

A Methodology for Using Intelligent Agents to provide Automated Intrusion Response

Curtis A. Carver Jr, John M.D. Hill, and Udo W. Pooch

Purpose

This paper proposes a new methodology for adaptive, automated intrusion response (IR) focusing on the role of software agents in providing that response. The majority of intrusion response systems (IRSs) react to attacks by generating reports or alarms. This introduces a window of vulnerability between when an intrusion is detected and when action is taken to defend against the attack. Research by Cohen indicates that the success of an attack is dependent on the time gap between detection and response. If skilled attackers are given ten hours after they are detected before a response, they will be successful 80% of the time. At thirty hours, the attacker almost never fails. Manual response to computer attacks is inadequate by itself.

With two exceptions, all automatic IRSs use a stateless decision table where a particular response is associated with a particular attack. If an attack occurs, the preprogrammed response executes. If the same attack occurs one thousand times, the IRS will execute the same response one thousand times. The two exceptions, Cooperating Security Managers and Event Monitoring Enabling Responses to Anomalous Live Disturbances, provide more robust IR mechanisms that are at the same time limited in terms of the criteria used to determine a response, support for single intrusion detection system (IDS), and a non-adaptive response methodology. This research addresses these issues.

Method

The proposed methodology is summarized in Figure 1. Multiple IDSs monitor a computer system and generate intrusion alarms. *Interface agents* maintain a model of each IDS based on number of false positives/negatives previously generated. It uses this model to generate an attack confidence metric and passes this metric along with the intrusion alarm to the *Master Analysis agent*. The *Master Analysis agent* classifies whether the incident is a continuation of an existing incident or is a new attack. If it is a new attack, the *Master Analysis agent* creates a new *Analysis agent* to develop a response plan to the new attack. If the incident is a continuation of an existing attack, the *Master Analysis agent* passes the attack confidence metric and intrusion alarm to the existing *Analysis agent* handling the attack. The *Analysis agent* analyzes an incident until it is resolved and generates an abstract course of action to resolve the incident. To generate this course of action, the *Analysis agent* involves the *Response Taxonomy agent* to classify the attack and *Policy Specification agent* to limit the response based on legal, ethical, institutional, or resource constraints. The *Analysis agent* passes the selected course of action to the *Tactics agent*. The *Tactics agent* decomposes the abstract course of action into very specific actions and then invokes the appropriate components of the *Response Toolkit*. Both the *Analysis and Tactics agents* employ adaptive decision-making based on the success of previous responses. The *Logger* records *Analysis and Tactics agents'* decisions for system administrator review.

Results

The Adaptive, Agent-based, Intrusion Response System (AAIRS) is the prototype implementation of this methodology.

Novel Aspects

This research presents a novel IR methodology that includes: response adaptation to intrusive behavior based on confidence in the intrusion detection mechanism; response adaptation to intrusive behavior based on the success of previous intrusion responses; and, synergistic support for multiple IDSs.

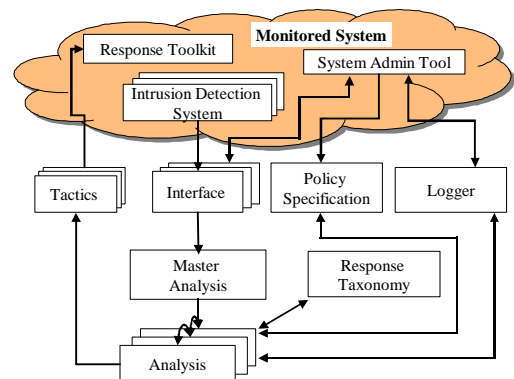


Figure 1: AAIRS Methodology

Conclusions

This paper proposes a new methodology for adaptive, automated IR using software agents. Manual response to computer attacks is inadequate and existing automatic IRSs are limited in their ability to respond to attacks. This methodology and the its associated prototype advance the state of the art in IRSs.