

Security Enhanced Linux (SELinux)

Mehr Sicherheit für alle?

Edin Dizdarević
edin@truesec.de

BRANDENBURGER LINUX INFOTAG

ANFASSEN, AUSPROBIEREN, ANWENDEN

22./23.04.2005

Br LUG



Was bisher geschah...

- Zugriffsregelungen (unter Linux):
 - Benutzer-Basierend und -geregelt – dem Ermessen des Besitzers überlassen (discretionary)
 - Nur 2 Benutzerarten: *root* und andere
 - Administrative Allmacht *root*
 - Übertragen bestimmter Rechte auf andere Benutzer möglich (*sudo*, *uid*, *gid*), schießt aber deutlich über das Ziel hinaus
 - **find / -perm +4000** liefert bei einer typischen Installation über 30 Files, alle gehören *root*

Problemstellung

- Ein amoklaufendes Programm besitzt alle(!) Rechte des jeweiligen Benutzers – im Falle *root* besonders schwerwiegend
- Ungeschulte Benutzer – **chmod 777** ist gar nicht so selten, wie man glauben möchte (Entwicklungsumgebungen, Testsysteme, ...)
- 0-day vulnerability:
 - (Noch) nicht bekannt gewordene Schwachstellen
- ...

Abhilfe

- *root* entmachten
- Bestimmten Zugriff erlauben, ohne die Sicherheit des Gesamtsystems zu gefährden
- „Sicherheitsnetz“ für sicherheitstechnisch unerwünschte Handlungen der Benutzer/Admins
- „Einfach“ *mehr* Sicherheit!

Eine (mögliche) Lösung: Security Enhanced Linux!

- Zugriff durch eine systemweite Policy geregelt
 - Mandatory (vorgeschrieben) Access Control – MAC
 - *root* ein „normaler“ Benutzer unter anderen
- Prozesse und Dateien in getrennten Sicherheitskontexten
- Rollenbasierte Rechte
 - Für spezielle Aufgaben entsprechend ausgeweitete Rechte möglich, aber nicht mehr! (Least Privilege)
- No-Do's (**neverallow**) kann in der Policy festgelegt werden (denn Admins sind auch („nur“) Menschen)
- Flexibles Logging (**audit/auditallow/dontaudit**) möglich
- ...

Was genau ist SELinux?

- Eine Erweiterung/Modul für den Kernel
 - Keine eigene Distribution!
 - RedHat:
 - “... Implementation of *mandatory access control (MAC)* in the Linux kernel,...”
 - “... a software product that ... that protects against attacks exploiting software vulnerabilities, including attacks on 0-day vulnerabilities.”
(B. McCarty, Autor Buch “SELinux”)

Wie entstand SELinux? (I)

- Forschungsprojekt der NSA
 - Basiert auf der FLASK-Sicherheitsarchitektur
 - Erste Implementierung im Forschungs-OS FLUKE
 - FLASK:
 - Trennt die Policy-Umsetzungslogik von der Entscheidungs-Logik
(Vorteil: das Sicherheitsmodell austauschbar)
 - Security Server mit der Access-Matrix?
 - Access Vector Cache (AVC) aus Performancegründen

Wie entstand SELinux? (II)

- NSA wollte eine Machbarkeitsabschätzung, ob FLASK in ein Mainstream-OS integriert werden kann
- SELinux wurde zunächst als Patch zur Verfügung gestellt
- Linus Torvalds wollte eine generische Lösung schaffen – Linux Security Modules (LSM)
- LSM: Hooks an strategisch wichtigen Stellen im Kernel
- LSM soll verschiedene Sicherheitsmodelle unterstützen, nicht nur SELinux
- Mehrere Sicherheitsmodelle sollen gleichzeitig nutzbar sein – stackbare Module
 - Der Zugriff wird von verschiedenen Modulen hintereinander überprüft

