Security Enhanced Linux

Eine Einführung

Tom Vogt
<tom@lemuria.org>

Carsten Grohmann
<mail@carstengrohmann.de>

Überblick

Was ist SELinux?

- Erweiterung des Kernels

Was bietet SELinux?

- Kapslung von Programmen untereinander und vom System
- Regelung aller Zugriffe über eine Policy
- Root hat keine Allmacht mehr
- Gleichbleibende Benutzeridentität

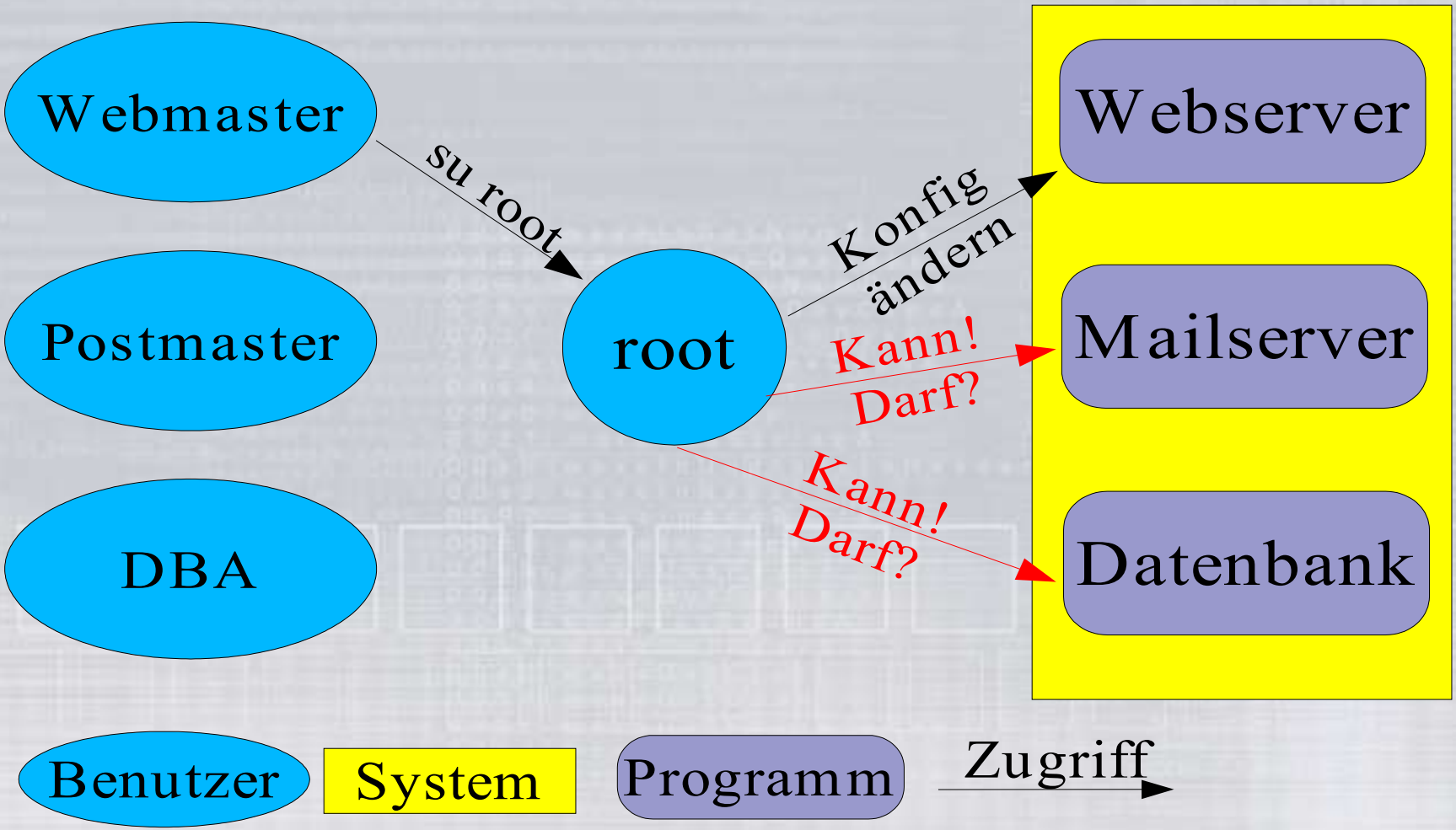
Überblick

SELinux intern:

