CounterStorm

Deploying Statistical Anomaly Detection to Improve Cyber Security: Strategy, Benefits, and Results

Dr. Greg Shannon, Chief Scientist, CounterStorm, Inc.

There will always be new vulnerabilities in the information networks that control our nation's critical infrastructure. Problems arise both in legacy systems and in any new device or software application that we deploy. This is a persistent problem because our adversaries work constantly to find new and inventive means to uncover our vulnerabilities and attack our information and control systems. Our current approach to the problem with signature-, rule- and policy- based intrusion detection is self-limiting; it only protects us from what has happened in the past. In contrast, anomaly detection (AD) tools allow us to recognize new conditions on the network that may be indications of previously unknown attack mechanisms, i.e. zero-day attacks. In this presentation, we describe the advantages and challenges of AD for protecting our critical information systems.

Some vendors advocate a broad-based approach to the problem; a one-system fits all solution. One such approach is exemplified by NBAD systems. These systems use anomaly detection but they use it to provide a system administrator with an overview of network performance statistics with the goal of maintaining the health of the network. Our view is much more focused; we are using anomaly detection strictly for security purposes. The Netflow data used by NBAD systems does not provide sufficient granularity for useful analysis of network security-related events. We use normal traffic on a healthy network as a baseline from which to learn when abnormal traffic flow indicates an impending attack.

We have deployed our anomaly detection software successfully to recognize targeted attacks, botnets, and worms. Our experience from use in the field makes us confident that our sensors detected threats for which there are as yet no known signatures; in fact signatures for these attacks were not developed until 4 to 48 hours later.

In this presentation, I first discuss the truly disruptive nature of anomaly detection technology. I'll describe the state of the art in AD and where I believe the technology will most benefit from a new research focus. Deployment considerations for AD sensors will be discussed along with the advantages and disadvantages inherent in each example. One commercially available AD system will be described in detail. Results from field deployment of CounterStorm's Active Threat Recognition Suite will be described along with results of a joint deployment with an Autonomous System Traceback program developed by Southwest Research Institute. The advantages of coupling these two systems – one that can recognize an impending or on-going network attack and one that determines attribution for that attack – will be discussed.

The challenges that need to be addressed with AD tools are similar to any network detection system: Once we have determined that network behavior is significantly different from normal, what should be done? What information does the end-user need and how best do we convey this information? How much of the mitigation of the threat should be done automatically and what oversight role should the human play in this mitigation? Many of these issues depend on the deployment environment. Will there be a CERT team in-place to address the problem? How do we reduce the number of false positives in the system? For a particular environment (such as the Insider Threat for the Intelligence Community), would it be better to not report than to over-report? Who sets these policies and how do we help to determine how they should be set?

Like any truly disruptive technology, adaptation through operational use is the key that will allow AD sensors to radically change the way we currently do business. The future is not in vulnerability patches and fast signature distribution; the future is in recognizing that the system is malfunctioning before the damage is done.

Copyright © CounterStorm, Inc. 2007

Dr. Greg Shannon: Dr. Greg Shannon is CounterStorm's primary representative to U.S. government agencies and system integrators. He is also the Company's Principal Investigator for its two DHS SBIR Phase II awards. Dr. Shannon's research, development and management experience spans two decades with industry, academic and government working on security, networks and data analysis. Prior to joining CounterStorm, Dr. Shannon worked at Lucent Technologies, Ascend Communications, his own startup, Los Alamos National Lab, and Indiana University on such projects as FCC-recommended cyber security best practices, normalization of encryption export controls for network security equipment, and building scalable network-security appliances. Dr. Shannon received his B.S. from Iowa State University in computer science with minors in mathematics, statistics and economics, and earned his Ph.D. in Computer Sciences from Purdue University.

Company Overview: CounterStorm is a leading provider of modular threat detection and mitigation software development kits (SDKs) to security and infrastructure companies, as well as sophisticated government and commercial end users. Headquartered in New York City, the company was formed in August 2001 to commercialize patent-pending technologies developed at Columbia University under grants from the Defense Advanced Research Projects Agency (DARPA). CounterStorm is venture funded, with Novak Biddle Venture Partners, JK&B Capital, and Paladin Capital Group as lead investors. The company has also been awarded Small Business Innovative Research (SBIR) grants by the Homeland Security Advanced Research Projects Agency (HSARPA) of the Department of Homeland Security's Science and Technology Directorate.

www.counterstorm.com

Copyright © CounterStorm, Inc. 2007