PACKET

CISCO SYSTEMS USERS MAGAZINE

SECOND QUARTER 2005

SELF-DEFENDING NETWORKS

CISCO SYSTEMS

CISCO.COM/PACKET

Stopping Bad Behavior at Endpoints

By Gene Knauer

LIKE A NATURAL DISASTER, when the Sapphire Worm, better known as "Slammer," was unleashed in December 2003, it shut down Websites, disabled automated teller machines (ATMs), flooded networks, and resulted in a massive loss of productivity, money, and peace of mind for numerous businesses and IT staffs. Meanwhile, however, some enterprise networks, including the University of California, Berkeley, remained uninfected, even though their servers and desktop PCs had yet to be patched to prevent Slammer from being transmitted and exploiting buffer overflow vulnerability in computers running Microsoft's SQL Server or Microsoft SQL Server Desktop Engine 2000.

Cisco Security Agent prevents attacks on servers and desktop PCs by enforcing behavioral policies.

These networks were protected by an endpoint security product from the small intrusion prevention software company Okena, which that same year was acquired by Cisco and the product rebranded as Cisco Security Agent.

Behavior-Based Endpoint Security

Cisco Security Agent software is considered an intrusion *prevention* tool. Working from network endpoints such as desktops and servers, it is designed to correlate appropriate and suspicious behavior and prevent new attacks, even before a security patch or "signature" can update the network's antivirus or other security software. In sum, Cisco Security Agent intercepts system calls between applications and the operating system, correlates them, compares the correlated system calls with a set of behavioral rules, and makes an "allow" or "deny" decision based on the comparison results. This process is called INCORE, which stands for "intercept, correlate, rules engine" (see Figure 1).

According to Ted Doty, product manager for Cisco Security Agent, the basic mechanisms behind keeping viruses and worms in check have not changed much over time. "I like to think of it as catching thieves in the bank before they can rob it," he says. "We're looking for malicious behavior based on system calls to files, network registry sources, or to dynamic, run-time resources."

Cisco Security Agent includes a management console that resides on a Microsoft Windows 2000 server and host-based agents deployed on desktops and servers. The agents use HTTP and 128-bit Secure Sockets Layer (SSL) for the management interface and agent-to-management console communications. Running between network applications and operating system kernels, Cisco Security Agent checks applications against their security policies and either allows or denies the operation. Such real-time prevention is based on enforcing security policies combined from distributed firewalls, operating systems, antivirus software, and audit event collection.