- Erweiterung des Kernels mit
  - TE: Type Enforcement
  - MAC: Mandatory Access Controls
  - RBAC: Role-Base Access Control
- Transparent für die meisten Programme
- Orthogonal zu Unix Zugriffsrechten

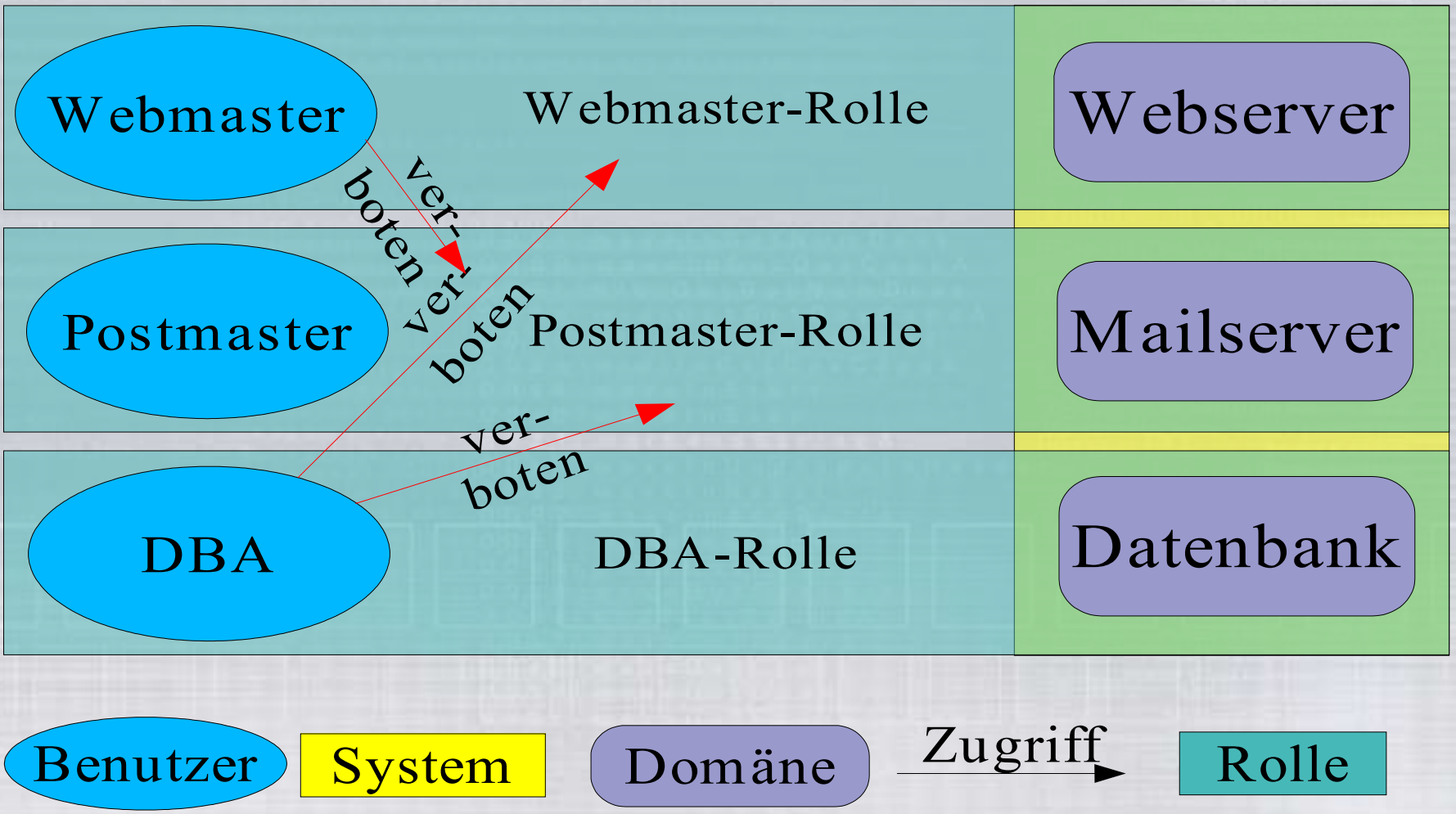
Überblick

Ohne SELinux



Überblick

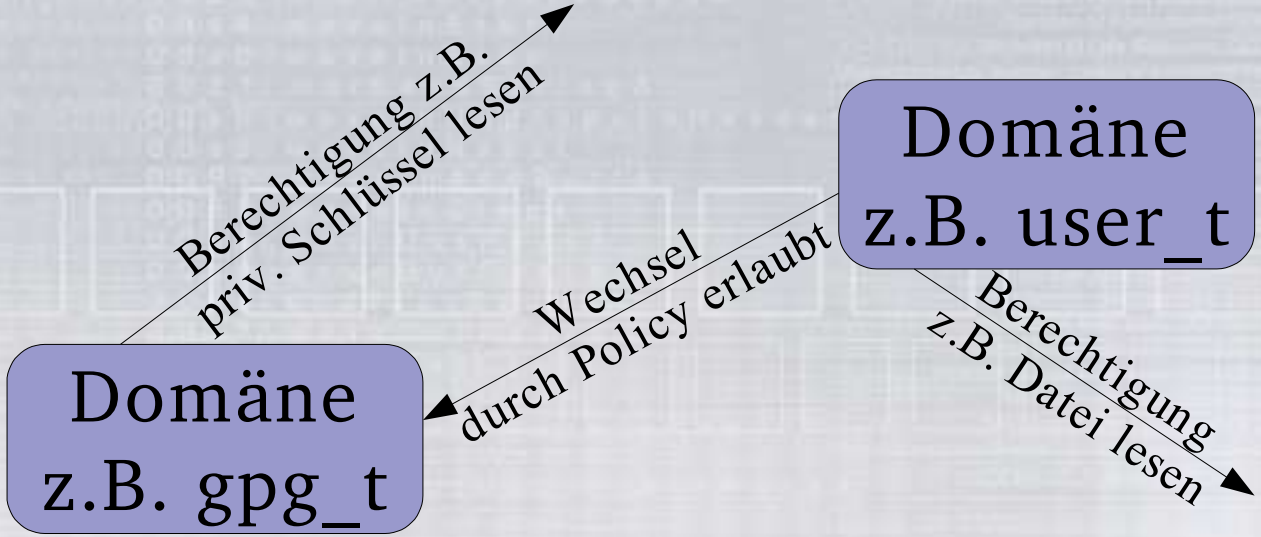
Mit SELinux



Hintergrund

Domäne

- „Raum“ in dem ein Prozeß läuft
- Zugriffsberechtigungen werden der Domäne zugeordnet
- Wechsel zwischen Domänen regelt die Policy



Hintergrund

Typ

- Menge von Objekten (Dateien, Verzeichnissen, Sockets...) und Subjekten (Prozessen) mit gleichen Rechten
- Domänen sind Typen, die an Prozesse gebunden sind
- Unterscheidung zwischen Domäne und Typ nur sprachlicher Natur, keine internen Unterschiede
- Policy definiert Typenwechsel

Hintergrund

Typenwechsel

- Policy legt zulässige Typenwechsel fest
- ... und definiert automatische Typen-wechsel

