

Novell AppArmor

June 20, 2006



Novell.[®]

[The Register](#) » [Security](#) » [Network Security](#) »

Original URL: http://www.theregister.co.uk/2005/01/12/hacker_penetrates_t-mobile/

Hacker breaches T-Mobile systems, reads US Secret Service email

By [Kevin Poulsen, SecurityFocus](#) (feedback at theregister.com)
Published Wednesday 12th January 2005 09:47 GMT

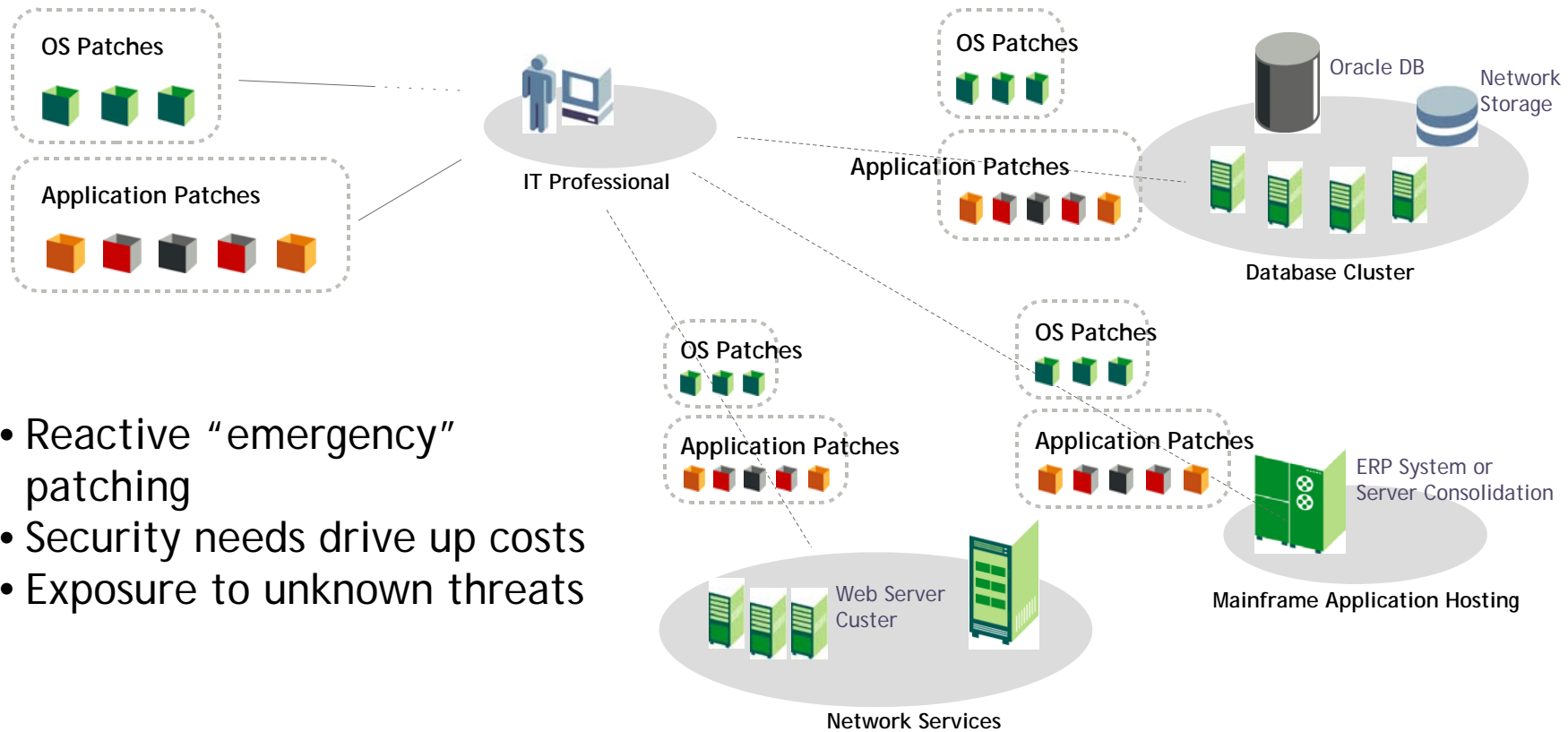
A sophisticated computer hacker had access to servers for at least a year, which he used to monitor US Secret Service customers' passwords and Social Security numbers, including those taken by Sidekick users, including Hollywood celebrities, it was learned.

