Linux Kernel Security (SELinux vs AppArmor vs Grsecurity)

Linux kernel is the central component of Linux operating systems. It is responsible for managing the system's resources, the communication between hardware and software and security. Kernel play a critical role in supporting security at higher levels. Unfortunately, stock kernel is not secured out of box. There are some important Linux kernel patches to secure your box. They differ significantly in how they are administered and how they integrate into the system. They also allow for easy control of access between processes and objects, processes and other processes, and objects and other objects. The following pros and cons list is based upon my personal experience.

SELinux

Security-Enhanced Linux (SELinux) is a Linux feature that provides a variety of security policies for Linux kernel. It is included with CentOS / RHEL / Fedora Linux, Debian / Ubuntu, Suse, Slackware and many other distributions.

SELinux features

1. Clean separation of policy from enforcement
2. Well-defined policy interfaces
3. Support for applications querying the policy and enforcing access control
4. Independent of specific policies and policy languages
5. Independent of specific security label formats and contents
6. Individual labels and controls for kernel objects and services
7. Caching of access decisions for efficiency
8. Support for policy changes
9. Separate measures for protecting system integrity (domain-type) and data confidentiality (multilevel security)
10. Very flexible policy
11. Controls over process initialization and inheritance and program execution
12. Controls over file systems, directories, files, and open file descriptors
13. Controls over sockets, messages, and network interfaces
14. Controls over use of "capabilities"

Pros and Cons

- Admin skill set (learning curve) - High
- Complex and powerful access control mechanism - Yes
- Detailed configuration required - Yes
- GUI tools to write / modify rules set - Yes
- CLI tools to write / modify rules set - Yes (see list of commands here)
- Ease of use - No (often described as horrible to use)
- Binary package - Available for most Linux distributions
- System performance impact: None
- Security Framework: Mandatory access controls using Flask
- Auditing and logging supported - Yes
- Typical user base - Enterprise users
- Documentation - Well documented

=> Official project website : nsa.gov

AppArmor

AppArmor (Application Armor) is another security software for Linux which maintained and released by Novell under GPL. AppArmor was created as an alternative to SELinux. AppArmor works with file paths. According to official Novell FAQ:

> AppArmor is the most effective and easy-to-use Linux application security system available on the market today. AppArmor is a security framework that proactively protects the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good program behavior and preventing even unknown software flaws from being exploited. AppArmor security profiles completely define what system resources individual programs can access, and with what privileges. A number of default policies are included with AppArmor, and using a combination of advanced static analysis and learning-based tools, AppArmor policies for even very complex applications can be deployed successfully in a matter of hours.

AppArmor is default in OpenSUSE and Suse Enterprise Linux. It was first successfully packaged for Ubuntu Linux.

Features

1. Full integration.
2. Easy deployment.
3. AppArmor includes a full suite of console and YaST-based tools to help you develop, deploy and maintain application security policies.
4. Protects the operating system, custom and third-party applications from both external and internal threats by enforcing appropriate application behavior.
5. Reporting and alerting. Built-in features allow you to schedule detailed event reports and configure alerts based on user-defined events.
6. Sub-process confinement. AppArmor allows you to define security policies for individual Perl and PHP scripts for tighter Web-server security.

Pros and Cons

- Admin skill set (learning curve) - Medium
- Complex and powerful access control mechanism - Yes.
- Detailed configuration required - Yes.
- GUI tools to write / modify rules set - Yes (yast2 and wizards).
- CLI tools to write / modify rules set - Yes.
- Ease of use - Yes (often described as less complex and easier for the average user to learn than SELinux).
- Binary package - Available for Ubuntu / Suse / Opensuse and distros.
- System performance impact - None.
- Security Framework - Mandatory access controls.
- Auditing and logging supported - Yes.
- Typical user base - Enterprise users.
- Documentation - Documented (mostly available from Opensuse and Suse enterprise Linux).

=> Official project website : novell.com

grsecurity

grsecurity is a set of patches for the Linux kernel with an emphasis on enhancing security. It utilizes a multi-layered detection, prevention, and containment model. It is licensed under the GPL.

Features

1. An intelligent and robust Role-Based Access Control (RBAC) system that can generate least privilege policies for your entire system with no configuration
2. Change root (chroot) hardening
3. /tmp race prevention
4. Extensive auditing
5. Prevention of arbitrary code execution, regardless of the technique used (stack smashing, heap corruption, etc)
6. Prevention of arbitrary code execution in the kernel
7. Randomization of the stack, library, and heap bases
8. Kernel stack base randomization
9. Protection against exploitable null-pointer dereference bugs in the kernel
10. Reduction of the risk of sensitive information being leaked by arbitrary-read kernel bugs
11. A restriction that allows a user to only view his/her processes
12. Security alerts and audits that contain the IP address of the person causing the alert

Pros and Cons

- Admin skill set (learning curve) - Low.
- Complex and powerful access control mechanism - No (it is simpler to administer than other two implementations. Also, policies are simpler to create, since there are no roles or complicated domain/file transitions).
- Detailed configuration required - No (works in learning mode).
- GUI tools to write / modify rules set - No.
- CLI tools to write / modify rules set - Yes (gradm tool).
- Ease of use - Yes.
- Binary package - Available for Ubuntu / RHEL / CentOS / Debian distros.
- System performance impact - None.
- Security Framework - Mandatory access controls (precisely, it is a RBAC implementation) using access control lists.
- Auditing and logging supported - Yes.
- Typical user base - Webserver and hosting companies.
- Documentation - unfortunately, is not well documented.

=> Official project website : grsecurity.net

Conclusion:

All three offers very good protection and I can select them based upon the following simple criteria:

- New user / ease of use : Grsecurity
- Easy to understand policy and tools : AppArmor
- Most powerful access control mechanism : SELinux

Feature	SELinux	AppArmor	grsecurity
Automated	No (audit2allow and system-config-selinux)	Yes (Yast wizard)	Yes (auto traning / gradm)
Powerful policy setup	Yes (very complex)	Yes	Yes
Default and recommended integration	CentOS / RedHat / Debian	Suse / OpenSuse	Any Linux distribution
Training and vendor support	Yes (Redhat)	Yes (Novell)	No (community forum and lists)
Recommend for	Advanced user	New / advanced user	New users
Feature	Pathname based system does not require labelling or relabelling filesystem	Attaches labels to all files, processes and objects	ACLs

My personal choice is grsecurity as it is easier to use and offers many other security features. I've used SELinux as it is default choice under RHEL. AppArmor was only tested in lab under OpenSuse. I suggest you download and install all 3 patches (also available via binary deb and rpm files) and compare them as per your setup to gain a deeper understanding of their differences.

Resources:

- AppArmor and SELinux Comparison
- SELinux and grsecurity: A Case Study Comparing Linux Security Kernel Enhancements
- SELinux and grsecurity: A Side-by-Side Comparison of Mandatory Access Control and Access Control List Implementations
- Hardening Linux - identifies many of the risks of running Linux hosts and applications and provides practical examples and methods to minimize those risks.
- SELinux by Example: Using Security Enhanced Linux - a very good book about security enhanced Linux with tons of examples.
- SELinux: NSA's Open Source Security Enhanced Linux - another good book explaining security enhanced Linux along with tons of examples for new and seasoned admins.
- Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort.
- Tutorial - A step-by-step guide to building a new SELinux policy module.
- Tutorial - AppArmor for Geeks
- Tutorial - AppArmor for Ubuntu Linux servers