

SELinux – Sicherheit auf Kernelebene

Thorsten Scherf
Red Hat EMEA



redhat.com

Agenda

- Warum sollte ich Security Enhanced Linux (SELinux) benutzen?
- Wie funktioniert SELinux?
- Wie haben wir SELinux in RHEL/Fedora implementiert
- Wie gehts es weiter mit SELinux?

Software Fehler und Patch Zyklus

- Software ist nicht fehlerfrei
- Die Frage lautet nicht:
Wird ein Fehler in meinem Programm gefunden
sondern
Wann wird ein Fehler in meinem Programm gefunden
- Klassischer Patch Zyklus
 - Eine Schwachstelle in der Software wird entdeckt
 - Hersteller wird benachrichtigt
 - Ein Patch wird (hoffentlich) bereitgestellt
 - Der Patch wird auf dem betroffenen Systemen eingespielt

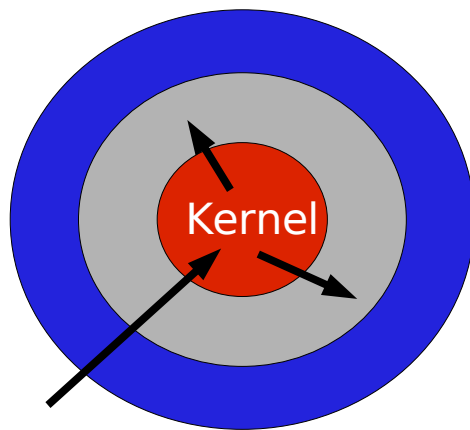
Was wenn...

- ...die falschen Leute die Schwachstelle finden?
- ...der Hersteller nicht benachrichtigt wird?
- ...der Hersteller sich viel Zeit lässt um einen Patch bereitzustellen?
- ...der Hersteller benachrichtigt wird und seine Antwort lautet:
Won't fix!

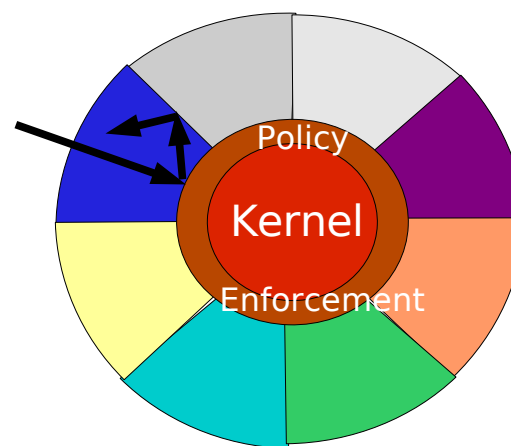
Klassische Linux-Systeme bieten hier keinen Schutz!

SELinux bietet Schutz

- SELinux benutzt Mandatory Access Control (MAC)
- Eine globale Policy unterbindet Zugriffe ausserhalb einer definierten Domäne
- Benutzer & Programme haben eingeschränkte Rechte
- Das gilt auch für den Benutzer root