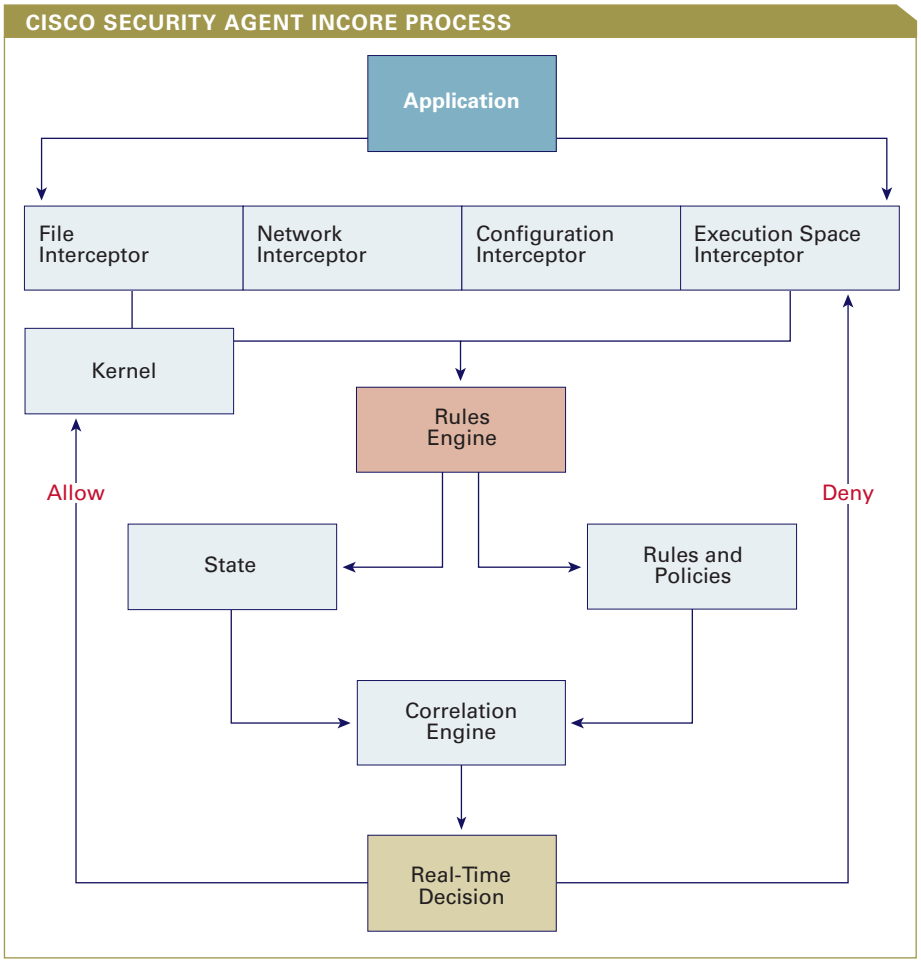

FIGURE 1 Cisco Security Agent applies an "intercept, correlate, rules engine" process—INCORE—that compares correlated system calls with a set of behavioral rules.

"Correlating events with policies to allow or shut down activity is what makes Cisco Security Agent unique on the market," says Doty. "Other solutions for viruses, worms, and spyware and adware detection rely on applying the latest security patches. From a couple of hundred patches issued per year in the mid-1990s, now there are about 4000 patches a year. Getting them tested and deployed on every server and desktop in a network has been bleeding customers dry in time and resources."

Defense in Depth for Siemens and IFF

For Kathy Taylor, information security officer at Siemens Energy and Automation in Alpharetta, Georgia, deploying Cisco Security Agent was like acquiring a staff of new security administrators to watch the 250 servers and 7000 desktops on the company's highly distributed network serving users throughout the US and Mexico.

"We had previously been hit hard by the W32/Blaster Worm in the summer of 2003 and soon after got the approval to install Cisco Security Agent," says Taylor. "The following spring, there was another global virus outbreak, but this time we had no issues." Taylor and her colleagues could see viruses trying to attack their computers, but none of these network operations were allowed to proceed.

"Cisco Security Agent gives us time to do the antivirus updates and test the new OS security patches before installation," she says.

With facilities in 32 countries, International Flavors & Fragrances Inc. (IFF), a creator and manufacturer of flavors and fragrances used in a wide variety of products, had a similar sobering experience before investing in endpoint prevention. The Welchia virus of early 2003 swept across the company's network globalwide.

"Welchia hit in our offices in China first," recalls Michael Wasielewski, senior manager for network systems at IFF, which is based in Union Beach, New Jersey. "By the time we realized we were dealing with a virus, two hours later it had spread to Europe and Asia, only because the western world wasn't yet awake. The antivirus signatures weren't available for another eight hours."

Though IFF squelched the Welchia virus without any serious disruptions, Wasielewski says, "We saw the agony other companies went through, and we made the decision to buy an endpoint security system." There were alternatives to Cisco Security Agent, and Wasielewski researched them. They included devices that would block network access to unpatched systems and others that would inspect systems to determine whether they were at the proper virus patch level.

"We still couldn't get around the fact that we had to deploy these patches," Wasielewski says. "And the process of getting them, and testing and deploying them was too slow. The viruses were coming too fast. Back then, Microsoft was patching patches. We decided that we needed 'Day Zero' protection, a solution that didn't depend on catching up to an already-detected new intrusion event."

Wasielewski and his network colleagues at IFF found Cisco Security Agent to be further ahead in its behavioral approach to preventive security than any other product they researched. They have since deployed Cisco Security Agent on 4500 desktop computers throughout IFF.

"It's the first product we've seen that really delivers this extra layer of endpoint security, which we now see as the first layer of protection even before antivirus or antispyware tools," says Wasielewski.

Thwarting Spyware and Adware

Among the intrusive network behaviors targeted by Cisco Security Agent Version 4.5, the latest release introduced in February, are spyware (programs that install themselves on computers without a user's consent and read and relay private information, including passwords and credit card numbers) and adware (marketing programs bundled with freeware that sprout pop-up ads and links). Cisco Security Agent 4.5 protects against spyware and adware infections by preventing these programs from initially installing and, if already installed, by preventing them from executing.

Cisco Security Agent is aptly suited to thwarting spyware and adware because these programs are rarely delivered through e-mail, which is subject to antivirus screening. This software is also an improvement over spyware detection

Continued on page 51

FIGURE 2 Cisco Security Agent Version 4.5 detects an attempted keystroke capture and alerts the user with courses of action.

FIGURE 3 A network status "Events" view summary report generated using the CSA MC Web-based interface.

