condition is also raised if the CMV receives information from the PLC where the information reported does not match the expected digital signature which corresponds to the PLC's HROT.
2. The CMV receives information from the PLC that indicates the PLC is within its specification, this information could be later repeated back to the PLC (if it is determined to be misconfigured) so that it can revert to the state requested by the CMV. This would be the normal/expected condition. Note that autonomous reconfiguration is not implemented, but a potential subject of future work.

These binary outcomes are important as it demonstrates how a device (in this case a PLC) may be protected by the HROT, and it also provides a third party a means by which to verify the information from that device. Additionally, the means for a third party to verify the information can be further evaluated to determine the potential for this party to detect attacks. The CMV is running a custom program that provides a determination as to whether the device is a trusted implementation.

The CMV serves essentially the same role as the Policy Engine within a Zero Trust Architecture network, defined in NIST Special Publication 800-207 [5]. In other words, the CMV can receive authentication information from each device before they are allowed to interact with other devices or can revoke devices' access if an attack or misconfiguration is detected. The use of open-source software allows for these programs to be edited to integrate the HROT during various operations. Additionally, the software can be edited and recompiled to simulate an attack on the device's firmware.

Three types of tests were developed to evaluate the protections provided by the HROT. These tests are:

1. Test 1: Malicious Substitution Attacks to evaluate the "high" protection assumed. The malicious substitution attacks make an alteration in at least one of three key places, which are (i) the OpenPLC program (ii) the signature and (iii) the private key used to sign the digest of OpenPLC. The expectation was that the CMV will detect any of these changes.
2. Test 2: Tampering, Configuration Manipulation to evaluate the "medium to high" protection assumed. The attack is a "replay" attack consisting of sending previously captured traffic to a device with the aim to fool the device into performing an undesired action. The expectation was that the CMV will detect the replay of messages via the nonce.
3. Test 3: Malicious Insertion to evaluate the "medium to high" protection assumed. The test consists of hardware measurements which are signed by the HROT and

provided to the CMV to verify that hardware changes have not occurred. The expectation that the CMV will detect changes to these hardware measurements.

4. RESULTS

The results of the tests were as expected, and the specifics of the experiment data can be found in the appendices of [3]. The test results are summarized in Table 1 and described below.

TABLE 1: SUMMARY OF TEST RESULTS

TEST	ATTACK	DETECTED AT CMV	DETECTION METHOD
1	Substitution of OpenPLC	True	Reported hash deviates from expectation / list of acceptable hashes.
1	Substitution of Report Signature	True	Mismatch detected between reported hash and included signa
1	Substitution of Device Private Key	True	Signature verification failure included signature does not verify to any public key in CMV trusted key list.
2	Replay Attack on Device Configuration	True	Nonce collision detected. Replayed device report includes previously seen number that should only be used once.
3	Insertion of Malicious Hardware Subcomponent	Likely	Reported device hardware list differentiates from expected result. This relies on accurate measurement by the device Operating System, which may be subverted by more sophisticated attacks.

Test 1 results demonstrated that the implemented trusted boot attestation provides proof of the PLC's base state (i.e., authenticity). A malicious substitution involves a complete substitution of the device or part of the device. This will result in changes to the report, which the CMV will detect as deviations from the base state and therefore indicators of compromise. A partial substitution will result in changes to the hash of the OpenPLC software or the reported signature, and a complete substitution or counterfeit must use a different private key. This test shows that the CMV can detect either one of these scenarios.

Test 2 provided two important results. The first result is that inclusion of a secure nonce prevents replay attacks in the testing environment. The second result is that the HROT provides the ability to securely generate random data in a timely manner. Combining these two results brings the logical conclusion that it is possible to develop a replay resistant reporting procedure using the HROT to report information that prevents tampering and configuration manipulation attacks.

Test 3 used tools for hardware measurements that rely on the PLC OS's understanding of its hardware, which is built during the boot process. During boot, the BIOS requests configuration information for subcomponents on the system bus. This leads to an implicit trust between the subcomponents and the PLC, and therefore an implicit trust between the greater OT environment and the PLC's subcomponents. It may be possible that a device that can serve as a client (such as a Field Programmable Gate Array (FPGA)) to perform an analysis of the system bus using timing or power analysis to improve the accuracy and completeness of the information provided to the HROT. In short, Test 3 shows that the HROT provides protections against malicious insertion attacks if there is an accurate way to measure the hardware components of the device.

