Open Source Security: Opportunity or Oxymoron?

George Lawton

As the computer industry focuses on system and network security, a growing number of users are taking a closer look at open source software in order to gauge whether its potential advantages outweigh its possible disadvantages.

Although open source security has been around for years, it has never been as widely used as open source products like the Linux OS or Apache Web server have been. John Pescatore, Internet-security research director at market-research firm Gartner Inc., said open source security tools now represent 3 to 5 percent of security-software usage but could comprise 10 to 15 percent by 2007.

A key factor in this potential growth is the quality of numerous open source security packages. "Some of the public-domain tools are very well maintained and have many people contributing new tools and patterns. In some senses, they rival commercial tools," noted Eugene Spafford, director of Purdue University's Center for Education and Research in Information Assurance and Security.

Open source software products include free tools that users can download from the Internet, packages that come with commercial vendor support, and tools bundled with closed-source products.

The most popular tools include Netfilter and iptables; intrusion-detection systems such as Snort, Snare, and Tripwire; vulnerability scanners like Nessus and Saint; authentication servers such as Kerberos; and firewalls like T.Rex.

Some companies are even beginning to use open source security to protect mission-critical applications.

GROWING INTEREST

IT people have used open source security to some extent for about 15 years. Now, there is increasing interest in the use of these tools by larger companies, a growing body of security consultants, and service providers that can tailor the software for specific users.

For example, Electronic Data Systems (EDS) has begun using open source security tools from Astaro to provide a security front end for several credit-union Web sites with transaction-processing capabilities.

Security-system integrators are finding users attracted to open source software's low prices. For example, said Richard Mayr, managing director at R2R Informations und Kommunikations AG, his company has been selling a proprietary firewall for many years but has found that 75 percent of its customers are opting for open source alternatives.

Guardent has launched a $1,500-per-month Internet security service based on the company's Security Defense Appliance. The appliance integrates proprietary components, such as Cisco Systems's PIX firewall, and open source components, including iptables, Nessus, and Snort. A comparable all-closed-source system could cost about $10,000.

Meanwhile, C2Net Software, which Red Hat recently purchased, created its commercial Stronghold Secure Web Server with Apache and OpenSSL. OpenSSL is an open source toolkit implementing the secure-sockets-layer and transport-layer-security protocols, as well as a general-purpose cryptography library.

According to security consultant Paul Robichaux of Robichaux & Associates, organizations with legal security requirements, in industries such as healthcare and finance, are least likely to use open source tools. Instead, they will probably continue to depend on vendors they can hold liable for security breaches. He said open source security is more likely to be used by service and consulting firms that already know and trust the tools, as well as companies in which IT departments have been experimenting with them.

Mark Cox, senior director of engineering of Red Hat's OpenSSL group, added, "Companies running Unix-based platforms, such as Linux and Solaris, are likely to use open source

tools like Nessus, Snare, and Snort because they were developed and run like Unix."

OPEN SOURCE SECURITY'S PROS AND CONS

There is a debate as to the relative merits of open source and proprietary tools based primarily on cost, quality, and support.

Cost. One of open source tools' main benefits is significantly lower cost. The tools are either free or have low prices, and they have either no licensing fees or lower fees than proprietary products. However, some users have a "you get what you pay for" outlook on open source tools.

Buddy Baxter, technical delivery manager for infrastructure needs for EDS's credit-union customers, said, "Just because a product costs a lot does not mean it will be more secure." He said EDS can deploy a security installation using Astaro's software for about 25 percent of the cost of using Check Point Software Technologies' commercial product.

Quality. Guardent Chief Technology Officer Jerry Brady said some open source security tools are as good as or better than their commercial counterparts. For example, he said, the Nessus vulnerability scanner offers better processing distribution, remote executability, and scheduling than most commercial products. With an open source methodology, he said, "You have a greater ability to focus on those things that are really important. Nessus is less concerned about marketability and more concerned with the quality of code."

However, replied security expert Marcus Ranum, president of NFR Security, "I don't think making [software] open source contributes to making it better at all. What makes good software is single-minded focus." An open source approach doesn't guarantee this, he said.

Purdue's Spafford agreed. "What really determines whether it is trustable is quality and care," he said. "Was it designed well? Was it built using proper tools? Did the people who built it use discipline and not add a lot of features? A lot of the open source software out there is built by people who don't have the experience, the tools, the time, or the resources to do it as carefully as you would want in a highly trusted environment."

One of open source tools' main benefits is significantly lower cost.

Open source proponents argue that a wide audience looking at freely available code will find problems faster than a limited number of people working for a product vendor. "Public-domain software [can] have a much broader group of people looking to identify and provide corrective action," said Mike Curtis, research director for the International Information Integrity Institute at Redsiren Technologies, a security-services provider.

Also, Curtis said, open source software developers can address security flaws more quickly than commercial companies can because they don't have the same overhead or bureaucracy. "Open source developers are more interested in fixing bugs than in getting a new feature in for the next release," he stated.

