Stop Disabling SELinux

Maciej Lasyk

Kraków, InfoSec meetup #1

2014-03-12

Does security matter?

- Business value and security

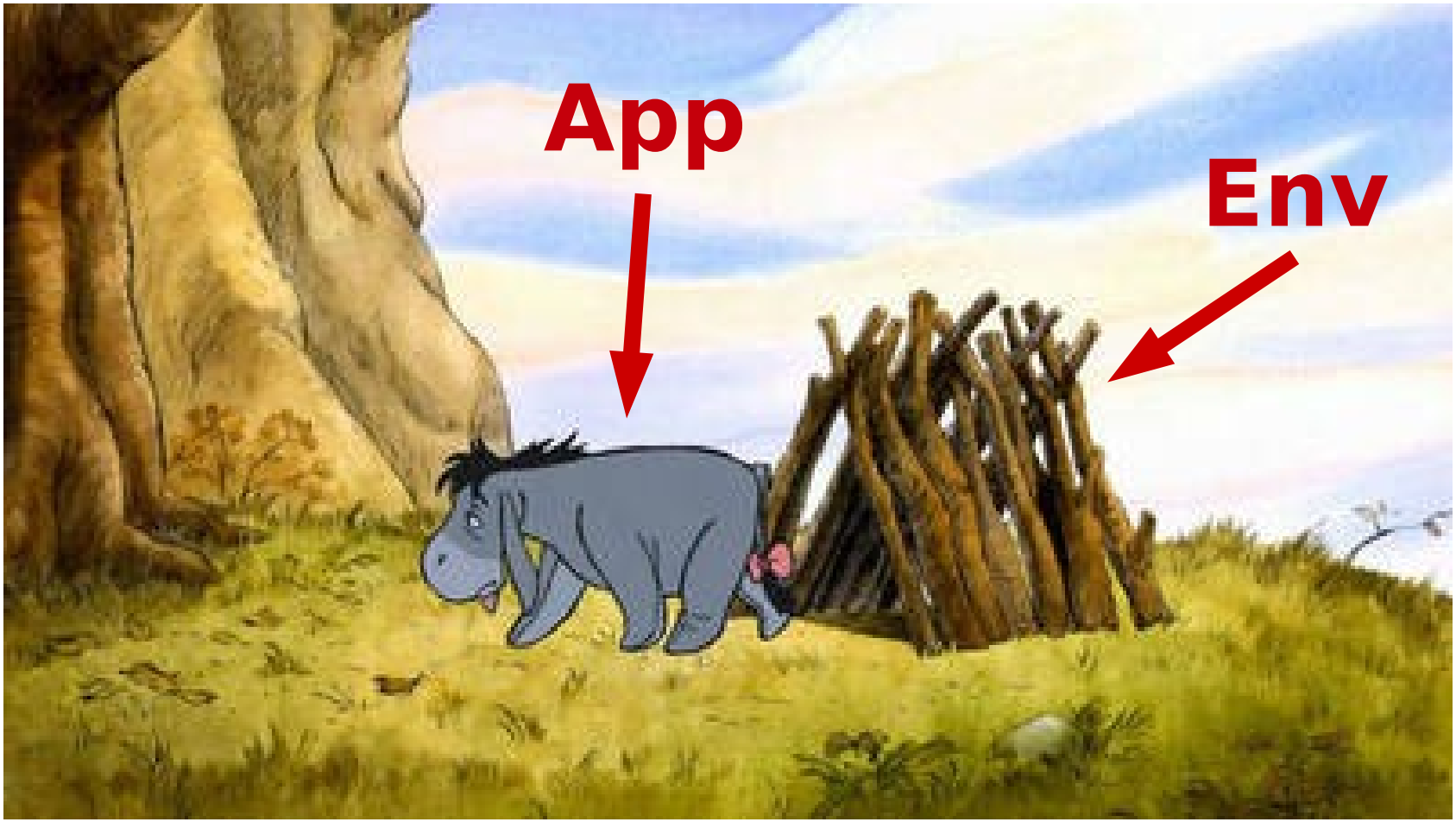
Does security matter?

- Business value and security
- Does stock price change after security fail?

Does security matter?

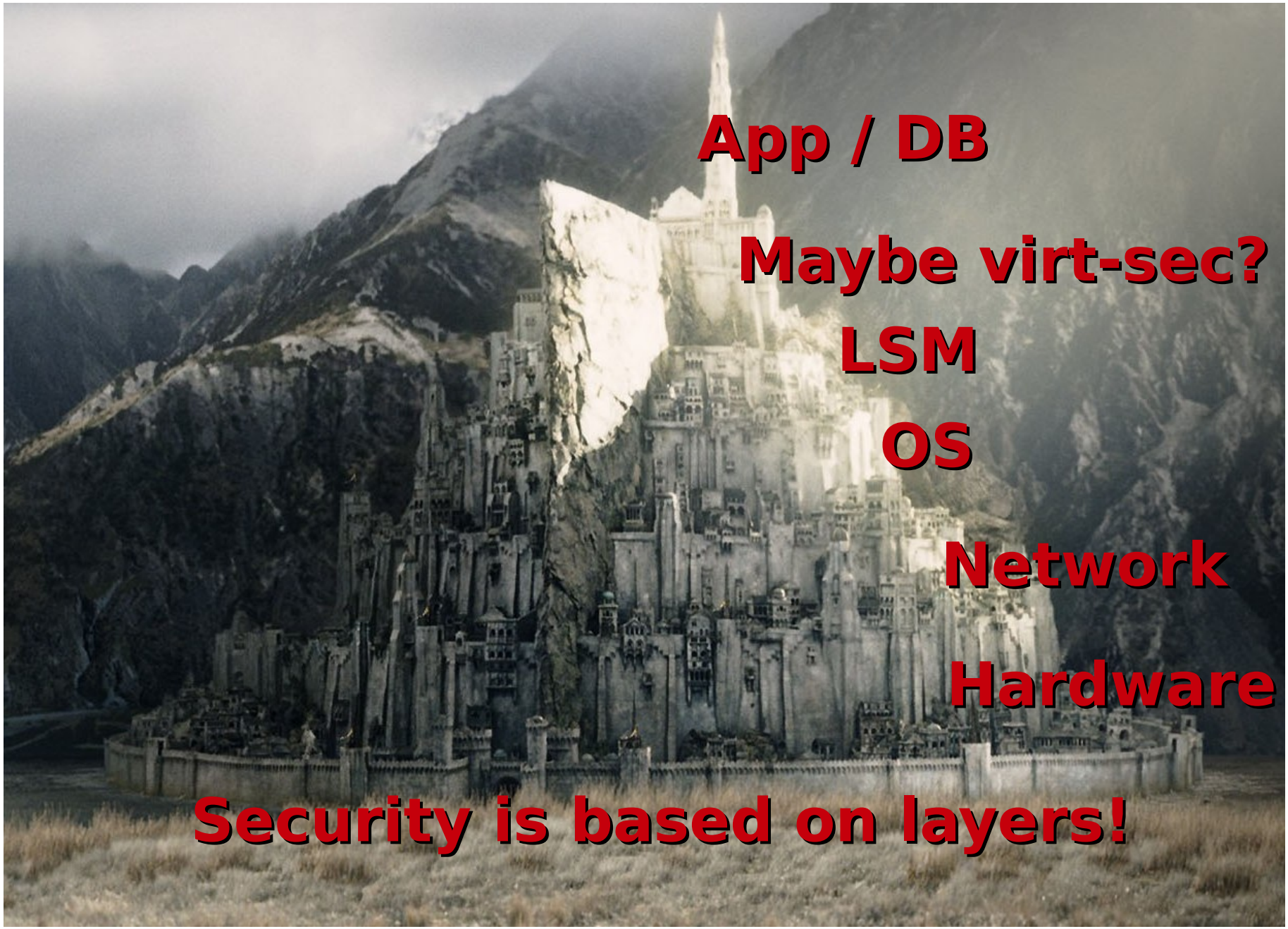
- Business value and security
- Does stock price change after security fail?
- Where to concentrate security – apps or env?

