SELinux – kort intro

Lars Strand
18. oktober 2007

STORM

Bare på Windows - ikkesant?

FEIL!

(Men MEST på Windows)

Sårbarheter

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

Begrense aksess?

SELinux!

Men først: Litt teori:

1. Tradisjonell UNIX (og Linux)

Linpro

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).

2. Mandatory access control

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

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

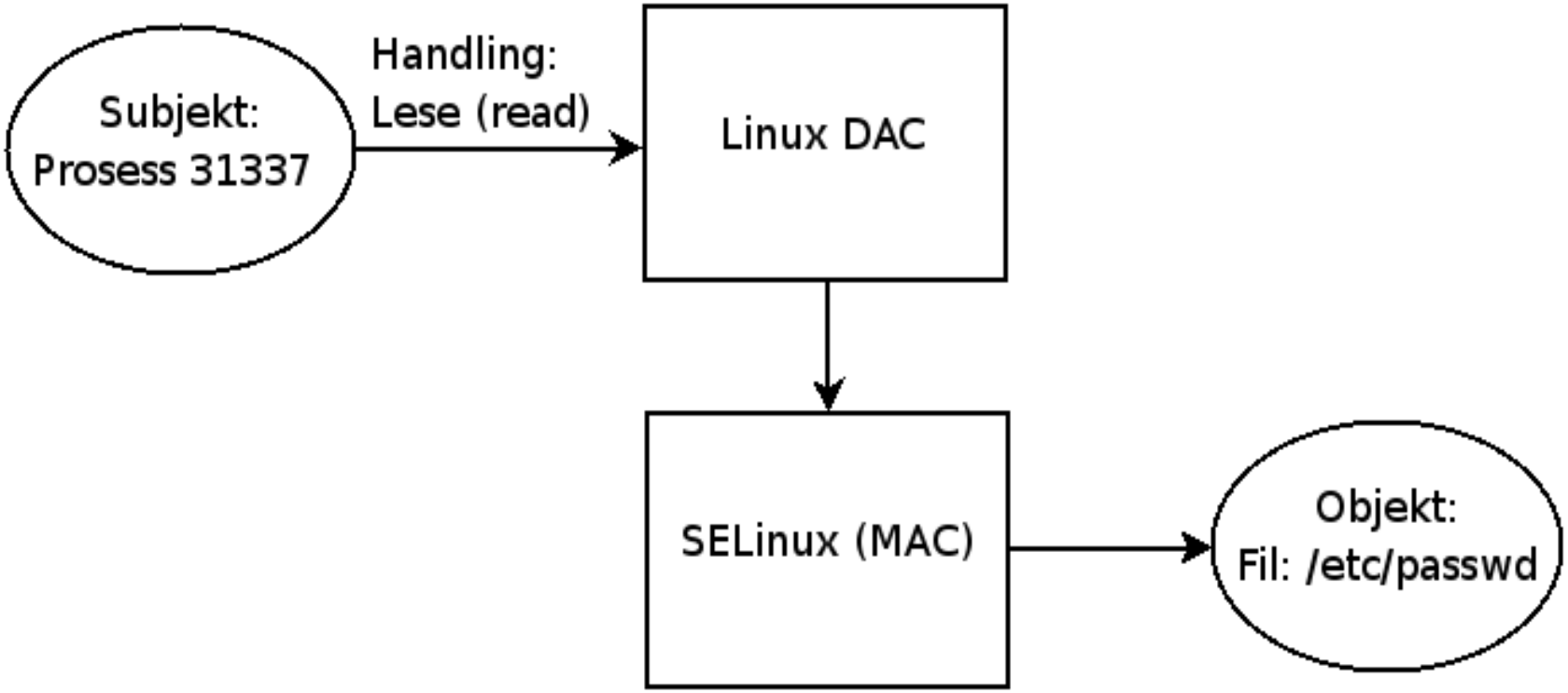
Systemet (OS) agjøre og håndhever sikkerhetspolicy.