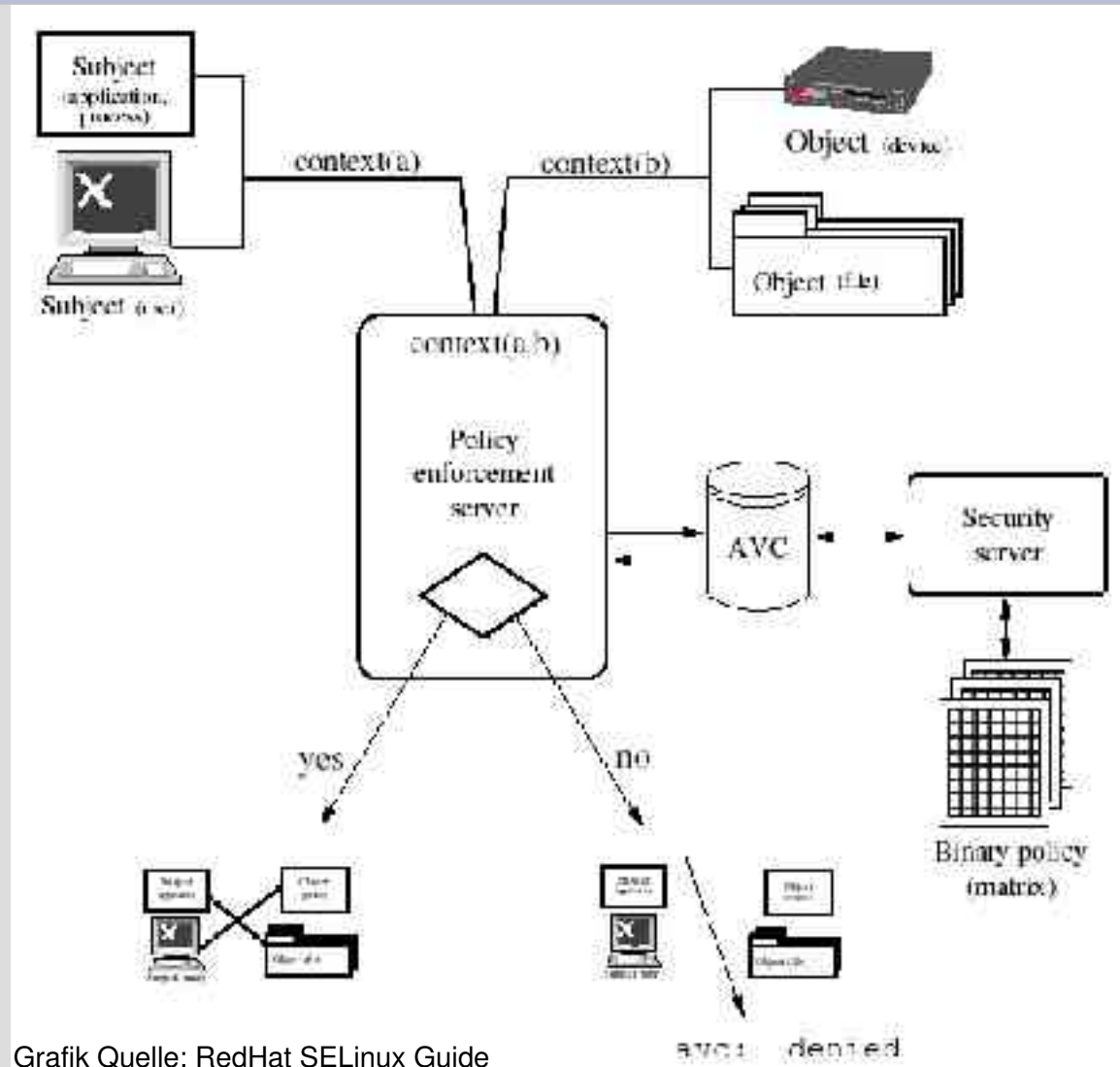
Was kann SELinux?

- Ein MAC-Sicherheitsmodell mit Kombination aus Kern-Subsystemen/Technologien:
 - Type Enforcement (TE)TM
 - Role Based Access Control (RBAC)
 - Multi Level Security (MLS, experimentell, noch nicht ausgereift)

Type Enforcement I

- Durch Type Enforcement haben:
 - Prozesse (Subjekte) zur Laufzeit und
 - Dateien (Objekte)(eigene) **Sicherheitskontexte**
- Ein Sicherheitskontext ist eine textuelle Darstellung von drei Objekt-/Subjektattributen:
User, Rolle und Typ/Domäne
user_u:role_r:type_t

Wie genau funktioniert es?