How does security look like?



How does security look like?

How does security look like?



How does security look like?

SELinux – what?

- Think about it as an internal firewall

SELinux – what?

- Think about it as an internal firewall
- Guarding procs, files, users

SELinux – what?

- Think about it as an internal firewall
- Guarding procs, files, users
- Users don't manage security, admin does

SELinux – short history recap

- 2000: NSA, GPL

SELinux – short history recap

- 2000: NSA, GPL

- 2001: Linux Kernel Summit, NSA vs Linus, LSM announced (SELinux, Apparmor, Smack, and TOMOYO Linux)

SELinux – short history recap

- 2000: NSA, GPL

- 2001: Linux Kernel Summit, NSA vs Linus, LSM announced
(SELinux, Apparmor, Smack, and TOMOYO Linux)

- 2003: Merge with mainline Kernel 2.6.0-test3

SELinux – short history recap

- 2000: NSA, GPL

- 2001: Linux Kernel Summit, NSA vs Linus, LSM announced
(SELinux, Apparmor, Smack, and TOMOYO Linux)

- 2003: Merge with mainline Kernel 2.6.0-test3

- RHEL4

SELinux – short history recap

- 2000: NSA, GPL

- 2001: Linux Kernel Summit, NSA vs Linus, LSM announced
(SELinux, Apparmor, Smack, and TOMOYO Linux)

- 2003: Merge with mainline Kernel 2.6.0-test3

- RHEL4

- Ubuntu LTS 8.04 Hardy Heron & rest (even Novell)

SELinux – use cases

- hosting multiple services on one box / vps

SELinux – use cases

- hosting multiple services on one box / vps
- virtualization host (imagine containers)

SELinux – use cases

- hosting multiple services on one box / vps
- virtualization host (imagine containers)
- libvirt-sandbox FTW!

SELinux – use cases

- hosting multiple services on one box / vps
- virtualization host (imagine containers)
- libvirt-sandbox FTW!
- any apps that are not secure or sec – aware

SELinux – use cases

- hosting multiple services on one box / vps
- virtualization host (imagine containers)
- libvirt-sandbox FTW!
- any apps that are not secure or sec – aware
- SELinux sandbox

SELinux – use cases

- hosting multiple services on one box / vps
- virtualization host (imagine containers)
- libvirt-sandbox FTW!
- any apps that are not secure or sec – aware
- SELinux sandbox
- root access for anyone :)

SELinux – use cases

- hosting multiple services on one box / vps
- virtualization host (imagine containers)
- libvirt-sandbox FTW!
- any apps that are not secure or sec – aware
- SELinux sandbox
- root access for anyone :)
    - DBAs, devs - whatever :)

SELinux – use cases

- hosting multiple services on one box / vps
- virtualization host (imagine containers)
- libvirt-sandbox FTW!
- any apps that are not secure or sec – aware
- SELinux sandbox
- root access for anyone :)
    - DBAs, devs - whatever :)
    - try it yourself: http://www.coker.com.au/selinux/play.html

SELinux – use cases

- hosting multiple services on one box / vps
- virtualization host (imagine containers)
- libvirt-sandbox FTW!
- any apps that are not secure or sec – aware
- SELinux sandbox
- root access for anyone :)
    - DBAs, devs - whatever :)
    - try it yourself: http://www.coker.com.au/selinux/play.html
    - Gentoo Hardened: https://wiki.gentoo.org/wiki/Project:Hardened

SELinux – use cases

- hosting multiple services on one box / vps
- virtualization host (imagine containers)
- libvirt-sandbox FTW!
- any apps that are not secure or sec – aware
- SELinux sandbox
- root access for anyone :)
    - DBAs, devs - whatever :)
    - try it yourself: http://www.coker.com.au/selinux/play.html
    - Gentoo Hardened: https://wiki.gentoo.org/wiki/Project:Hardened
- Desktops (yes!)

SELinux – performance

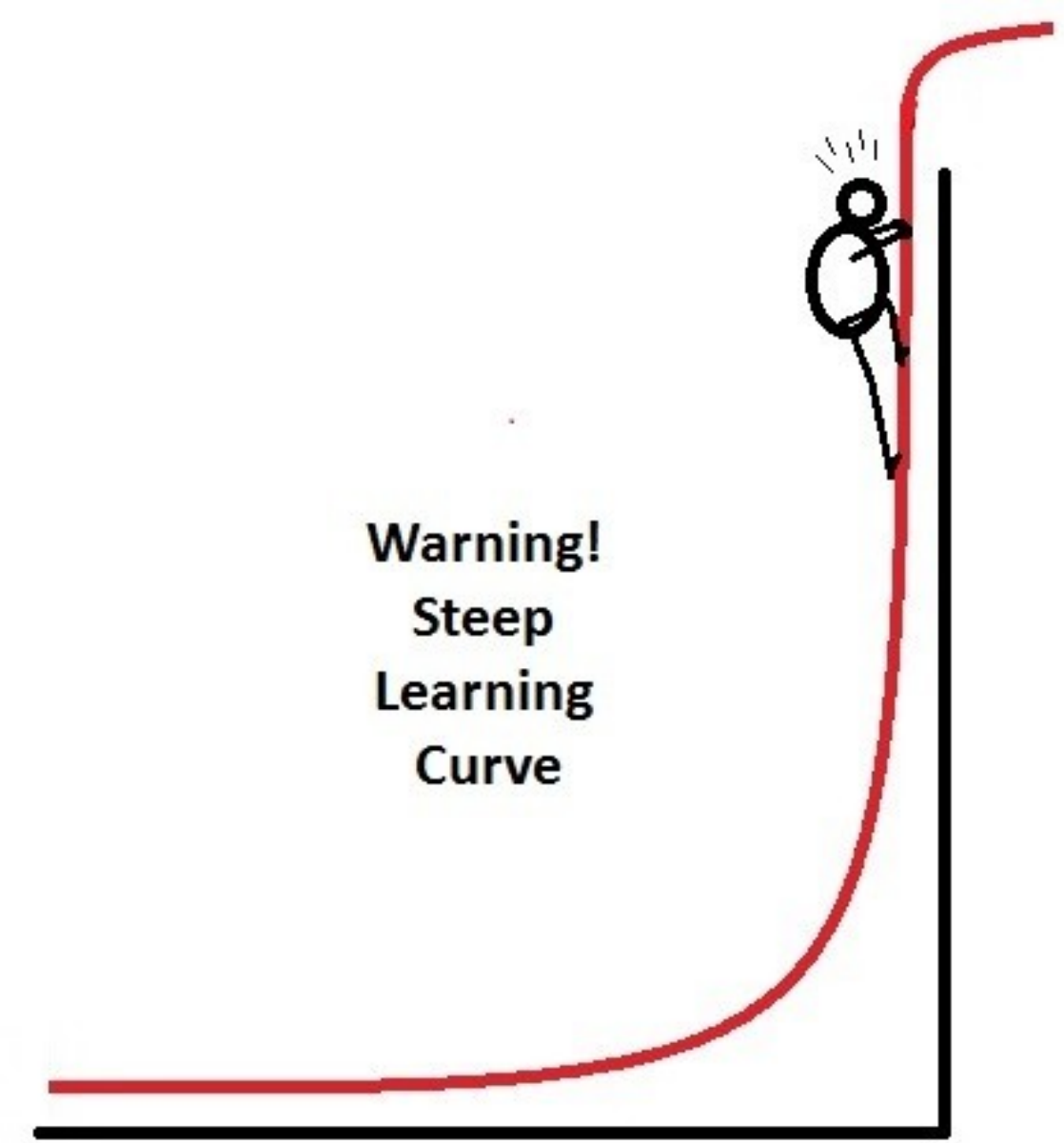
- http://www.nsa.gov/research/_files/selinux/papers/freenix01/node18.shtml#sec:perf:macro