"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).

Sikkerhetsmodell

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



- Nøkkelegenskap = supplerer tradisjonell DAC med MAC:

Security Enhanced Linux

- *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).

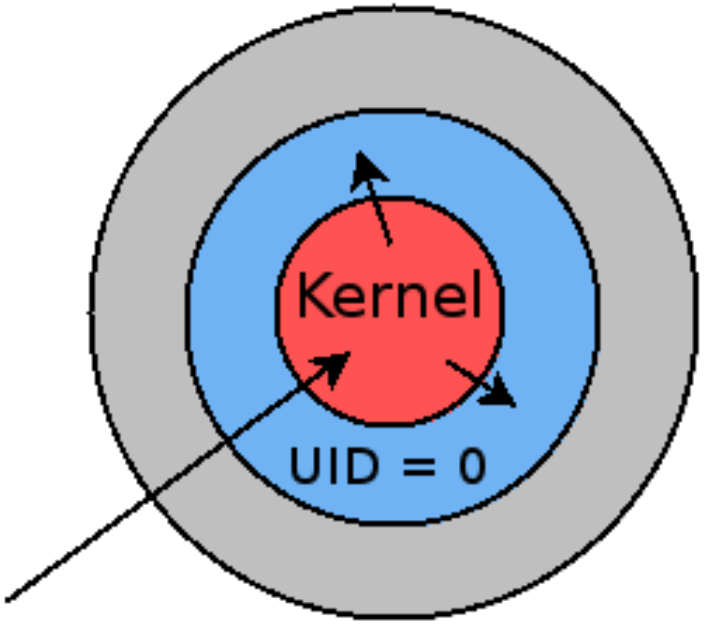
SELinux komponenter

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

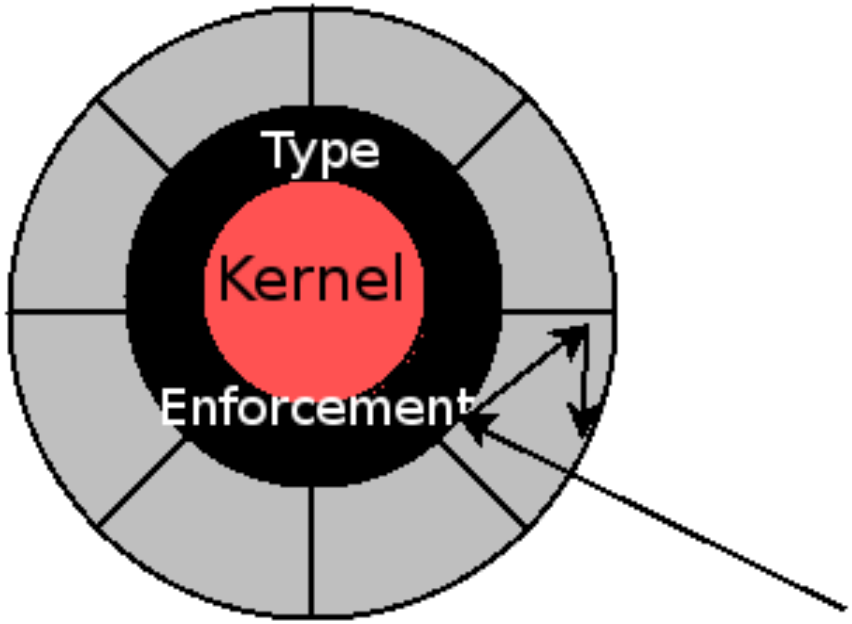
SELinux MAC

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

SELinux – Type Enforcement



Klassisk aksesskontroll.
UID 0 har full aksess.



Domain/Type aksesskontroll
Grupper med sandkasser.

