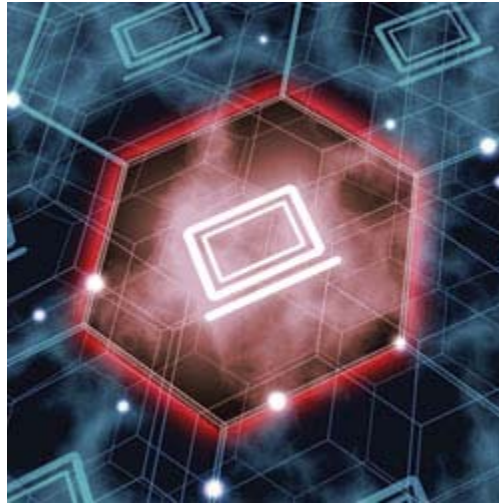


Eyeing the Evil Insider

Written by Karen E. Thuermer



MIT 2011 Volume: 15 Issue: 8 (September)



In the wake of highly publicized incidents and under pressure from Congress, the military and intelligence communities are searching for new ways to identify insiders who have the ability to access systems and information that, if compromised, could pose a threat to national security. As they do so, a number of companies are offering technologies for identifying and countering the insider threat.

The mounting appreciation for the value of Department of Defense information technology and data, coupled with the realization that DoD has already been compromised, is creating pressure for action.

The Defense Advanced Research Projects Agency (DARPA), for example, is soliciting novel approaches and tools for information security personnel for detecting and responding to insider threats on DoD and military interest networks. Dubbed the Cyber Insider Threat (CINDER), the program is charged with greatly increasing the accuracy, rate and speed with which insider threats are detected.

In May, the House Intelligence Committee also called on the director of national intelligence to establish an automated insider threat detection program to deter and detect unauthorized access to, or use of, classified intelligence networks.

"Incidents like the unauthorized disclosure of classified information by WikiLeaks ... show us that despite the tremendous progress made since 9/11 in information sharing, we still need to have systems in place that can detect unauthorized activities by those who would do our country harm from the inside," said the

committee in its report on the intelligence authorization bill. The committee called for full operating capability to be required by October 1, 2013.

More recently, Senator John McCain of Arizona has called for establishment of a Select Committee on Cyber Security and Electronic Intelligence Leaks, which he said was “necessary in order to develop comprehensive cybersecurity legislation and adequately address the continuing risk of insider threats that caused thousands of documents to be posted on the website WikiLeaks.”

“Even those who have been in the military for a long time realize that it is the information technology that is the crown jewel of the DoD going forward, not bombs and the missiles,” remarked John Gohstand, vice president of product management for PacketMotion, a company involved in developing user activity management and security investigations, alerting, and reporting solutions.

DARPA defines “insider threat” in two ways. One is “malevolent (or possibly inadvertent) actions by an already trusted person with access to sensitive information and information systems and sources.” The other regards “any efforts within an environment (computer systems, networks, communications mediums, infrastructure devices, etc.) that are being performed in support of an adversary mission or goal.”

Technology Developments

A number of companies are involved in addressing these needs.

PacketMotion, for example, offers a solution called PacketSentry, which Gohstand describes as very easy to implement since it does not require software to be installed on the parking system or an appliance on the network. Instead it can be installed as a Guest VM (virtualization software) into the VMware Data Center.

PacketSentry operates using a virtual probe that is ubiquitously deployed and offers a consistent, unified solution for traditional, virtual and cloud environments. The system, which runs through that data to locate an issue, is designed to audit and model all functions that people do in the internal network. PacketSentry’s data is inputted in further upstream systems that combine with other data from other forensic solutions.

“We are basically one data point in a system,” Gohstand said. “We have an application programming interface that allows our data to be exported and put into a larger database.”

Most “physical” solutions don’t work in guarding against insider cyber-attacks, company executives say, because they lack VM-to-VM audit and control. They also have insufficient trust level separation and segregation of duties. In addition, security vendors are slow to develop virtual products. There are also evolving risks and threats such as the loss of intellectual property or other sensitive data, attacks between VMs, and a drive for cloud deployments without security strategy.

PacketSentry provides information about what is going on in the network. Its probes capture user activity records and apply real-time policy controls.

"This is important since first you need to know the system in order to put controls on it," Gohstand explained. Today's security controls also need flexibility and agility, particularly since network traffic is not always on the network and existing security schemes lack the ability to offer unrestricted freedom of VM movement.

Gohstand points out that PacketSentry excels in that its virtual probe is not dependent on network topologies or attributes. In addition, PacketSentry Manager automates policy through the integration of identity.

