

SELinux – kort intro

Lars Strand
18. oktober 2007

STORM



FEIL!

(Men MEST på Windows)

- Problem: Sårbarhet i applikasjoner.
 - (Vellykkede) angrep.
 - Bugs. Mye dårlig skrevet programvare!
- Konfigurasjonsfeil (oftere enn du tror).
- Begrense skadeomfanget/handlingsrommet til angriper!
- Hvordan?

SELinux!

Men først: Litt teori:

Subjektet avgjør/bestemmer aksess til sine objekter.

Eks: En bruker kan selv bestemme hvem som kan aksessere hans filer.

Ofte kalt: “Discretionary access control” (DAC):

“If an **individual user** can set an access control mechanism to allow or deny access to an object, that mechanism is a *discretionary access control* (DAC), also called *identity-based access control* (IBAC).”

-- M. Bishop, computer security (2003).

Når systemet (sentralt) bestemmer aksesskontroll, som subjektet (brukeren) ikke selv kan overstyre.

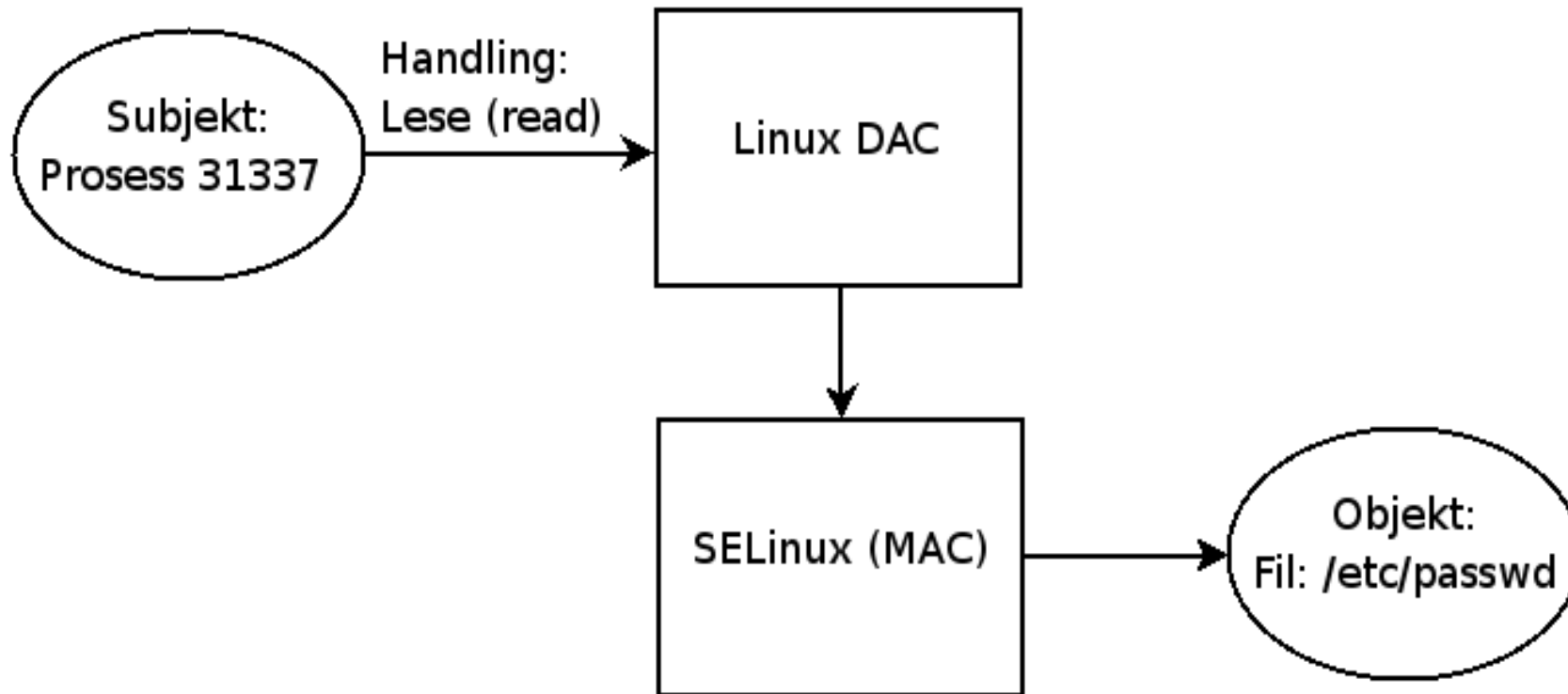
Dvs: Brukeren ikke lengre (full) kontroll over sine filer/prosesser.

