SELinux

Mika Pflüger

9. Juli 2013

Table of contents

Warum mehr Sicherheit?

"Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it."
– Edward Snowden

Warum mehr Sicherheit?

- Verschlüsseln nützt nichts, wenn bei Versender, Empfänger oder Zwischenstationen mitgelesen werden kann.
- Beispiel Email, NormalnutzerInnen: Nutzung nur über Webclient, Email unverschlüsselt auf Servern.
- Metadaten sind immer auch auf Servern.

Historisches

- Entwickelt von der University of Utah und dem Department of Defense
- Weiterentwickelt und and Linux angepasst von der NSA
- Heutzutage in Mainline Linux
- Seit einigen Jahren in allen wichtigen Distributionen

Was ist SELinux?

- “Firewall für syscalls”
- Zusätzlich zu traditionellen Unix-Permissions
- Genauere, feiner unterteilte Rechte
- Definierte Policy wird vom Linux-Kernel durchgesetzt

Policy – wer darf was wann

- SELinux policy definiert, wer was wann darf oder nicht darf
- Wird vom Administrator geschrieben
- Referenzimplementierung: refpolicy
- Darauf aufbauend policies in den Distributionen

Policy – subjects und objects

- *subjects* führen Aktionen aus (Prozesse, User)
- Auf *objects* wird dabei zugegriffen (Dateien, Netzwerk-Ports, Speicherbereiche, SQL Tabellen, IP-Pakete etc.)

Verbotene Zugriffe werden gelockt (AVC-Denials).

Grundlagen

- Refpolicy ist modular aufgebaut
- Base-Modul enthält Port Definitions, policy für coreutils etc.
- Sonst ungefähr: Ein Modul pro Dienst

Grundlagen

Ein Module besteht aus:

- file contexts definitions: *.fc
- type enforcement rules: *.te
- interface definitions: *.if

Einfaches Beispiel: GnuPG

File contexts: gpg.fc

```
HOME_DIR/\.gnupg(/.+)? \
 gen_context(system_u:object_r:gpg_secret_t,s0)

/usr/bin/gpg(2)? -- \
 gen_context(system_u:object_r:gpg_exec_t,s0)

/usr/lib(64)?/gnupg/.* -- \
 gen_context(system_u:object_r:gpg_exec_t,s0)
```

Einfaches Beispie: GnuPG

Type Enforcement: gpg.te

```
allow gpg_t self:process { signal signull setrlimit \
 getcap setcap setpgid };

manage_files_pattern(gpg_t, gpg_secret_t, gpg_secret_t)
corecmd_exec_shell(gpg_t)
corecmd_exec_bin(gpg_t)
```

Exkurs: manage_files_pattern

Grundlegendes Makro von refpolicy

file_patterns.spt:

```
define(‘manage_files_pattern’,‘
allow $1 $2:dir rw_dir_perms;
allow $1 $3:file manage_file_perms;
’)
```

obj_perm_sets.spt:

```
define(‘manage_file_perms’,‘{ create open getattr \
 setattr read write append rename link unlink ioctl \
 lock }’)
```

Type Enforcement Rules

Wichtigste Statements:

- *allow subject object action;*
- *dontaudit subject object action;*
- *interface($1, $2,...)*

Einfaches Beispiel: GnuPG

Interface Definitions: gpg.if

```
## <summary>
## Send generic signals to user gpg processes.
## </summary>
interface(‘gpg_signal’,‘
          gen_require(‘
                  type gpg_t;
          ’)
          allow $1 gpg_t:process signal;
’)
```

Postifx – Übersicht

- Postfix hat für jede Aufgabe einen Dienst: Master, SMTP Dämon, SMTP Client, Local Delivery Agent
- Policy: Jeder Dienst hat einen eigenen Typ

Postfix – Policy

Ein paar Beispiele aus der SMTP Dämon policy:

```
allow postfix_smtpd_t postfix_master_t:tcp_socket \
 rw_stream_socket_perms;

# Connect to policy server
corenet_tcp_connect_postfix_policyd_port(postfix_smtpd_t)

# for OpenSSL certificates
files_read_usr_files(postfix_smtpd_t)

mta_read_aliases(postfix_smtpd_t)
```

SELinux installieren

- In Fedora/Red Hat ist SELinux vorinstalliert
- Debian: aptitude install selinux-policy-default

Policy anpassen

- Für vieles gibt es booleans, Beispiel: httpd_enable_homedirs
- Sonst am einfachsten: apt-get source refpolicy

Policy neu schreiben

Entweder von vorhandener Policy von ähnlichem Programm ausgehen, oder:

- SELinux in permissive Modus einschalten
- Das Programm ausführen
- audit2allow benutzen, um eine basic-policy zu bekommen.

Lesetipps

- http://wiki.debian.org/SELinux
- The SELinux Notebook – The Foundations
- Red Hat Security-Enhanced Linux User Guide