Rule Set Based Access Control (RSBAC) for Linux

Freie Sicherheitserweiterung für den Linux-Kern

Amon Ott <ao@rsbac.org>

Inhalt:

Inhalt II:

Inhalt III:

Inhalt IV:

1 Einführung

1.1 Motivation
1.2 Überblick RSBAC

1.1 Einführung: Motivation

- Klassische Zugriffskontrolle unter Linux/Unix ist unsicher
  - Geringe Granularität
  - Diskrete Kontrolle
    - Vertrauenswürdiger Benutzer?
    - Malware: Einladung für Trojaner und Viren
  - Superuser root
    - Voller Zugriff
    - Zu oft benötigt
    - Zu viele erfolgreiche Angriffe (root kits, kernel module attacks etc.)
- Bessere Modelle für andere Administrationsziele
- Flexible Modellauswahl und -kombination
- Gute Portierbarkeit.

1.2 Einführung: Überblick

- Open Source mit GPL
- Flexible Struktur
  - Trennung zwischen Durchsetzung (AEF), Entscheidung (ADF) und Datenhaltung (ACI)
  - Nur AEF und Teil der Datenhaltung systemabhängig
  - Praktisch jede Art von Sicherheitsmodell implementierbar
  - Modellunabhängig durch eine Meta Policy
  - Runtime Module Registration (REG)
- Leistungsfähiges Logging-System
  - Default-Matrix: Anfragetyp, Entscheidung und Zieltyp
  - Individuell: Benutzer, Programm und Ziel-Objekt.

1.4 Einführung: Überblick II

- Stabiler Produktionsbetrieb seit März 2000
- Unterstützt aktuelle Linuxkerne
- Downloads und Feedback wachsen stetig
- Neue Adamantix-Linuxdistribution mit RSBAC
- Aktuelle stabile Version 1.2.2 für Kernels 2.2.25 und 2.4.21-25
- Vorversion 1.2.3-pre4 für Kernels 2.4.24-25 und 2.6.3-4.

2 Aufbau des Rahmenwerks

2.1 Subjekte, Objekte und Entscheidungsanfragen
2.2 Architektur-Diagramm

2.1 Rahmenwerk: Subjekte

- Subjekte: Prozesse, die
  - im Namen von Benutzern agieren,
  - dabei jeweils ein Programm ausführen
  - und eine Anzahl dynamischer Bibliotheken eingebunden haben.

