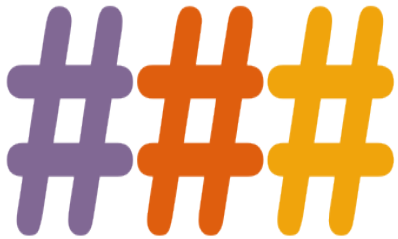


RootConf India 2017

12 May 2017

An Introduction to SELinux

Life is too short to live unsecurely

Toshaan Bharvani - VanTosh bvba

<toshaan@vantosh.com>

$ whoami

Toshaan Bharvani

- From Antwerp, Belgium
- Self-employed engineer/trainer (available for hire)
  http://www.vantosh.com
- Involved with Enterprise Linux, RPM packaging : RHEL, CentOS, IBM AIX, BSD, SLES, ...
- Likes to keep everything secure : SELinux, WebSec, ...
- Lives in a virtual world : KVM, Xen, LXC, PowerVM, z/VM, ...
- Likes automation CfgMgmt / DevOps : Ansible, Foreman, Puppet
- Involved with hardware, software and conferences
- Wants to take over the universe
- Twitter : @toshywoshy
- Blog : http://www.toshaan.com
- Social : @toshywoshy

Table of contents

1

Introduction

Misconceptions about SELinux (1)

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 Ts'o ("Life is too short for SELinux")

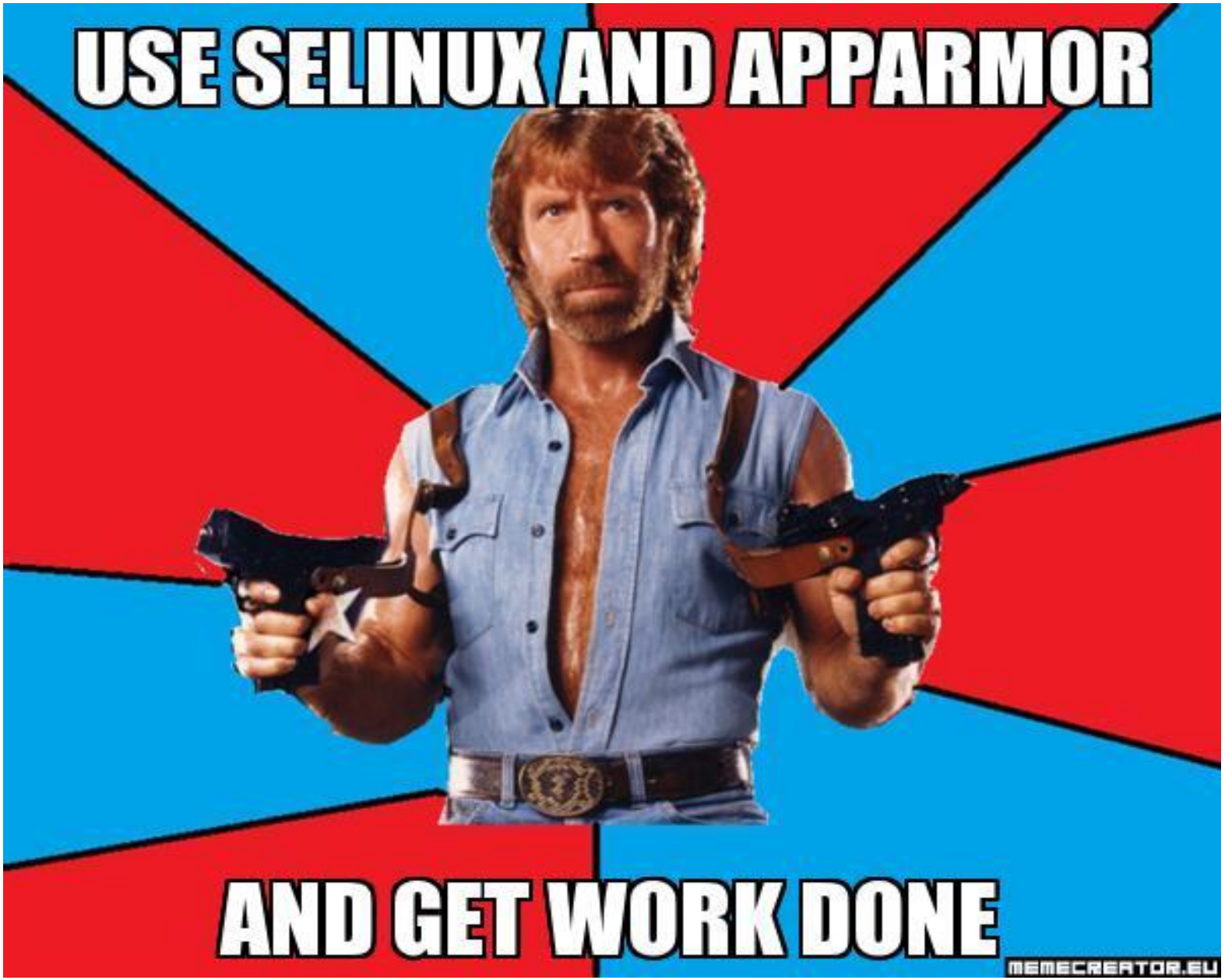
Misconceptions about SELinux (2)