Sikkerhetsmodell

- 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

Security context

- 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	_u	user_u
Rolle	_u	object_r
Type	_t	unconfined_t
Kategori / nivå	(ingen)	s0:c0

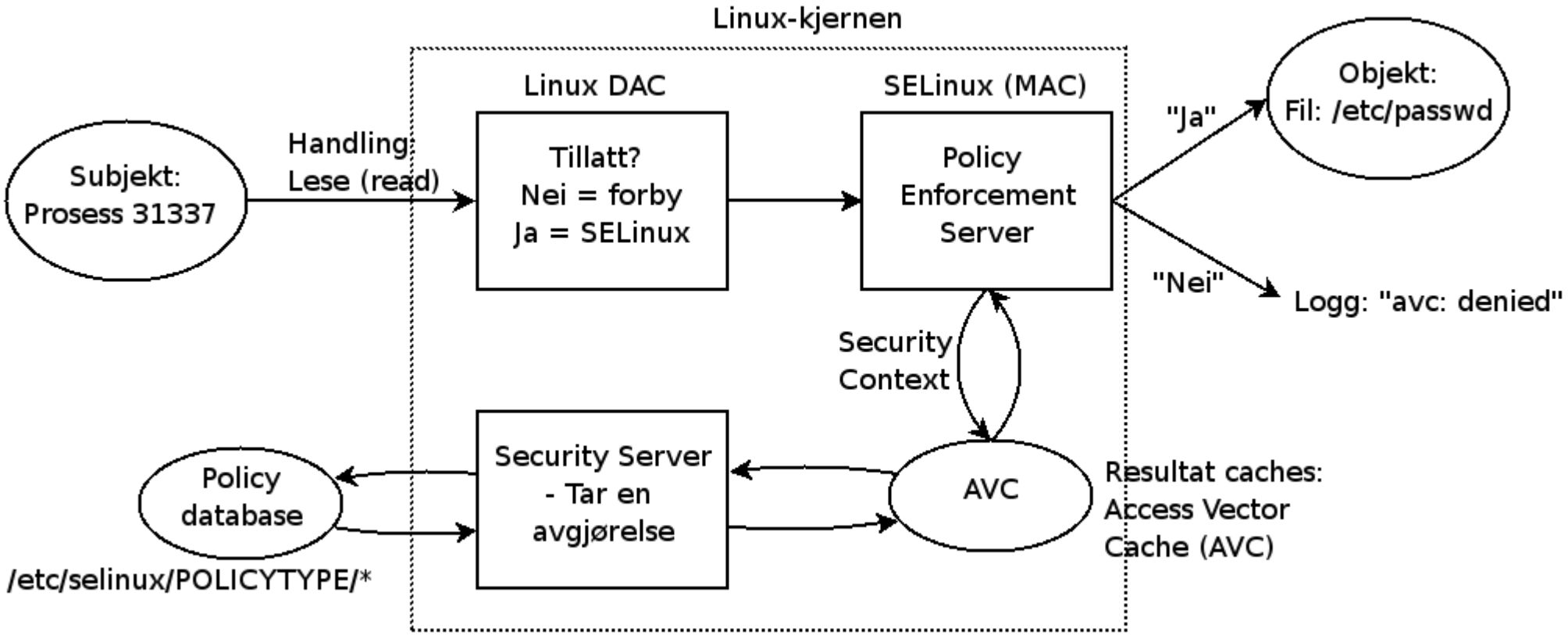
- SELinux kan kjøre i
  - Enforcing – sikkerhetspolicy håndhevet.
  - Permissive – sikkerhetspolicy aktiv, men ikke håndhevet.
  - Disabled – ingen SELinux aktivert.

- Hva er beskyttet av SELinux' policy?