Systemet (OS) agjøre og håndhever sikkerhetspolicy.

“When a **system mechanism controls access** to and an individual user cannot alter that access, that control is a *mandatory access control* (MAC), occasionally called a *rule-based access control*.”

-- M. Bishop, computer security (2003).

- Eks: Prosess 31337 lov å lese /etc/passwd?

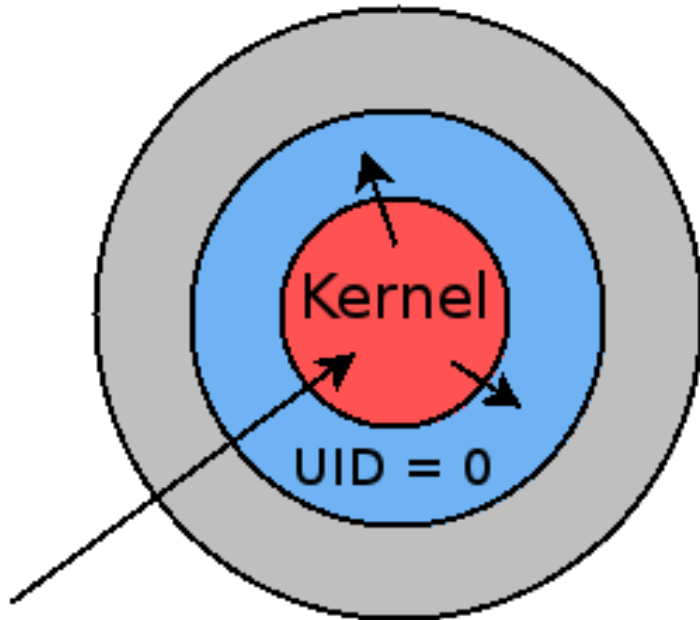


- Nøkkelegenskap = supplerer tradisjonell DAC med MAC:

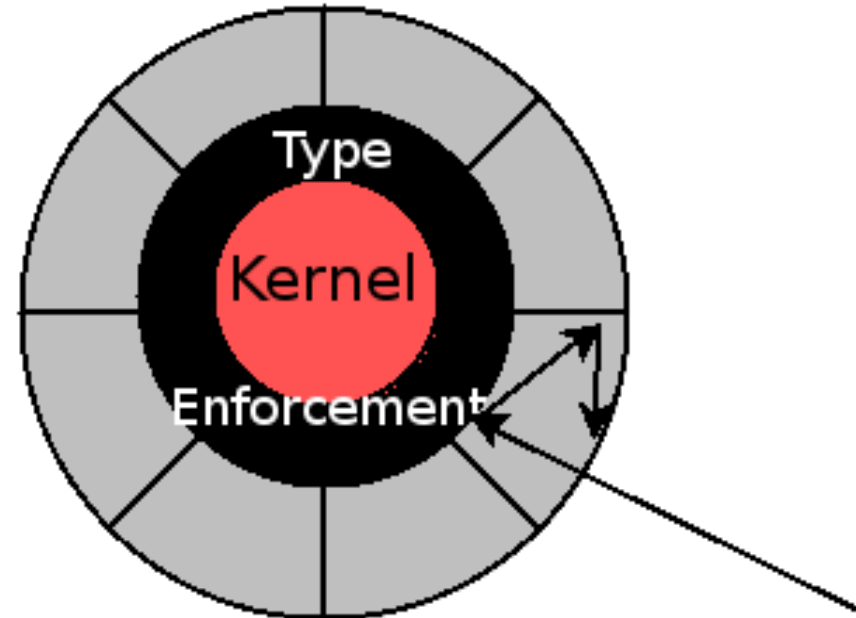
- *Security-Enhanced Linux* = SELinux.
- Opprinnlig utviklet av NSA.
- NSA overrasket alle ved å gjøre SELinux fri programvare.
- I det offisielle kjernetreet fra 2.6.
- Benytter “Linux Security Modules” (LSM).
- I dag: Fedora og Redhat.
- Runner-up: Debian, Gentoo, (Ubuntu).

1. Kernel – en del av standard kjernetreet.
2. SELinux bibliotek 'libselinux' (ls, ps, id, ..)
3. SELinux administrasjonsverktøy
4. Policy

- SELinux introducerer MAC vha:
 - SELinux user identities.
 - Role Based Access Control (RBAC)
 - **Type Enforcement (TE)**



Klassisk aksesskontroll.
UID 0 har full aksess.