"SELinux is a pain in the ass" – urban legend

Misconceptions about SELinux (3)

Upstream vendors requires me to disable SELinux

Misconceptions about SELinux (4)



The good of SELinux

- "Let me assure you that this action by the NSA was the crypto-equivalent of the Pope coming down off the balcony in Rome, working the crowd with a few loaves of bread and some fish, and then inviting everyone to come over to his place to watch the soccer game and have a few beers. There are some things that one just never expects to see, and the NSA handing out source code along with details of the security mechanism behind it was right up there on that list." – Larry Loeb[1]

[1] Security author and researcher

2

What is SELinux

Traditional Linux Permissions

- Everything is a file
- 3 x 3 file level security
  - user, group, others
  - read, write, execute
  - 0/-, 4/r, 2/w, 1/x[2]

[2] If you didn't notice this is binary.

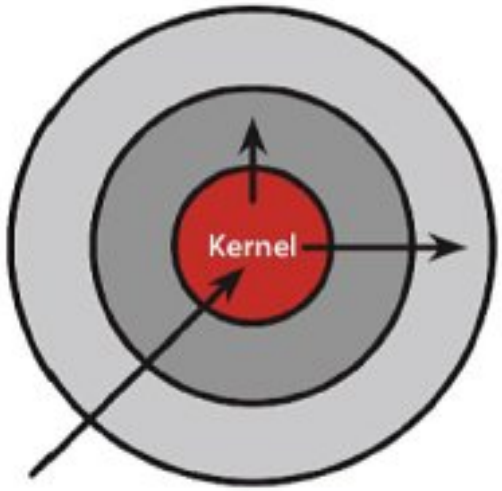
What is SELinux

- SELinux = Security-Enhanced Linux
- Mechanism for supporting Mandatory Access Control security policies
- Linux Security Modules (LSM) run in the Linux kernel
- Everything is a context
- Several security models
  - Type Enforcement (TE)
  - Role Based Access Control (RBAC)
  - Multilevel Security (MLS)
- Developed by the NSA

Access Control

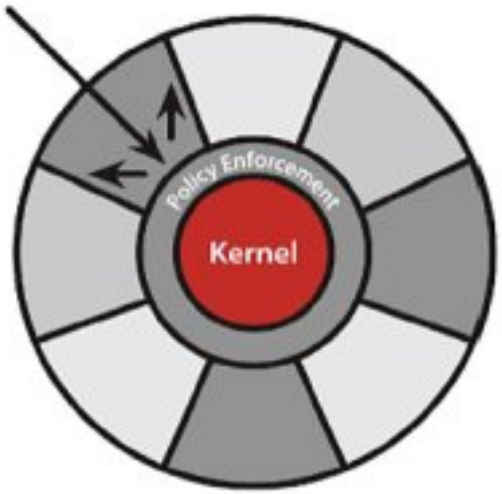
- Type Enforcement (TE)
  - The primary mechanism of access control used in the targeted policy
- Role-Based Access Control (RBAC)
  - Based around SELinux users (not necessarily the same as the Linux user)
- Multi-Level Security (MLS)
  - Not used and often hidden in the default targeted policy.

SELinux visually



Discretionary Access Control

Once a security exploit gains access to priveleged system component, the entire system is compromised.



Mandatory Access Control

Kernel policy defines application rights, firewalling applications from compromising the entire system.