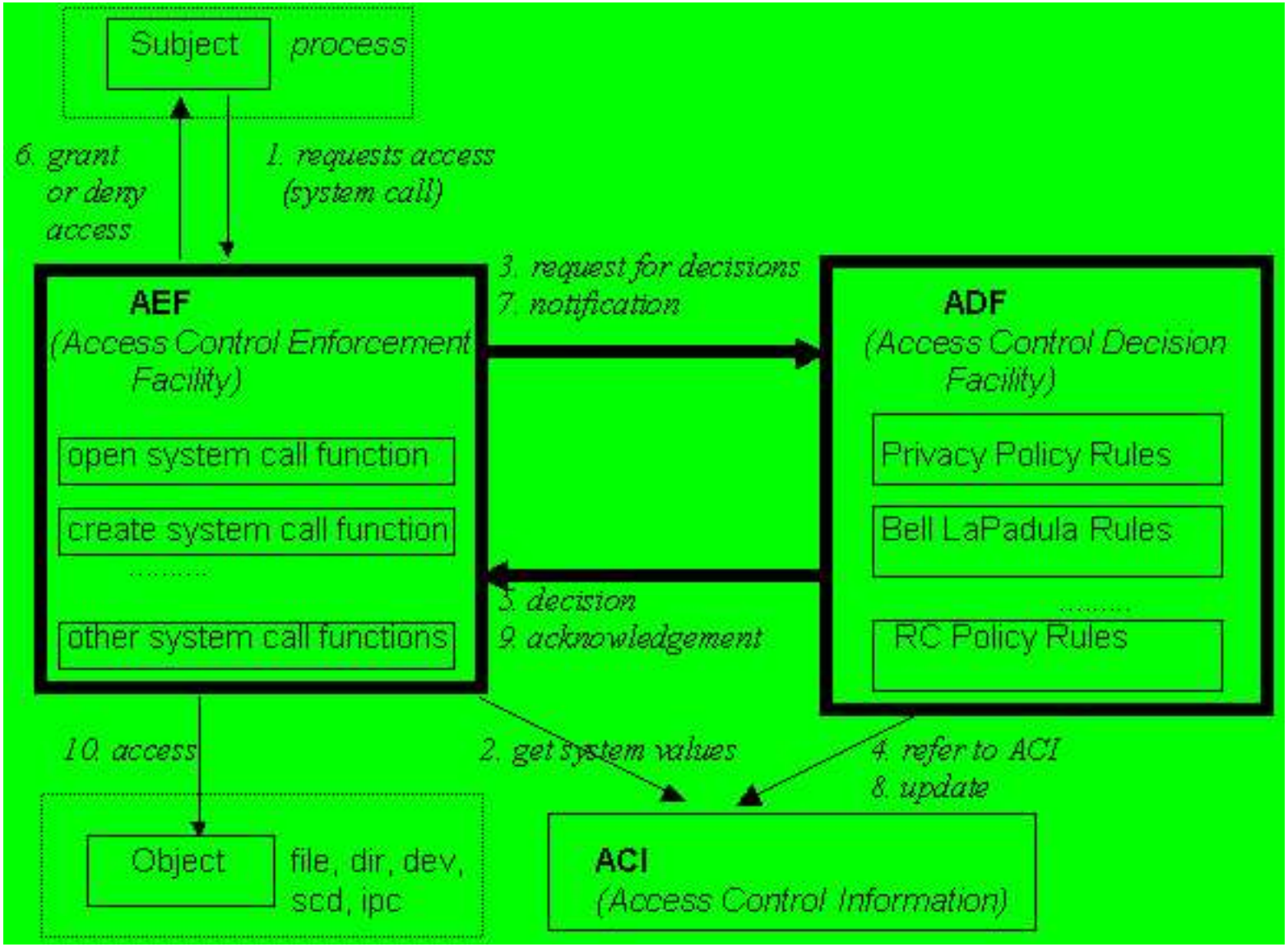
2.1 Rahmenwerk: Objekte

- Objekttypen (Zieltypen, target types):
  - FILE
  - DIR
  - FIFO
  - SYMLINK
  - DEV (Devices nach block/char und major:minor)
  - IPC (Inter Process Communication = Prozesskommunikation)
  - SCD (System Control Data = systemweite Konfigurationsdaten)
  - USER
  - PROCESS
  - NETDEV (Network Devices)
  - NETTEMP (Network Object Templates)
  - NETOBJ (Network Objects (Sockets etc.)).

2.1 Rahmenwerk: Entscheidungsanfragen

- Anfragetyp (request type):
  - Abstraktion dessen, wie ein Subjekt auf ein Objekt zugreifen möchte
- Entscheidungsanfrage (decision request):
  - Konkrete Anfrage an die Entscheidungskomponente.

2.2 Architektur-Diagramm



3 Implementierte Entscheidungsmodule

3.1 AUTH
3.2 RC
3.3 ACL
3.4 FF
3.5 CAP
3.6 JAIL
3.7 RES
3.8 PAX

3.1 Modelle: AUTH

- Authentication (AUTH):
  - Beschränkt CHANGE_OWNER mit Zieltyp PROCESS (setuid)
  - Optional: Beschränkung von CHANGE_DAC_{EFF|FS}_OWNER (seteuid/setfsuid)
  - Setuid capabilities (von der Programmdatei zum Prozess vererbt): Mengen erreichbarer Benutzer-IDs
  - auth_may_setuid und auth_may_set_cap
  - Kann Daemon-basierte Authentisierung erzwingen:
    - Prozess authentisiert gegen Daemon
    - Daemons setzt capability für authentisierten Benutzer am Prozess
    - Prozess setzt Benutzer-ID.

3.1 Modelle: AUTH II

- Beschränkte Lebenszeit für alle AUTH Capability-Einstellungen
- Neu in 1.2.3-pre: Learning Mode setzt benötigte Werte selber.

3.2 Modelle: RC

- Role Compatibility (RC):
  - Benutzer-Standard- und aktuelle Prozess-Rollen
  - Objekttypen (getrennt nach Zieltyp: FD, PROCESS, etc.)
  - Kompatibilität von Rollen mit Objekttypen nach Anfragetyp (Objektzugriffe)
  - Kompatibilität von Rollen mit anderen Rollen (aktuelle Rolle wechseln)
  - Erzwungene und Initial-Rollen für Programmdateien.

