Audit BoFS

Steve Grubb
Red Hat

RHEL4 Audit

RHEL4 Audit

CAPP/EAL4+ with IBM

Certified by NIAP

HP and Unisys under eval

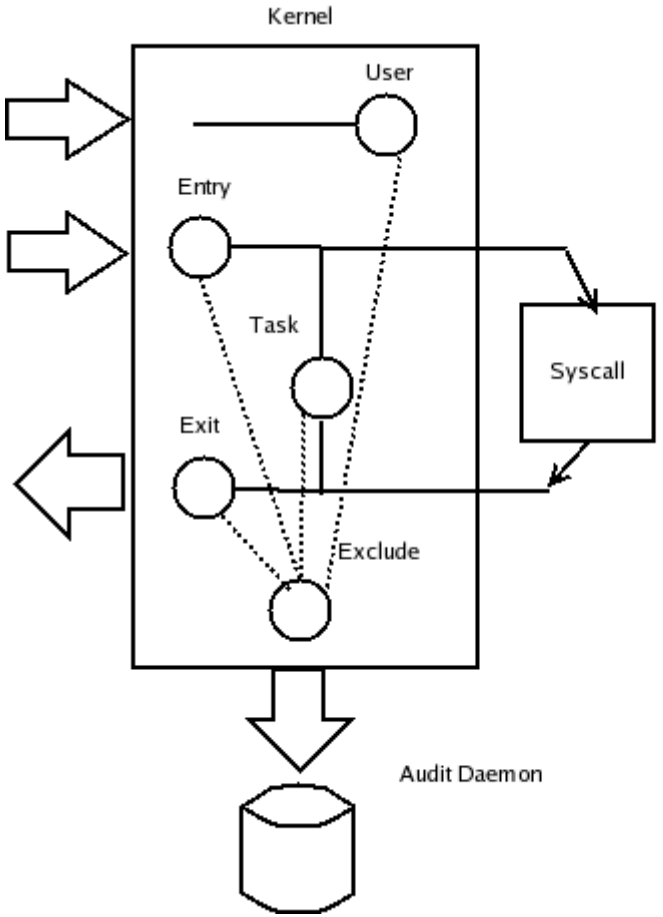
Changes Needed

Amtu, at, coreutils, dbus, gdm, glibc, kdm, openssh, pam, passwd, shadow, util-linux, vixie-cron, vsftpd, xdm.

All entry point programs must set loginuid

Apps that modify trusted databases updated to send audit event records

Audit Filters



Known Uses

- Resource utilization review
  - Cron & aureport
- Boot performance analysis
  - filemond bootchart.org
- SE Linux policy guidance
  - Ausearch & audit2allow

Current Work

RHEL4

RHEL4 U2 – CAPP

RHEL4 U3 – NISPOM

RHEL4 U4 – SOX

Fedora Core 5 – LSPP

NISPOM

Audit-1.0.12

Login/Logout – gdm, sshd, login

Black listing tty & accts - pam_tally

Report tools - aureport

Sarbanes-Oxley

Audit-1.0.15

Execve enhancements

Collect all parameters in aux record

Add tty to record

LSPP

Add context to all record

Add ability to audit by SE Linux user, role, type

Add terminal to syscall records for RBAC

Search by SE Linux user, role, type

Audit records hardcoded in kernel for policy load, boolean change, SE Linux enable/disable

LSPP

Cups audit events

Device allocator audit evens

Other

Performance update

Future Work

Library to Parse Events

Create framework to allow apps to pull audit events from the logs

Ausearch & aureport will use

Encapsulate log format knowledge so apps don't need to know

Kernel

Ability to track child processes

Needed for autrace

Audit Event Dispatcher

To meet DCID 6/3 Audit 9 need to respond in realtime to suspicious events

Auditd forks and exec's dispatcher

Comm is done via socketpair

Dispatcher reads stdin for events

Example in contrib/skeleton.c

Audit Event Dispatcher

/sbin/audispd

Will be plugin based

Relay events

- Ssl, syslog, dbus, snmp

Input events, other systems, iptables

Audit Event Dispatcher

Analyze events - anomalies

- Failed logins within certain time
- Logins at strange times
- Max concurrent sessions reached
- Logins from certain accounts
- Logins from certain locations
- Certain number of DAC failures

Audit Event Dispatcher

Analyze events

- Certain number of MAC failures
- Failure of amtu
- Failure of LSPP/RBAC self test
- Failure of crypto test
- Attempt to access certain directory
- Attempt to execute certain programs

Audit Event Dispatcher

Analyze events

- Adding account
- Deleting account
- Changes to account

Audit Event Dispatcher

React to anomaly events

- Ignore
- Log it
- Alert admin – console message, dbus, email, snmp
- Kill process
- Kill session
- Terminate access – logout, forge FIN packet, iptables

Audit Event Dispatcher

React to anomaly events

- Lock account for time
- Lock account for remote access
- Lock account
- Lock terminal
- Set SE Linux boolean
- Execute script

Audit Event Dispatcher

React to anomaly events

- Change to Single user mode
- Halt system

Audit Explorer

Gui to review logs

Likely to look like spreadsheet with cells

Right click on cell to list searches

Based on aureport as bottom layer

Questions ?

User space tools:

http://people.redhat.com/sgrubb/audit

Mail list:

http://www.redhat.com/mailman/listinfo/linux-audit