SELinux features

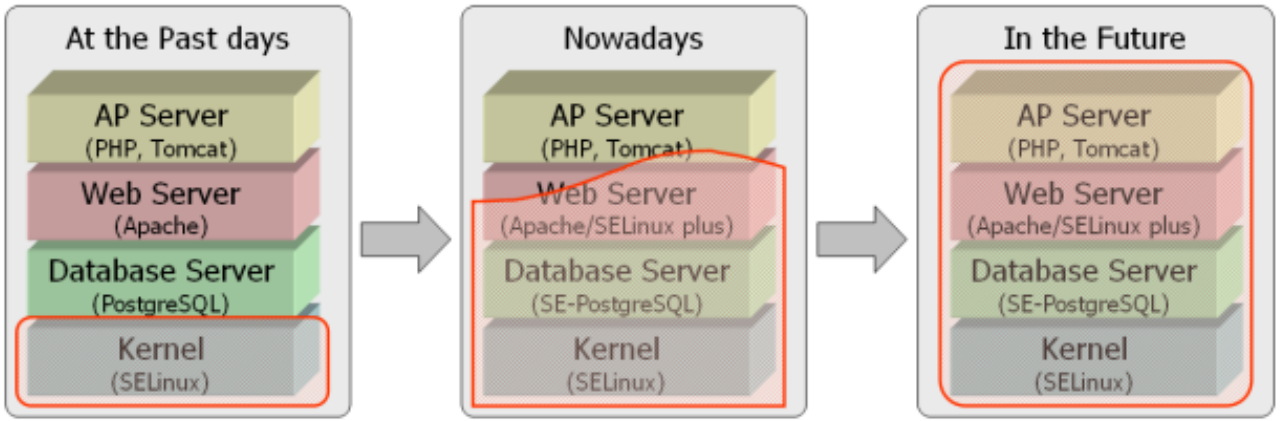
- Separation of policy from enforcement
- Predefined policy interfaces
- Support for applications querying the policy and enforcing access control
- Independent of specific policies, policy languages, security label formats and contents
- Caching of access decisions for efficiency
- Policy changes are possible (!!!)
- Separate measures for protecting system integrity and data confidentiality
- Controls over process initialization and inheritance and program execution
- Controls file systems, directories, files, and open file descriptors
- Controls over sockets, messages, and network interfaces

SELinux hidden features (from hell)

- Breaks systems that are not secure
- Disallows services of misbehaving
- Annoyment tool for juniors
- Will take over the world
- Restricts the root user
- Cannot be disabled just like that for daemons
- Inappropriate processes will be excommunicated

Past, Today, Future

Figure: SELinux coverage and LAPP - web application software stack



Where is SELinux

- In the kernel from 2.6.0 - 2002
- Redhat Enterprise Linux : from v4
- CentOS : from v4
- Fedora : from Core 2
- Novell SLES, OpenSuSE
- Gentoo
- Debian (Etch), Ubuntu (8.04)
- Android. AndroidSE
- ...

Why use SELinux?

- It confines processes,services,users in compartments
- Allows use of one compartment of a systems :
  - virtual machine : sVirt (qemu, lxc, . . .)
  - user : xguest
  - hardware : usbredir, automobile, smartphone, . . .
- Stops daemons going bad
- Really increases security
- No, it isn't difficult
-

3

How to use SELinux

Changing SELinux states

- Enforcing
  - Enable and enforce the SELinux security policy on the system, denying access and logging actions
- Permissive
  - Enables, but will not enforce the security policy, only warn and log actions
- Disabled
  - SELinux is turned off

Checking the state of SELinux

- sestatus
  - Enforcing
  - Permissive
- - Z
  - ls -Z
  - netstat -Z
  - ps -Z

File labels

- Objects (Processes, files, inodes, superblocks etc.) in the OS are labeled
- Files persistently labeled via extended attributes
- Labels are called security contexts
- Labels contain all SELinux security information

Relabelling files

- chcon -R -t httpd_sys_content_t /usr/srv/www
- semanage fcontext -a -t httpd_sys_content_t "/usr/srv/www(/.*)?"
- restorecon -Rv -n /var/www/html
- Relabelling whole the filesystem
  - genhomedircon
  - touch /.autorelabel
  - reboot
- For first time use : fixfiles specfile /your/path

Enabling bools & ports

- Managing ports
  - semanage port -l
  - semanage port -a -t http_port_t -p tcp 8181
- Managing file contexts
  - semanage fcontext -l
  - semanage fcontext -a -t samba_share_t '/var/nmbd(/.*)?'
- Managing predefined policies
  - getsebool -a | grep samba
  - setsebool -P samba_enable_home_dirs on
  - togglesebool

