SELinux - Grundlagen

SELinux

SELinux

- SELinux (Security-Enhanced Linux; engl. „sicherheitsverbessertes Linux“) ist eine Erweiterung des Linux-Kernels. Es implementiert die Zugriffs-Kontrollen auf Ressourcen im Sinne von Mandatory Access Control. SELinux wurde von der NSA für eigene Bedürfnisse entwickelt und wird von dem Linux-Distributor Red Hat gepflegt.
- SELinux ist Open-Source-Software und setzt sich aus einem Kernel-Modul, Hilfsprogramme und aus zahlreichen Erweiterungen für System-Programme zusammen.

Vorteile von SELinux

- SELinux ermöglicht die Definition einer feinkörnigen Richtlinie für Prozesse
- Die Prozesse sind nicht in der Lage, auf Dateien zuzugreifen oder andere Prozesse außerhalb der SELinux-Regeln zu manipulieren
- Das SELinux-System kann die Ausweitung von Privilegien durch Sicherheits-Schwachstellen in Software verhindern

SELinux Richtlinien

- Kern-Bestandteil von SELinux sind die Richtlinien (Policies), welche sehr detailliert beschreiben, welche Zugriffe (Dateisystem, Syscalls, Netzwerk) einem Prozess oder einem Benutzer erlaubt sind.

SELinux Policy-Modi

- SELinux kann mit verschiedenen Policy-Einstellungen betrieben werden:
  - `full` - alle Ressourcen und Anwendungen im Linux-System sind von der SELinux Policy abgedeckt. Dies ist sehr aufwändig und wird von den Linux-Distributionen **nicht** angeboten
  - `targeted` - SELinux Policies existieren für kritische Komponenten im Linux-System (z.B. Systemd, Webserver, Mailserver etc). Nur diese Komponenten sind von SELinux abgesichert, alle anderen Komponenten befinden sich im `unconfined` Modus und werden von SELinux **nicht** beschränkt. Die Linux-Distributionen bieten Policies für den `targeted` Modus an.
  - `minimum` - Minimale SELinux Richtlinie

SELinux Enforcement Modi

- SELinux kann in drei verschiedenen Modi betrieben werden
  - **Enforcing**: Die Richtlinien sind geladen und werden aktiv durchgesetzt
  - **Permissive**: Die Richtlinien sind geladen, werden aber nicht durchgesetzt. Verstöße gegen die Richtlinien werden im Audit-Log protokolliert
  - **Disabled**: Die Richtlinien sind nicht geladen, SELinux ist nicht aktiv

SELinux Konfiguration

- Die SELinux Enforcement-Modi und Richtlinien-Modi werden in der Datei `/etc/selinux/config` konfiguriert

```
SELINUX=enforcing
SELINUXTYPE=targeted
```

Multi-Level-Security (MLS)

- SELinux kann mit Multi-Level-Security (MLS) betrieben werden
  - Bei MLS werden Dateien, Prozesse und Benutzer einer von 1024 Vertrauens-Ebenen zugeordnet
  - Benutzer einer Vertrauens-Ebene können nur mit Prozessen und Dateien unter oder gleich der eigenen Ebene agieren

Multi-Level-Security (MLS)

- Mit MLS können Geheimhaltungsgrade implementiert werde
  - Z.B. STRENG GEHEIM, GEHEIM, VS-VERTRAULICH, VS-NUR FÜR DEN DIENSTGEBRAUCH
  - MLS wird von den Linux-Distributionen **nicht** vorkonfiguriert oder unterstützt und muss ggf. manuell konfiguriert werden
  - MLS ist nicht Teil dieser Schulung