3.2 Modelle: RC II

- Trennung der Administrationsaufgaben
  - Admin Roles
  - Assign Roles
  - Zusätzliche Zugriffsrechte auf Typen: Admin, Assign, Access Control, Supervisor
- Beschränkte Lebenszeit der Kompatibilitäts-Einstellungen.

3.3 Modelle: ACL

- Access Control Lists (ACL)
  - Welches Subjekt darf auf welches Objekt wie zugreifen
  - Subjekte:
    - RC-Rollen (!)
    - Benutzer
    - ACL-Gruppen
  - ACL-Gruppen:
    - Jeder Benutzer kann individuelle Gruppen verwalten
    - Private und globale Gruppen
  - Vererbung der Rechte am übergeordneten Objekt, beschränkt durch Maske am Objekt
  - Default-ACLs als oberster Vererbungsanker.

3.3 Modelle: ACL II

- Administrationsrechte:
  - Access Control
  - Forward
  - Supervisor
- Beschränkte Lebenszeit für ACL- Einträge und Gruppenmitgliedschaften
- Neu in 1.2.3-pre: ACL Learning Mode setzt benötigte Dateisystem-ACLs für alle Benutzer automatisch.

3.5 Modelle: FF

- File Flags (FF):
  - Vererbbare Attribute für Dateisystemobjekte (FILE, DIR, FIFO und SYMLINK)
  - Z.B. read-only, no-execute, secure-delete, no-mount.

3.5 Modelle: CAP

- Linux Capabilities:
  - Minimale und maximale Linux Capability Sets für Benutzer und Programme
  - Anwendung beim CHANGE_OWNER auf Prozesse (setuid) und EXECUTE
  - Vorrang von Minimum vor Maximum
  - Vorrang der Programmattribute vor den Benutzerattributen
  - Normale Benutzer mächtiger machen oder Rechte von root-Programmen beschränken
  - Nur Verwaltung vorhandener Linux-Rechte.

3.6 Modelle: JAIL

- Process Jails:
  - Prozesse in verstärkten chroot-Käfigen einsperren
  - Vorkonfektionierte Kapselung von Serverprozessen
  - Viele weitere Beschränkungen, einige optional
  - Besonders Administrationszugriffe und Netzwerknutzung stark eingeschränkt.

3.7 Modelle: RES

- Linux Resources:
  - Minimale und maximale Resourcen-Schranken für Benutzer und Programme
  - Anwendung bei CHANGE_OWNER auf Prozesse (setuid) und EXECUTE
  - Vorrang von Minimum vor Maximum
  - Vorrang der Programmattribute vor den Benutzerattributen
  - Nur Verwaltung vorhandener Linux-Prozess-Attribute:
  - Maximale Dateigröße, Anzahl Prozesse, Hauptspeicher je Prozess, ...

3.8 Modelle: PAX

- PageExec:
  - Verwaltung der Prozess-Attribute der separaten PaX-Kernerweiterung
  - PaX schützt vor gängigen Angriffsmethoden auf fehlerhafte Programme
  - Schutz speziell vor eingeschleustem Programm-Code, z.B. per Buffer Overflow
  - Mehr Info: pax.grsecurity.net.

4 Installation unter Linux

4.1 Linux-Kern
4.2 Administrations-Programme
4.3 Der erste Start

4 Installation unter Linux

- Linux-Kern
  - Tar-Archiv im Kernquellenverzeichnis auspacken
  - Kern patchen (mit patch-x.y.z.gz)
  - Alternative: Download vorgepatchter Kernquellen
  - make menuconfig, touch Makefile, kompilieren und installieren
  - Normaler oder Maintenance-RSBAC-Kern
  - Softmode zum Testen
- Administrationprogramme
  - Tar-Archiv auspacken
  - ./configure && make && make install.

4 Installation unter Linux II

- Der erste Start
  - Kern-Parameter rsbac_auth_enable_login
  - Benutzer 400 anlegen (Security Officer etc.)
  - AUTH capabilities für Daemons setzen

  - Alternativ (ab v1.2.3-pre): AUTH Learning Mode benutzen.