DAC-System



MAC-System

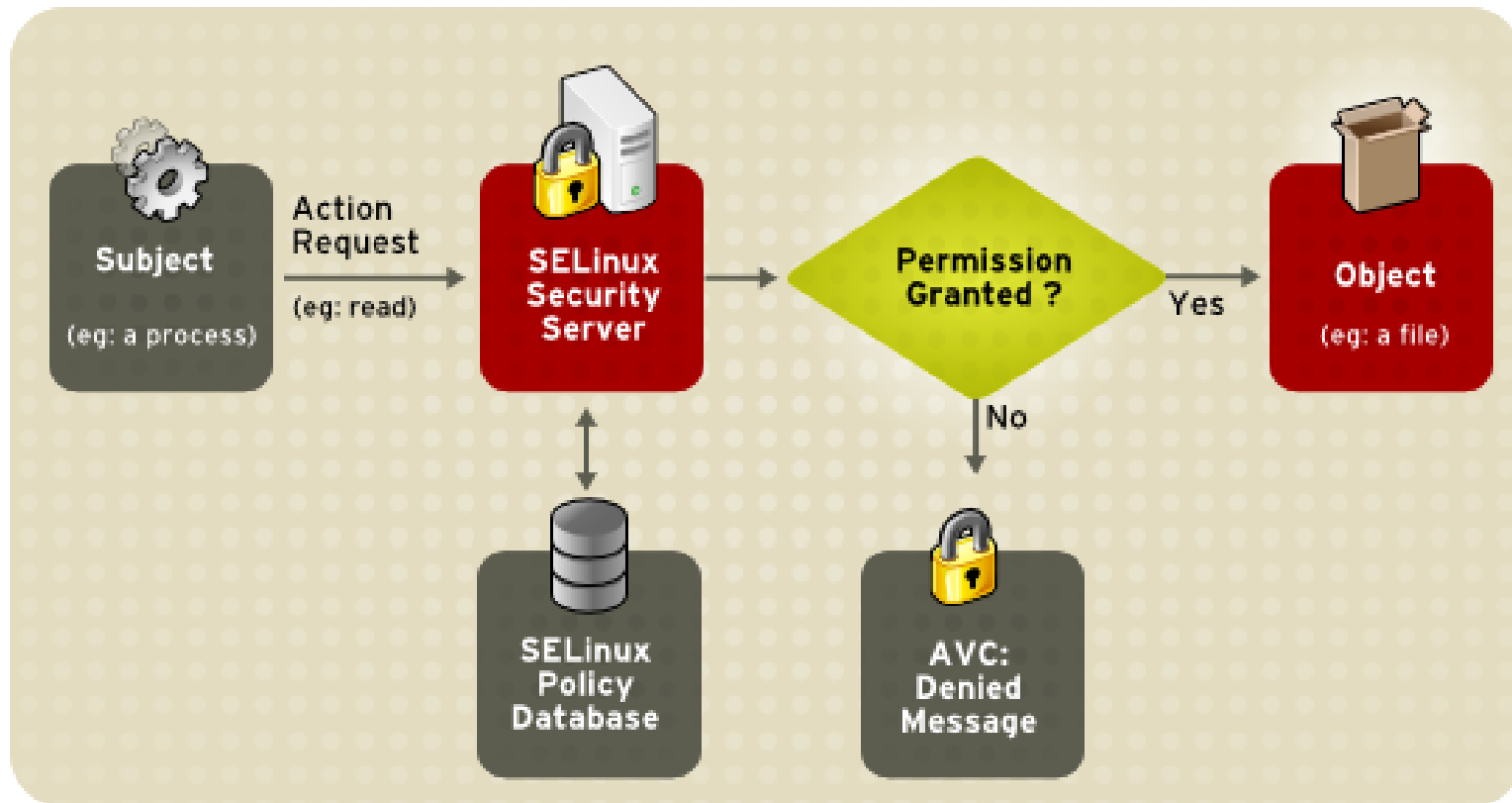
SELinux Key Komponenten I

- Der SELinux-Kernel
 - Patch ist upstream
 - benutzt Linux-Security-Modules (LSM)
 - besteht aus dem Security-Server und der Policy
 - Enforcement und Regelwerk sind also getrennt
 - Sourcen: `$KERNELSRC/security/selinux/`

SELinux Key Komponenten II

- Die SELinux-Policy existiert in 3 Versionen
 - Targeted Policy
 - Strict-Policy
 - MLS-Policy (RHEL5)
- Die zu schützenden (Userspace-) Applikationen müssen nicht SELinux-aware sein
- Nur einige Management Tools sind auszutauschen
 - z.b. coreutils, policycoretutils, usw...

Architektur



Anpassung des SELinux-Systems I

- Booleans
 - Bieten die Möglichkeit gewisse Eigenschaften der Policy zu verändern
 - `httpd_enable_cgi --> off`
 - `httpd_enable_homedirs --> off`
- Policy
 - Das Regelwerk selbst kann angepasst werden:
 - `/etc/selinux/$POLICY/src/` (RHEL4)
 - `/usr/share/selinux/devel/` (RHEL5)

Anpassung des SELinux-Systems II

- Security-Kontexte des Filesystems können verändert werden
 - `chcon -t httpd_sys_content_t /var/www/html/`

- SELinux Logmeldungen
 - `/var/log/messages` (ohne auditd – RHEL4)
 - `/var/log/audit/audit.log` (mit auditd - RHEL5)

SELinux – Where do you go tomorrow?

- Modulare statt monolithische Policy
 - Policy kann direkt mit einem RPM installiert werden
- Neue Management-Tools
 - policygentool, semanage, semodule
- Erweiterte targeted-Policy (~150 targets)
- ~ 200 Booleans verfügbar
- Xen-Support
- EAL4+/LSPP Zertifizierung

Key Points

- SELinux bietet eine zusätzliche Sicherheitsschicht basierend auf der Mandatory Access Control (MAC)
- Sehr grosse Flexibilität (targeted, strict, MLS, Booleans)
- Keine Anpassung der Applikationen notwendig
- Ausführliche Dokumentation und aktive Mailinglisten
- LSPP Zertifizierung nach Common Criteria
- Red Hat bietet als erster Distributor Enterprise-Level Support

Vielen Dank für Ihre Aufmerksamkeit

SELinux-Wiki: <http://fedoraproject.org/wiki/SELinux>

Feedback: tscherf@redhat.com