Table: Macrobenchmark results. The elapsed and system times for a ``time make'' on the Linux 2.4.2 kernel sources are shown in minutes and seconds. The latency in seconds and throughput in MBits per second are shown for the WebStone benchmark.

	Base	SELinux	Overhead
elapsed	11:14	11:15	0%
system	00:49	00:51	4%
latency	0.56	0.56	0%
throughput	8.29	8.28	0%

Just test it yourself: git://git.selinuxproject.org/~serge/selinux-testsuite

SELinux – learning curve



SELinux – installation

apt-get install selinux-basics selinux-policy-default auditd

SELinux – installation

apt-get install selinux-basics selinux-policy-default auditd

Gentoo is.. like always – little complicated..

emerge hardened-sources

SELinux – installation

apt-get install selinux-basics selinux-policy-default auditd

Gentoo is.. like always – little complicated..

emerge hardened-sources

EC2? yum install libselinux* selinux-policy* policycoreutils

SELinux – installation

apt-get install selinux-basics selinux-policy-default auditd

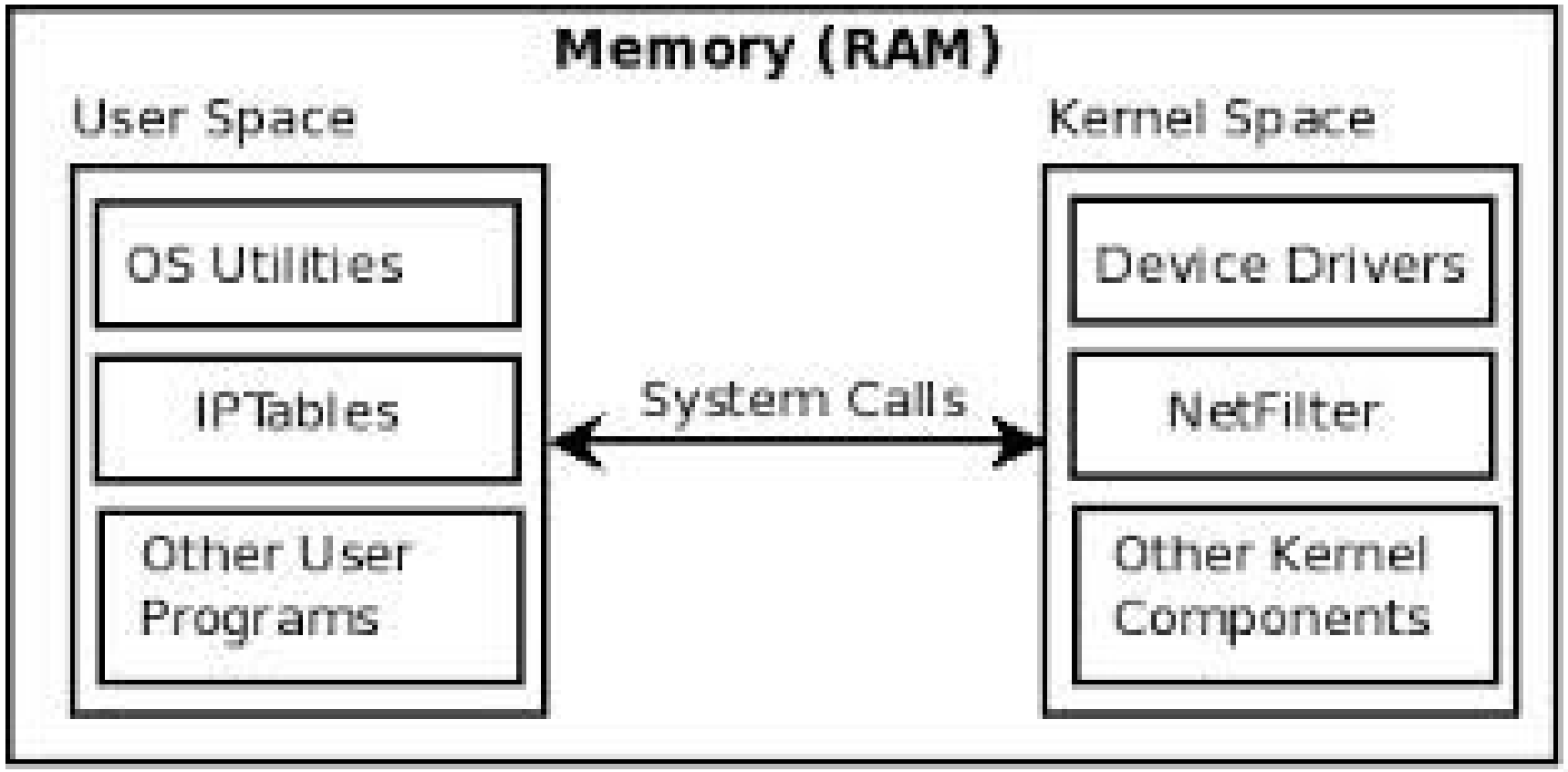
Gentoo is.. like always – little complicated..

