Linux Audit Subsystem

Olaf Kirch
Software Engineer
SUSE Labs, Novell

Novell

Overview

Things we'll cover in this presentation

- What's and why's of security evaluations
- Security evalution of SUSE LINUX Enterprise Server
- Linux Audit Subsystem

© December 11, 2003 Novell Inc.

Common Criteria

- Multinational security evaluation criteria
- Define functional and assurance requirements
- Evaluation Assurance Levels EAL1-EAL7
- Mutual recognition up to EAL4
- CC Evaluation a requirement for selling to various governments

© December 11, 2003 Novell Inc.

CC Protection Profiles

Select a set of requirements

Controlled Access Protection Profile (CAPP) for discretionary access control

CAPP is similar to Orange Book C2

Labeled Security Protection Profile (LSPP) for mandatory access control

More profiles being developed

© December 11, 2003 Novell Inc.

Linux Security Certifications

SLES security certifications done jointly with IBM

Evaluation by @sec

Submitted to German BSI

July 2003: SLES 8 receives CAPP EAL2+

- First open source product to receive certification
- “+” means additional flaw remediation assurances

January 2004: SLES 8 receives CAPP EAL3+

© December 11, 2003 Novell Inc.

Target of Evaluation (TOE)

SLES 8 on IBM eServer (xSeries, pSeries, iSeries, zSeries, Opteron)

Authentication based on PAM framework

Discretionary Access Control: POSIX ACLs on ext3

Trusted network applications: SSH, vsftpd, stunnel

Including the crypto components of SSH and vsftpd

© December 11, 2003 Novell Inc.

Certification Requirements

A large part of it is documentation

- Functional Specification
- High-level Design
- User Documentation
- Documentation of our Processes

No additional code was written for EAL2

For EAL3, we needed two new components:

- Audit subsystem
- TSF protection (AMTU - abstract machine test)

© December 11, 2003 Novell Inc.

Audit Subsystem

Linux Audit Subsystem

Implemented by SUSE, open sourced

For lack of a better name, we called it LAuS, and it stuck

RedHat uses LAuS for their EAL2 and EAL3 certifications

© December 11, 2003 Novell Inc.

CAPP Audit Requirements

Log activities of users at the system call level

Configuration changes (e.g. of the network interface)

Identify user based on login uid (across uid changes)

Display audit trail, allow selection of records

Must never lose audit records

© December 11, 2003 Novell Inc.

Design Goals

Zero overhead when audit is turned off

Low overhead when enabled

Minimally intrusive kernel patch

© December 11, 2003 Novell Inc.

Mode of Operation

Kernel Module decides to record an event

Generates binary blob and enqueues it to /dev/audit

Audit daemon reads record the device and writes them to disk

Utilities such as aucat and augrep allow to display and sift the audit trail

© December 11, 2003 Novell Inc.

Auditing system calls

Intercept incoming call as process enters kernel (entry.S)

Intercept return to user space to capture result (aka outcome) of the call

Decide whether system call needs to be logged or not (rules configured when audit daemon starts)

If yes, collect arguments, build record and enqueue it

Lots of architecture specific code

© December 11, 2003 Novell Inc.

Auditing configuration changes

Some are system calls, such as loading a module or setting the system time

Some should be logged by the application, such as changing the password

Some are ioctls (have some aspirin handy)

Some are netlink messages

© December 11, 2003 Novell Inc.

What's in a record?

Binary format for better performance and unambiguous representation

login ID, user and group ID, timestamp

system call number(s)

system call arguments

pointers may have to be dereferenced (file names), and file descriptors must be mapped to path names

© December 11, 2003 Novell Inc.

Careful with that Axe!

CAPP mandates we must not lose records, ever

Reliable transport from kernel module and user space applications to auditd

Audit daemon needs to deal with disks filling up

- can write to multiple bins and archive full bins
- monitors disk space and can be configured to react in a variety of ways

All audited processes “hang” when auditd is starved

© December 11, 2003 Novell Inc.

Filtering events

Filtering is done inside the kernel; anything else will ruin performance completely

Per system call boolean expression that indicates whether to log the call or not

Expression can reference positional arguments, user identity, etc. For instance, "*log this call if the first argument references a file in /etc and the caller's login UID is greater than 50*"

Rules are stored in a file and loaded into the kernel by auditd

© December 11, 2003 Novell Inc.

Auditing in SLES 9

Slightly different mechanism to capture system calls

EAL3 certified as well

© December 11, 2003 Novell Inc.

Future Work

Kernel 2.6 has a light-weight audit framework

Work is underway to create an audit implementation for mainline that is able to achieve certification

© December 11, 2003 Novell Inc.

Novell®

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.

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.

Novell