5 Administration

5.1 Attribute
5.2 Kommandozeilen-Programme
5.3 Menüs

5.1+2 Administration: Attribute und Kommandozeilenprogramme

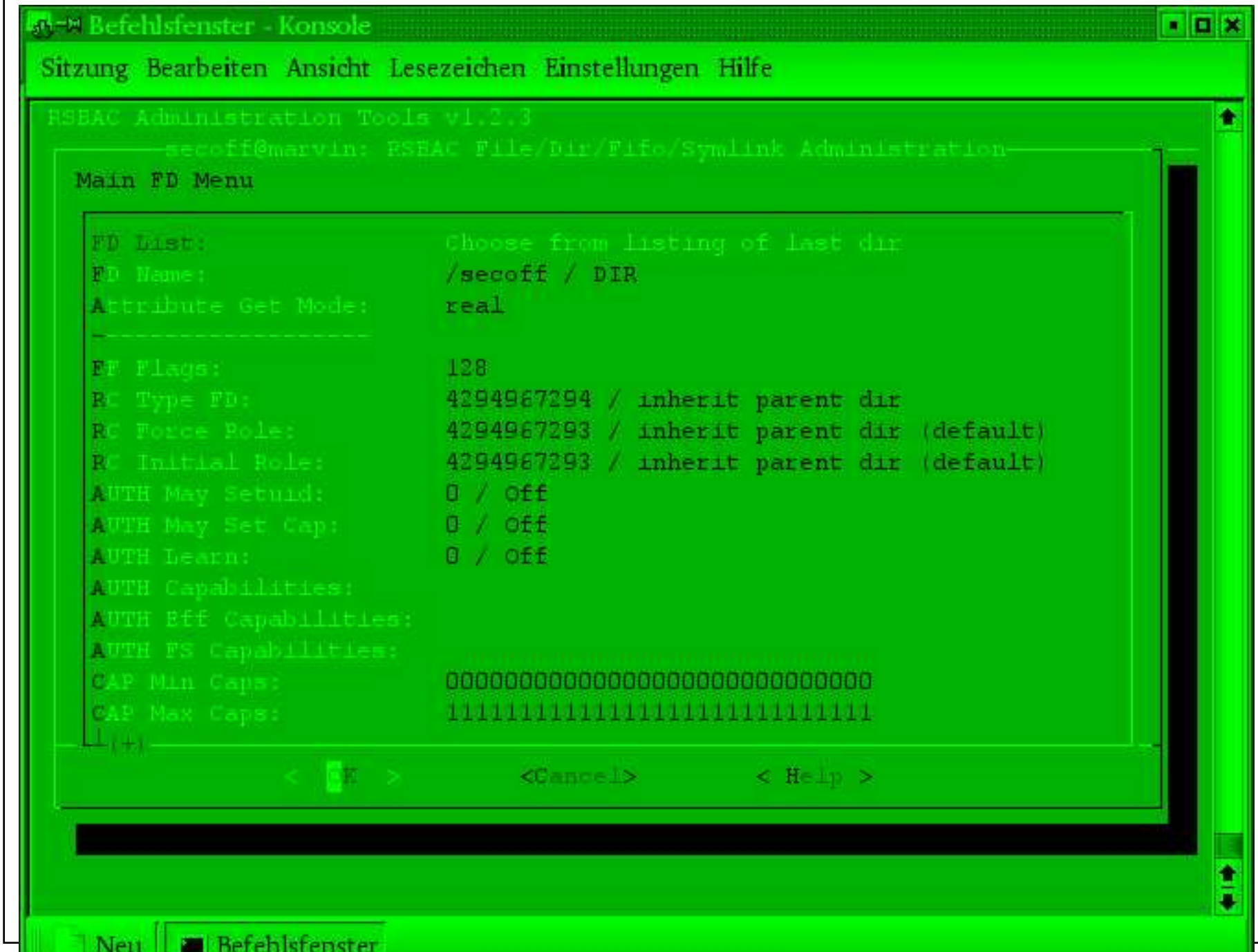
- Generelle und modell-spezifische Attribute

Befehlsfenster - Konsole

Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

```
acl_grant (RSBAC 1.2.3-pre4)
***
Use: acl_grant [switches] subj_type subj_id [rights] target-type file/dirname(s)
  -v = verbose, -r = recurse into subdirs,
  -p = print right names, -s = set rights, not add
  -k = revoke rights, not add, -m remove entry (set back to inherit)
  -b = expect rights as bitstring, -n = list valid SCD names
  -u, -g, -l = shortcuts for USER, GROUP and ROLE
  -t = set relative time-to-live for this trustee in seconds (add and set only)
  -T = set absolute time-to-live for this trustee in seconds (add and set only)
  -D = set relative time-to-live for this trustee in days (add and set only)
  -V version = supply RSBAC integer version number for upgrading
  subj_type = USER, GROUP or ROLE,
  subj_id = user name or id number,
  rights = list of space-separated right names (requests and ACL specials),
         also request groups R (read requests), RW (read-write), W (write)
         SY (system), SE (security), A (all)
         S (ACL special rights)
         and NWx with x = S R W C E A F M (similar to well-known network system)
  target-type = FILE, DIR, FIFO, SYMLINK, DEV, IPC, SCD, USER, PROCESS, NETDEV,
                NETTEMP_NT, NETTEMP, NETOBJ or FD
  (FD: let acl_grant decide between FILE, DIR, FIFO and SYMLINK, no DEV),
```