Domain/Type aksesskontroll
Grupper med sandkasser.

- Subjekt og objekter grupperes i ulike klasser.
- Eks: Alt som har med apache i en “klasse”/”gruppe”.
- Konstrueres vha. “security attributes”.
- Fire attributter:
 1. brukeridentitet
 2. rolle
 3. type / domain
 4. nivå og/eller kategori

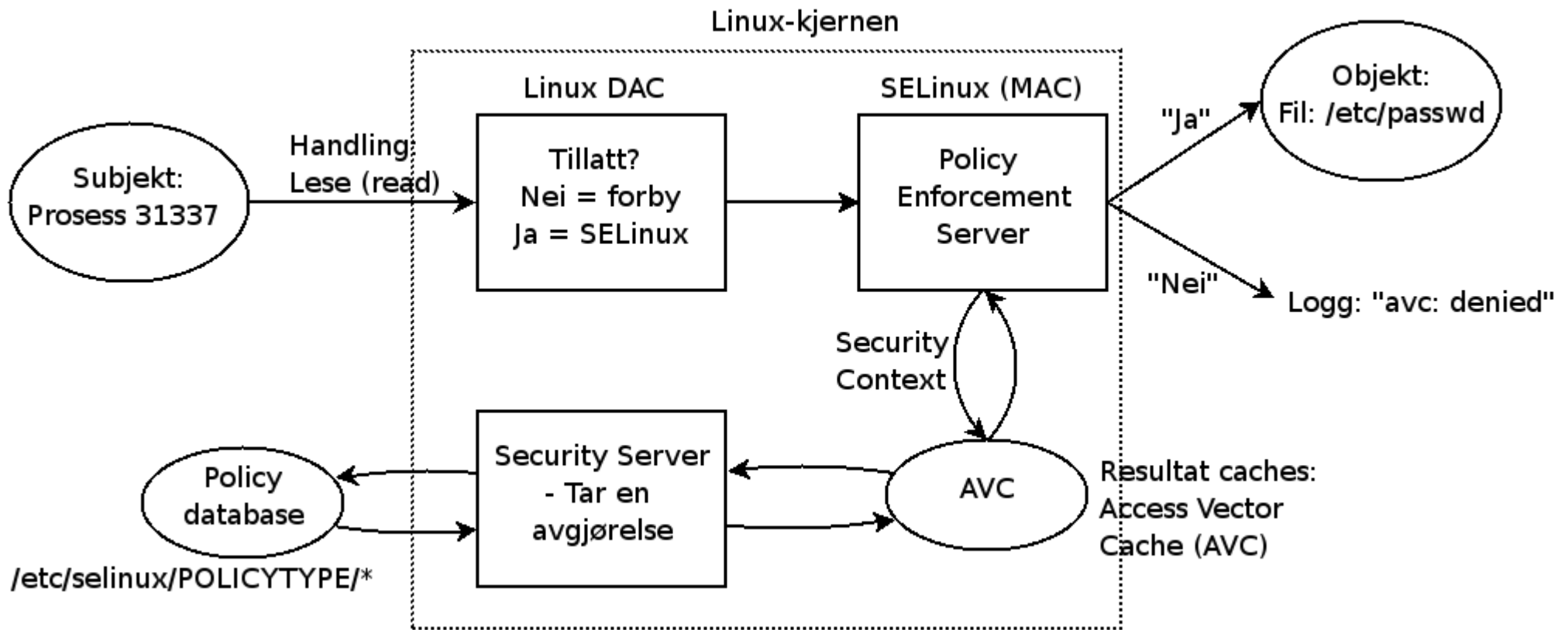
- Bygges opp av
`<bruker>:<rolle>:<type>:<kategori/nivå>`
- Eks:
`system_u:system_r:unconfined_t:s0:c0`
- Disse attributtene danner en “security context”:

Security attribute	Navnkonvensjon	Eksempelnavn
Bruker	<code>_u</code>	<code>user_u</code>
Rolle	<code>_u</code>	<code>object_r</code>
Type	<code>_t</code>	<code>unconfined_t</code>
Kategori / nivå	(ingen)	<code>s0:c0</code>