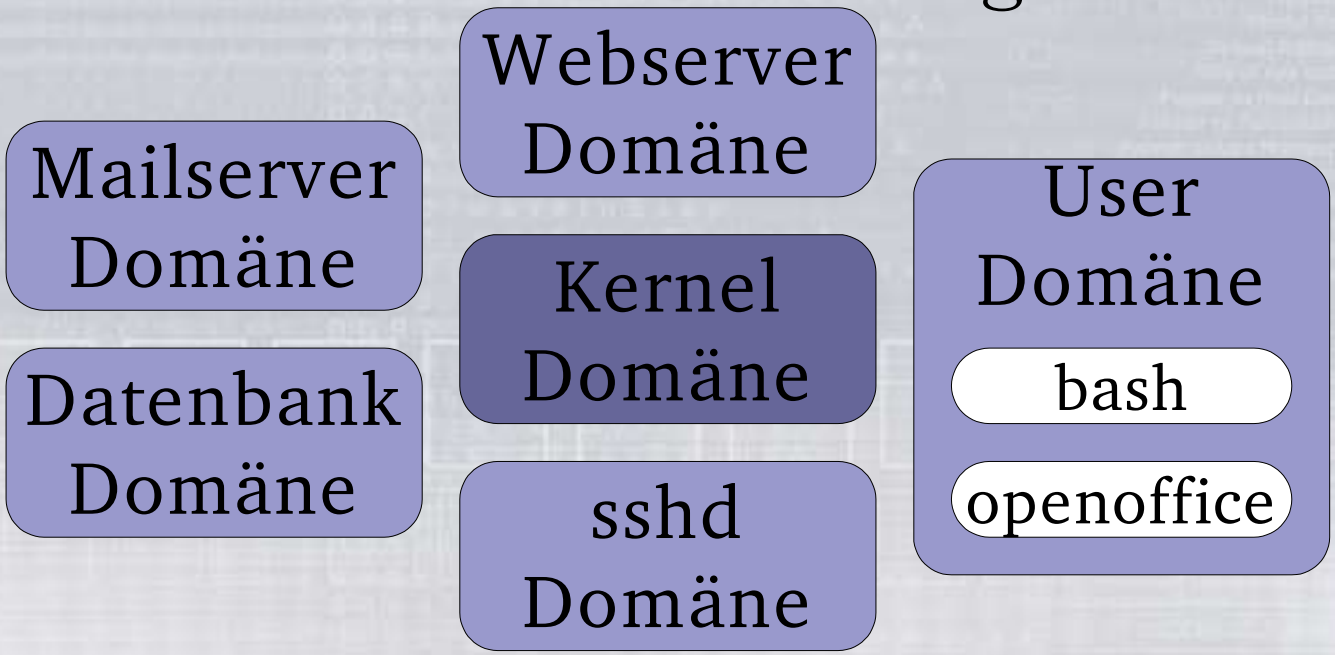
Einschränkungen für Domänen

- Nur erlaubt bei exec Aufrufen
- Also keine Domänenwechsel zur Laufzeit eines Programmes
- ...oder wenn externer Code als Modul ausgeführt wird.

Hintergrund

Type Enforcement

- Starke Trennung zwischen Betriebssystem und Programmen
- Sowie zwischen einzelnen Programmen



Hintergrund

Mandatory Access Control

- Standard Unix: Discretionary Access Control (DAC)
- DAC: Besitzer von Objekten bestimmen die Zugriffsrechte
- MAC: Policy und Labels bestimmen die Zugriffsrechte
  - Policy legt fest, wer Labels setzen und verändern kann
  - und welche Voreinstellungen gelten