emerge hardened-sources

EC2? yum install libselinux* selinux-policy* policycoreutils

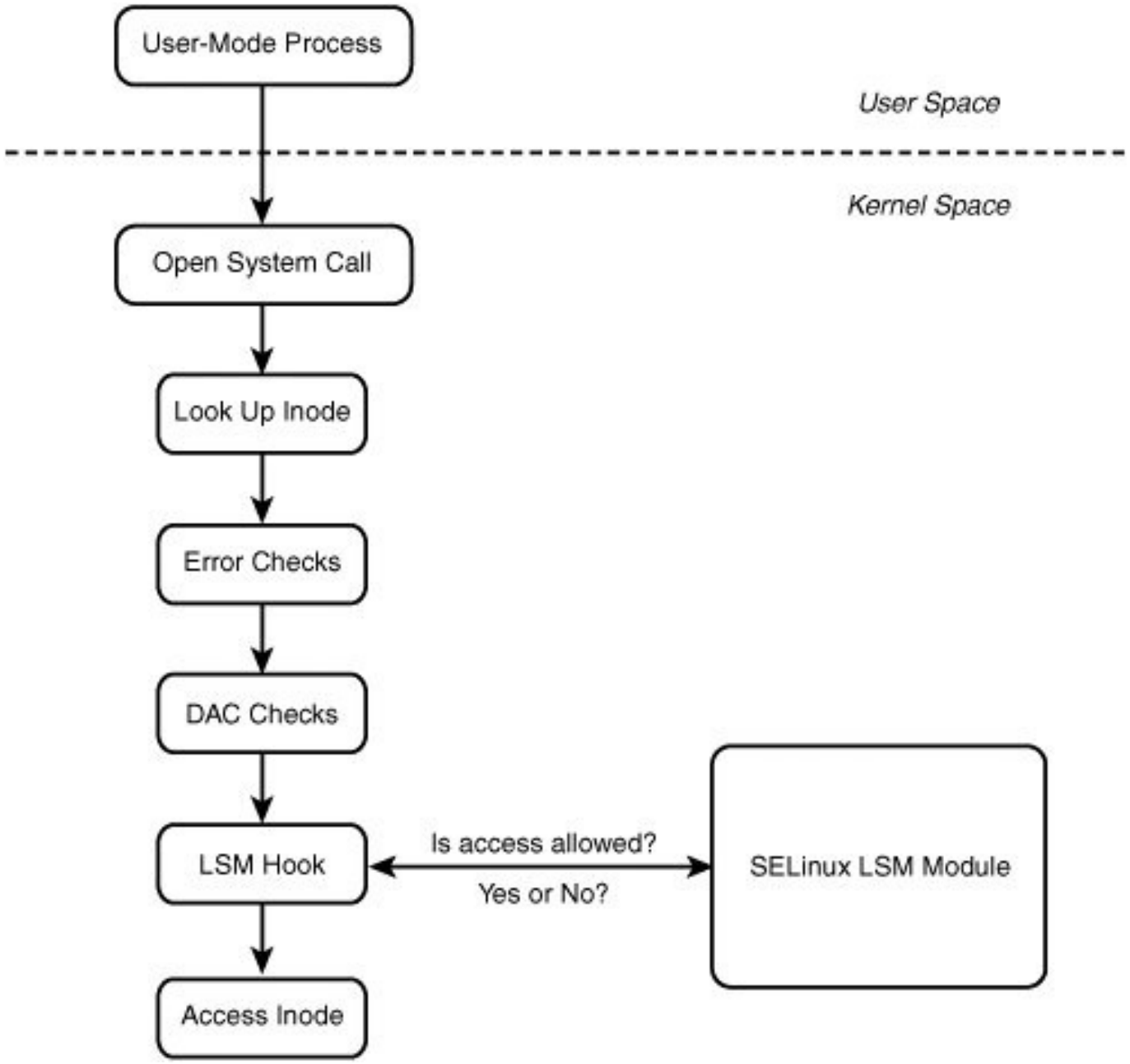
RHEL / CentOS / Fedora is rdy

SELinux – how it works?

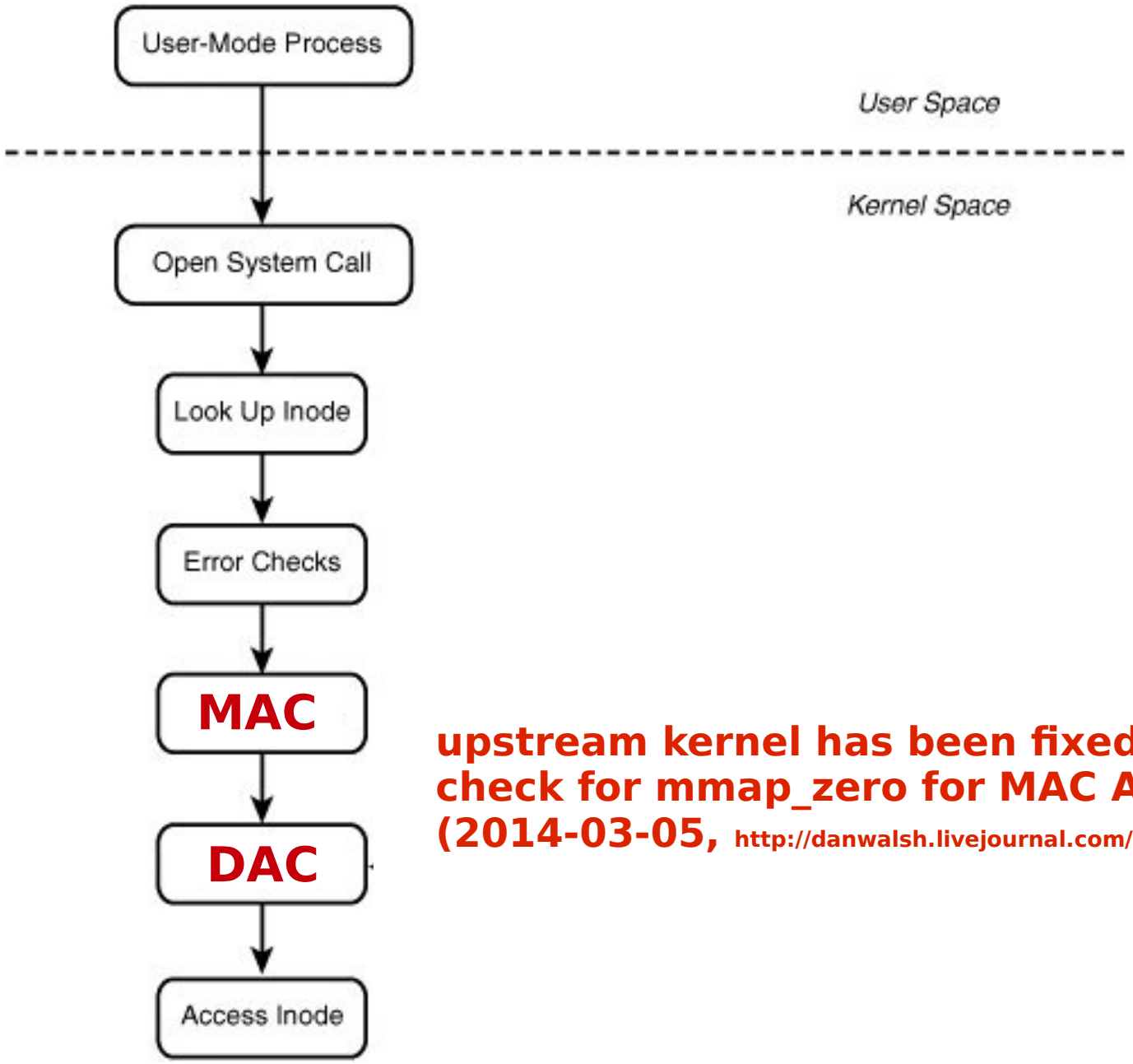


syscalls work like interfaces for accessing some resources

SELinux – how it works?