However, said NFR Security's Ranum, "In my experience, not many people actually read through the code. They just look at the readme files. When I wrote the first public firewall toolkit, there were probably 2,000 sites using it to some degree, but only about 10 people gave me any feedback or patches. So I am way unimpressed with the concept of open source."

Many closed source software proponents say that it's the quality, not the number, of the eyes looking at code that counts. They contend that a company's software experts who work on products for a living will do a better job than the people who review open source software.

Added Spafford, "We have seen many pieces of open source software that had flaws of one kind or another after they had been deployed for years and looked at literally hundreds of thousands of times. [Flaws were] not discovered because people looking at the code did not have the training to know what to look for. In many cases, people are looking at the code to do customization and not to do an in-depth code review."

Support. Proprietary-software advocates say that companies, unlike open source organizations, offer users a help desk or other resources to turn to when a problem arises. However, this could also boost support for enterprises that manage open source security software for users. Guardent's Brady said, "A service offers better guarantees to a customer [and] can give the customer recourse. You can articulate a service-level agreement and leave it to the vendor to find the right tools and help the customer deal with changes in the technology."

Other issues. Some closed source proponents say the availability of open source software's code makes it too easy for hackers to figure out how to defeat the security. However, open source supporters say this is not really an issue because hackers have also been able to defeat closed source security. Meanwhile, proponents say that open source security tools are easier to customize because the code is available.

CURRENT OPEN SOURCE PROJECTS

There are several important open source security tools.

Kerberos

Kerberos authentication and encryption technology (http://web.mit.edu/kerberos/www/) was developed by the Massachusetts Institute of Technology and released in 1987. The technology has since matured into a standard managed by the Internet Engineering Task Force's Common Authentication Technology Working Group.

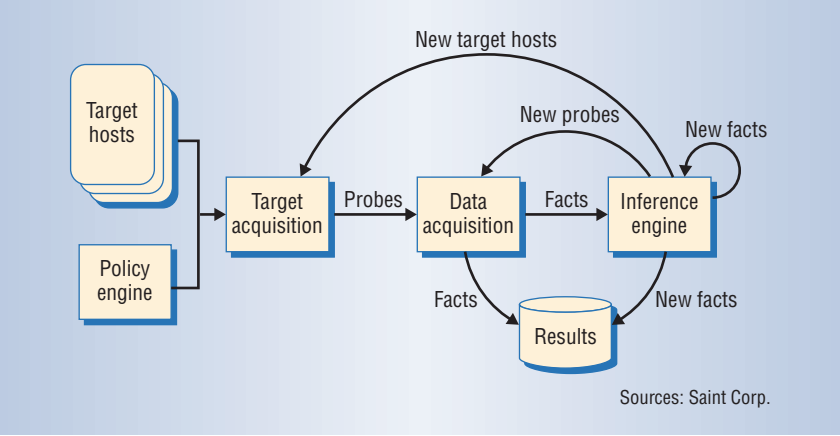

Figure 1. Saint is a scanner that examines systems for vulnerabilities. Based on a specific configuration, the policy engine determines whether and to what extent Saint can scan a set of hosts. The target acquisition subsystem creates a list of probing test attacks to run on hosts. The data acquisition subsystem collects facts about the probe's results. Using a rule base, the inference engine processes the facts while data is being collected and generates new target hosts, probes, and facts. The results subsystem takes the collected data and displays it as a hyperspace that users can work with via a browser.

Open source versions are available for Macintosh, Unix, and Windows platforms. Commercial implementations are available from Microsoft, Oracle, Qualcomm, and other companies. Microsoft created a stir by incorporating a version of Kerberos into Windows 2000 that isn't standards-compliant.

Snort

Snort (http://www.snort.org) is considered one of the most successful open source security tools. Primary developer Marty Roesch estimated 250,000 to 500,000 people use the application. The software has an active user community and considerable documentation.

Snort is a lightweight network-intrusion-detection system, capable of performing real-time traffic analysis and packet logging on IP networks. Released in 1998, the network-based Snort helps detect potential intrusions by performing protocol analysis of packets, as well as content searching and matching. It can detect various intrusions and probes, such as buffer overflows, stealth port scans, and common-gateway-interface attacks.

The tool runs on multiple platforms including FreeBSD, Linux, MacOS, Solaris, and Windows.

Snare

The System Intrusion Analysis and Reporting Environment (http://www.intersectalliance.com) is a host-based intrusion-detection system for Linux systems. The InterSect Alliance, a security-consulting firm, developed and released Snare last November.

Snare uses dynamically loadable modular technology to interact with the Linux kernel at runtime. By using only the modules necessary for a task, Snare reduces the burden on the host system. And because Snare is dynamically loadable, users don't have to reboot the system or recompile the kernel, as is the case with some Linux enhancements.

Tripwire

Purdue's Spafford and former student Gene Kim developed the Tripwire Academic Source intrusion-detection system, which has been downloaded more than a million times since its 1992 release. Tripwire Inc.(http://www.tripwire.com), which Kim cofounded, later reengineered Tripwire from scratch as a commercial closed source program. Tripwire makes a free version available for Linux systems but sells commercial versions for Unix and Windows NT platforms.

