TCIPG

Trustworthiness Enhancement Tools for SCADA Software and Platforms

Julian Bangert, Sergey Bratus, Peter C. Johnson, Jason Reeves, Rebecca Shapiro, Anna Shubina, Sean W. Smith
(along with many others)

Today's Power Grid

- The power grid is a real-time system that requires a cyber infrastructure to control and maintain it.
- The grid presents a unique IT challenge, since devices in the grid are fairly static and expected to run for many years/decades.
- The rise of the "smart grid" (computational power plus network connectivity) has increased the grid's attack surface.
- Availability trumps all other security needs; any security solutions employed on a grid device *cannot* interfere with the device's primary function.
- *How do we maintain the trustworthiness of devices inside the power grid without affecting their functionality?*
  - Our idea: Build flexible, lightweight security systems that can operate at many different levels inside the device.

The Stack of Trust: A Multi-Layered Protection Strategy

Process-Level Mediation

ELFBac *(Bangert, Bratus, Reeves, Shapiro, Shubina, Smith)*

- Instrumentation system for binary programs
- Allows users to isolate/secure pieces of a program without rewriting it (useful for legacy power programs)
- ***STATUS: In development, and looking for collaborators!***

System Call Mediation

Behavior-Based Policy *(Bratus, Locasto, Otto, Shapiro, Smith, Weaver)*

- Policy languages that clearly identify what behaviors are trustworthy, and what programs are allowed to engage in them
- Involves defining context-dependent goals, enforcing counting primitives to limit computation, and using isolation primitives for separation
- ***STATUS: In development, and looking for collaborators!***

Kernel Host Intrusion Detection System

Autoscopy Jr. *(Reeves, Ramaswamy, Locasto, Bratus, Smith)*

- Lives within the operating system kernel (no need for a hypervisor)
- Watches for control-flow anomalies that could indicate a compromise
- Imposes minimal overhead on the host device
- ***STATUS: Complete. Technology being transitioned to SEL.***

Hardened Kernel

grsecurity/PaX (http://grsecurity.net)

- Kernel-hardening patches for Linux devices
- Includes address space layout randomization, memory-page execution protections, and role-based access control, as well as other behavioral features
- ***STATUS: Commercially available***

Custom Trapping Scheme

FlexTrap *(Bangert, Bratus, Locasto, Ramaswamy, Smith)*

- Scheme that enables variable-sized caching in the Translation Lookaside Buffer (TLB) of a system
- Allows administrator to define memory accesses to be as coarse (for performance) or granular (for protection) as desired
- ***STATUS: In development, and looking for collaborators!***

Kernel Drivers

CrossingGuard *(Johnson, Bratus, Smith)*

- Application of traditional network defenses to the USB interface
- Involves a complete mapping of the USB attack surface
- Currently examining the interface to see where mediation will be most effective
- ***STATUS: In development, and looking for collaborators!***

Network Hardware

Predictive YASIR *(Solomahkin, Tsang, Smith)*

- Low-latency message authentication system
- Predicts plaintext based on previous observations, and pre-sends ciphertext before entire message is received
- Significant latency improvement shown in testing on SCADA protocols
- ***STATUS: Complete***

NOTE: indicates a project developed at Dartmouth. grsecurity is © Open Source Security, Inc., 2011.