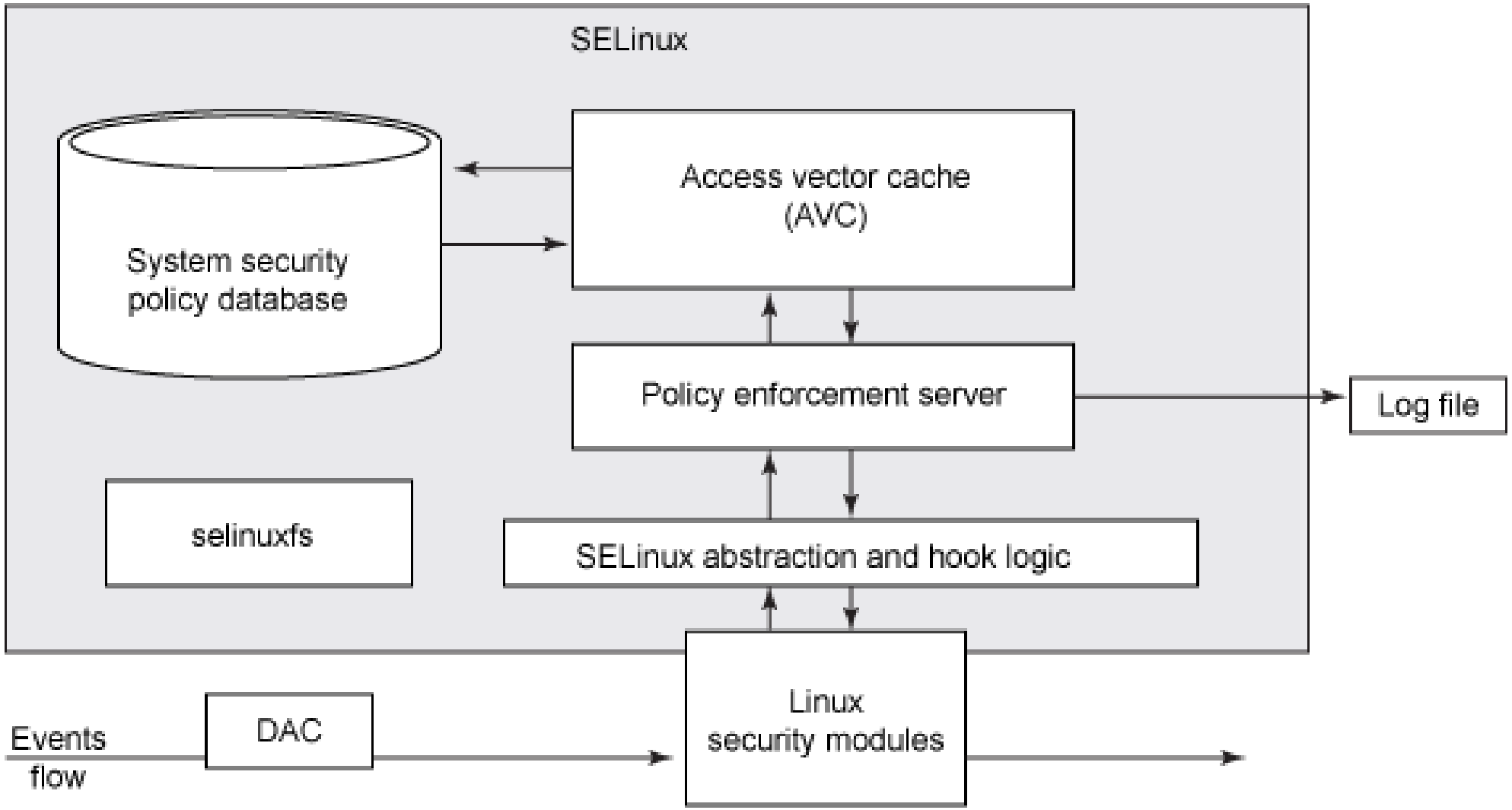


SELinux – how it works?



upstream kernel has been fixed to report check for mmap_zero for MAC AFTER DAC (2014-03-05, http://danwalsh.livejournal.com/69035.html)

SELinux – how it works?



SELinux – need assistance?

- IRC: freenode, #selinux

SELinux – need assistance?

- IRC: freenode, #selinux
- Mailing list: selinux@lists.fedoraproject.org

SELinux – need assistance?

- IRC: freenode, #selinux
- Mailing list: selinux@lists.fedoraproject.org
- URLs:
  - http://stopdisablingselinux.com/
  - http://www.nsa.gov/research/selinux/faqs.shtml
  - https://fedoraproject.org/wiki/SELinux

SELinux – need assistance?

- IRC: freenode, #selinux
- Mailing list: selinux@lists.fedoraproject.org
- URLs:
  - http://stopdisablingselinux.com/
  - http://www.nsa.gov/research/selinux/faqs.shtml
  - https://fedoraproject.org/wiki/SELinux
- Books?
  - SELinux System Administration, Sven Vermeulen, 2013, ISBN-10: 1783283173 ($15)
  - SELinux by Example: Using Security Enhanced Linux, Frank Mayer, Karl MacMillan, David Caplan, 2006, ISBN-10: 0131963694

SELinux and...

SELinux and Android

- from 4.3 – permissive
- from 4.4 enforcing
- Will help us with BYOD :)
- No setuid/setgid programs (4.3)

http://selinuxproject.org/page/SEAndroid

http://source.android.com/devices/tech/security/se-linux.html

libvirt-sandbox!

- Currently RPM based (but could build from sources)

- Sandboxes for LXC / Qemu / KVM

- Rather with systemd

- virt-sandbox -c lxc:/// /bin/sh

- virt-sandbox-service create ... httpd.service myhttpd

- systemctl start myhttpd_sandbox.service

libvirt-sandbox!

- The libvirt guest is created when the virt-sandbox command starts

- The libvirt guest is automatically deleted when the virt-sandbox command completes, or dies from a signal

- The sandboxed command sees a read-only view of the entire host filesystem

- Specific areas can be made writable by mapping in an alternative host directory

- There is no network access inside the sandbox by default

- Virtual network interfaces can be associated with libvirt virtual networks

- The stdin/stdout/stderr file handles of the sandbox command will be connected to the controlling terminal.

So what about other LSMs?

Feature	SELinux	AppArmor	grsecurity
Automated	No (audit2allow and system-config-selinux)	Yes (Yast wizard)	Yes (auto traning / gradm)
Powerful policy setup	Yes (very complex)	Yes	Yes
Default and recommended integration	CentOS / RedHat / Debian	Suse / OpenSuse	Any Linux distribution
Training and vendor support	Yes (Redhat)	Yes (Novell)	No (community forum and lists)
Recommend for	Advanced user	New / advanced user	New users
Feature	Pathname based system does not require labelling or relabelling filesystem	Attaches labels to all files, processes and objects	ACLs

http://www.cyberciti.biz/tips/selinux-vs-apparmor-vs-grsecurity.html

So what about other LSMs?

- AppArmor identifies file system objects by path name instead of inode

- There is no notion of multi-level security with AppArmor

- AppArmor user rather flat files based configuration

- SELinux supports the concept of a "remote policy server"

- There is no apparmor or grsec in android :)

