



Information System Security Operation

System Health and Intrusion Monitoring

Dynamic Behavioral Constraints as an Aid to Detect Novel Attacks

Overview

Despite the advances in security and software engineering, it is unquestionable that computer systems today still contain vulnerabilities. The System Health and Intrusion Monitoring (SHIM) project research focuses on:

- Accurate and effective detection of zero-day exploits and attacks; and
- Strategic and accurate information about the detected intrusive events to allow for intelligent response.

To detect novel attacks, SHIM employs a set of dynamic behavioral constraints that can be tailored to different environments. The constraints describe the correct operation of a system at different levels of abstraction – system-level, system-service, host-level, and application-specific constraints which deal with data integrity, program integrity, interaction between programs, temporal properties of programs, and resource usage.

In addition, this research identifies attack information that is useful for response analysis that may include the information about rogue processes and objects being damaged or service disrupted. This research also investigates a systematic way to associate the identified attack information to violations of constraints.

Approach

Even with the best security mechanisms, we must expect that a determined adversary will be able to penetrate our defense. The current state-of-the-art is that only known attacks can be accurately detected and primitive response performed. We are vulnerable to zero-day

exploits that attackers exploit vulnerability on the same day as learned about by the vendor and no patch is available. To enhance a system's resiliency to attacks, we are investigating a new approach, SHIM, to continuously monitor and assess the health of a large system that could accurately detect novel attacks and provide strategic information to effectively tolerate attacks.

SHIM continuously monitors the health of a large system so that system abnormalities (e.g., attacks or operational errors) can be promptly detected and handled appropriately. Instead of focusing on vulnerabilities and attacks, SHIM employs a hierarchy of behavioral constraints that model the expected or correct system behavior at different levels of abstraction. The constraints are systematically developed from a system policy model, which takes into account system semantics, security principles, existing attacks, and vulnerabilities. The constraints also provide hints on the possible consequences (e.g., object damaged) if the constraints are violated. The constraints will be checked at run time for unexpected behavior. As the constraints model correct system behavior, SHIM can detect attacks or exploitation of vulnerabilities without knowledge about the attacks or vulnerabilities. Therefore, SHIM is able to detect zero-day attacks. In addition, SHIM technology can be integrated with the attack-tolerance mechanisms such as the mechanisms developed in the Intrusion Tolerant Distributed Object System Project at SPARTA to completely tolerate attacks.

We are developing a generic constraint model that can be instantiated to different environments. The model includes the following types of constraints:

- Data-integrity: restricts the value of critical data (e.g., a file, an attribute of a file, or

This work sponsored by DARPA through the Cyber Panel program, under Air Force Research Laboratory (AFRL) Contract Number F30602-00-C-0201.

- kernel data structure) and how it can be modified.
- Program-behavior: restricts the behavior of critical programs in a system, such as the files a program should access.
- Interaction: confines the way programs interact with each other to avoid unnecessary sharing of mechanisms or data (the principle of least common mechanisms).
- Temporal: confines the way distributed programs access shared objects (e.g., atomicity and serialization), and how the system should progress.

- Resource-usage: limits how resources should be used to ensure availability.

We have developed SHIM host monitors that detect intrusions on Linux machines. SHIM is effective in detecting known and unknown attacks including zero-day exploits, Internet worms, external penetrations, and internal misuses that cause programs to behave differently from their expected behavior. In addition, SHIM host-based technology, which intercepts user and kernel-level operations without sacrificing performance, is not affected by evasion techniques that elude many network-based intrusion detection systems (IDS).

Overview of SHIM