Grafik Quelle: RedHat SELinux Guide

Type Enforcement II: Typen und Domänen

- Mit dem Typen wird festgelegt, welcher Benutzer auf welche Art Zugriff bekommt
- Eine Domäne bestimmt welche Aktionen auf welche Objekttypen erlaubt sind
- Programme sind Entry-Ponts für Domänen
- Intern wird nicht zwischen Typen und Domänen unterschieden:
 - Domänen sind „einfach“ Typen, die nur auf Prozesse anwendbar sind

Type Enforcement III

- Die Sicherheitsskontexte werden im Dateisystem in Extended Attributes (xattr) abgelegt

- `getfattr -n security.selinux /etc/shadow`
`getfattr: Removing leading '/' from absolute path names`
`# file: etc/shadow`
`security.selinux="system_u:object_r:shadow_t\000"`
- Im Moment unterstützen ext2, ext3, (xfs, ReiserFS) xattr

- Andere Dateisysteme (ISO9660 & Co.) bekommen beim Mounten einen **kernelinternen**

Sicherheitskontext:

```
$ mount -v -t iso9660 -o \
context=system_u:object_r:removable_device_t \
/dev/hdc /media/cdrecorder
```

Type Enforcement IV:

Beispiel: Snort

- `/etc/selinux/targeted/src/policy/domains/program/snort.te:`
 - `daemon_domain(snort)`
`log_domain(snort)`
`can_network(snort_t)`
`type snort_etc_t, file_type, sysadmfile;`

 - `# Create temporary files.`
`tmp_domain(snort)`

 - `# use iptable netlink`
`allow snort_t self:netlink_socket create_socket_perms;`
`allow snort_t self:packet_socket create_socket_perms;`
`allow snort_t self:capability { setgid setuid net_admin net_raw };`
`r_dir_file(snort_t, snort_etc_t)`
`allow snort_t etc_t:file { getattr read };`
`allow snort_t etc_t:lnk_file read;`
`allow snort_t self:unix_dgram_socket create_socket_perms;`
`allow snort_t self:unix_stream_socket create_socket_perms;`

 - `# for start script`
`allow initrc_t snort_etc_t:file read;`

Type Enforcement V:

Beispiel: Snort

- `/etc/selinux/targeted/src/policy/file_contexts/program/snort.fc:`
 - `# SNORT`
 - `/usr/sbin/snort-plain -- system_u:object_r:snort_exec_t`
 - `/etc/snort(/.*)? system_u:object_r:snort_etc_t`
 - `/var/log/snort(/.*)? system_u:object_r:snort_log_t`
- Im Verzeichnis `/etc/selinux/targeted/src/policy/:`
 - `make reload ; make relabel`
 - `ls -laZ /usr/sbin/snort-plain`
 - `-rwxr-xr-x root root system_u:object_r:snort_exec_t \`
 - `/usr/sbin/snort-plain`

Role Based Access Control I

- Durch RBAC haben:
 - Benutzer und ihre Prozesse eine oder mehrere festgelegte Rollen, die ihnen bestimmte Rechte einräumen
 - RBAC verbindet Benutzer mit ihren Rollen bzw. dem Sicherheitskontext
`ed@mobile ~]$ id -Z`
`user_u:system_r:unconfined_t`
 - Ein Rollenwechsel nach Authentisierung möglich
`newrole -r sysadm_r`

Role Based Access Control II

- Beispiel:

```
/etc/selinux/targeted/src/policy/users:
```

```
- user system_u roles { system_r } ;  
  user user_u roles { user_r sysadm_r system_r } ;  
  user root roles { user_r sysadm_r system_r } ;
```

Fedora Core 3 SELinux Facts

- Für den (produktiven) Einsatz bereits vorbereitet
- Wird bei der Installation auf Wunsch aktiviert, Debian- und SuSE-Pakete verfügbar
- 2 mögliche Policies
 - Targeted: Deckt “nur” ausgewählte Dienste ab:
httpd, mysqld, named, nscd, ntpd, portmap, postgres, snmpd, squid, syslogd, winbind
 - Strict: Restriktive Policy
- Enthält bereits modifizierte Versionen von
 - id, ps, passwd, ls, init, star, ...
- Als Ausgangsbasis für eigene Policies gut geeignet

