

Protecting Systems with Novell® AppArmor

Linux* Application Security

www.novell.com

TECHNICAL GUIDE



Novell.

Table of Contents

Protecting Systems
with Novell AppArmor
Linux Application Security

2	OVERVIEW	4	SETUID PROGRAMS
2	INTRODUCTION	5	CRON JOBS
2	APPLICATION PROFILE CHOICE	5	PROFILE BUILDING
3	NETWORK AGENTS	5	GENPROF
3	NETWORK APPLICATIONS	5	LOGPROF
4	WEB APPLICATIONS	6	RESULT CONFIRMATION
4	SCRIPTING LANGUAGES	6	SUMMARY

Overview



Novell® AppArmor, powered by Immunix™, is the most effective and easy-to-use Linux*-application security system available today. AppArmor protects your operating system and applications from the effects of attacks, viruses and malicious applications. As a result, your business can minimize threats, protect key corporate data, reduce network administration costs and comply with regulations.

With AppArmor, you can create security policy for each Linux program requiring protection. For developing security policy, AppArmor includes a robust set of tools that can be accessed from the SUSE™ LINUX YaST interface or from the Linux command console. This document describes the process for developing security policies using the Linux command console.

INTRODUCTION

The classic advice to secure a computer is to minimize the opportunities for attackers to hijack applications by doing the following:

- Closing all unnecessary ports
- Maximizing security of open port applications as much as possible
- Minimizing the number of setuid root applications
- Minimizing the amount of software installed in general

All of these steps take considerable effort, and all of them compromise the convenience of using the hardened machine. Novell AppArmor makes all of these steps easier—and makes the resulting hardened configuration more secure and easier to use. AppArmor effectively secures the

required applications, providing substantially more security value than does merely minimizing the number of exposed applications.

APPLICATION PROFILE CHOICE

One of the important ease-of-use features of Novell AppArmor is scalable security. Other solutions require security policy to be applied to the entire system, and in some cases, it is impossible to exclude any part of it from the policy. If the policy is wrong, you might have a broken system that prohibits you from logging in to your own computer.

With the scalable security in AppArmor, you can decide which programs need protection. This drastically reduces the amount of work required to harden your computer, as you need only profile the programs that are exposed to attack in your environment.

Effective hardening of a computer system requires minimizing the number of programs that mediate privilege and then securing the programs as much as possible. AppArmor profiles enforce policies to make sure that programs do what they are supposed to do, but nothing else. Create an AppArmor profile for each privilege-mediating program:

- **Network Agents.** Programs (servers and clients) have open network ports, and network agents are server programs that respond to those network ports. User clients (such as mail clients and Web browsers) also have open network ports and mediate privilege. These programs run with the privilege to write to the user's home directories and process input from potentially hostile remote sources, such as hostile Web sites and malicious code transmitted via e-mail.
- **Web Applications.** CGI PERL scripts, PHP pages and more complex Web applications can be invoked through a Web browser.
- **Setuid Programs.** Setuid or setgid programs run as the user or group that owns the program file rather than as the user and group of the person invoking the program.
- **Cron Jobs.** Programs that the cron daemon periodically runs read input from a variety of sources. They might run with special privilege, sometimes with as much as root privilege (e.g., cron runs `/usr/bin/updatedb` daily to keep the slocate database up to date and with sufficient privilege to read the names of all system files).

NETWORK AGENTS

To find network server daemons that need profiling, inspect the open ports on your machine, consider the programs that are answering on those ports and provide profiles for as many of those programs as possible. If you provide profiles for all programs with open network ports, the attacker cannot get to the file system on your machine without passing through a Novell AppArmor profile.

Scanning your server for open network ports can be done manually from outside the machine using a scanner such as nmap or from inside the machine using netstat and then inspecting the machine to determine which programs are answering on the open ports.

NETWORK APPLICATIONS

A more automated method is to use the Novell AppArmor tool "Unconfined." The tool inspects your open ports from inside your computer (using the command "netstat -nlp"), detects the associated programs, inspects the set of AppArmor profiles you have loaded and reports these programs (along with their associated AppArmor profiles). If a program is not confined, it will not be reported.

Note: Unconfined requires root privilege and should not be run from within an AppArmor profile.

Unconfined does not distinguish between one network interface and another, so it will report all unconfined processes, even those that may be listening to an internal LAN interface. If a program is listening to more than one network interface, it may be reported more than once. Therefore, duplicate entries may be in the output.

WEB APPLICATIONS

To find Web applications, you should analyze your Web server configuration. The Apache Web server is highly configurable, and Web applications can be stored in many directories, depending on your local configuration. SUSE LINUX Enterprise Server 9, by default, stores Web applications in `/srv/www/cgi-bin/`.

Confining each Web application with its own Novell AppArmor profile minimizes the privileges that the Web application has and thus minimizes the attacker's opportunities to hijack the program. However, you can also choose to spend less effort hardening your system (at the expense of security) by choosing instead to run a Web application within the Apache AppArmor profile.

The selection of whether a Web application has its own profile or uses Apache's profile happens in the `genprof` and `logprof` profiling utilities described in the "Profile Building" section. When Apache executes a child process, the profiling utilities ask whether to profile the child application or inherit Apache's profile.

SCRIPTING LANGUAGES

Many Web applications are written in interpreted "scripting" languages such as PERL, PHP or Python. To enhance performance, many Web sites use `mod_perl`, `mod_php` and `mod_python` to place interpreters for these programming languages directly inside the Apache Web server. This improves performance because Apache no longer has to execute a large interpreter program to run a small script. Instead, it can just open the script file and

interpret it directly. However, this also compromises security because these Web applications run inside the Apache process using Apache's privileges.