Twenty-one year-old Nicolas Jacobsen was quietly caught in October, after a Secret Service informant helped investigate agency documents that were circulating in underground circles. The informant also produced evidence that Jacobsen was using T-Mobile customers' personal information to identify himself on a bulletin board, according to court records.

[Adblock](#)

“[The Hacker] could access information on any of the... company's 16.3 million customers, including many customers' Social Security numbers and dates of birth, according to government filings in the case.”

Securing Linux Applications Today



- Reactive “emergency” patching
- Security needs drive up costs
- Exposure to unknown threats

Today's Security Imperatives

- Protect against unknown threats
- Comply with government regulations
- Increase security, not IT complexity

N Solution: Linux Application Security

Security drivers causing IT to plan for host-based security

Linux Security Modules (LSM)

- Foundation for access control in the Linux kernel 2.6
- Enable policy-driven protection
- Creates firewall around programs
- Prevents unauthorized access to system resources

Business-critical platforms require host-based security to protect the expanding enterprise perimeter. Mobile computing and Web services will drive this need across the enterprise.

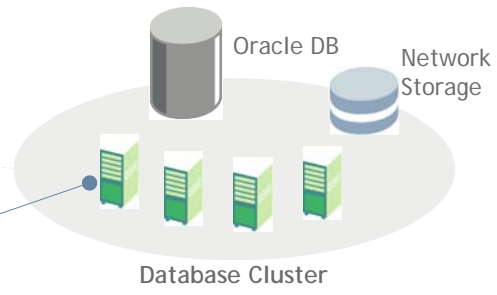
Gartner,
March 2004

AppArmor Increases IT Productivity

Increased IT Productivity. Emergency patching mitigated, update systems based on business need



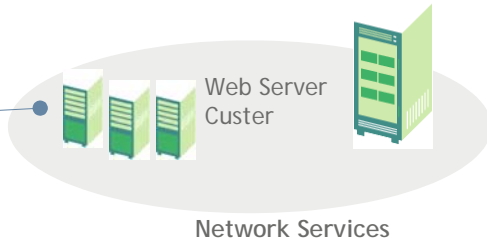
Scalable Security. Security policies are easy to build and deploy across servers