SELinux: Die Policy

- Nachinstallieren:
 - selinux-policy-targeted-sources
 - /etc/selinux/policy/targeted/src/...
 - Optional: selinux-doc

Das Verhalten

- Möglichkeiten

Policy-Eintrag	Operation erlaubt	Protokolleintrag
Keine Regel	Nein	Ja
allow	Ja	Nein, außer gleiche auditallow-Regel vorhanden
auditallow	Nein , außer gleiche allow-Regel vorhanden	Ja
dontaudit	Nein	Nein

Fehlersuche

- **audit2allow**

- [root@mobile]# audit2allow -d
allow snort_t self:netlink_route_socket
{ create nlmsg_read };
- **Achtung: audit2allow ist gefährlich!**

Grafische Werkzeuge

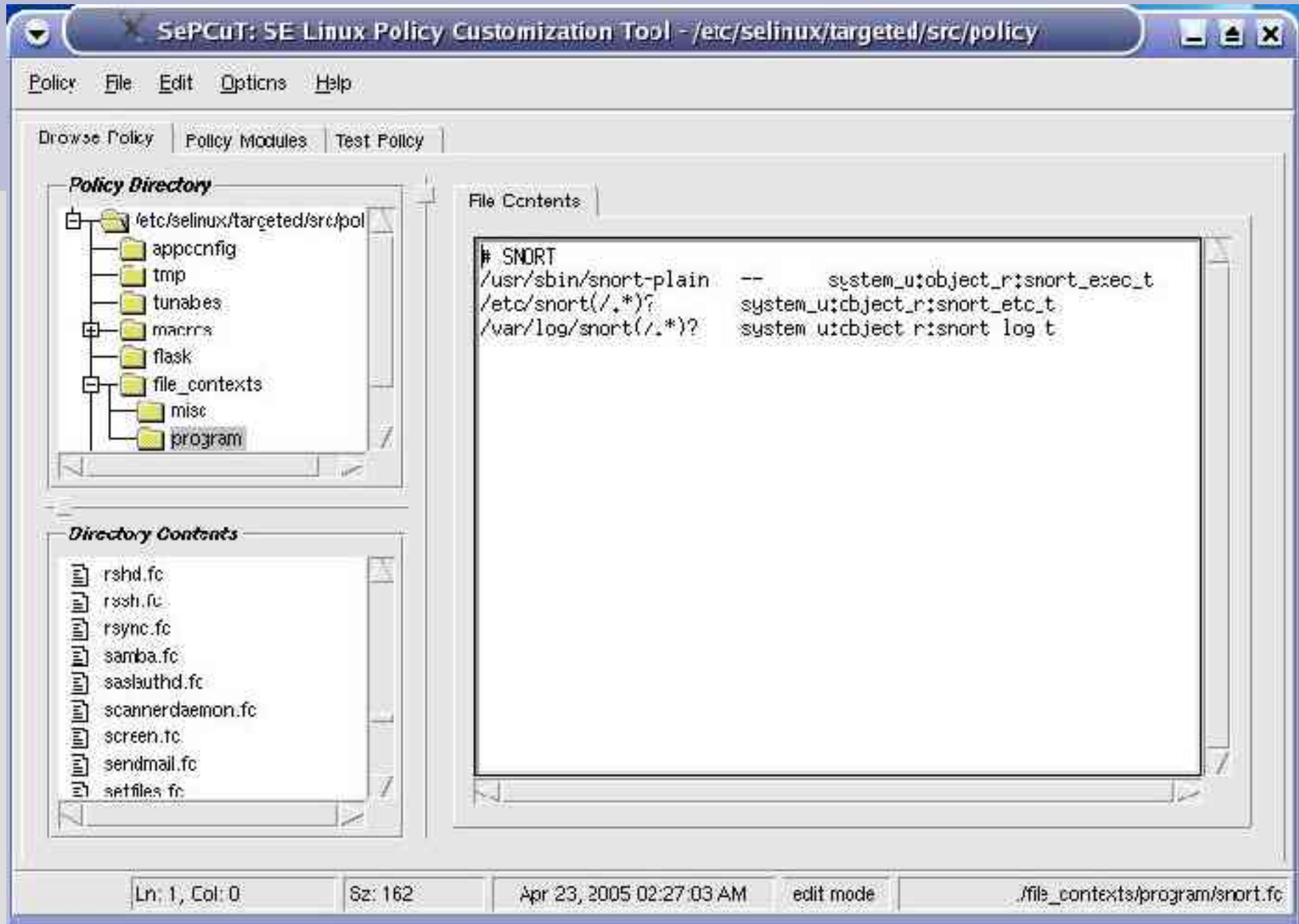
- RPM-Paket setools-gui
- apol – Policy-Analyse
- seaudit – Analyse der Logmeldungen
- seuser – Benutzerverwaltung
- sepcut – Policy Administration