Hintergrund

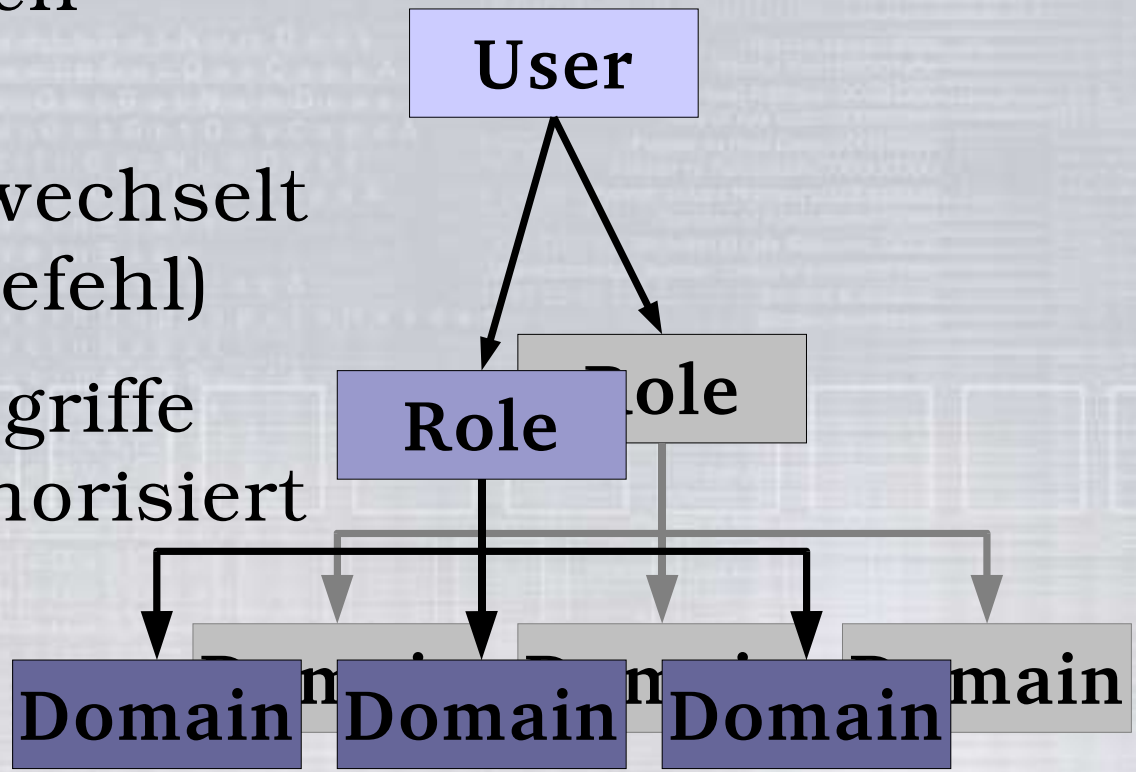
Role-Based Access Control

- Die Rolle dient der Abstraktion bei der Zuordnung von Zugriffsrechten an Benutzer
- Rollen können gut definiert und eingegrenzt werden
- Benutzer können zwischen Rollen wechseln
- Die Policy legt dabei fest, welche Rollen für welche Benutzer zugänglich sind

Grundlagen

Benutzer, Rollen, Domänen

- Benutzer sind für eine oder mehrere Rollen authorisiert
- Rollen können gewechselt werden (newrole Befehl)
- Rollen sind für Zugriffe auf Domänen authorisiert



