Intrusion Detections Systems (IDS) for Inhibiting Attacks on Network Applications

“Lead Inventors: Michael Locasto, Salvatore Stolfo, Angelos Keromytis, and Ke Wang

Network Defense Systems Require Reliable, Targeted, Adaptive Response to Evolving Threats One key problem for network defense systems is the inability to mount a reliable, targeted, and adaptive response to evolving threats. Currently, intrusion detections systems (IDS) are used in conjunction with firewalls. IDS are fundamentally passive since their primary task is classification, and they do nothing to prevent an attack from succeeding. Attack prevention is left to the firewall. Since neither the firewall nor the IDS know how a packet is going to be processed by the host, they may make an incorrect decision.

These obstacles motivate the argument for placing the protection mechanisms closer to the end-host. The current invention details such a system deployed on the end-host using a hybrid approach to adaptively react to new and evolving threats.

Hybrid Approach, FLIPS (Feedback Learning Intrusion Prevention Systems), for Host-Based Application-Level Firewall The invention, FLIPS (Feedback Learning Intrusion Prevention Systems), employs a hybrid approach to host-security that prevents code-injection attacks. The three main components of the invention are: an anomaly-based classifier, a signature-based filtering system, and a supervisor that employs an instruction-randomization framework to detect and prevent code-injection attacks. Furthermore, the supervisor can identify the offending code and train the classifier and the filter to repulse future similar attacks.

Applications: The invention is a host-based application-level firewall. It provides a precise high-confidence filtering mechanism that adapts to new malicious input in order to stop the spread of zero-day attacks such as Internet worms.

Advantages: • Invention catches the entire class of binary code injection attacks and not just simple buffer overflows • Capturing the malicious injected code allows the system to construct signatures for the code and to respond to threats quickly and in an ongoing manner. • These signatures can be exchanged with other instances of the system and can potentially inoculate the entire network against a zero-day worm attack. • Invention can be deployed transparently to clients with minimal impact on servers. • Invention does not require access to source code. Thus, the invention is applicable to commercial off-the-shelf software.
• Invention is self-contained and does not require additional hardware or system components. It can thus be marketed directly to end-users.


Publications: FLIPS: Hybrid Adaptive Intrusion Prevention, Recent Advance in Intrusion Detection (RAID), Sept. 2005

Licensing Status: Available for Licensing and Sponsored Research Support

Inventors
Salvatore Stolfo