NETWORKWORLD

[illegible] server software: SELinux blocks real-world exploits

By Don Marti

LinuxWorld-(US) |

FEB 24, 2008 12:00 AM PT

A security framework originally published by the US National Security Agency has begun to rack up an impressive list of protections agains security holes.

Linux security experts are reporting a growing list of real-world security situations in which the US National Security Agency's SELinux security framework contains the damage resulting from a flaw in other software. These so-called "mitigations" are showing that a Linux feature that began as an esoteric security measure is starting to prove its worth.

The US National Security Agency first published SELinux in 2000, and Linus Torvalds accepted it into the mainstream kernel in 2002, but for much of the time since then it has been largely of academic interest. Many Linux administrators first saw SELinux in the form of a long article or tutorial that started with a whole new glossary of security terminology. And if you put SELinux on a real system, and the error messages for a failed configuration were confusing.

But the announcements of several recent security holes tell a new story: SELinux, if turned on, can prevent an attacker from using an exploit to its full destructive potential. For example, one vulnerability in the Hewlett-Packard Linux Imaging and Printing Project's software would have allowed an attacker to run arbitrary commands as root. However, according to the company's security advisory on the bug, "On Red Hat Enterprise Linux (RHEL) 5, the SELinux targeted policy for hpssd which is enabled by default, blocks the ability to exploit this issue to run arbitrary code."

Dan Walsh, an SELinux developer at Red Hat, covered another, higher profile mitigation on his blog. Samba, the software that acts as a file server for Microsoft Windows systems, had a vulnerability that would have allowed an attacker to run commands as root. However, "while the exploit might be able to take advantage of a buffer overflow, when the attacker tries to execute the code, SELinux would stop it," he wrote.

"SELinux got a bit of a black eye by hitting it big a bit earlier than it should have," said Chad Sellers, Lead Software Architect for Tresys Technology, LLC, in an email interview. He adds, "SELinux systems have become much easier to use while at the same time protecting more and more things. The tools are much improved now so that if there's a problem, it's usually fairly easy to fix."

Tresys maintains a list of "mitigation news" on its SELinux page. Software with security bugs that SELinux mitigated includes the Apache web server, the Mambo content management system, the Sendmail MTA, and a commonly-installed PHP module, in addition to the HP and Samba bugs.

Users are seeing an increasing number of mitigations today because SELinux is now integrated with more of the software on the system, Sellers says. "RHEL4 targeted about 11 services by default, while RHEL5 targets an order of magnitude more with the default targeted policy," he says.

"The policies are protecting more and more, making it the security feature that administrators really shouldn't live without. So my advice to administrators is to try it out. If they hit a problem, don't turn it off. We have an active user community that can probably resolve the problem in an email or two," Sellers says.

What is SELinux?

The conventional security features on Linux date back to early UNIX. Although UNIX permissions are relatively easy to explain to a new administrator, they fail to block some routes of attack that a more sophisticated system would catch. For example, any process running as "root" can read and write any file on the system. An attacker who "gets root" by compromising the mail server software can modify the system password file, even if the mail server never needs to write to that file in normal operation.

SELinux adds a finer-grained level of access control. The mail server might need to run as "root" but the system would prevent it from changing the password file.

Faye Coker, in the Writing SE Linux policy HOWTO, explains. "For example, a system with SELinux enabled might allow only the mail server software to make an outgoing connection to other systems on the SMTP port (port 25). An SELinux system can treat server software running as "root" differently from an administrator running a shell logged in as "root." If an intruder compromises the server software and starts a shell as "root", he or she would not be able to modify programs or configuration files as the administrator could.

Making SELinux practical to use

SELinux developer and Red Hat employee James Morris says that the company's focus has been on automating SELinux from the administrator's point of view, and doing more of the configuration work up front, as part of the design of the distribution.

"The model we are trying to use with Fedora/RHEL is that policy is supplied with the system, and should not need to be modified by the user," he said in an email interview. Much of the SELinux configuration is now integrated with the standard management tools, Morris says, making it easier to implement site-specific policies without editing SELinux policies manually. For example, an administrator can use a menu to configure an FTP server to allow or disallow access to users' home directories.

Adding SELinux support to new software is getting easier too, Morris says. "For third-party packages, we now have infrastructure in place to allow modular security policy, so that it can be distributed with packages," he says.

A new "policy wizard" is a tool that developers can use to easily add SELinux policy for a new application. Applications' legit uses of system resources have common patterns—for example, a server application might bind to a port, read from a configuration file, and write to a log file. The wizard helps a developer codify the patterns in an SELinux-compatible way. Tresys also offers an IDE and other tools for developing SELinux policies.

"Getting third-party apps to run under SELinux is often not that hard any more, though there are a few common gotchas for applications that don't behave themselves," Sellers says.

"Now we're seeing more ISVs embaracing it," says Red Hat product marketing manager Andrew Cathrow. The availability of more SELinux tools for developers translates into more functionality for working administrators. "This is all developer focused, and we want higher level abstractions for end users and only then as a last resort," Morris says.

[illegible]s an "setroubleshoot" tool for diagnosing problems, Cathrow adds. The system log files also show more helpful information. In place of some SELinux-specific codes, the logs now clearly show the application that failed, and the system call that it was trying to perform.

Future directions

While SELinux is proving itself in server-side applications, the desktop remains a challenge. Users don't necessarily trust all of their complicated desktop software with access to all of their data, even though under the conventional UNIX-style permisssions model, all of a user's files have the same ownership.

In a presentation entitled "Towards a Least Privilege Desktop" at the SELinux Symposium, Red Hat's Colin Walters wrote, "Protecting 'root' is not the highest priority, as all of the interesting data on a desktop is owned by the user anyways."

For now, though, SELinux has become a solid protection layer for server applications. "In the first year (of RHEL5 availability) if you installed every single package, none of the critical exploits would have been exploitable," Cathrow says.

Learn more about this topic

What’s new in SELinux for Red Hat Enterprise Linux 5? (http://www.redhatmagazine.com/2007/05/04/whats-new-in-selinux-for-red-hat-enterprise-linux-5/) by Dan Walsh

Red Hat Enterprise Linux 5 Guide (http://www.nsa.gov/snac/downloads_redhat.cfm?MenuID=scg10.3.1.1) from the National Security Agency

This story, "A seatbelt for server software: SELinux blocks real-world exploits" was originally published by LinuxWorld-(US).

Join the Network World communities on Facebook and LinkedIn to comment on topics that are top of mind.