Nessus

Nessus (http://www.nessus.org) is a vulnerability scanner for remotely auditing a Web site's security. Nessus's developers released the tool in April 1998. Nessus supports POSIX-based servers working with Java, Win32, and X11 X-Windows clients.

Saint

The Security Administrators Integrated Network Tool is a vulnerability scanner (shown in Figure 1) that runs on most Unix versions, including Linux. Saint is based on the Satan (Security Administrator's Tool for Analyzing Networks) open source vulnerability-assessment tool. The Saint Corp. (http://www.saintcorporation.com) gives away older versions of the scanner but sells the latest release, as well as the SAINTwriter for generating customized reports and SAINTexpress for automatic vulnerability updates.

Netfilter and iptables

A group of open source developers designed Netfilter and iptables for incorporation into the Linux 2.4 kernel. Netfilter (http://www.netfilter.org) lets users track callback functions associated with a network intrusion, thereby recognizing that an attack is occurring. The iptables system (http://www.iptables.org) lets users define actions the system should take when it detects an attack.

T.Rex

T.Rex (http://www.opensourcefirewall.com) is an open source firewall that Freemont Avenue Software released in 2000. It runs on the AIX, Linux, and Solaris platforms and has been distributed to about 31,000 users.

THE COMING YEARS

Widespread adoption of open source security faces numerous concerns and challenges.

Fear of open source

Some companies have been reluctant to buy open source software because it is not the privately developed and supported software they are used to buying. Because of this, predicted David Moskowitz, chief technology officer of the Productivity Solutions consultancy, most open source technology will come to companies after IT people have played with it and gradually migrated it into the enterprise.

Fear of backdoors

Because the source code is available, some companies fear hackers could place back doors in open source tools that could permit unauthorized entry to systems. Consultant Robichaux said, "[This] is one of the biggest limiting factors for open source [adoption]. That doesn't mean it's a reasonable or credible fear. Nonetheless, I see customers doing things like requiring that all open source software used in their facilities be built from scratch, with no prebuilt and downloaded packages."

Performance certifications

Government certification of a product for use by public agencies can boost its general adoption. The US government requires that security and other IT products pass a Federal Information Processing Standard audit, administered by the National Institute of Standards and Technology (NIST), before US agencies can buy them.

The cost of compatibility testing can range from tens of thousands of dollars to hundreds of thousands of dollars. This could prevent open source organizations, which generally have small budgets, from certifying their technologies. In fact, said Annabel Lee, director of NIST's Cryptographic Module Validation Program, she is not aware of a single open source product that has been certified.

Ease of use and management

Open source vendors have tended to focus on features rather than ease of use and management. Consequently, the applications can be difficult to deploy and manage. For example, said Roesch, "The installation and management of Snort can get pretty hairy, particularly if you are not comfortable with writing Unix tools."

Gartner's Pescatore explained, "When you use open source tools, a lot of knowledge is captured in the heads of the people using them, whereas the commercial vendors have been forced to put a lot of that knowledge into the product."

"I don't think open source will ever approach the mass market for security tools," he said. "Most people just want an easier approach."

Open source security has tended to focus on features rather than ease of use and management.

This has generated a small but growing market for security-systems integrators and service providers—such as Guardent, Redsiren, and Silicon Defense. These companies can provide management tools and otherwise take the complexity out of open source products, as well as provide a guaranteed level of service and support.

Astaro's approach has been to create a complete security infrastructure that bundles numerous open source technologies into a single, easier-to-use interface. Ernst Kelting, president of Astaro's US Division, said, "Customers don't want to rely on unsupported software. We are taking the difficulties on our shoulders and charging for it."

Simon Perry, vice president of security solutions at Computer Associates, predicted continued growth in the use of open source-based security appliances, although not across large companies. He said organizations that develop open source software don't have the resources or management tools necessary to perform the integration needed to make security work across big companies' multiple platforms.

An interesting trend in the open source security market could be the development of business models that couple an open source code base with dedicated hardware, proprietary front-end tools, and/or service-level guarantees. For example, Guardent's Brady said, vendors could couple their knowledge of hardware optimization with open source technology to create products, such as security appliances, capable of securing fast network connections.

Red Hat's Cox said, "Open source adoption will grow because the development model supports the rapidly changing landscape of the Internet and security. Rapid response to functionality requirements, new attacks, and bug fixes are hard to duplicate in a closed source environment."

Nonetheless, Gartner's Pescatore predicts the percentage of all security-product revenue generated by the sale of commercially supported open source tools will grow from 1 percent today to only 2 percent by 2007, in part because many companies will use free tools, rather than commercial open source packages.

One danger of open source tools is that users can be lulled into a false sense of invincible security because so many people examine the code. According to Dan Geer, Kerberos developer and chief technology officer of @Stake, a security-services firm, "Making something open source does not mean it does not have flaws; it just improves the odds. It is no panacea." ■

George Lawton is a freelance writer based in Brisbane, California. Contact him at glawton@glawton.com.

Editor: Lee Garber, Computer, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org