Information Compartments

Although the advantages of cross-service access are manifest for missions requiring on-demand intelligence, the opportunities for privileged users to compromise classified information rises exponentially. It is no longer sufficient to monitor and control who has access to data, since insiders have all the credentials and entitlements to access protected data.

Consequently, a different paradigm in information protection is necessary to ensure authorized users cannot access or mishandle classified information outside of the mission scope.

One company addressing that issue is Verdasys, which offers enterprise information protection solutions and has developed a technology platform called Verdasys Digital Guardian, which is designed specifically to detect, deter and prevent risks to sensitive data by a malicious insider.

"WikiLeaks is but the latest reminder that insider threats remain the most difficult security risks to manage; doing so requires a special class of enforcement technology that deters and prevents compromise without impacting the mission," remarked Bill Munroe, Verdasys vice president of marketing. "Digital Guardian is currently the only scalable solution shown to prevent most types of insider threats, while also generating evidentiary-quality event logs to support investigations and prosecutions."

Digital Guardian agents survey and control classified information, independent of user clearance, with the ability to remain stealth and/or tamper resistant at all times. It identifies and compartmentalizes information at the moment of creation or discovery; transparently applies encryption, usage controls or tactical warnings to deter noncompliant use; and alerts central administrators to events of interest in real time from anywhere in the world.

When Digital Guardian's countermeasures are used in combination as a "defense in depth" strategy, the insider threat would almost always be prevented, developers say. Any privileged user would be accurately identified in real time attempting to compromise data with forensic evidence that could be used for investigations and litigation. Security team members would be alerted to the attempted compromise, and no data would leave a secured system unauthorized.

Munroe described Digital Guardian as a stealth and tamper-proof solution that combines kernel-mode “endpoint” agents, such as workstations, laptops, file servers and virtual machines, with network-based “sensors” under an integrated management infrastructure.

Training is Essential

Software offers many benefits for detecting insider threats. Yet, none can take the place of people when it comes to detecting espionage and sabotage traits even amongst trusted employees who have special access and privileges.

Recognizing this fact, a company called Aptima developed a training system in conjunction with Battelle/Pacific Northwest National Laboratory, Altadyn Corp., and Florida State University to thwart insider threats to cyber-systems geared specifically at DoD employees. The Air Force Research Laboratory in Mesa, Ariz., is sponsoring the effort.

Dubbed RESIST-EM (Resisting Espionage and Sabotage with an Intelligent System for Training Expert Managers), the Aptima approach will be a “serious game” for training frontline DoD managers. Aptima executives maintain that because the problem involves human elements, there must be a human-centered solution to some of the problem. Consequently, its mandate is to help supervisors detect early but important cues so that potential threats do not escalate into actual incidents.

“Managers may have the best vantage point from which to monitor, assess and address these threats, but they need to be trained to observe and understand the subtle dynamics of individual behavior and the state of the environment from the telltale signals of the discontented employee, to the stressors in the company workplace that can aggravate them to act,” said Jared Freeman, Aptima’s chief research officer and program manager for RESIST-EM.

RESIST-EM takes a game-based instruction approach where everyday supervisors are given a realistic environment and task and use resources to first assess whether or not they face an insider threat, attribute that assessment to something in particular, and finally determine what action should be taken.

“It’s one thing to suspect someone may pose an insider threat,” says Freeman. “It’s another thing to understand why.”

One important aspect to RESIST-EM is that it is based on conveying knowledge about behaviors that typically concern security specialists, not personalities or deep-rooted psychological issues.

“We are trying to ensure that supervisors put their attention on the things people do, not theories of whether an individual is good or bad, and that they have some rationale for taking the next action to someone in security or human resources,” Freeman explained. “The larger policy problem for organizations is to ensure that the atmosphere is productive and collegial and does not have a taint of ‘big brother’ in it. This is a challenge beyond a mere training tool.”

Currently, the program is midway through the second year of its contract. Aptima executives hope to employ students in August.

Key to its work on RESIST-EM is how the company has constructed or designed the training so that it is easy to take specific content from different organizations and adjust it to the specific needs of an organization. In other words, the actions they would take for military personnel would not be the same for a contractor or a DoD civilian employee.

The training educates students in behavioral cues that human resource and security specialists find troubling. It also helps personnel attribute cues to activities within an organization that might result in insider threat behavior.

For instance, has there been a rash of layoffs that could trigger resentment? Security characteristics of an organization may also make it more vulnerable to insider threats. For example, are files protected? Are login routines not changed frequently enough?

“Bad behavior often percolates to the top in good organizations under stressful situations,” Freeman explained. ♦

[Back to Top](#)