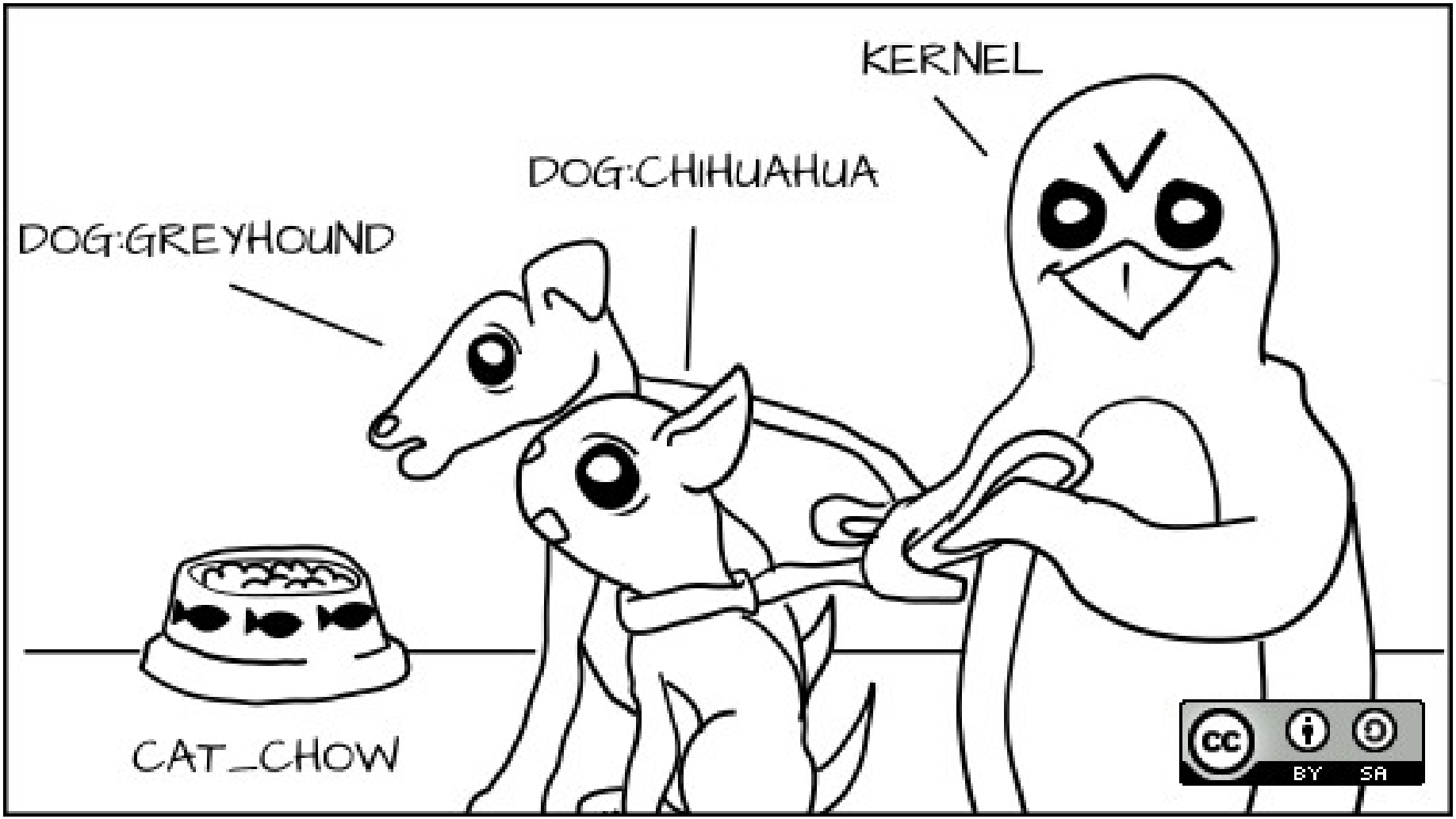
SELinux primer

stopdisablingselinux.com

or

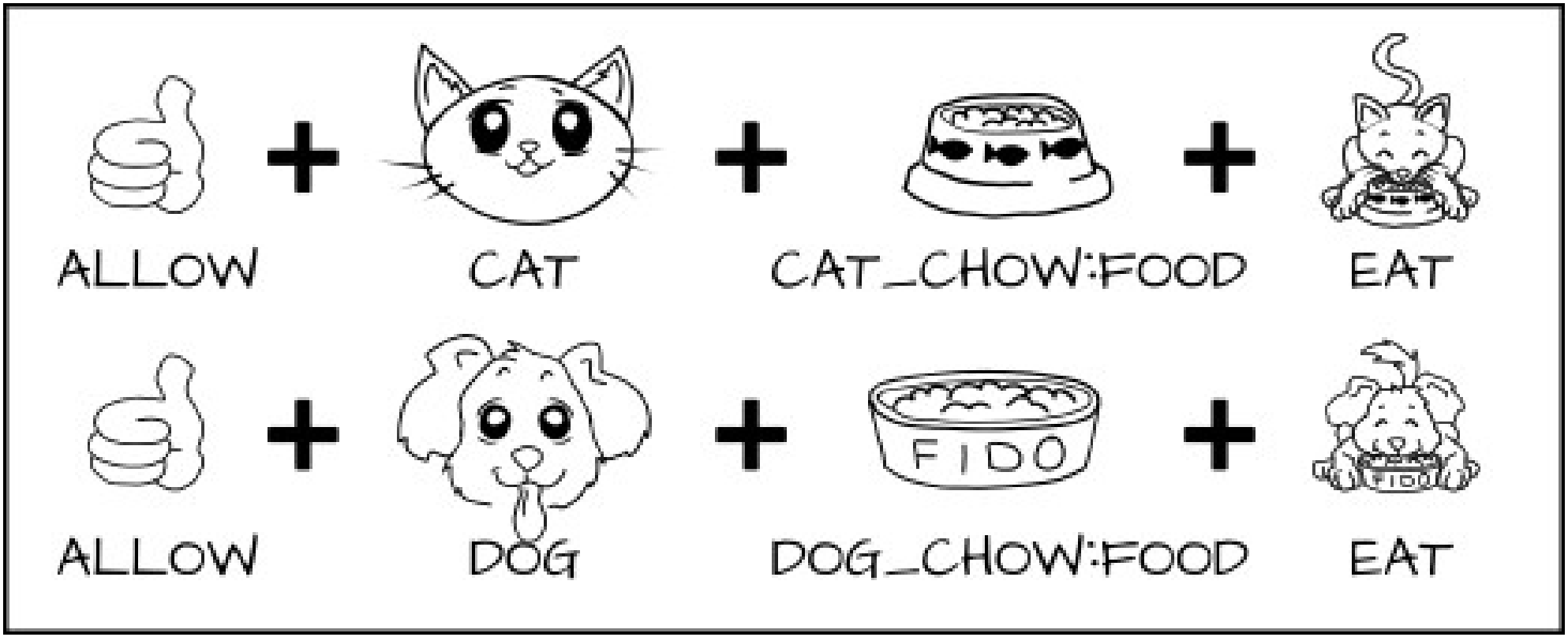
http://opensource.com/business/13/11/selinux-policy-guide

SELinux primer



Everyone gets a label!

