Position Paper: Protecting Process Control Systems against Lifecycle Attacks Using Trust Anchors

Adrian R Chavez
Sandia National Laboratories[1]
adrchav@sandia.gov

Abstract

Critical infrastructure systems are vulnerable to physical and cyber attack. Securing these systems is a top priority for the U.S., but ongoing efforts ignore important aspects of the information technology (IT) lifecycle and focus primarily on securing the operational phase of these systems. Adversaries have ample opportunity to compromise our critical systems at every stage of those systems' lifecycles. We propose the use of trust anchors—functional elements that can be developed through trustworthy processes and introduced into process control systems to provide critical security services that cannot be influenced by malicious content— to address the lifecycle threats of the process control system. Secure obfuscation technology developed by Sandia National Laboratories enables one of the most important capabilities of trust anchors: It obfuscates trust anchors' functions and renders them tamper-proof in a cryptographically secure manner.

Introduction

Development and implementation of process control systems is a global industry; these critical systems are designed, integrated, and maintained with varying degrees of trustworthiness. The global supply evolved to satisfy economic goals, and is counter to basic security needs. In these systems, cyber vulnerabilities exploited in a process control system can lead to physical vulnerabilities.

Our current security techniques, analyzing and testing systems to find vulnerabilities followed by patching those vulnerabilities, is inadequate. This approach can never prove system security; it can only identify specific shortcomings. These systems are too complex to analyze for security issues; this makes it impossible to detect and remove all potential vulnerabilities.

This task explores a fundamentally different approach for ensuring process control system security. We introduce the concept of a trust anchor—an independent monitoring and control device that has access to a component's inner workings—that may be integrated into an untrustworthy system to inspect and verify its functions at the lowest level. Program obfuscation technology developed by Sandia National Laboratories enables one of the most important features of trust anchors: It obfuscates their functions and renders them tamper-proof in a cryptographically secure manner. This technology enables the trust anchor to dynamically monitor software integrity in real time, which greatly increases the risk to an adversary intending to insert malicious code. Sandia has already developed prototype trust anchors, but this technology has not yet been applied to process control system security.

Trust Anchors

Trust anchors are functional elements that can be introduced into information systems to provide unbiased measurement and unimpeded control capabilities. Trust anchors provide verification that systems function correctly and a foundation for additional, independent security services. Sandia's cryptographically secure obfuscation technology ensures that trust anchors are tamper-proof and that their function cannot be derived by an adversary. Although the overall security of a system can never be completely proven, trust anchors serve to greatly increase the risk to an adversary attempting to insert malicious function.

The threat model that trust anchors address

[1] Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. This work was supported by the National SCADA Test Bed (NSTB) program at the United States Department of Energy's Office of Electricity Delivery and Energy Reliability.

comprises of four components:

- Hardware and software supply chains must be assumed to be untrustworthy.
- Routine system administration, configuration, and updates cannot be proven trustworthy.
- Unbiased measurement of operational system components is currently impossible.
- Our systems are too complex to reliably analyze.

Trust anchors provide two core services—unbiased monitoring and unimpeded control—that provide a flexible foundation for multiple security services. The ability to provide unbiased measurements at the lowest levels of a system enables trust anchors to independently verify system function, reveal deceptive malicious function, independently attest to system state, and verify the correctness of system tests. Trust anchors' control capabilities make it possible to implement trusted control functions, remove discovered malicious content, execute system tests, and conduct experiments on and analysis of a suspected compromise. A trust anchor at the lowest level of a system provides a root of trust, and additional trust anchors can be promoted dynamically to ensure correct operation at all system levels.

Trust anchors have several important security properties that enable them to serve as an effective security tool. First, because of their low complexity, trust anchors can be built and managed in a trusted lifecycle completely removed from the systems that they protect. The lack of complexity also allows for meaningful and effective security analysis with conventional analysis techniques.

The remainder of trust anchors' security properties are provided by Sandia's secure obfuscation technology. Although it may be possible for a system to detect the physical presence of a trust anchor device, our obfuscation technology ensures that an adversary

- Cannot be aware of what the device is measuring
- Cannot understand the function or modify it, and
- Cannot subvert the system, as any modification will be immediately evident.

These properties introduce a significant element of uncertainty into an adversary's attempts to compromise a system. By hiding the actual function of the device, including what system tests it may perform, an adversary will not have any predictable test vectors to work around. This greatly increases the risk to an adversary intending to insert malicious function.

Secure Obfuscation Technology

Sandia's secure obfuscation technology[1] is mathematically provable obfuscation that enables some of our trust anchors' most important capabilities. Code obfuscation is an active area of academic research, but most findings have merely demonstrated that general obfuscation is impossible. By modifying the security model such that we may rely on the presence of a small, tamper-protected device, however, Sandia has developed an effective method for obfuscating code.

Our secure obfuscation technology uses a customized compiler to obfuscate a software program, hiding the program's functionality from analysts and reverse engineers. The obfuscated code can then be executed with the aid of a small tamper-protected device, an *oracle*, which interprets the obfuscated code and ensures its integrity. This oracle must be protected, as it is the key to deriving the function of the obfuscated code. The obfuscated code can execute only when in communication with the oracle, and the code remains obfuscated regardless of whether it is executing or at rest. Figure 1 shows the obfuscation model.

The computations that the oracle must make are very simple, and its required storage space is minimal and independent of the size of the obfuscated code. The oracle's computation is sufficiently simple that it can be implemented on a variety of platforms: a network server, USB drive, crypto card, or even a smartcard. The system is also scalable, as a single oracle can be made to execute a variety of obfuscated programs.

