AIMD (Adaptable, Intelligent, Malfeasance Detection)

Adaptable, Intelligent, Malfeasance Detection (AIMD) - Recent successful cyber attacks against computer networks at several major government sites have clearly demonstrated that dangerous vulnerabilities are unaddressed. Cyber security was previously addressed via Network Intrusion Detection Systems (NIDS), together with firewalls and virus detection. However, such defenses are much less effective against these new attacks.

The Cyber Space and Information Intelligence Research Group (CSIIR) at Oak Ridge National Laboratory has listed the most critical threats as social engineering, malware and companyware, advanced malware, and the nuanced insider.

- *Social engineering* is the art of tricking users into enabling an exploit.
- *Malware* is software deliberately inserted into a system for a harmful purpose.
- *Companyware* is functionality that benefits the software vendor (but not the user) and can create exploitable vulnerabilities. Companyware is automatically installed with commercial software and is contractually protected from reverse-engineering and analysis.
- *Advanced malware* includes zero-day attacks, polymorphic binaries, process hiding, targeted exploitation (e.g., spear phishing), and covert channels for data exfiltration.
- *Insider threats* arise from inadvertent, neglectful, indifferent, and malicious activity. Most users fit in one of these categories, and the perfectly trustworthy insider is rare.

These diverse threats are far more difficult to counter than traditional cyber attacks, and are poorly addressed even by distributed NIDS.

CSIIR addresses these threats and vulnerabilities through construction of a network-based, Adaptable, Intelligent, Malfeasance Detection (AIMD) system that relies on sophisticated, multi-dimensional decision algorithms, rather than signature-based detection. AIMD construction has three distinct components to complement existing cyber security tools:

1. Data collection. To augment existing data collection, the AIMD project will deploy Commercial-off-the-shelf (COTS) computers as sensors to collect data on internal network activity. The goal is user-transparent, transportable, scalable sensors;
2. Advanced data fusion and decision algorithms analyze the sensor data to give attack alarms. Viable decision algorithms include support vector machines, random forests, Bayesian belief networks, neural nets, clustering, and anomaly detection. The goal is adaptive, intelligent fusion of the sensor data into meaningful alarms for cyber operations staff;
3. Training data for the decision algorithms will rely on novel combinations of sensor data. Automatic feedback from cyber operations staff can be inferred by their HTML interactions with the data.

The objective is real-time awareness of incidents and a near-real-time response capability to dramatically reduce the impact of network malfeasance.

POC: Michael Neergaard, MS; Erik Ferragut, PhD; Lee Hively, PhD; Frederick Sheldon, PhD
Cyberspace Sciences & Information Intelligence Research (CSIIR) Group
Oak Ridge National Laboratory P.O. Box 2008, Oak Ridge, TN 37831-6418
www.ioc.ornl.gov