SELinux Status

- Der aktuelle Status des SELinux-Systems kann mit dem Befehl `sestatus` abgefragt werden

```
# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   permissive
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

SELinux Design

DAC und MAC

- Klassische Unix/Linux Systeme implementieren Discretionary Access Control (DAC) oder "benutzerbestimmbare Zugriffskontrolle"
    - Zugriffsrechte werden durch Dateiattribute bestimmt und können vom Benutzer frei gewählt werden

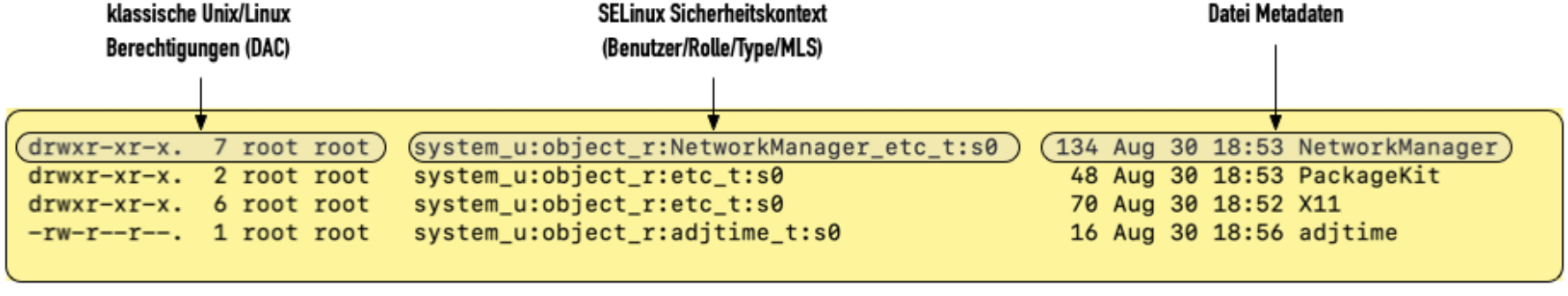
- SELinux implementiert Mandatory Access Control (MAC), zu Deutsch etwa: "zwingend erforderliche Zugangskontrolle", bei dem die Zugriffsrechte **zusätzlich** zum DAC in einer systemweiten Sicherheitsrichtline definiert ist.
    - Eine MAC kann in der Regel **nicht** vom Benutzer oder von Prozessen geändert werden

SELinux Richtlinie (Policy)

- Die SELinux Richtlinie beschreibt sehr detailliert die Zugriffsrechte von Benutzern und Prozessen auf Dateien und System-Funktionen (Systemcalls)
- Im Quellcode ist die SELinux Richtlinie modular
    - Der Quellcode wird beim Laden der Richtlinie in einen monolithischen Binäercode übersetzt (compiliert) und in den Linux-Kernel geladen
    - Es wird dabei immer das gesamte Regelwerk übersetzt und ausgetauscht (CPU intensiv und nicht schnell)

Label auf Dateien

- Beispiel-Ausgabe des Befehls `ls -lZ /etc`



Datei-Label anpassen

- SELinux Dateisystem Label können manuell mittels `chcon` (Change Context) gesetzt werden:

```
# chcon --type httpd_sys_content_t /var/www/html/index.html
```

Datei-Label anpassen

- Alternativ kann das passende Label aus der SELinux Richtlinie gelesen und angepasst werden

```
# restorecon -v /var/www/html/index.html
```

Datei-Label anpassen

- Wurde ein SELinux System mit ausgeschaltetem SELinux betrieben, so stimmen möglicherweise die SELinux Dateisystem-Label nicht mehr
    - Dateien welche bei ausgeschaltetem SELinux angelegt wurden erhalten kein Label
    - Die Label müssen vor der Aktivierung von SELinux korrekt gesetzt sein

Datei-Label anpassen

- Existiert beim Systemstart die Datei `.autorelabel` im Root-Verzeichnis `/` so werden alle Dateien mit neuen SELinux-Label versehen und danach das System neu gestartet

```
# touch /.autorelabel && reboot
```

Autorelabel / FixFiles

- Der Autorelabel Prozess startet das Sktipt `/usr/sbin/fixfiles`
- Dieses Script kann auch benutzt werden, um fehlende oder falsche SELinux Label auf Dateien zu finden

```
# fixfiles -v check /etc
Would relabel /etc/ssh/keys/ssh_host_ecdsa_key from system_u:object_r:sshd_key_t:s0 to system_u:object_r:etc_t:s0
Would relabel /etc/ssh/keys/ssh_host_ecdsa_key.pub from system_u:object_r:sshd_key_t:s0 to system_u:object_r:etc_t:s0
Would relabel /etc/ssh/keys/ssh_host_ed25519_key from system_u:object_r:sshd_key_t:s0 to system_u:object_r:etc_t:s0
Would relabel /etc/ssh/keys/ssh_host_ed25519_key.pub from system_u:object_r:sshd_key_t:s0 to system_u:object_r:etc_t:s0
Would relabel /etc/ssh/keys/ssh_host_rsa_key from system_u:object_r:sshd_key_t:s0 to system_u:object_r:etc_t:s0
Would relabel /etc/ssh/keys/ssh_host_rsa_key.pub from system_u:object_r:sshd_key_t:s0 to system_u:object_r:etc_t:s0
Would relabel /etc/hosts~ from unconfined_u:object_r:etc_t:s0 to unconfined_u:object_r:net_conf_t:s0
```

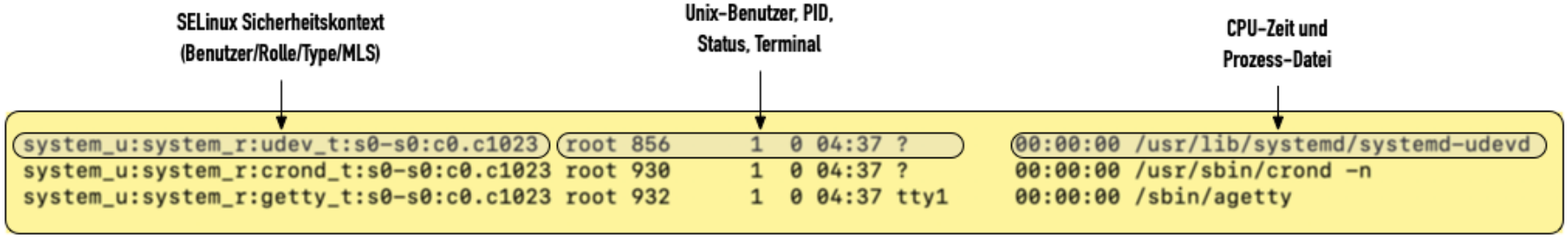
Label von RPM-Paketen prüfen und berichtigen

- Das Script `fixfiles` kann die Datei-Pfade aus den RPM-Paketbeschreibungen lesen und die Dateien von RPM-Paketen prüfen und berichtigen