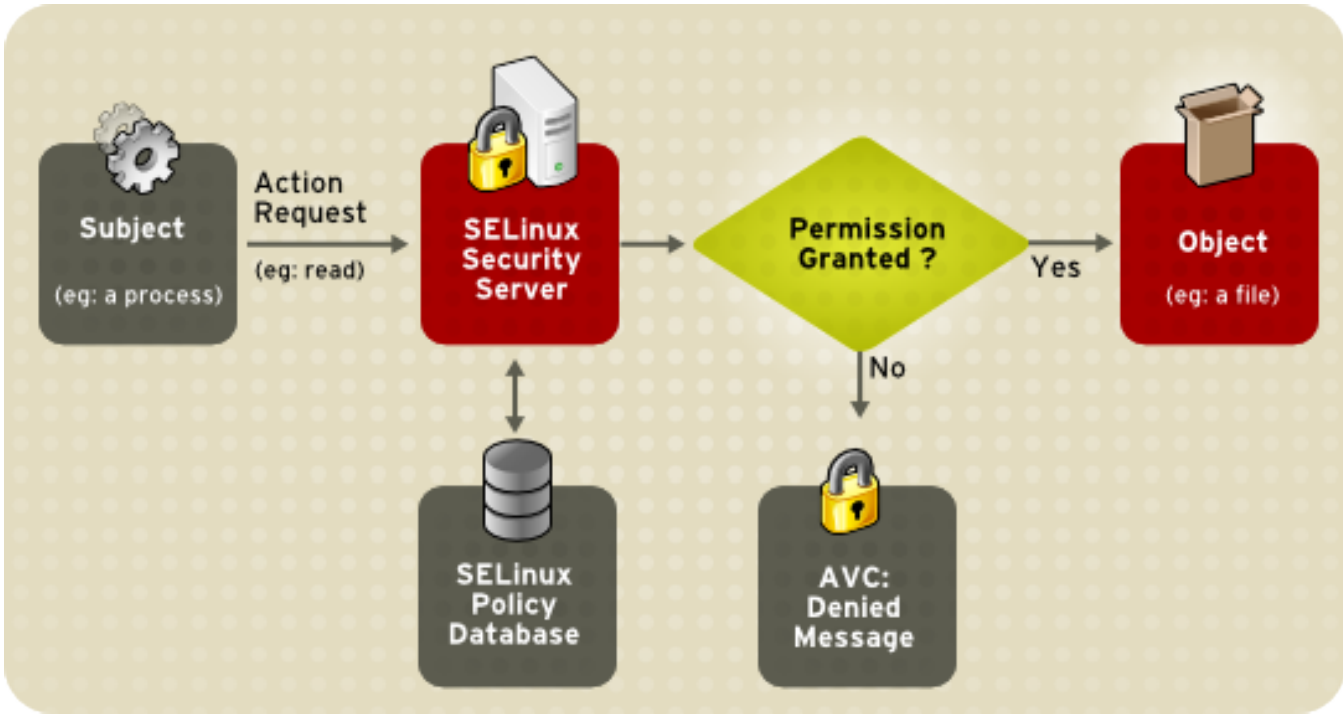
Looking at SELinux problems

- Audit Log
- audit2why
- setroubleshoot
- semanage boolean -l

What is a SELinux Policy

- Labeling policy
  - Describe how objects are to be labeled
- Access policy
  - Describe how subjects access objects (and other subjects)
- Compiled into binary form and loaded into kernel
- Enforced by the kernel

SELinux Policy Flow



SELinux Database

- Database of rules : allow a process in one context to do operations on an object in another context
- Switches/Booleans turn groups of rules on or off
  - getsebool -a
  - semanage boolean -l
  - sesearch -b <seboolean> -AC
  - sesearch -s <subject> -AC
  - sesearch -t <type> -AC
  - setsebool
  - setsebool -P

Generating policies

- less /var/log/audit/audit.log
- grep galera /var/log/audit/audit.log | audit2allow -m galera > galera.te
- checkmodule -M -m -o galera.mod galera.te
- semodule_package -o galera.pp -m galera.mod
- semodule -i galera.pp

Galera Policy

```
1
2  module mariadbgaleracluster 1.1;
3
4  require {
5          type hostname_exec_t;
6          type rsync_exec_t;
7          type mysqld_t;
8          class process setpgid;
9          class file { execute read execute_no_trans getattr open
             };
10 }
11
12 #============= mysqld_t ==============
13 allow mysqld_t hostname_exec_t:file { read getattr open execute
     execute_no_trans };
14 allow mysqld_t rsync_exec_t:file { read getattr open execute
     execute_no_trans };
15 allow mysqld_t self:process setpgid;
```

Some Policy

?

?

?

More information

- Main Project page : http://selinuxproject.org/
- SELinux News Blog : http://selinuxnews.org/
- Daniel Walsh : http://danwalsh.livejournal.com/
- RHEL/CentOS Wiki : http://wiki.centos.org/HowTos/SELinux
- Fedora Wiki : http://fedoraproject.org/wiki/SELinux
- Gentoo Wiki : http://en.gentoo-wiki.com/wiki/SELinux
- Debian Wiki : http://wiki.debian.org/SELinux

The End

Thank You for your attention

Toshaan Bharvani - VanTosh bvba <toshaan@vantosh.com>

http://www.vantosh.com/

Made with Beamer LaTeX

a TeXbased Presentation program