Uptime. Security policies can be updated without disruption to applications

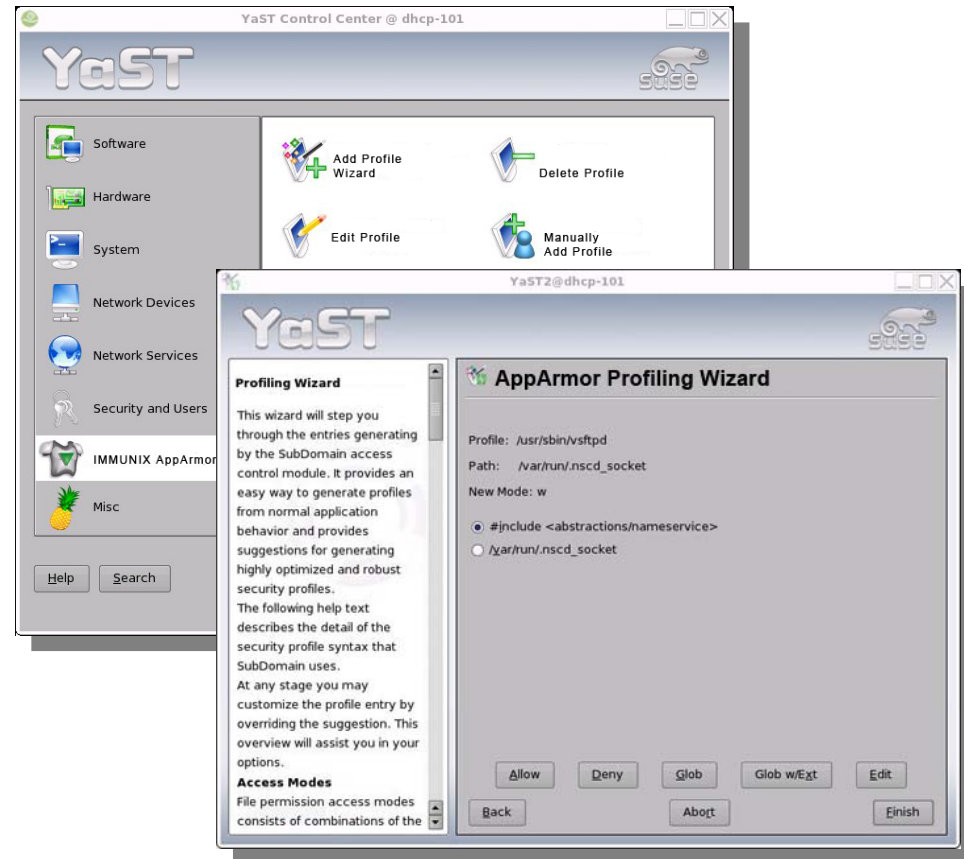


Confidence. Complete protection against unknown attacks



Easiest to Learn and Use

- YaST-based tools provide unmatched ease of use
- Profiling Wizard automates the task of developing security policy