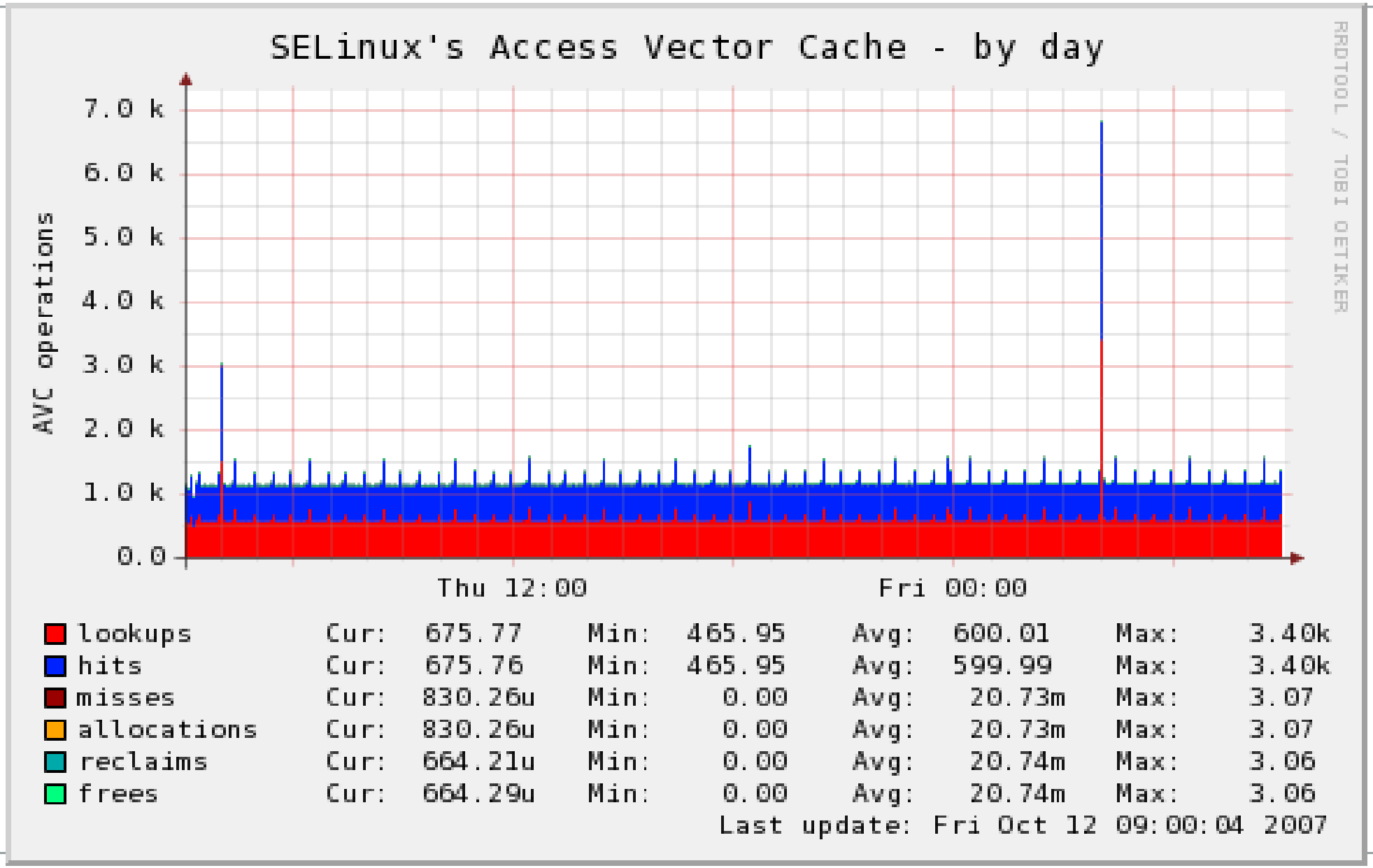
Targeted policy

- 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.

