TCIPG Trustworthy Cyber Infrastructure for the Power Grid | tcipg.org

Trustworthiness Enhancement Tools for SCADA Software and Platforms

Overview and Problem Statement

Our ultimate goal is to preserve the trustworthiness of the various control systems being rolled out as part of the smart grid. These systems present a unique challenge from an IT perspective, since they a) are fairly static devices, b) are expected to remain in service for up to several decades, and c) must perform their prescribed tasks in the face of both accidents and malicious intrusions. On top of all that, any security solutions installed on such systems must be lightweight enough not to get in the way of the system's primary function.

To address those issues, we have built a number of flexible, lightweight security systems that can live at many different levels inside a device, ranging from process-level protection to low-level network message encryption. The complete list of solutions can be found below.

The Stack of Trust: A Multi-Layered Protection Strategy

Trust Stack Level	Our Solution
Process-Level Mediation	ELFBac: An instrumentation system for programs that allows users to isolate and secure pieces of a binary without needing to rewrite the original program. *Status: Linux prototype exists; looking for collaborators!*
System Call Mediation	Behavior-Based Policy: Policy languages that clearly identify trustworthy behaviors, and use techniques such as context-dependent goals and isolation primitives to enforce the policy. *Status: In development; looking for collaborators!*
Kernel Host Intrusion Detection System	Autoscopy Jr.: An intrusion detection system that lives within the OS kernel itself, monitoring for control-flow anomalies while imposing minimal overhead. *Status: Complete*
Hardened Kernel	grsecurity/PaX*: A set of kernel hardening patches that include additional OS protection mechanisms. *Status: See * note below table*
Custom Trapping Scheme	FlexTrap: A system that allows for variable-sized caching in the Translation Lookaside Buffer (TLB) of a system, letting users define their memory accesses to be as coarse or granular as needed. *Status: In development; looking for collaborators!*
Kernel Drivers	CrossingGuard: An application of traditional IP network defenses to the USB interface. *Status: In development; looking for collaborators!*
Network Hardware	Predictive YASIR: A low-latency message authentication system that tries to predict the plain-text content of messages and pre-send the ciphertext before receiving the entire message. *Status: Complete*

*Note that grsecurity/PaX is © Open Source Security, Inc., and is NOT a Dartmouth product, but rather a set of patches that are freely available at http://grsecurity.net.

Results and Benefits

- We have developed an ELFBac prototype and demonstrated its potential by using it to protect sensitive data within a parsing library, even after a bug in the library had been exploited.
- We evaluated the performance impact of Autoscopy Jr. on a non-embedded kernel configuration, and found that after our profiler was applied, it imposed less than a 5% overhead on our benchmark tests. We have since provided the program to Schweitzer Laboratories, which used it as the basis for their own protection system for their product line.
- In testing using the Modbus protocol, Predictive YASIR offered a significant latency improvement over both its non-predictive YASIR predecessor and the AGA SCM bump-in-the-wire device.
- Our ELFbac implementation for Linux x86-64 is in code review; an ARM feasibility study has concluded.
- We developed the concept of Intent-level semantics for application security policies, presented at a variety of industry events, including Intel and Microsoft invited talks.
- We demonstrated a new threat model for embedded systems firmware, which allows an unscrupulous vendor or a supply chain attacker to plant an innocent-looking “bug door” in the interrupt-handling code, which nevertheless allows exfiltration of secrets or sensitive parts of firmware from a “bugdoored” device. To be presented at the ACSAC 2014 conference.
- **Technology Readiness Level:** Varies by product; see table above.

Researchers

- Sergey Bratus, sergey@cs.dartmouth.edu
- Peter C. Johnson, pete@cs.dartmouth.edu
- Jason Reeves, reeves@cs.dartmouth.edu
- Rebecca “bx” Shapiro, bx@cs.dartmouth.edu
- Anna Shubina, ashubina@cs.dartmouth.edu
- Sean W. Smith, sws@cs.dartmouth.edu
- And many others! (ask one of the above for contact info)

Industry Collaborators

- Schweitzer Engineering Laboratories (Autoscopy Jr., ELFbac)