- Easy deployment, short learning curve, no Linux or security expertise required
- Reporting and alerting features facilitate regulatory compliance



Out-of-the-Box Security Profiles

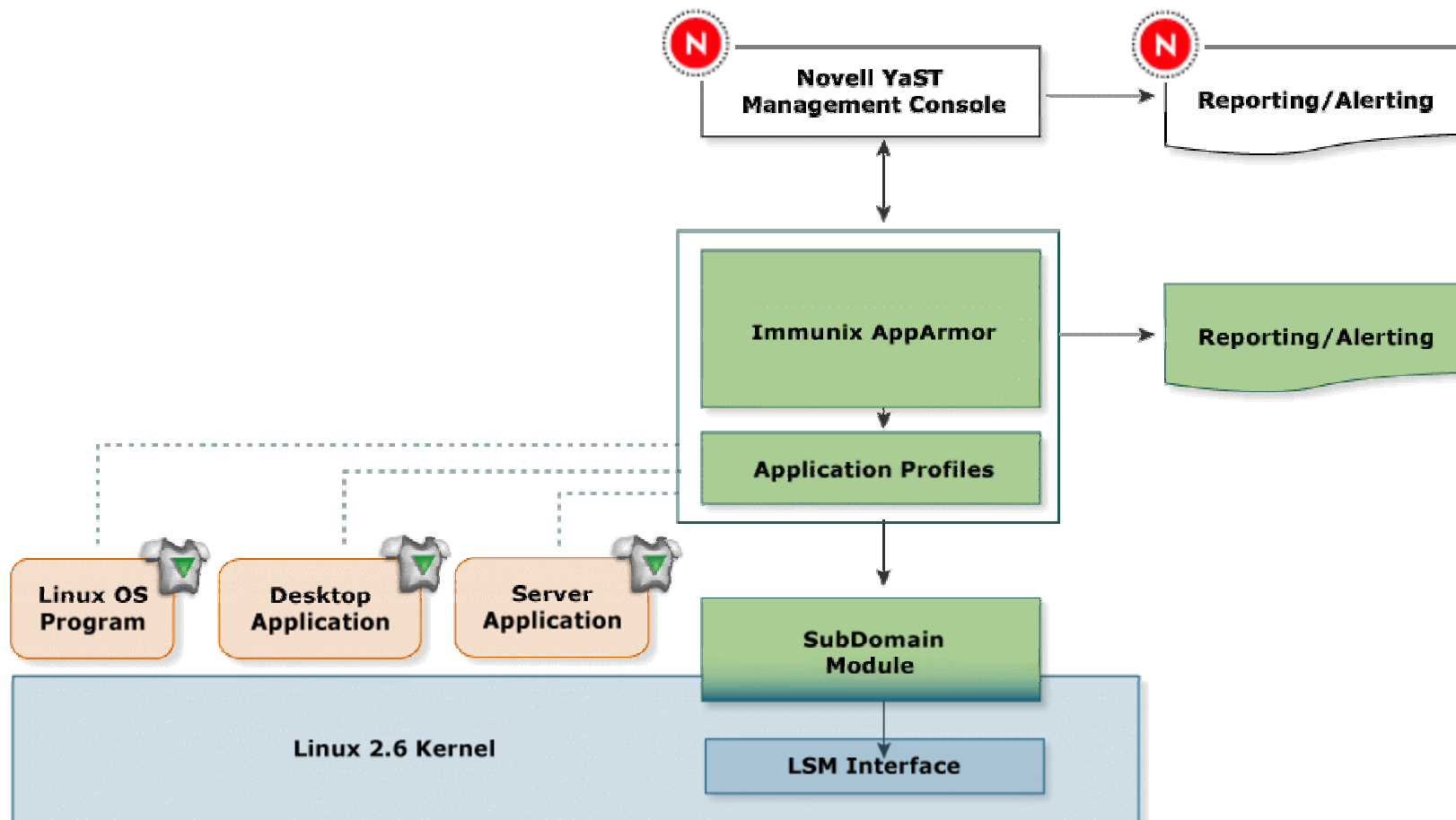
Component library includes fully-configured profiles for common operating system services and applications:

- Apache Web server
- Postfix mail server
- Sendmail mail server
- OpenSSH
- Squid
- ntpd
- nscd
- Others

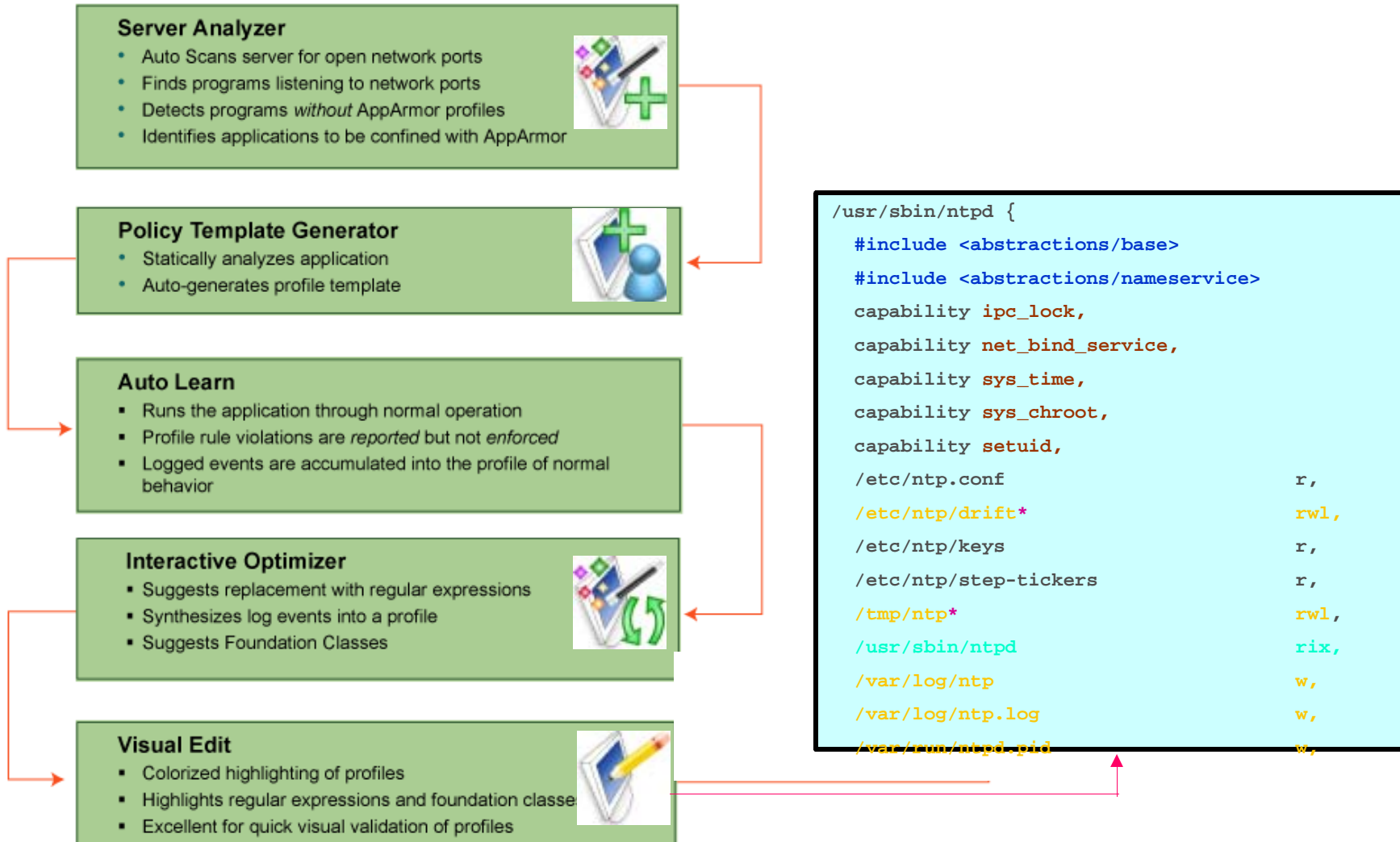
N Things to Remember

- Best Linux application security solution
- Easiest to use
- Security policies that scale
- Low cost of ownership for maintaining secure environment