5.3 Administration: Menüs



6 Typische Serveranwendungen

- Grundschutz des Basissystems
- Kapselung von Diensten
- Firewalls
  - DNS, Proxies, etc.
  - Besonderer Grundschutz wegen hoher Angriffswahrscheinlichkeit
- (Virtual) Webserver
  - Apache, Zope etc.
  - Trennung der virtuellen Domänen
  - Schutz kritischer Daten
  - Kapselung der CGIs.

6 Typische Serveranwendungen II

- (Virtuelle) Mailserver
  - postfix, qmail, POP3, IMAP, Mailing Lists etc.
  - Trennung der Mailbereiche
- Fileserver
  - Samba, Coda, FTP, etc.
  - Trennung der organisatorischen Einheiten
- Applikationsserver
  - Trennung der Benutzerbereiche
  - Schutz gegen lokale Angriffe
  - Schutz vor Netzwerkangriffen durch lokale Benutzer
- Andere Server.

7 Praktische Erfahrungen

7.1 Laufende Systeme

7.2 Stabilität

7.3 Performanz

7.1 Praktische Erfahrungen: Laufende Systeme

- Linux-Distribution Adamantix mit RSBAC
- m-privacy Diva-Pro
  - Sehr umfangreiche Nutzung von RSBAC
  - Server-System zur sicheren Internetnutzung
  - Starke Kapselung aller Netzwerk-Dienste und Benutzer
  - Benutzt fast alle genannten Modelle
- Viele Test- und Produktionssysteme anderer Administratoren.

7.2 Praktische Erfahrungen: Stabilität

- Vier Jahre sehr hoher Stabilität
- SMP-Systeme mehr als drei Jahre mit hoher Stabilität.

7.3 Erfahrung: Performanz

- Einflußfaktoren für die Performanz
  - Anzahl und dynamisches Verhalten der Attributobjekte
  - Art und Anzahl der Entscheidungsmodule
  - Logging

- Benchmarks
  - Celeron 333 system, 2.4.19 kernel, RSBAC 1.2.1
  - Mittelwerte dreier Linux-Kern-Kompilierungsläufe
  - Laufzeit mit leerem Rahmenwerk: +0.68% (Kern +11.33%)
  - Laufzeit mit RC, AUTH, Netzwerk, alle Logging-Optionen: +2.30% (Kern +43.02%)
  - Laufzeit mit REG, FF, RC, AUTH, ACL, CAP, JAIL, Netzwerk, alle Logging-Optionen (def. config): +4.21% (Kern +82.47%).

8 Weitere Informationen

- RSBAC Homepage: http://www.rsbac.org
- Mailing-Liste
  - Requests: rsbac-request@rsbac.org
  - Mails: rsbac@rsbac.org
  - Archiv verfügbar (siehe rsbac.org/contact.htm)
- IRC Channel: irc://irc.debian.org/rsbac
- RSBAC-Artikel: iX 8/2002, Linux-Magazin Nr. 1 und 4/2003, Linux-Magazin Sonderheft 1/2004
- Adamantix: www.adamantix.org
- PaX: pax.grsecurity.net

9 Ausblick

- Intensivere Entwicklung in den nächsten Jahren
- Listenreplikation auf andere RSBAC-Systeme
- Später: Verteiltes RSBAC-System / RSBAC Cluster
- ??? - Anregungen werden gerne angenommen

10 Cebit-Kontakt

- 18.-21.03.: Gemeinsamer Stand von RSBAC und Adamantix in der OpenBooth, Halle 6, C52 / 565
- Gesamte Cebit: m-privacy-Stand, Halle 6, F10/1
- Ich freue mich auf gute Gespräche!

Rule Set Based Access Control

Freie Sicherheitserweiterung für den Linux-Kern

Amon Ott <ao@rsbac.org>

Danke für Ihre Aufmerksamkeit!