Sicherheitsvorteile

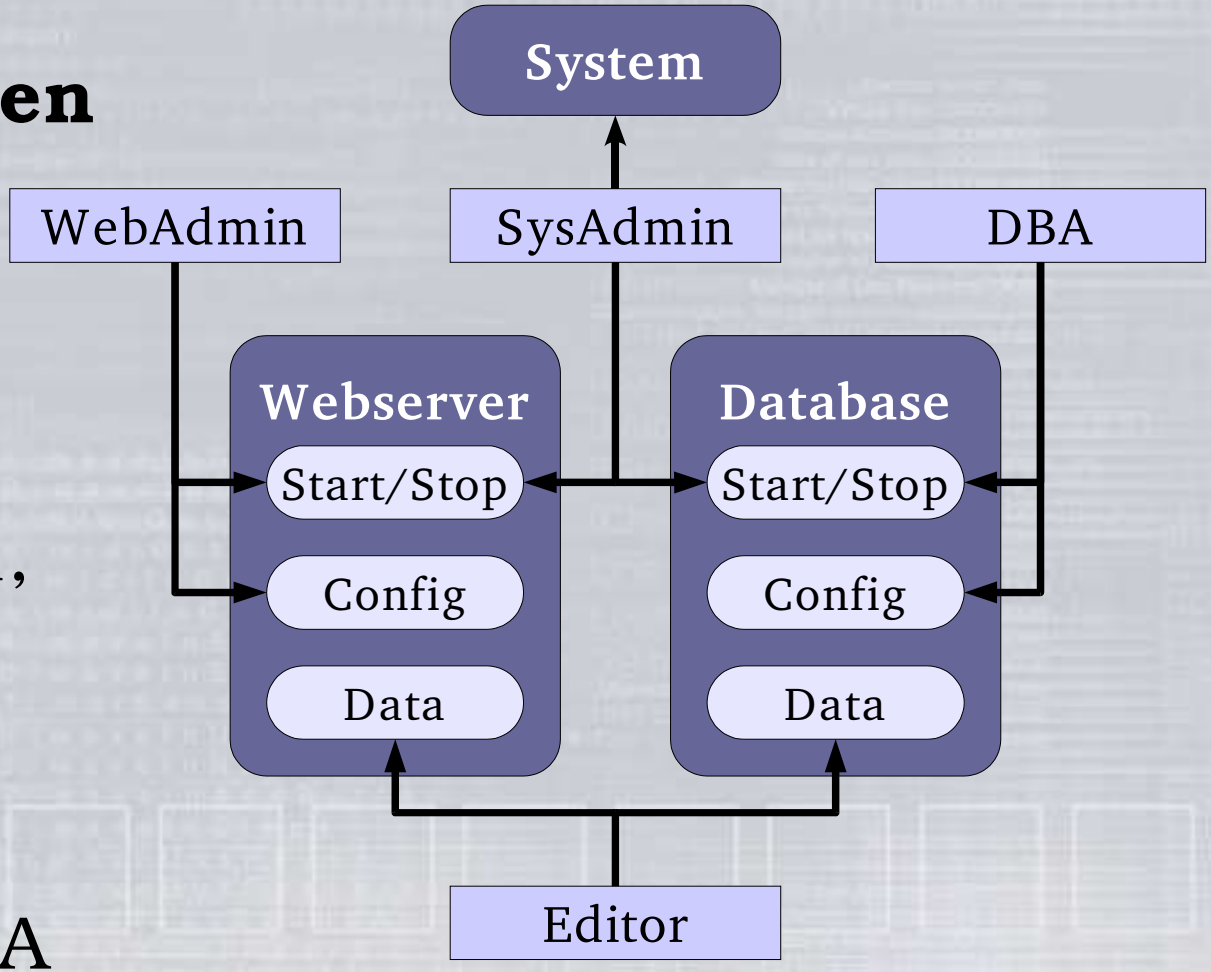
Rollen und Domänen:

- Domänen können vollständig voneinander getrennt werden
- Sicherheitsvorfälle bleiben auf die betroffenen Domänen beschränkt
- …auch wenn der Angreifer root-Zugang erreicht hat
- Unbekannte und fragwürdige Programme können in „Quarantäne“ gestellt werden

Sicherheitsvorteile

Beispiel für Rollen

- Vier Rollen
- Trennung von Aufgaben
- Überlappungen, wo notwendig
- Hinweis: durch Rollenwechsel können der DBA und der WebAdmin die gleiche Person sein



