HrOUG 2009

Zaštita na razini Linux Jezgre

Vlatko Košturjak, IBM ISS / HULK
<kost@linux.hr>
<vlatko.kosturjak@hr.ibm.com>

Agenda

- Uvod – sigurnost
- Opcije
- Capabilities
- SELinux
  - Uvod
  - Dizajn
  - Uključivanje
  - podešavanja
- Smack, GrSecurity, PaX, Apparmor...
- Pitanja i odgovori

30 minuta

Sigurnost

- Javna računala
- Svjetski kriminalci
- Napadi
  - Pravo ne radi preko granice
  - Napadači DA :)
- Udaljenost nema razlike
  - Dobro, par milisekundi...
- ...

Što ima?

- Linux jezgra
  - **Kontrola pristupa (Access Control)**
    - DAC (user-group other)
  - Capabilities
  - Enkripcije/Hashing, ..
  - Filesystem Extended ACLs
- Dodatne zakrpe
  - AppArmor
  - PaX
  - Grsecurity

DAC

- Usual Unix/Linux permissions
  - Naredbe: chown, chmod, chgrp, ...
  - User
  - Group
  - Other
  - Some flags:
    - Setuid, sticky, ...
- Attributes:
  - append(a), Immutable(i), undelete(u), synch(S),
  - Naredbe: chattr, lsattr