Grafische Werkzeuge: seuser

The screenshot shows the SE Linux User Manager application window. The title bar reads "SE Linux User Manager" and includes standard window controls (minimize, maximize, close) and a "Help" button. The main content area is titled "System Users" and displays a table of system users. The table has four columns: "User", "Policy Type", "Roles", and "Groups". Below the table, there are several buttons: "Add", "View/Change", "Delete", "Advanced", "Update Policy", and "Exit".

User	Policy Type	Roles	Groups
adm	generic	sysadm_r system_r user_r	adm sys
bin	generic	sysadm_r system_r user_r	bin daemon sys
caemon	generic	sysadm_r system_r user_r	caemon bin adm lp
dbus	generic	sysadm_r system_r user_r	dbus
ed	generic	sysadm_r system_r user_r	users ed
ftp	generic	sysadm_r system_r user_r	ftp
games	generic	sysadm_r system_r user_r	users
gdm	generic	sysadm_r system_r user_r	gdm
gopher	generic	sysadm_r system_r user_r	gopher
halddaemon	generic	sysadm_r system_r user_r	halddaemon
halt	generic	sysadm_r system_r user_r	halt
lp	generic	sysadm_r system_r user_r	lp
mail	generic	sysadm_r system_r user_r	mail
mailnull	generic	sysadm_r system_r user_r	mailnull
rared	generic	sysadm_r system_r user_r	rared
retdump	generic	sysadm_r system_r user_r	retdump
news	generic	sysadm_r system_r user_r	news
nobody	generic	sysadm_r system_r user_r	nobody
rscd	generic	sysadm_r system_r user_r	rscd
rtmp	generic	sysadm_r system_r user_r	rtmp
operator	generic	sysadm_r system_r user_r	roct
pcap	generic	sysadm_r system_r user_r	pcap
root	defined	sysadm_r system_r user_r	root bin daemon sys
rpc	generic	sysadm_r system_r user_r	rpc
rpm	generic	sysadm_r system_r user_r	rpm
reiner	defined	user_r	reiner
shutdown	generic	sysadm_r system_r user_r	halt

Grafische Werkzeuge: apol



Grenzen von SELinux

- Filesysteme ohne xattr
- Policy-Erstellung nach wie vor sehr komplex
- Multi-Level-Security (MLS) noch nicht ausreichend getestet?

Warum SELinux? Alternativen?

- RSBAC – www.rsbac.org
 - MAC
 - RBAC
 - Schutz vor Buffer Overflows – PaX
 - ...
- Grsecurity – www.grsecurity.net
 - RBAC
 - Rollen
 - Lernmodus
 - PaX
 - ...
- LIDS – www.lids.org
 - PaX
 - ...

Links/Literatur

- <http://www.nsa.gov/selinux/>
- <http://www.nsa.gov/selinux/info/faq.cfm>
- <http://selinux.sourceforge.net/>
- <http://fedora.redhat.com/docs/selinux-faq-fc3/>
- <http://fedora.redhat.com/docs/selinux-apache-fc3/>
- https://sourceforge.net/docman/display_doc.php?docid=21959&group_id=21266
- <http://www.crypt.gen.nz/selinux/faq.html>
- <https://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/selinux-guide/>

Fragen

- Vielen Dank für die Aufmerksamkeit!
- Beitrag im Anschluß: Grsecurity...