Sicherheitsvorteile

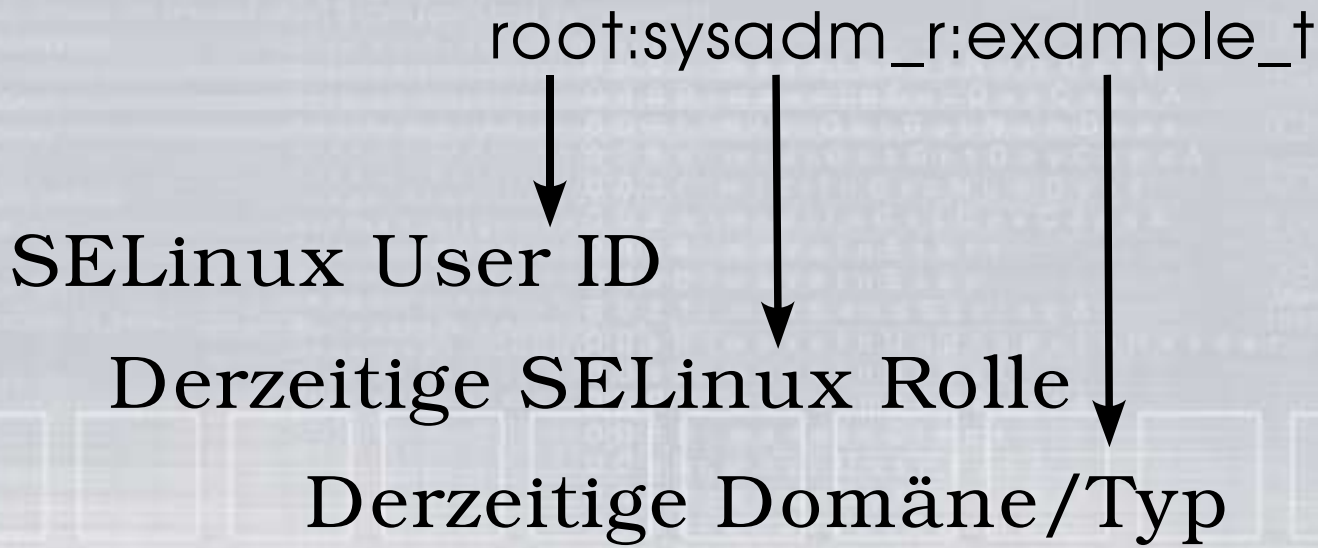
Policy und ihre Durchsetzung:

- Sehr feine Zugriffskontrollen (syscalls)
- Selbst kleinste Verletzungen können festgestellt werden
- „Management by policy“
- Minimierung des Schadens, der durch Fehler und Unwissenheit entsteht
- Zwingt Benutzer, die Policy einzuhalten

Arbeiten mit SELinux

Security Contexts

- Abbildung der SELinux-Benuterinformation als Zeichenkette



Die Policy

- Verwendet eine einfache deklarative Sprache
- M4 Makros
- Einfache dateibasierte Struktur
- GUI Programme sind verfügbar
- Eine Default Policy wird mitgeliefert