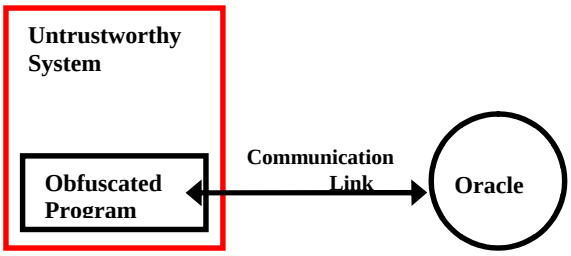

Figure 1: The obfuscation model.

Effective program obfuscation provides a significant advantage in safeguarding information systems that protect our national security assets. Unlike many security technologies, Sandia's obfuscation technology has been mathematically proven to be secure. Under our model, an adversary is allowed to make queries to the tamper-protected device and view its

outputs, but is not allowed to examine its internal computations. The obfuscation routines are based on established and widely accepted cryptographic standards that are provably secure. The model satisfies two important security properties:

- The obfuscated code behaves as a true black box, assuming the oracle is properly protected.
- The original algorithm will at most only see a polynomial time slowdown. Internal testing has shown a linear slowdown with a coefficient of two.

Trustworthy Process Control Systems

Introducing trust anchors into otherwise untrustworthy process control systems affords both a higher level of confidence in the correctness of a system and the ability to assume control of a system to ensure correct operation. Once this concept has been demonstrated and proven, we envision ubiquitous use of trust anchors in process control systems to ensure security.

While trust anchors' protective functions will make the process control system lifecycle harder to compromise, the unpredictable nature of the tests the trust anchors will execute, made possible by Sandia's secure obfuscation technology, will greatly increase the risk to an adversary attempting to effect such a compromise.

Under current security models, an adversary can assess the risk of an operation and make an informed decision about whether to proceed with an attack based on an estimable cost, benefit, and risk. Trust anchors affect such risk analyses in two ways: First, trust anchors serve as an effective defensive technology, and will increase the probability of an attack failing or being detected. Second, because trust anchors are obfuscated and an adversary therefore cannot predict their behaviors, they add uncertainty to any adversary's risk analysis equation. If the probability of success or failure cannot be accurately quantified, risk assessment and decision-making processes are made much more difficult.

Trust anchors could be integrated into process control systems through requirements that manufacturers incorporate trust anchor interfaces into new products. The specification for these interfaces can be entirely open without revealing significant information about the trust anchors or their behaviors. Sandia is currently implementing a prototype process control system with an integrated trust anchor, ordering an independent vulnerability assessment of that device, and developing use cases and a plan for commercialization.

Cyber Physical Security Applications

When physical actions are controlled through cyber means, validation and anti-reverse engineering become necessary to begin to address insider and lifecycle threats. Trust anchors posses the required security properties needed to satisfy these requirements.

Trust anchors have been applied and tested on a prototype control systems through Sandia's Virtual Control System Environment (VCSE). Trust anchors were used to verify and monitor the state of a virtual Remote Telemetry Unit (RTU) in VCSE reported by a Human Machine Interface (HMI). To integrate the trust anchor into the virtual RTU, the register values were extracted and modifications to those register values were treated as transitions in a Finite State Machine (FSM). The resulting FSM was then obfuscated and added to the RTU to monitor register values and authenticate those values to an oracle machine residing on a separate system. The oracle has a relatively small footprint (roughly 5KB). Part of this design decision was made to keep costs low and to make commercialization scalable. Through this proof of concept demonstration, trust anchors did not negatively impact system performance or latency within VCSE.

From the properties that trust anchors provide, system verification, monitoring, and function obfuscation can easily be achieved and integrated into a cyber physical environment. Minimal system resources are required to implement the trust anchor software and are a promising technology to begin to address the lifecycle threats.

Research Advances

Our current work has proven that we can securely obfuscate FSM's. However, FSMs have the drawbacks of manually translating source code to FSMs and exponential state blowup, making them unusable in large, time-sensitive applications. Our work can be extended by developing a more generalized solution that can be used in a much greater number of applications. Code obfuscation has traditionally failed because the methods used have relied strictly on the ability to obfuscate code before (not during) execution and on the assumed restrictions of adversaries' analytical capabilities; these limitations have made such obfuscation techniques inherently weak. Our unique techniques obfuscate code before and during code execution and assume the adversary has state-of-the-art analytical capabilities.

Extending this work by demonstrating that we can successfully obfuscate an arbitrary piece of software is a research area of interest. The methods used to accomplish this will once again utilize FSMs, but with the addition of an obfuscated memory stack to keep track of the symbol table variables. The memory stack will be obfuscated similarly to the way the FSM was obfuscated. A customized source-to-source compiler is necessary to accomplish this goal. Once complete, executing obfuscated C code will, ideally, be as simple as making a standard C function call.

A prototype of an obfuscated piece of source code functioning in a large scale system will be a useful data point in assessing the technologies capabilities. Performance testing would need to be conducted on our solution along with an analysis of the efficiency of the algorithms. The customized compiler would be responsible for generating an executable C program from a piece of source code that implements a critical function. It is important to note that only the critical functions necessary for a system to operate properly need to be extracted and obfuscated. The obfuscated code will be called from non-critical code that depends on the critical obfuscated functions to operate correctly.

Acknowledgments

The authors gratefully acknowledge the National SCADA Test Bed (NSTB) program at the United States Department of Energy's Office of Electricity Delivery and Energy Reliability which provides the funding for this research.

References

[1] W. Erik Anderson, On the Secure Obfuscation of Deterministic Finite Automata, Sandia National Laboratories, Cryptology ePrint Archive (http://eprint.iacr.org), Report 2008/184