```
fixfiles -v -R nginx,httpd restore
```

Label auf Prozessen

- Beispiel-Ausgabe des Befehls `ps -efZ`

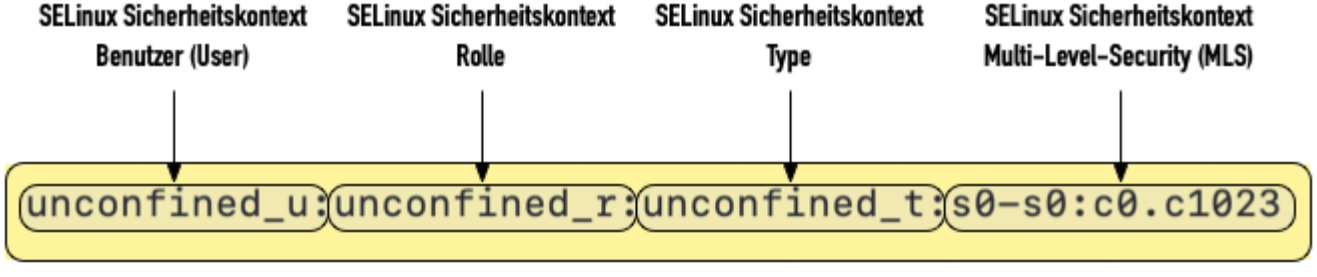


Label auf Prozessen

- Prozesse erhalten die SELinux Label aus der geladenen SELinux Policy

Label auf Benutzer

- Beispielausgabe des Befehls `id -Z`



Label auf Benutzer

- Der SELinux Sicherheits-Kontext auf Benutzer wird bei der Anmeldung über ein spezielles SELinux PAM-Modul gesetzt

SELinux Label

- Der Befehl **`seinfo`** liefert Informationen über die verfügbaren Label

```
seinfo -u    # Übersicht der SELinux Benutzer
seinfo -r    # Übersicht der SELinux Rollen
seinfo -t    # Übersicht der SELinux (Datei-) Typen
```

SELinux Status

- Der Befehl `sestatus -v` liefert Informationen über den SELinux Status der aktuellen (Login) Sitzung

```
[..]
Process contexts:
Current context:                unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
Init context:                   system_u:system_r:init_t:s0
/sbin/agetty                    system_u:system_r:getty_t:s0-s0:c0.c1023
/usr/sbin/sshd                  system_u:system_r:sshd_t:s0-s0:c0.c1023

File contexts:
Controlling terminal:           unconfined_u:object_r:user_devpts_t:s0
/etc/passwd                     system_u:object_r:passwd_file_t:s0
/etc/shadow                     system_u:object_r:shadow_t:s0
/bin/bash                       system_u:object_r:shell_exec_t:s0
/bin/login                      system_u:object_r:login_exec_t:s0
/bin/sh                         system_u:object_r:bin_t:s0 -> system_u:object_r:shell_exec_t:s0
/sbin/agetty                    system_u:object_r:getty_exec_t:s0
/sbin/init                      system_u:object_r:bin_t:s0 -> system_u:object_r:init_exec_t:s0
/usr/sbin/sshd                  system_u:object_r:sshd_exec_t:s0
```

SELinux Richtlinien

Richtlinien-Module

- Red Hat Linux basierte Distributionen liefern eine große Anzahl von vorgefertigten SELinux Richtlinien-Modulen
- Diese Module werden aktiv sobald die entsprechende Software installiert wurde

Richtlinien-Module

- Der Befehl `semodule -l` listet alle SELinux Module dieses Systems

```
# semodule -l | head
abrt
accountsd
acct
afs
aiccu
aide
ajaxterm
alsa
amanda
amtu
```

Richtlinien-Quellcode

- Die SELinux Policy Module sind (meist) in der `m4` Makro-Sprache geschrieben
- Beispiel aus der BIND 9 SELinux Policy

```
########################################
## <summary>
##      Create, read, write, and delete
##      BIND configuration files.
## </summary>
## <param name="domain">
##      <summary>
##      Domain allowed access.
##      </summary>
## </param>
#
interface(`bind_manage_config',`
     gen_require(`
             type named_conf_t;
     ')

     manage_files_pattern($1, named_conf_t, named_conf_t)
')
```

Ende Kapitel "SELinux Grundlagen"