Implementierung

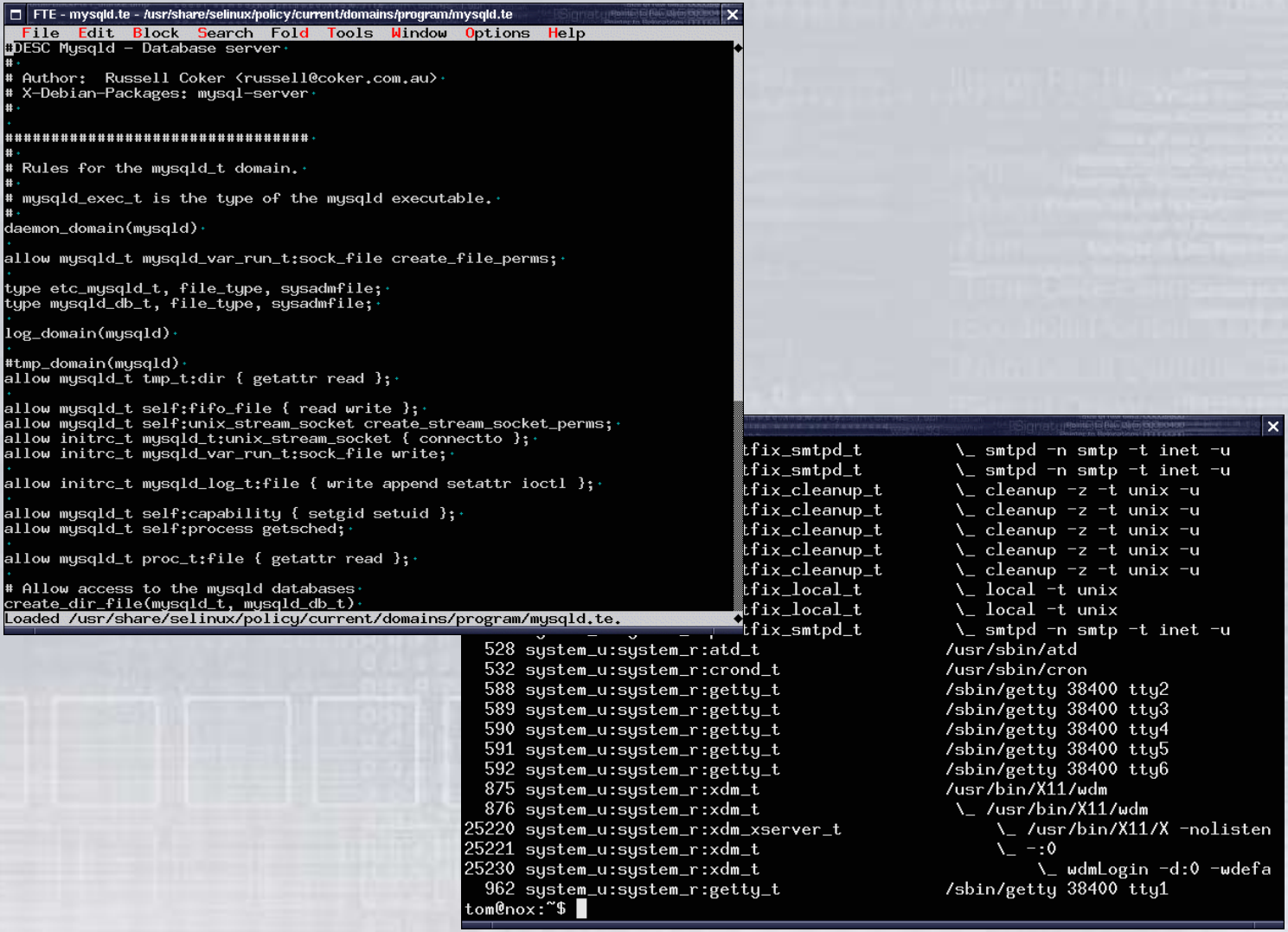
Die Implementierung

- Im 2.6-er Kernel standardmäßig enthalten
- Einige Patches für Programme
- Zentrale Policy mit Verwaltungsprogrammen
- Dateisystem mit Security Context Labeln versehen (in ext2/ext3/xfs xattr gespeichert)
- Prozesse sind ebenfalls mit Security Contexts versehen

Aktueller Status

- Bestandteil des 2.6-er Kernels
- Pakete für alle großen Distributionen verfügbar
- Sehr aktive Weiterentwicklung
- Gentoo Live-CD

Demonstration



Links

- http://www.nsa.gov/selinux/
- http://sourceforge.net/projects/selinux/
- http://www.securityenhancedlinux.de
- http://selinux.lemuria.org

Security Enhanced Linux

Vielen Dank

Fragen ?