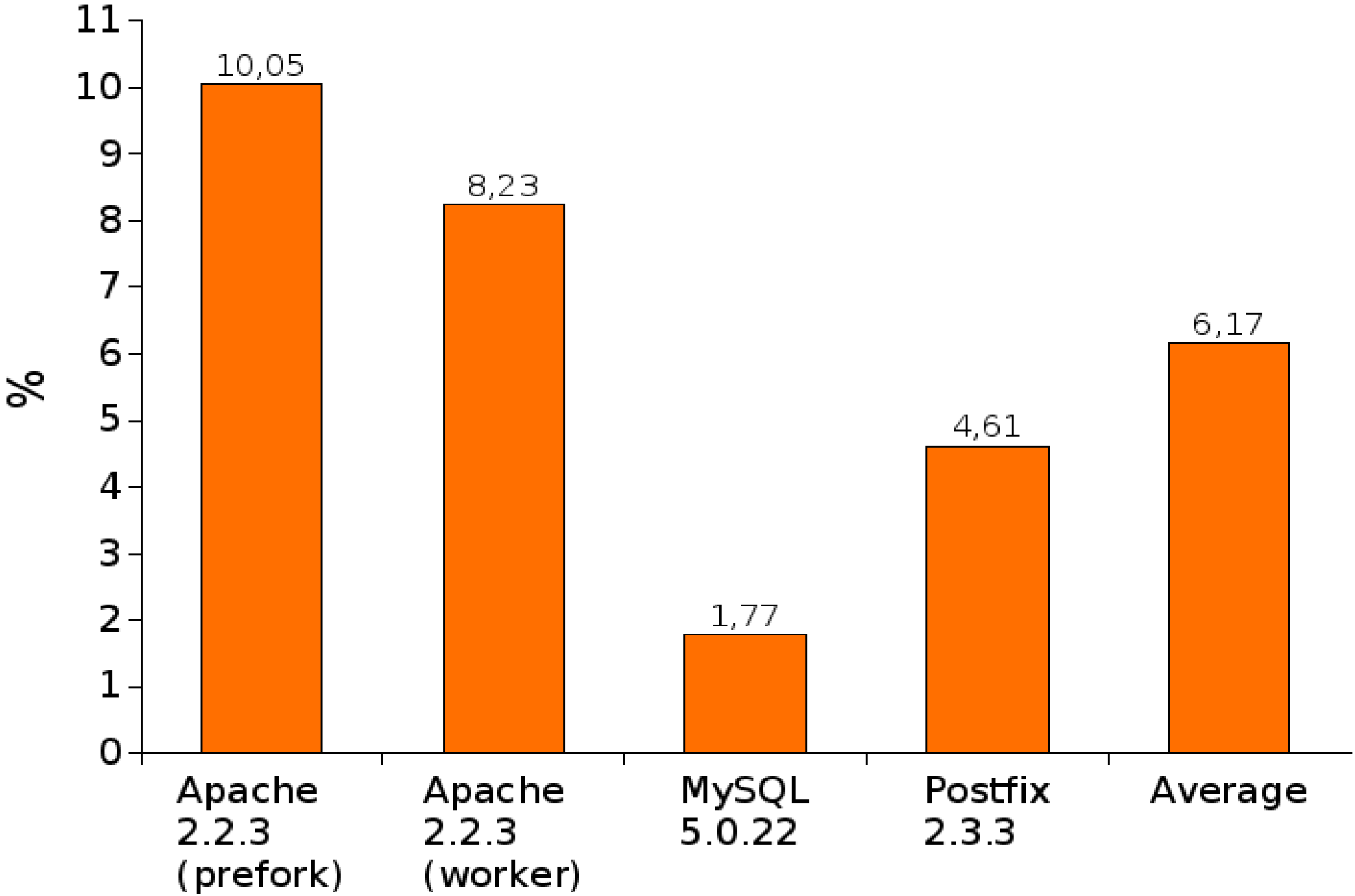
SELinux – avgjørelsesprosess



Munin: AVC overvåkning



RHEL5 SELinux: Average penalty



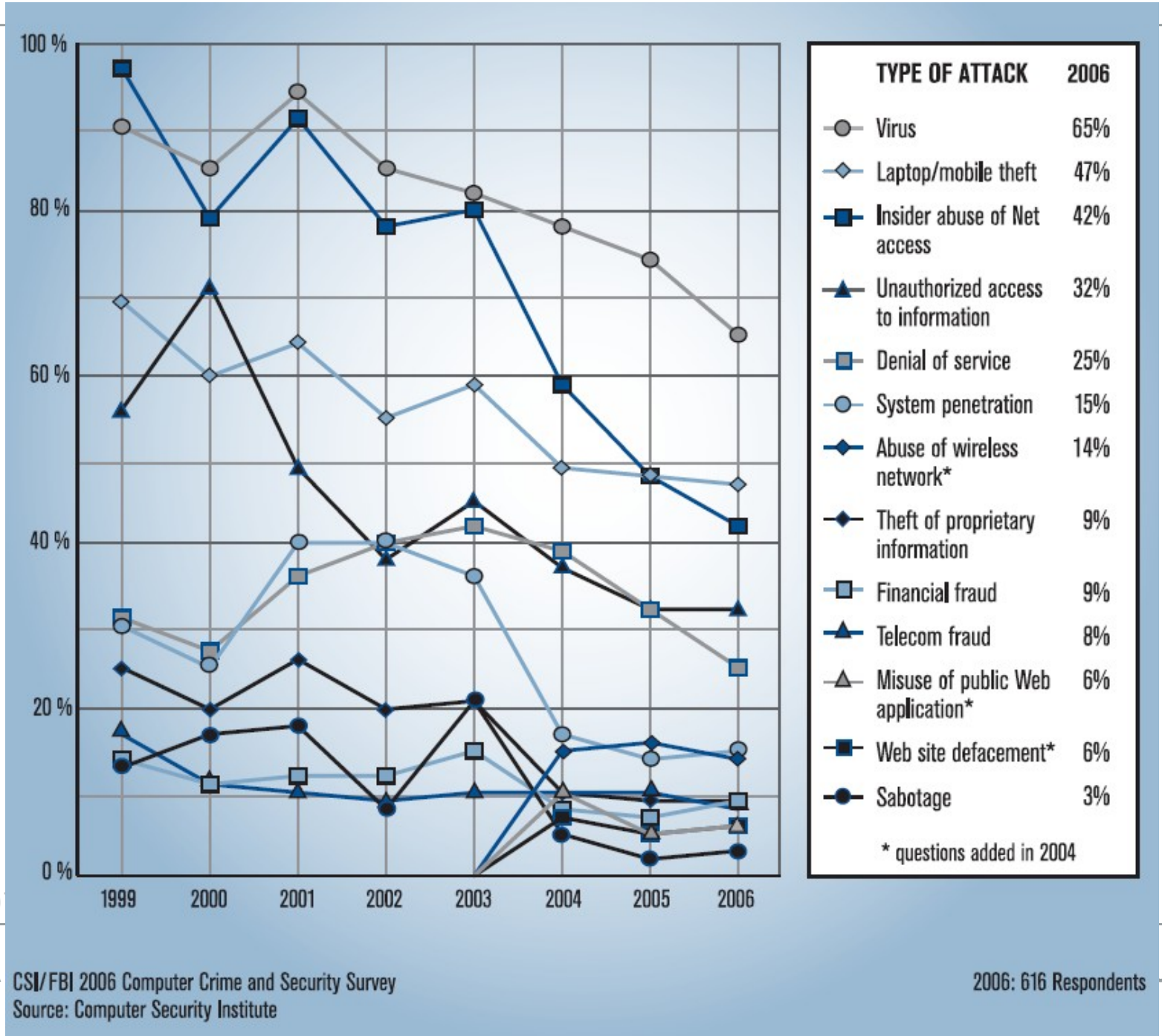
SELinux fremover

- 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

- 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)



Spørsmål?