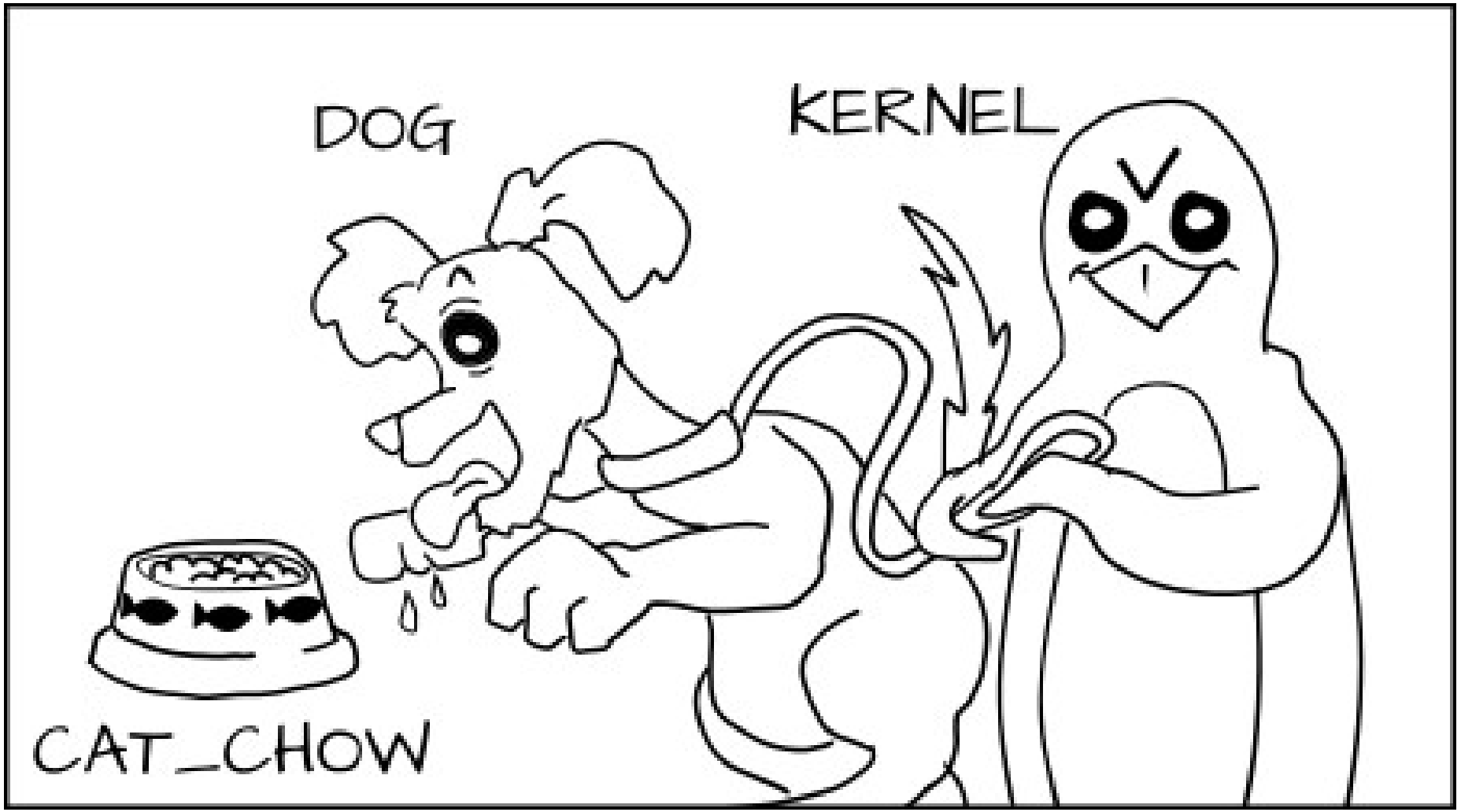
SELinux primer



allow cat cat_chow:food eat;

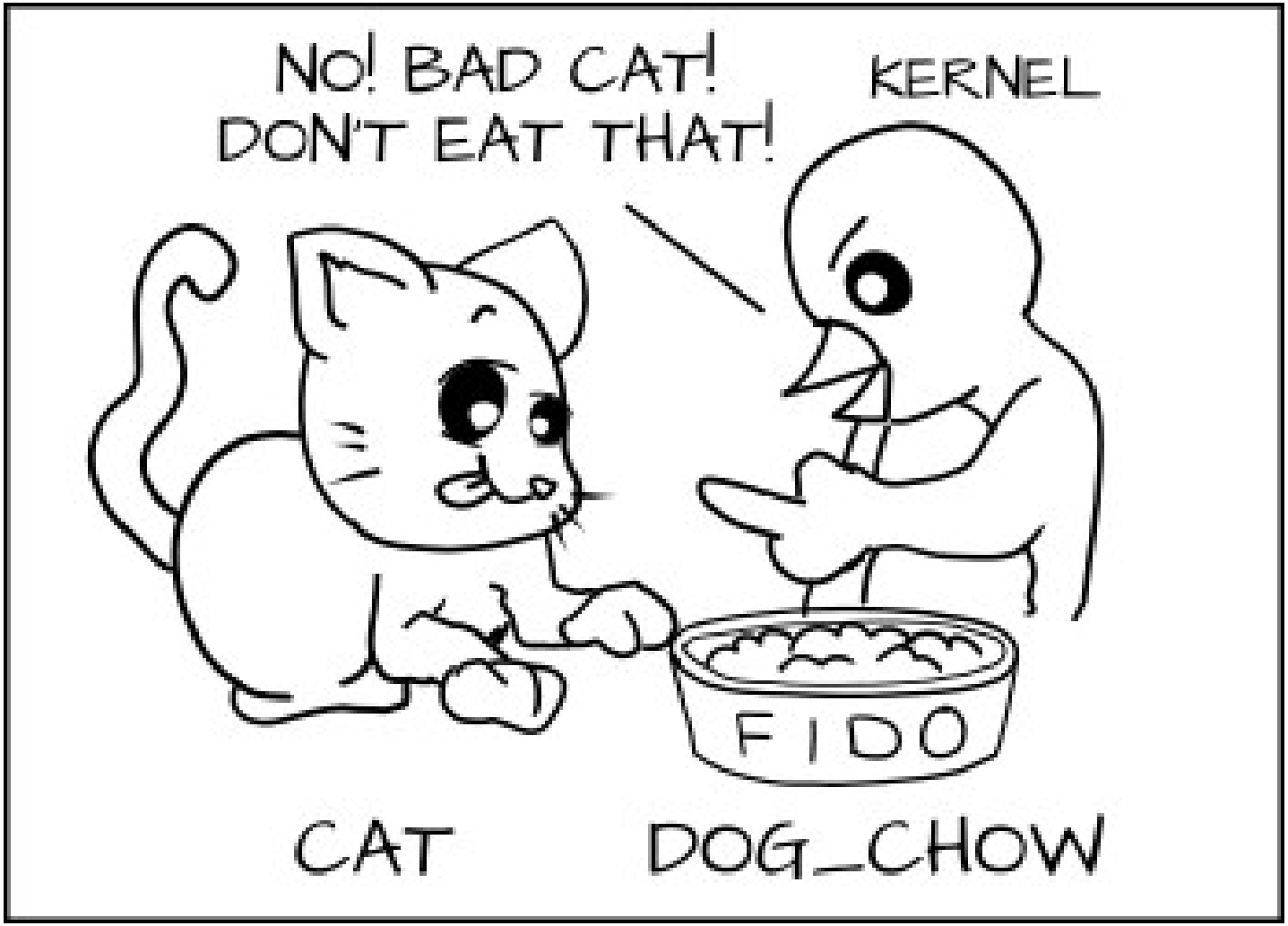
allow dog dog_chow:food eat;

SELinux primer



AVC (Access Vector Cache)

SELinux primer



AVC (Access Vector Cache)

SELinux primer

In real world...