Novell AppArmor provides a powerful capability to confine individual Web applications even though they are executed inside Apache using modules such as `mod_perl`, `mod_php` or `mod_python`. The AppArmor Apache module `mod_change_hat` induces a call to the AppArmor `change_hat()` API, causing Apache to change to a sub-profile corresponding to the name of the script about to be executed. If no specific profile for the script is found, a default profile associated with the interpreter can be used. This could, for example, increase security by confining all PHP pages to a similar profile permissive enough for all of the PHP pages to work but more restrictive than the Apache profile.

SETUID PROGRAMS

You can inspect your file system to find setuid programs. For instance, this command will find files that are setuid root:

```
find/-user root -perm -4000 -print
```

Programs that are setuid or setgid should be confined with Novell AppArmor because they enable any user to assume the privileges of the setuid or setgid settings. To defend these privileges, the only line of defense is the correctness of the programs; if there is a bug that allows a non-privileged user to force the program to run arbitrary code by presenting "creative" input, that user can gain root permissions. AppArmor confinement ensures that the program can only do the tasks it needs

to do, making such attacks by non-privileged users futile.

CRON JOBS

To find programs that will be run by cron, you need to inspect your local cron configuration. Unfortunately, cron configuration is rather complex, so there are numerous files to inspect. Periodic cron jobs are run from these files:

- `/etc/crontab`
- `/etc/cron.d/*`
- `/etc/cron.daily/*`
- `/etc/cron.hourly/*`
- `/etc/cron.monthly/*`
- `/etc/cron.weekly/*`

For root's cron jobs, you can edit the tasks with `"crontab -e"` and list root's cron tasks with `"crontab -l."`

PROFILE BUILDING

Once you have selected the programs to be profiled, you need to generate profiles for them. The Novell AppArmor utilities `genprof` and `logprof` automate most of this process, and ask you interactive questions about security decisions to complete the program profiles.

GENPROF

The `genprof` utility is the place to start. At a command line prompt in a root shell, say `"genprof foo"` where `"foo"` is the name of the program you want to profile. `Genprof` will scan your `foo` program and produce an initial estimate of the program's profile, and then set the profile into `"learning mode"`

where the profile rules are not actually enforced but where violations of the rules are logged.

`Genprof` will then invite you to run your program in another window, and as you run the program through its operation, it builds up a log file of events that characterize the correct behavior of your program.

Run your program through a thorough QA cycle, exercising all of its major functionality and being careful not to run any attacks against the program. When you are done, return to the `genprof` window and press the `"s"` (for `"scan"`) key. `Genprof` will then ask you a series of questions about how to respond to various file-access events.

Typically, your `foo` program will have accessed some file, and `genprof` will ask you if you want to grant explicit access to precisely that literal file name or if you would like to grant access to some file pattern. The pattern might include wild cards or a `#include` of a set of rules that satisfy not just this event but many others in the log file and future events.

LOGPROF

The `logprof` utility works very much like the `genprof` utility except that it is designed for the ongoing improvement of Novell AppArmor profiles rather than for initial generation. When you run `logprof`, it scans your current system log for AppArmor events and asks you what to do with each event, suggesting patterns as above in `genprof`.

You can even decouple QA testing from profile generation. For large applications with large QA suites, you can simply send the application and a

set of AppArmor profiles in learning mode to the QA department for testing. The AppArmor profiles will not alter the behavior of the applications being tested, although logging actions are not overtly permitted by the profile. The log files can then be collected at the end of the QA test and e-mailed back to security profile developers. They then run logprof offline from the program being tested to incrementally improve the profiles for these programs without ever having any access to the QA machines or the test suite.

RESULT CONFIRMATION

The last step of all computer security hardening procedures is to verify the security of your configuration, a principle Novell AppArmor follows. To verify the security of your AppArmor profiling efforts, run the unconfined program again (see "Network Agents" on page 3) and inspect the output to see that all programs exposed to attack have been profiled.

If your computer system is a network server, your threats likely come from the network. Thus, the standard output of unconfined reporting by all network services listening to network ports exactly reflects the threats to which your computer is exposed. When all of the programs that produce unconfined reports are associated with AppArmor

profiles, it is impossible for an attacker to directly access your file systems without going through the AppArmor policies you have set.

To do a worst-case analysis, for example, of the corruption an attacker could cause on your computer system, inspect each profile listed by unconfined. Viewing the profiles in vim is ideal, as that will show the profiles highlighted in color. (Rules highlighted in yellow are write rules.) The entire set of files an attacker can corrupt on your system is represented by the writable files listed in your profiles. This set is now a great deal smaller than the set a network attacker could access without the AppArmor enforcement.

SUMMARY

For protecting network servers, all threatened programs listed as unconfined should have an associated Novell AppArmor profile. If any program is listed as unconfined, go back to the relevant section of this document and apply an AppArmor profile to the program. Repeat this until all programs have been profiled. Once complete, AppArmor profiles will protect your systems against the effects of a hostile outsider, ensuring your business can minimize threats, protect key corporate data, reduce network administration costs and comply with regulations.

© 2005 Novell, Inc. All rights reserved. Novell, the Novell logo and the N logo are registered trademarks, and Immunix is a trademark of Novell, Inc. in the United States and other countries. SUSE is a trademark of SUSE LINUX Products GmbH, a Novell business.

*Linux is a registered trademark of Linus Torvalds. All other third-party trademarks are the property of their respective owners.

Novell Product Training and Support Services

For more information about Novell worldwide product training, certification programs, consulting and technical support services, please visit:
www.novell.com/services

For More Information

Contact your local Novell Solutions Provider, or visit the Novell Web site at:
www.novell.com

You may also call Novell at:

1 888 321 4272 U.S./Canada
1 801 861 4272 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA

www.novell.com