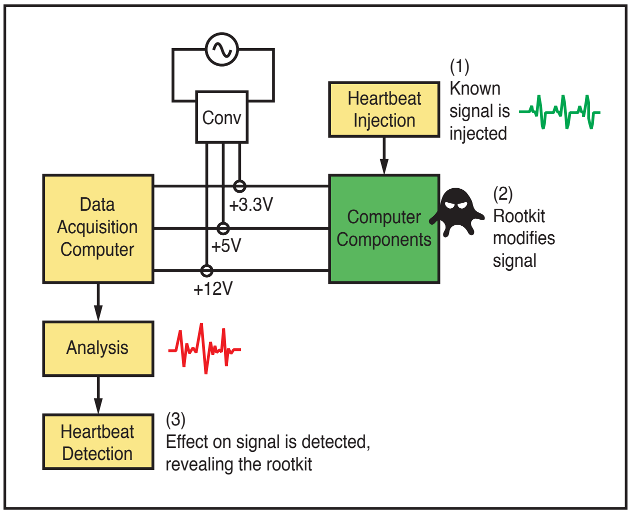
Heartbeat – Cyber Anomaly Detection through Side-Channel Analysis of Periodic System Function Invocation

Problem: Malware infections and cyberattacks are escalating in frequency, sophistication, and severity, creating an urgent demand for next generation sensor and analysis technologies. In response to this, the cyber security market reached $150 billion in 2017. However, legacy signature or heuristics-based solutions are unable to keep up with the flood of new polymorphic malware samples, or to address the powerful and stealthy tactics of kernel-level rootkits.

Solution: Heartbeat responds to this problem by focusing instead on the physical behavior of the device being protected, under the hypothesis that malware infection will produce a measureable change in the power consumption state of a device that can be picked up by an outside detector. All code execution uses power, so the execution of malware—especially polymorphic variants—will leave a trace on a power consumption record. The Heartbeat system collects power trace measurements directly from the hardware and so is invisible to malware and resilient to internet service interruption. By collecting power measurement data only during the periodic invocation of a single or of several system functions, Heartbeat will address several challenges that plague current anomaly-based intrusion detection systems and is operational-context agnostic.

Impact: Heartbeat will provide a significant market advantage to three main industries: threat intelligence, endpoint security, and unified threat management industries. First, Heartbeat will achieve efficiency, scalability, and flexibility by implementing a data collection process that has low computational requirements, is fast, and makes use of mechanisms—namely, system and API calls—that are present in almost all modern computing systems. Second, Heartbeat will achieve accuracy through execution-independent data collection and a flexible algorithm that is modular and analysis-agnostic, permitting different analysis techniques for different device classes. Finally, because the Heartbeat data collection will require minimal configuration and user knowledge, Heartbeat will achieve ease of use and user friendliness.



Conv
Heartbeat Injection
(1) Known signal is injected
Data Acquisition Computer
+3.3V
+5V
+12V
Computer Components
(2) Rootkit modifies signal
Analysis
Heartbeat Detection
(3) Effect on signal is detected, revealing the rootkit

Publications

- J. M. Hernández, R. A. Bridges, J. A. Nichols, K. Goseva-Popstojanova, and S. Prowell, "Towards a Malware Detection Framework Based on Power Consumption Monitoring," Proc. of the 12th Annual Cyber and Information Security Research (CISR) Conference, Oak Ridge, TN, April 4–6, 2017.
- J. M. Hernández, A. Ferber, S. Prowell, and L. Hively, "Phase-Space Detection of Cyber Events," Proc. of the 10th Annual Cyber and Information Security Research (CISR) Conference, Oak Ridge, TN, April 7–9, 2015.
- S. J. Prowell and C. Rathgeb, "Statistical Fingerprinting for Malware Detection and Classification," US Patent 9,135,440, filed July 31, 2013.

Stacy Prowell, PhD
Computing and Computational Sciences Directorate

Dr. Stacy Prowell serves as the chief cyber security research scientist in the Computing and Computational Sciences Directorate at ORNL and is the program manager for the lab's Cybersecurity for Energy Delivery Systems program. Dr. Prowell's research focuses on exploiting physical sensors and properties to detect and prevent intrusion, on deep semantic analysis of compiled software, and on the security of safety critical systems. Dr. Prowell's work on a system for deep analysis of compiled software led to the Hyperion system, which received a 2015 R&D 100 award and two awards for technology transfer. Previously, Dr. Prowell worked in the CERT Program of the Software Engineering Institute on automated analysis of malware.

Intellectual Property

Tampering Detection Heartbeat; 62/506,170

System and Method for Monitoring Power Consumption to Detect Malware; 62/506,114

An Anomaly Detection Ensemble for Time-Series Data; 62/608,750

For more information, please contact
David Sims
Commercialization Manager
simsdl@ornl.gov
865-241-3808