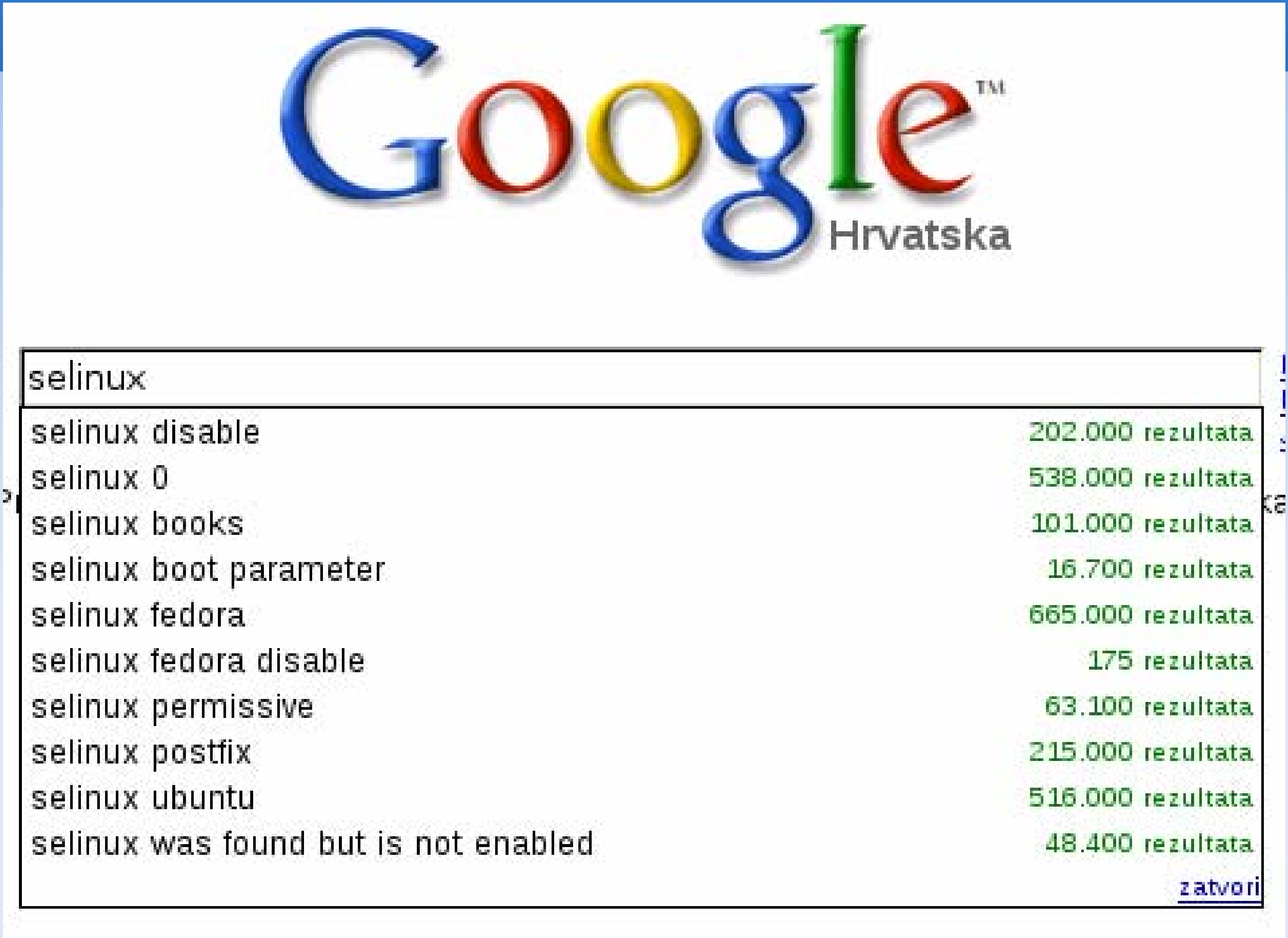
Capabilities

- Kernel 2.2+
- Privilegirani korisnik
- Po threadu
- Primjeri
  - CAP_NET_RAW
  - CAP_NET_BIND_SERVICE
  - ...
- Instalacija: apt-get install libcap2-bin
- Naredbe: capset, capget, ...

SELinux

- Što će mi to?
- ”To je ono kad isključim, i onda mi sve radi...”
- ”selinux=0”
- ”Kako se to ono isključuje?”
- ”To moram isključit da mi rade moje 2.0 aplikacije”
- ...

Google



Google Hrvatska

selinux

selinux disable	202.000 rezultata
selinux 0	538.000 rezultata
selinux books	101.000 rezultata
selinux boot parameter	16.700 rezultata
selinux fedora	665.000 rezultata
selinux fedora disable	175 rezultata
selinux permissive	63.100 rezultata
selinux postfix	215.000 rezultata
selinux ubuntu	516.000 rezultata
selinux was found but is not enabled	48.400 rezultata

Linux

- SELinux = Security Enhanced Linux
- GPL licenca
- Izdan od strane NSA
    - 22.12.2000
- Implementira MAC sigurnosne politike
    - Trusted Computer System Evaluation Criteria (TCSEC)
    - trusted computing base (TCB)