5. DISCUSSION

The proof-of-concept test bed design limited what could be inferred about the HROT protections and specifically its applicability in actual I&C systems.

For instance, timing for operations done on the HROT is very important as many of the digital I&C devices will need to provide real time or near real time performance. Testing performed for the baseline evaluation of the smart card used for this research indicates that operations such as secure random number generation are done in a timely manner. The difference between a request for 8 bytes of random data's max recorded time and the max recorded time for 8 bytes of static data was 3 milliseconds, and both performed the same during their minimum recorded time. This indicates that the time required for random number generation on the card is negligible, but there is certainly room for improvement on the communications speed. It should also be noted that the communications occur over a standard USB card reader. The speed of communications would likely improve through upgrade of the card reader to a faster interface such as USB-C (i.e., the limiting factor of the communications speed in the experiments was the Bus speed). Additionally, there response times would likely be even lower if the device was connected over a bus such as I2C or SPI where the HROT could be directly interfaced.

Additionally, the current test bed design limits the finding associated with Test 2 by not handling extended APDU (i.e., larger messages). This means that the protocol used to communicate with the HROT is of insufficient size in the APDU to include both the nonce and the signature. This limits the protection offered by the HROT as the signature cannot be verified because there is a "fresh" nonce prepended to the message. This is a limitation of the current testbed implementation and not the HROT technology. A smart card with a more recent or feature-rich version of the Java Card OS could leverage the extended APDU to overcome this challenge.

A possible solution could be to implement a secondary command in which after the signature is returned the device sends an additional APDU requesting the last random nonce used for signature generation. Preferably, the implementation would utilize a signature routing such as Elliptic Curve Digital Signature Algorithm (ECDSA) which implements a random nonce by default [6]. It is vital that a final solution ensure that random number generation be secure and used only once, as improper use of random numbers or faulty random number generation can have critical impacts, such as allowing recovery of the private key [7]. Newer versions of Java Card and other smart card Operating Systems support both extended APDU and ECDSA.

Solutions to the timing challenges and the limitations with respect to APDU are being actively investigated. One of the goals of this research is to minimize the challenges to adoption for HROT to defend against supply chain attacks and act as a trust anchor for possible future implementations of ZTA.

6. CONCLUSION

The research has found that assumptions on protection from categories of supply chain attacks listed in Section 2, are qualitative but can be improved based upon the findings of the report [3]. The HROT demonstrated detection of the evaluated supply chain attacks and should lead to increased confidence of the against both tampering/configuration manipulation attacks and hardware substitution attacks and replay attacks, with less protection provided against malicious insertion attacks.

ACKNOWLEDGEMENTS

This article has been authored by an employee of National Technology & Engineering Solutions of Sandia, LLC under Contract No. DE-NA0003525 with the U.S. Department of Energy (DOE). The employee owns all right, title and interest in and to the article and is solely responsible for its contents. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains a non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this article or allow others to do so, for United States Government purposes. The DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan https://www.energy.gov/downloads/doe-public-access-plan.

REFERENCES

[1] ENISA, *ENISA Threat Landscape for Supply Chain Attacks*. 2021, European Union Agency for Cybersecurity (ENISA).

[2] Rowland, M. and B. Karch, *A Review of Technologies that can Provide a 'Root of Trust' for Operational Technologies*. 2022, Sandia National Laboratories.

[3] Karch, B. and M. Rowland. *Security Evaluation of Smart Cards and Secure Tokens: Benefits and Drawbacks for Reducing Supply Chain Risks of Nuclear Power Plants.* 2022, Sandia National Laboratories.

[4] Eggers, S. and M. Rowland. *Deconstructing the Nuclear Supply Chain Cyber-Attack Surface*. in *Proceedings of the INMM 61st Annual Meeting*. 2020

[5] National Institute of Standards and Technology, *Zero Trust Architecture*, SP 800-207. 2020.

[6] National Institute of Standards and Technology, FIPS PUB 186-4, in Federal Information Processing Standards Publication, NIST. p. 130, 2013.

[7] Schmid, M., ECDSA - Application and Implementation Failures, UC Santa Barbara, 2015.