Red Hat Enterprise Linux: Mehr Sicherheit mit SELinux

Joachim Schröder
joachim.schroeder@redhat.com
Red Hat GmbH

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

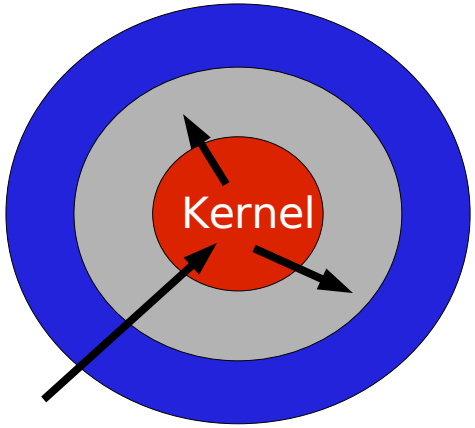
Was wenn...

- ...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!*

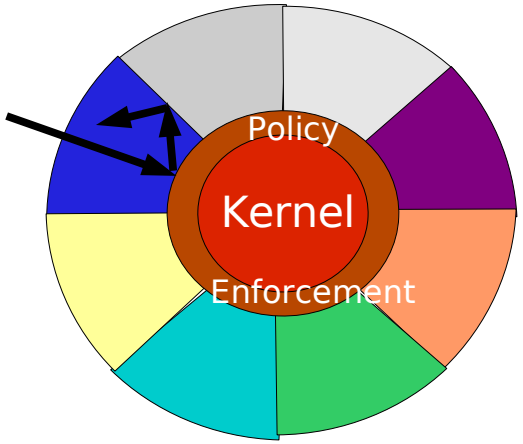
Klassische Linux-Systeme bieten hier keinen Schutz!

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

Historie

Aufbauend auf jahrelanger OS Sicherheits-Entwicklung der NSA

- DTMach -> Flask -> SELinux
- Separiert eindeutig Policy von Enforcement durch wohldefinierte Policy-Schnittstellen
  - Policy: Security-Server
  - Enforcement: Kernel-Subsysteme (Filesystem, Networking, ...)
- Fein-granulare Kontrolle über Kernel Services

SELinux Key Komponenten I

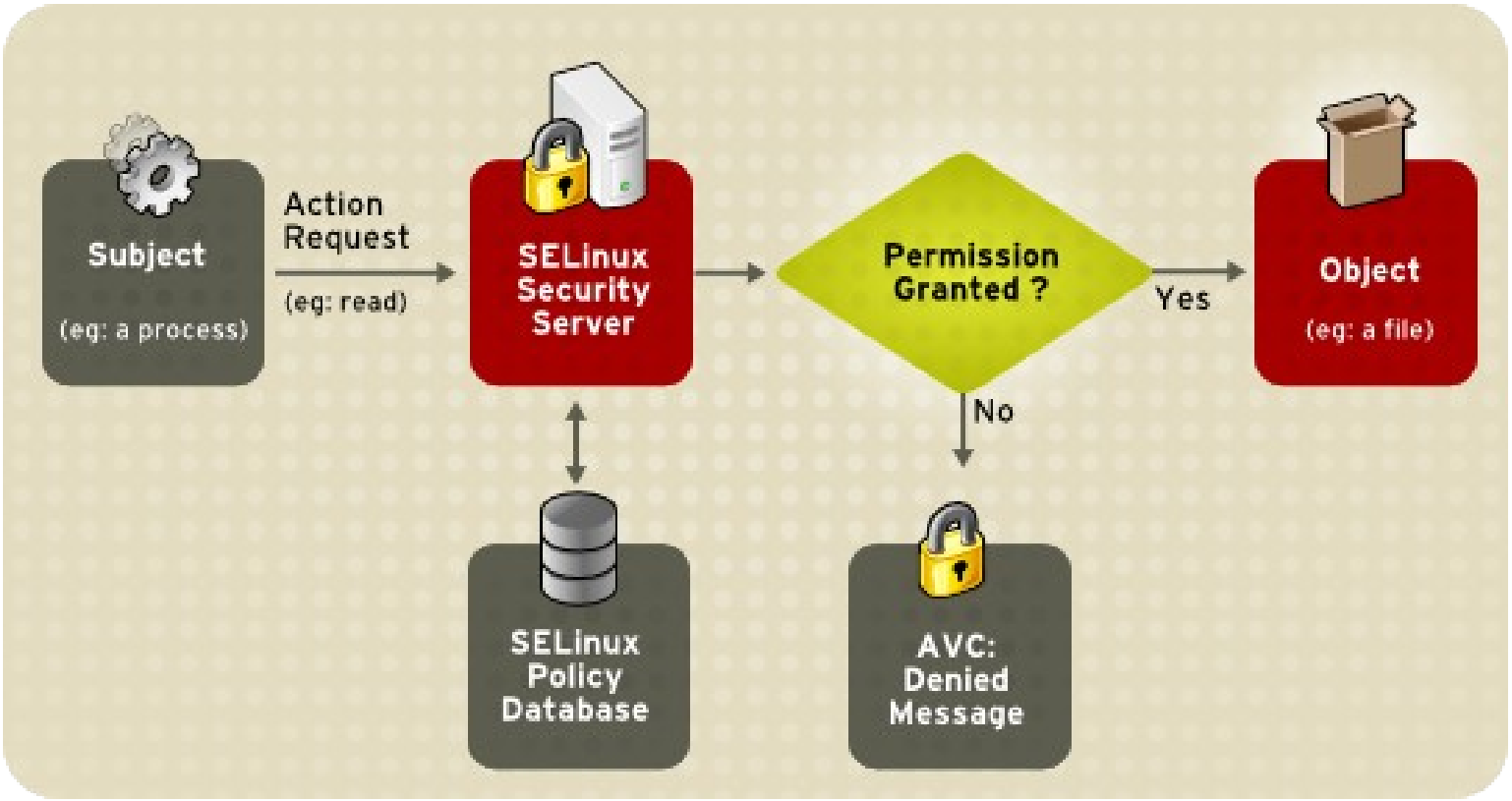
- Der SELinux-Kernel
  - Patch ist upstream
  - benutzt Linux-Security-Modules (LSM)
  - besteht aus dem Security-Server und der Policy
  - Enforcement und Regelwerk sind also getrennt
  - Sourcen: $KERNELSRC/security/selinux/

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...

SELinux Architektur



Permissive vs. Enforcing

SELinux kann in 3 verschiedenen Modi laufen

- Permissive mode
  - Policy geladen
  - Auditing enabled
  - Kein denial, nur logging
  - Nützlich zum Policy schreiben und Troubleshooting
- Enforcing mode
  - Policy geladen
  - Auditing enabled
  - Action denial oder grant abhängig von der Policy
- Disabled

Only enforcing mode provides more security

Anpassung des SELinux Systems

- 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

- 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 – Wher e 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 Dokumention und aktive Mailinglisten
- LSPP Zertifizierung nach Common Criteria
- Red Hat bietet als erster Distributor Enterprise-Level Support

Questions?

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

Vielen Dank!

Joachim Schröder, Solution Architect
joachim.schroeder@redhat.com