

Security Enhanced Linux (SELinux)

Workshop/BOF auf dem LinuxTag 2003
in Karlsruhe

Carsten Grohmann <mail@carstengrohmann.de>

11. Juli 2003

Agenda

I. Kleine SELinux-Kunde

- Erweiterung für Linux
- feinere Zugriffssteuerung
- Programme laufen in Domänen

II. Vorführung eines SELinux-Systems

Begriffe

- Security Context (Benutzer:Rolle:Typ/Domäne)
- SID/PSID
- TE Type Enforcement
- RBAC Role Based Access Control
- MAC Mandatory Access Control
- DAC Discretionary Access Control
- Typen / Domänen und Rollen
- Objekt/Subjekt

Elemente

- RBAC (role based access control)
- Security Context (Benutzer:Rolle:Typ/Domäne)
- Jedes Objekt und jedes Subjekt hat einen Security Context
- Berechtigungen abhängig von
 - Autorisierten Rollen
 - Domänen in der Rolle
 - Wechsel zwischen zwei Rollen oder zwei Typen
- Erzwingen der Berechtigungen

Funktionsweise

- Regelbasiertes System mit TE, RBAC und MAC
- Alle Prozesse laufen in eigenen Domänen
- Policy autorisiert:
- Wechsel zwischen Typen (Domänen)
- Zugriff auf alle Typen (auch die eigenen)
- Wechsel nur bei Start eines Programms möglich
- Berechtigungen sind parallel zu Linux

Betriebsmodi

- Permissive Mode
 - Gewährung aller Zugriffe
 - Protokollierung aller Verstöße
- Enforcing Mode
 - Policy erlaubt und verweigert Zugriffe
 - Protokollierung aller Verstöße

Installation

- Aus den Quellen der NSA(Red Hat 9.0) basiert
- Alternativ Pakete für
 - Debian
 - SuSE

Neue Befehle

- `avc_enforcing` aktueller Modus von SELinux
- `avc_toggle` Wechsel in den anderen Modus
- `newrules.pl` `log2rule`
- `newrole` Wechsel in eine andere Rolle
- `Wrapper` sichereren Zugriff auf Systemressourcen
 - z.B. `schfn`, `spasswd`, `schsh` und andere

Vorteile

- Feinere Zugriffsrechte
- Besserer Schutz vor „bösen“ Code
- Allmacht root gebrochen
 - dennoch Henne-Ei-Problem, da ein Admin Regeln ändern kann
- Kein chroot() mehr notwendig

Nachteile

- Höherer Verwaltungsaufwand durch die Policy
- Regeln pro Programmpaket
- Tiefere Systemkenntnisse notwendig
- Erhöhter Installationsaufwand bei Nicht-RH-Distributionen (Ausnahme Debian)
 - Teilweise Probleme beim Patchen / Anpassen der Systemprogramme

Resümee

- Mehr Sicherheit mit vertretbarem Aufwand
- Leicht zu administrieren
- Hürden bei der Installation

Quellen

- <http://www.nsa.gov/selinux/index.html>
- <http://www.securityenhancedlinux.de>
- <http://sourceforge.net/projects/selinux/>