"We decided that we needed 'Day Zero' protection, a solution that didn't depend on catching up to an already-detected new intrusion event."

Michael Wasielewski, senior manager for network systems, IFF

Endpoint Security, Continued from page 49

ENDPOINT SECURITY AND NETWORK ADMISSION CONTROL

Cisco Security Agent can be considered a first-order dampener to the effects of virus and worm propagation. Making sure endpoints are compliant with OS patches and antivirus software updates is an effective second-order dampener to such propagation. Enter Cisco's Network Admission Control (NAC) program. The NAC industrywide initiative was created to help ensure that every endpoint complies with network security policies before being granted access to curtail damage caused by viruses and worms.

NAC technologies control access by interrogating devices connecting to the network to determine whether they comply with network security policy. For example, NAC can determine if Cisco Security Agent or antivirus software is installed and current, along with the current OS and patch level. NAC uses this information to determine appropriate network admission policy enforcement for every endpoint based on the security state of the OS and associated applications rather than simply on who is requesting access. In addition to controlling access, NAC gives IT administrators the means to automatically quarantine and remediate noncompliant endpoints. Launched in June 2004, NAC is supported on routers running Cisco IOS Software Release 12.3(8)T and higher.

The Cisco NAC program is open to vendors who design and sell third-party client and server applications that incorporate features compatible with the NAC infrastructure. To date, more than 30 vendors are actively integrating their technologies into the network. For more information on this program, visit cisco.com/packet/172_6d1.

tools because, like antivirus and other forms of security software, these tools are passive and reactive, with patches lagging behind new and mutating spyware attacks. Instead, Cisco Security Agent 4.5 hardens the Windows operating system with its behavior correlation engine, preventing spyware from executing.

In Figure 2 (page 49), for example, Cisco Security Agent detects the problem SilentLog.exe, a "keystroke logger" program that quietly captures all keyboard input and logs it to a file. Spyware often installs such keystroke loggers to capture passwords entered by users.

In response to stealthily downloaded spyware or adware attempting to execute, Cisco Security Agent alerts the user with a message screen and will default to terminating the application unless the user allows the process to continue (by clicking "Yes"). Administrators can configure Cisco Security Agent to automatically stop the application from executing without user intervention. If the spyware attempts to swamp users with repeated requests to download—a form of social engineering intended to trick or frustrate users into selecting "Yes"—they need only select "Don't ask me again" to stop the requests.

Cisco Security Agent does not require cryptographic analysis of file system contents, so its impact on performance is negligible.

Other Benefits of Cisco Security Agent

Besides detecting, analyzing, and acting on network behavior, Cisco Security Agent can track which applications are installed on a single computer or workgroup; which applications use the network; the identity of all remote IP addresses with whom a server or desktop computer communicates; and the state of all applications on remote systems, including user-specific installation information and whether undesired applications are attempting to run.

Administrators can perform detailed forensics of any application on any computer, collect information about the application's behavior, and create a control policy based on that application's "normal" behavior. All Cisco Security Agent policies are configured and deployed via the Cisco Security Agent Management Center (CSA MC) Web-based user interface. CSA MC also provides a reporting tool, allowing administrators to generate reports with various views of their network's health and status (see Figure 3, page 49).

Cisco Security Agent Version 4.5 also adds compatibility with international operating systems and expands platform support to include Linux servers and desktops and Windows clusters. It ships at no additional charge with all Cisco IP telephony products, including Cisco CallManager and Cisco Unity.

"Now we're considered the most robust IP telephony solution from a security perspective," says Doty, adding that more than two million desktop PCs and servers have installed Cisco Security Agent since 2001.

Frontline of the Self-Defending Network

"Cisco Security Agent complements Cisco's Self-Defending Network strategy. In addition to providing a first line of real-time intrusion prevention, its presence on endpoints allow them to acquire state information that might not be available at the network edge," says Joshua Huston, a technical marketing engineer in Cisco's VPN and Security Business Unit specializing in Cisco Security Agent marketing. "This capability provides a feedback loop between the endpoints and the network, so the network can readily adapt to emerging threats." (For more on the Self-Defending Network strategy and new security products from Cisco, see "In Self Defense," page 26.)

Cisco Security Agent embodies other attributes of a Self-Defending Network, adds Huston: It's flexible, future-proof, and highly effective whether a user is at work, at home, or on the road. ■

FURTHER READING

- White paper: *Cisco Security Agent—an Enterprise Solution for Protection Against Spyware and Adware* cisco.com/packet/172_6d2
- Cisco Security Agent home page cisco.com/go/csa