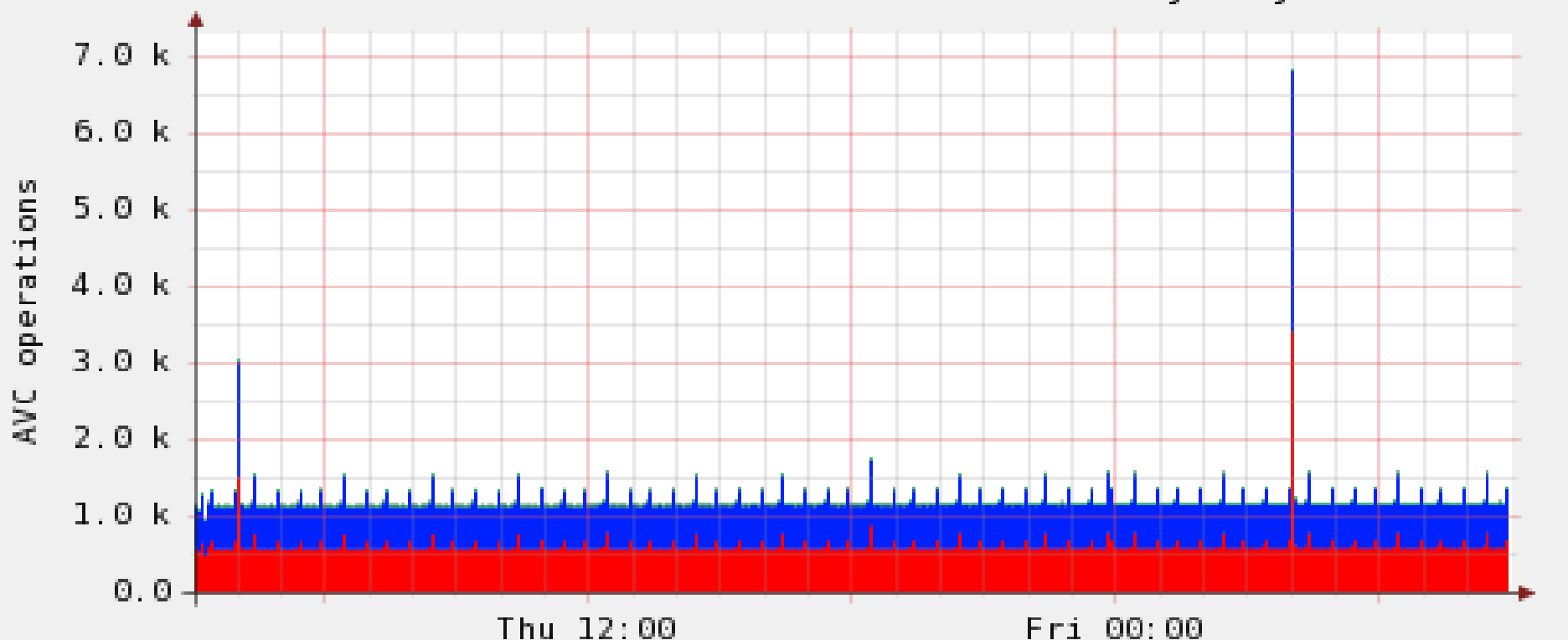
- SELinux kan kjøre i
 - Enforcing – sikkerhetspolicy håndhevet.
 - Permissive – sikkerhetspolicy aktiv, men ikke håndhevet.
 - Disabled – ingen SELinux aktivert.

- Hva er beskyttet av SELinux' policy?

- Et sett med daemoner omfavnet av policy:
 - RHEL4, 15 programmer: dhcpd, apache, named, nscd, ntpd, portmap, squid,..
 - RHEL5, ~200 programmer.
 - Dvs. disse har skreddersydd policy.
 - Mål – fuldekkende policy!
- Resten har “full aksess”.
 - Puttet i en “unconfined” domain.
 - 'unconfined_t' eller 'initrc_t'
 - Samme aksess som om SELinux var skrudd av.