How AppArmor Works



Automated Workflow

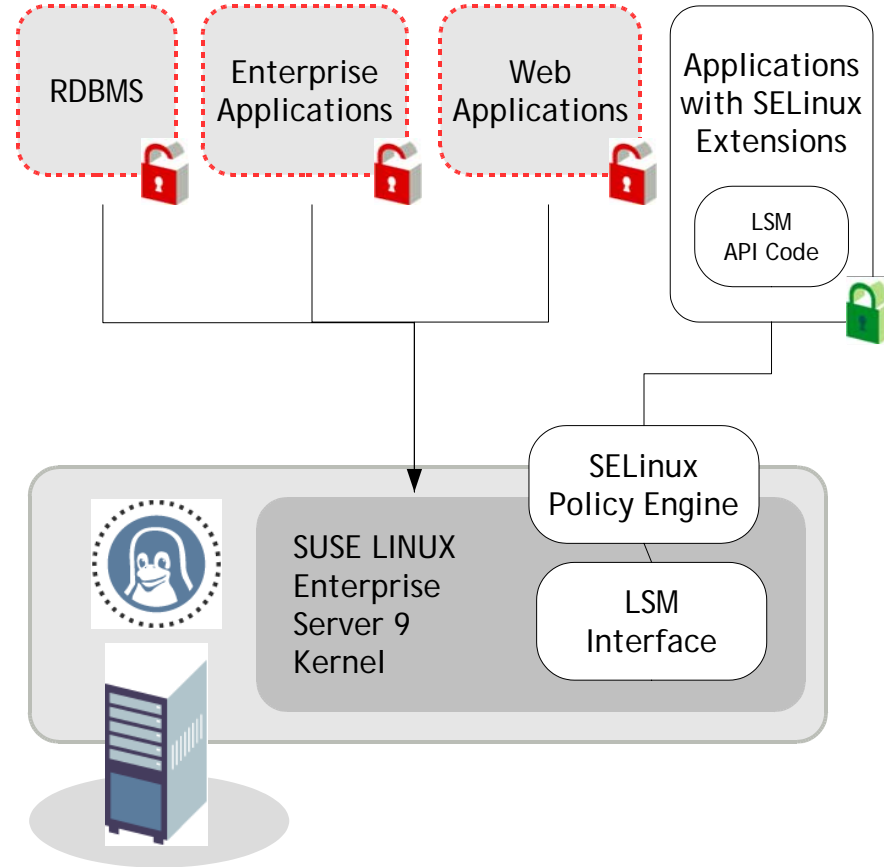
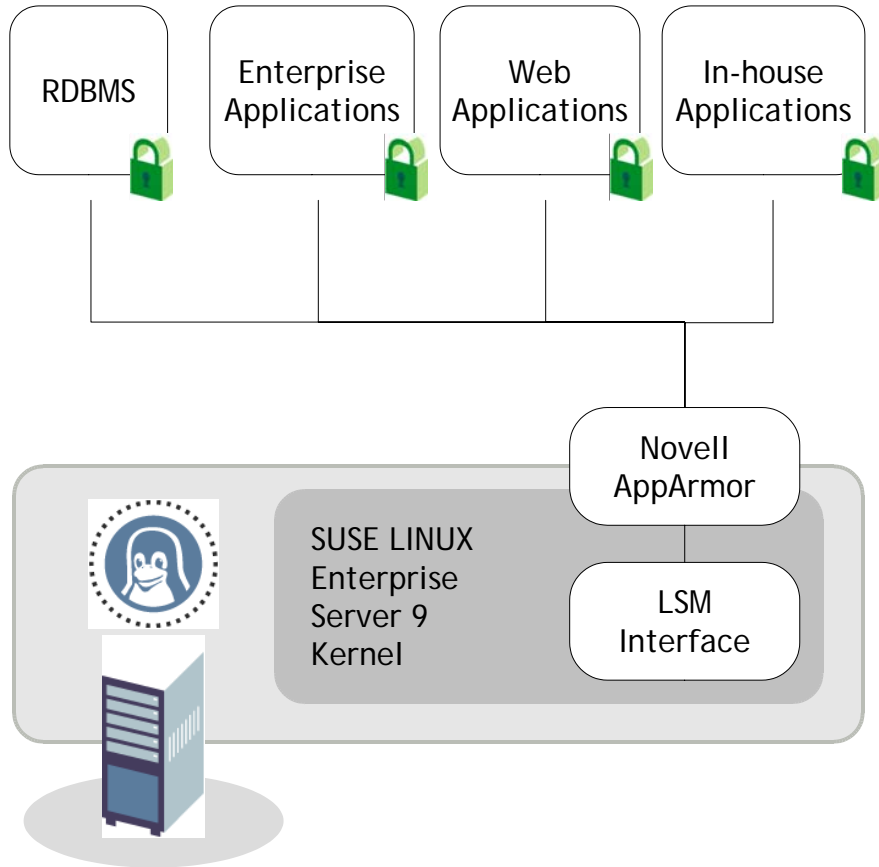


Performance

- 0% to 2% overhead
- Measured by using Webstone against Apache
 - common case: overhead too small to measure (approx. 0%)
 - extreme case: 2% overhead for *trivially* small `mod_perl` scripts that have very small base cases
- Measured by a customer (large dot.com site) their application benchmark showed
 - Common case: too small to measure (approx. 0%)

:: Competitive Information

Novell AppArmor or SELinux?



AppArmor vs. SELinux

- Both provide application security through access controls to confine users and programs
 - Both provide non-bypassable security using LSM interface
 - LSM standard in Linux 2.6, built by Novell for Linus

AppArmor advantages

Easier to Use / Maintain

- Individual profiles 4X smaller
- System profiles 100X smaller
- Automated tools
- Classical Unix syntax makes profiles easier to understand
- YaST interface integration
- Robust reporting/alerting facilitates regulatory compliance

Granular Security

- Can confine sub-processes like individual PHP pages

Scalable

- SELinux forces you to apply policy to the entire machine, all at once
- AppArmor lets you incrementally apply security to each application as you go

Faster

- AppArmor 0-2% overhead (SELinux 6-15%)

Questions & Answers

Novell.[®]

Unpublished Work of Novell, Inc. All Rights Reserved.

This work is an unpublished work and contains confidential, proprietary, and trade secret information of Novell, Inc. Access to this work is restricted to Novell employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of Novell, Inc. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. Novell, Inc., makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All Novell marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