Citati - NSA

- *NSA backdoor?*
  - Adams

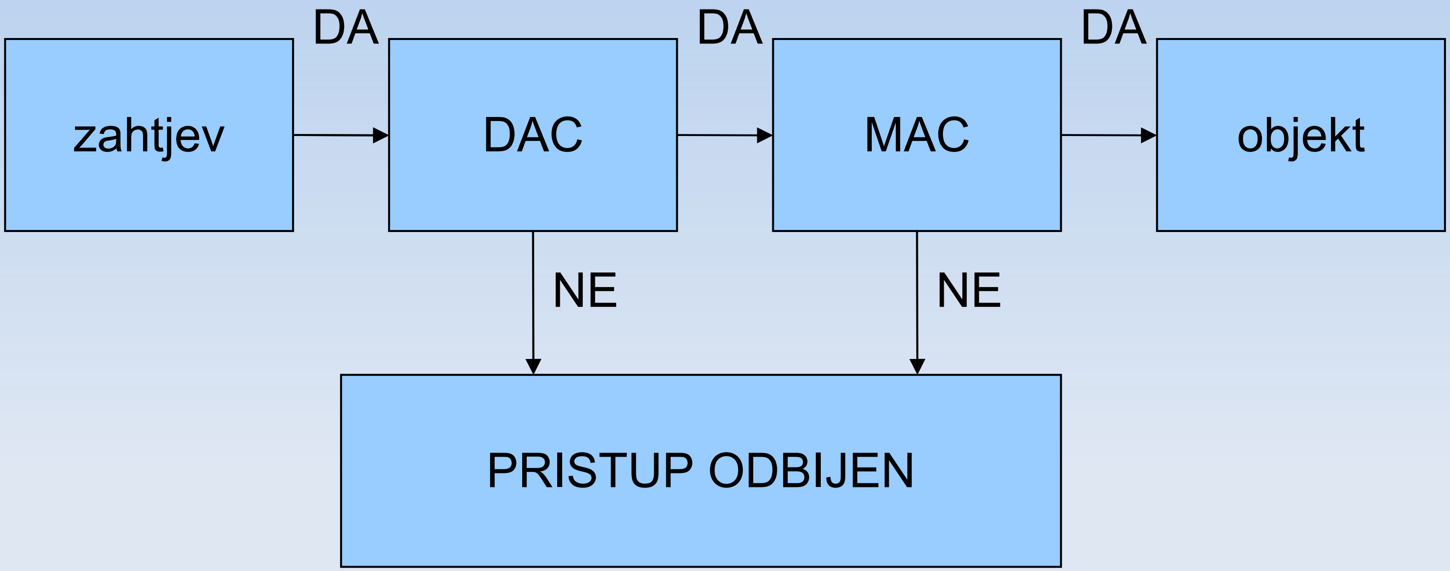
- *No backdoor. NSA doesn't want your data, they already have it. They just want to deny others access to your data.*
  - DarkLogic

Gdje postoji?

- Linux 2.6.0
- Dolazi sa
  - Red Hat Enterprise Linux (RHEL)
  - Fedora
  - CentOS
  - Debian
  - Ubuntu
  - OpenSuSE
  - Suse Linux Enterprise Server (SLES)

SELinux dizajn

- LSM



SELinux Uključivanje

- Tipovi uključivanja
  - Enforcing
  - Permissive
  - Disabled
- Tipovi
  - Targeted
  - Strict
- Enforcing=1 kao boot parametar
- /etc/sysconfig/selinux

Korištenje

- Pogledati sigurnosne oznake možemo sa -Z opcijama u normalnim naredbama
- ls -Z
- ps -Z
- id -Z
- ...

Podešavanje

- /var/log/audit/audit.log
- audit2allow -m httpd_newperm > httpd_newperm.te
- check_module -m -M -o httpd_newperm.mod httpd_newperm.te
- semodule_package -o httpd_newperm.pp -m httpd_newperm.te
- sudo semodule -i httpd_newperm.pp

Loše strane

- Brzina
  - Overhead...
- Ne radi na svakom ds
  - NFS
- Kompliciranost
- Kompliciranost
- Kompliciranost
- ...

Zanimljivi citat

“...given the threat models and capabilities of the adversaries involved, that's probably appropriate... But that’s not necessarily appropriate for all users. SELINUX is so horrible to use, that after wasting a large amount of time enabling it and then watching all of my applications die a horrible death since they didn't have the appropriate hand-crafted security policy, caused me to swear off of it. For me, given my threat model and how much my time is worth, life is too short for SELinux.”

Theodore T'so

AppArmor

- Implementacija MAC
  - Pokušaj jednostavnijeg SELinuxa
- Linux Security Module (LSM)
- SUSE i UBUNTU podrška
- Ne ovisi o tipu datotečnog sustava
- 2005-2007 Novell financira
- Nije ušao u Linux kernel
- 9.2007 Novell raspušta razvijatelje
- ...

GrSecurity

- Pruža Role Based Access Control (RBAC)
- PaX
  - Non-executable memory locations (stack, ...)
  - address space layout randomization (ASLR)
- Chroot dodatna sigurnost
- Razno
- Nije uključen u Linux kernel
- ...

Smack

- Simplified Mandatory Access Control
- Implementira MAC
- Koristi LSM
- Jednostavnost – glavna odlika
- Izdan pod GPL
- Uključen u kernel
  - 2.6.25
- ...