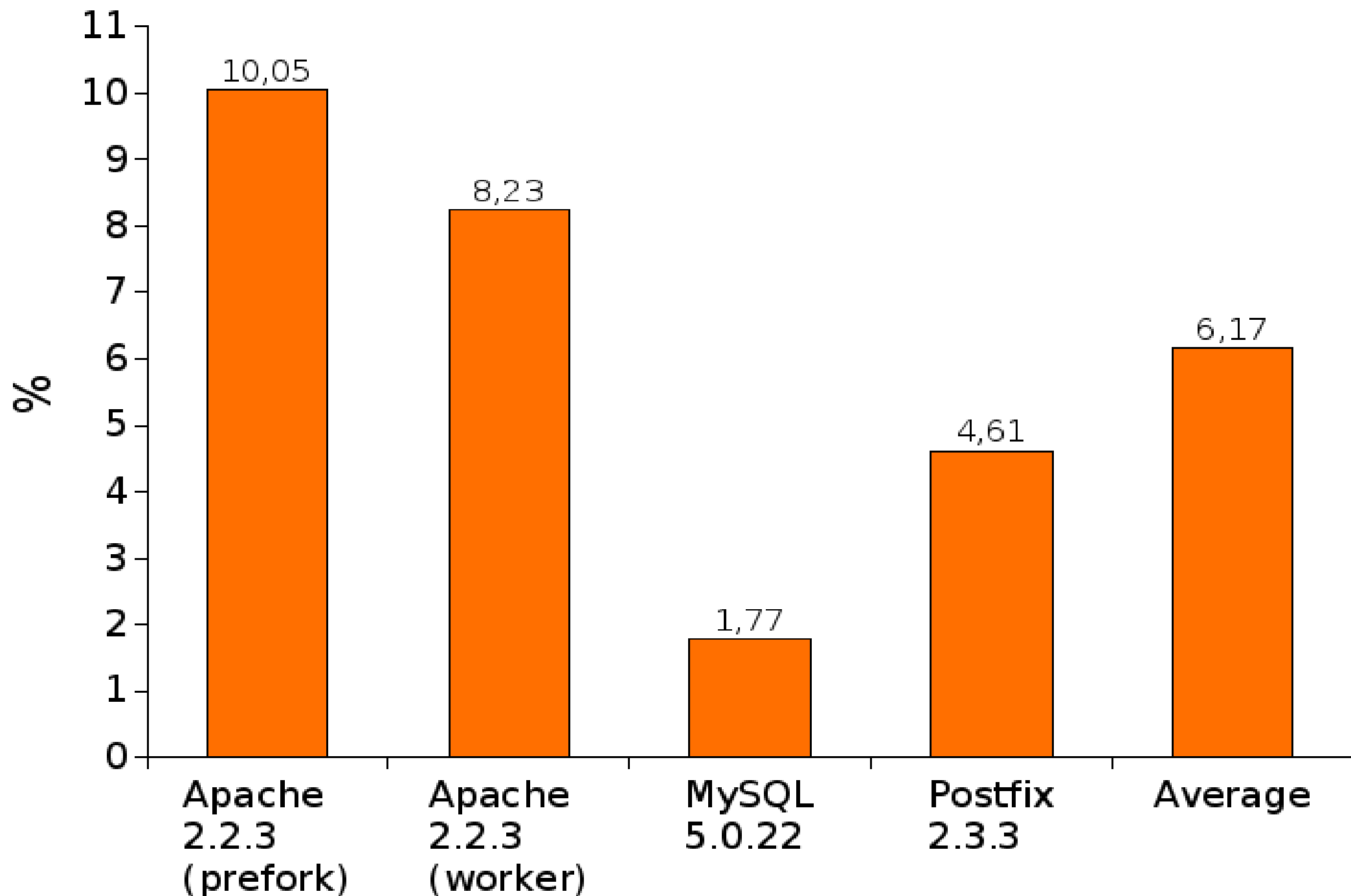
SELinux's Access Vector Cache - by day



lookups	Cur: 675.77	Min: 465.95	Avg: 600.01	Max: 3.40k
hits	Cur: 675.76	Min: 465.95	Avg: 599.99	Max: 3.40k
misses	Cur: 830.26u	Min: 0.00	Avg: 20.73m	Max: 3.07
allocations	Cur: 830.26u	Min: 0.00	Avg: 20.73m	Max: 3.07
reclaims	Cur: 664.21u	Min: 0.00	Avg: 20.74m	Max: 3.06
frees	Cur: 664.29u	Min: 0.00	Avg: 20.74m	Max: 3.06

Last update: Fri Oct 12 09:00:04 2007

RHEL5 SELinux: Average penalty



- Policy optimeres og øker i omfang.
 - dvs. flere tjenester skal beskyttes av policy.
- Økt fokus på brukervennlighet!
 - flere (grafiske) verktøy.
- RHEL legger grunnlaget for videre sikkerhetsmodellering.
 - MLS og MCS.
 - For å oppnå sertifiseringer (EAL4+, LSPP, ..)
 - For tappe DoD og US Gov markedene?

- AppArmor er en konkurrerende teknologi.
- Primær utvikler: Novell Suse
- AppArmor benytter også LSM og tilbyr MAC.
- Enklere?
- Medfølger Ubuntu 7.10 som kommer i dag.

FBI/CSI rapport (2006)

