The Embedded Sensors Project

Center for Education and Research in
Information Assurance and Security (CERIAS)
Purdue University
http://www.cerias.purdue.edu/homes/esp/
cerias-proj-esp@cerias.purdue.edu

The Embedded Sensors Project is an advanced research project in intrusion detection. Internal sensors and detectors are placed at critical points inside operating system, network stack, and application source code. The sensors and detectors, which consist of relatively small amounts of source code, detect attacks against the system. Information collected by sensors is passed to an internal support framework for logging and reporting purposes. Sensors are difficult for attackers to circumvent, tamper-resistant, provide both host and network attack detection, consume few system resources, and provide near real-time detection.

The research prototype was developed on OpenBSD, an open source operating system. This operating system platform was chosen because of the OpenBSD developers' strong stance on system security, availability of inexpensive and reliable hardware, and availability of the source code.

We plan to expand upon the initial research and port the sensor support framework and the sensors themselves to a FreeBSD release and make it available to other researchers and experimenters. We also plan to do further research into designing sensors that detect unknown attacks and the issues of large-scale sensor deployments. To demonstrate the efficacy of the embedded sensor concept, we plan to make the sensor support framework portable so that other systems and applications can incorporate sensors and detectors.

What are Sensors and Detectors?

ESP uses both internal sensors and embedded detectors. An internal sensor is a piece of code built into a program that monitors a specific variable or condition of that program. The program in question could be the Unix kernel, a system utility, or a high-level application. By being built into the program that it is monitoring, an internal sensor can perform direct monitoring on the system, which allows it to obtain information that is reliable (very difficult to modify, either by accident or by a malicious attack) and near real-time (obtained almost at the moment it is generated). An embedded detector is a piece of code built into a program that looks for specific signs of specific attacks or intrusions. An embedded detector bases its decisions on an internal sensor, either explicitly (when the sensor is clearly differentiable from the detector) or implicitly (when the sensor is part of the detector, this is usually the case when the checks are very simple).

Benefits

Embedded sensors operate in a different manner in comparison to other intrusion detection systems. The sensors are themselves resistant to attack. They are also effective in detecting attacks in near real-time with minimal impact on system performance.

Difficult to Circumvent

Sensor code is internal to the kernel, executable code, and libraries. Sensors are also placed at specific and critical points in the execution path of running code. An attacker is unable to bypass the sensor and still exploit the vulnerability.

Tamper-resistant

Because the sensor is part of the code that it protects, it is difficult extract or remove it. This limits ways in which an attacker can disable a specific sensor.

Host and Network Attack Detection

The sensors detect attacks against the operating system kernel, services, and applications. They also detect network-based attacks for other operating systems (i.e. WinNuke, Ping of Death, NetBSD TCP Race Condition, etc).

Low Resource Overhead

Sensors are only active when checking specific areas of code where attacks occur; they do not run all the time or as independent agents. Sensor code is not executed until the vulnerable code is about to be executed. Sensors do not impact the normal operation of the system.

Near Real-time Detection

The attack is detected at the exact moment that the vulnerability is exploited. An attack is immediately detected thus allowing administrators more time to deal with the issue. Because attack detection is near real-time, ESP does not require storage and analysis of large amounts of data.

Almost No False Negatives

The initial research showed that out of 150 sensors implemented for specific vulnerabilities, only one (Fraggle attack detector) occasionally generated a false positive alarm. Meanwhile, the system detected all known attacks tried against it. The overall results of the research prototype showed favorable detection rates.

Current Work

We are currently investigating the following:

- **Sensor Placement in High Profile/Volume Network Services: Apache, BIND, OpenSSH, Sendmail**
- **Sensor Message Management System for processing IDS messages**
- **Performance Evaluation of Sensor-Enabled Services**
- **Scalability Analysis over a Range of Network Services**
- **Building Testbed for Sensor Development**
- **FreeBSD-based Implementation**

Future Research

Research for the Embedded Sensors Project is ongoing. There are a several interesting avenues that we plan to explore.

Meta-detector Design

Research has shown that unknown attacks can be detected using sensors and detectors. We explore more formal ways in which to design and implement them.

Portable Sensor Framework

We plan to create a portable framework that will support the implementation of sensors for other operating system platforms.

Modular Response Mechanism

Handling attack data after the attack occurs is needed. We plan to design and build a mechanism to respond to attacks or borrow interesting technology from other projects.

Selected References

- Diego Zamboni. Using Internal Sensors for Computer Intrusion Detection. Ph.D. Thesis, Purdue University, August 2001.
- F. Kerschbaum, Eugene H. Spafford, and Diego Zamboni. Using embedded sensors for detecting network attacks. In Deborah Frincke and Dimitris Gritzalis, editors, *Proceedings of the 1st ACM Workshop on Intrusion Detection Systems*. ACM SIGSAC, November 2000.
- Eugene H. Spafford and Diego Zamboni. Design and implementation issues for embedded sensors in intrusion detection. Presented at the Third International Workshop on Recent Advances in Intrusion Detection (RAID2000), October 2000.
- Diego Zamboni. Doing intrusion detection using embedded sensors-- thesis proposal. CERIAS Technical Report 2000-21, CERIAS, Purdue University, West Lafayette, IN, October 2000.
- Eugene Spafford and Diego Zamboni. Data collection mechanisms for intrusion detection systems. CERIAS Technical Report 2000-08, CERIAS, Purdue University, 1315 Recitation Building, West Lafayette, IN, June 2000.
- Florian Kerschbaum, Eugene H. Spafford, and Diego Zamboni. *Embedded sensors and detectors for intrusion detection.* Journal of Computer Security*, 2001.*