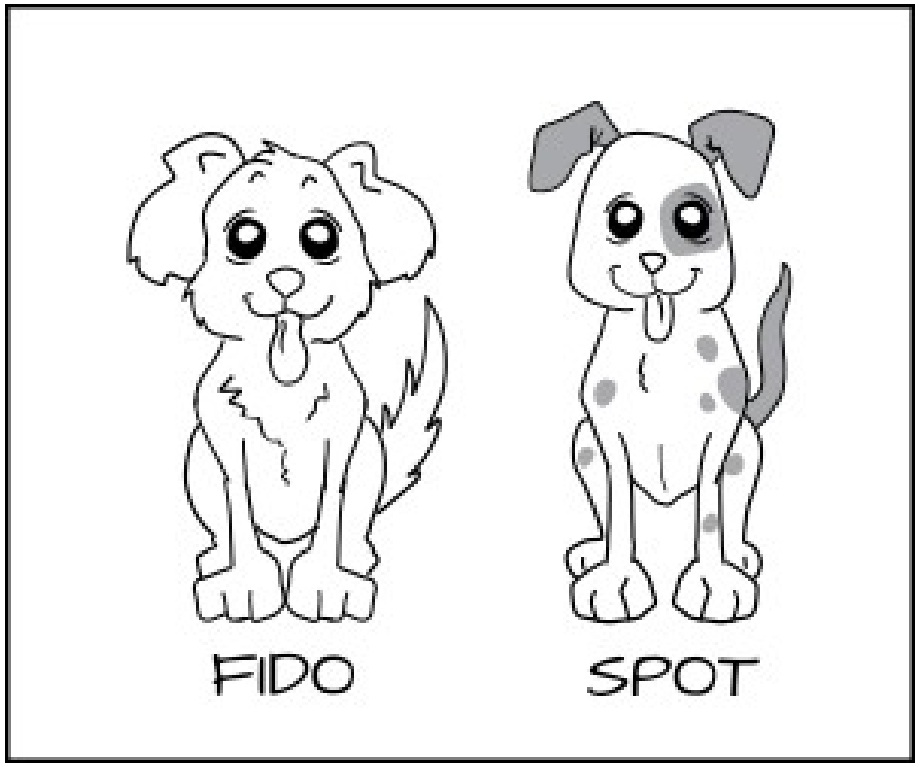
process: httpd_t

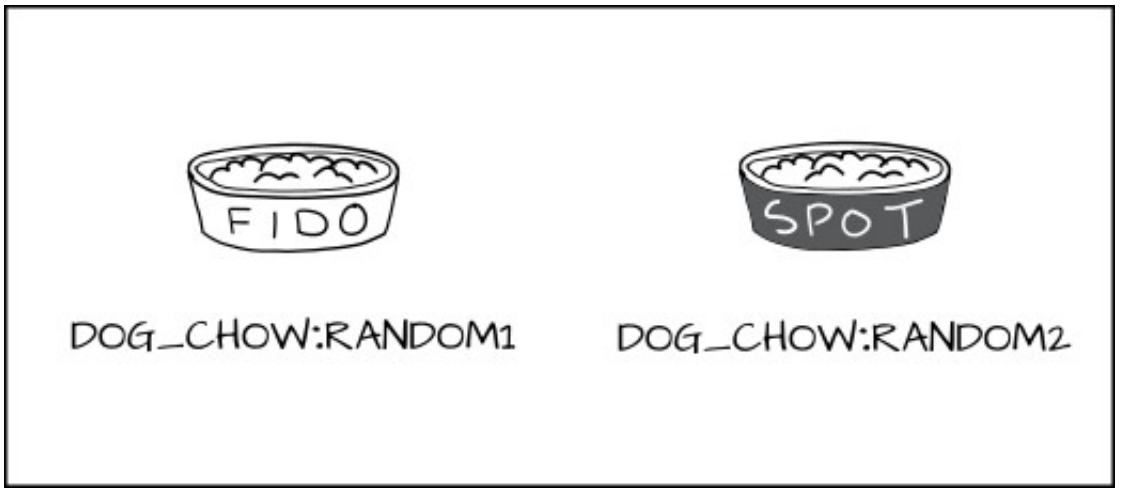
files under Apache: httpd_sys_content_t

database data: mysqld_data_t

hacked Apache process can not access mysqld files!

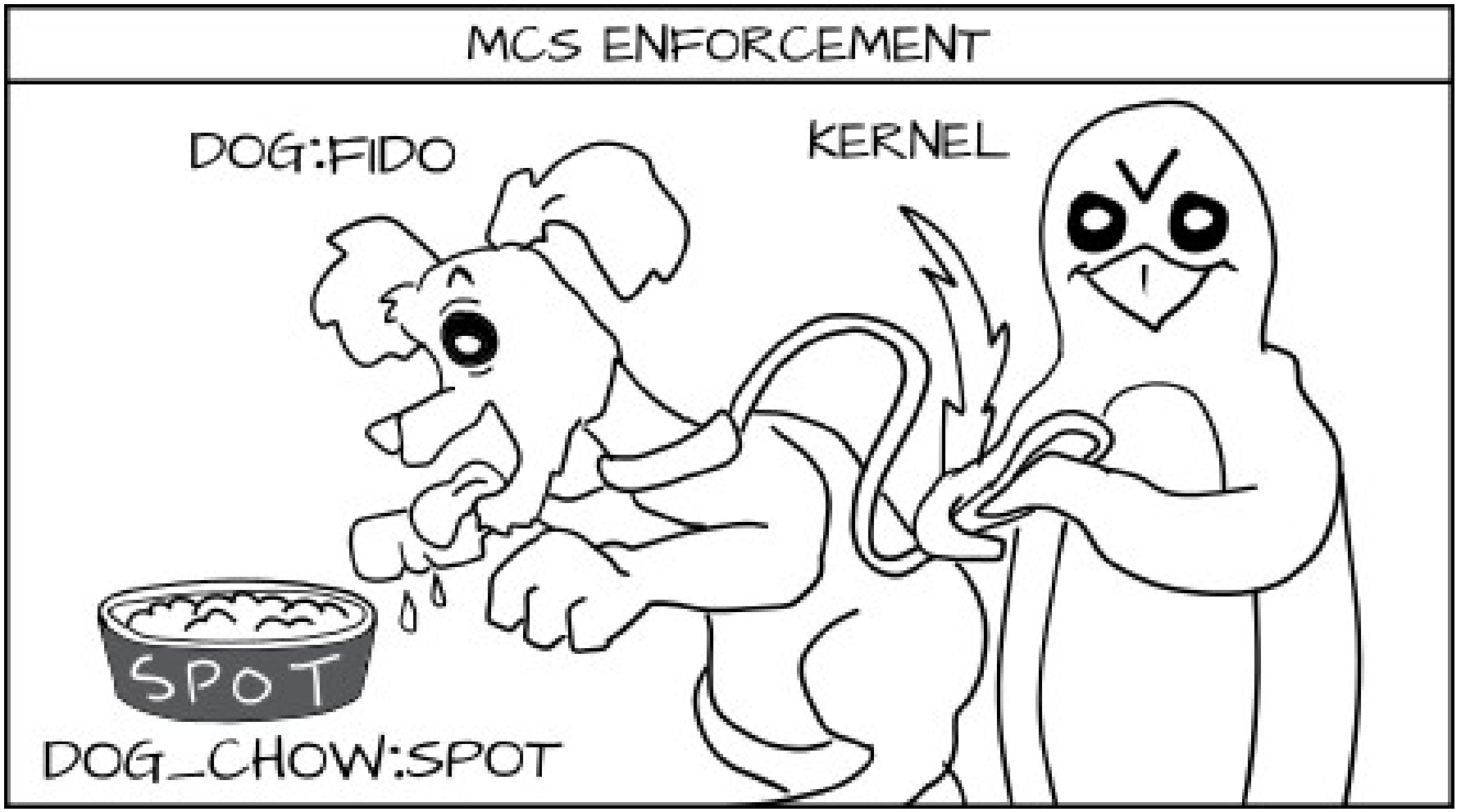
SELinux primer





Can same type of process be confined differently?

SELinux primer



Yes! With MCS enforcement!

SELinux primer

In real world...

2 processes: httpd_t

files under httpd: httpd_sys_content_t

So how to deny files from differ instances of httpd_t?

With MCS labels like s0:c1,c2 ; s0:c3,c4 etc

s0, s1, s2 – sensitivity levels

c1,c2,c3... - categories (up to 255)

So remember..

Every time you run setenforce 0, you make Dan Walsh weep

Dan is a nice guy and he certainly doesn't deserve that.

Thank you :)

Stop Disabling SELinux

Maciej Lasyk

Kraków, InfoSec meetup #1

2014-03-12

http://maciek.lasyk.info/sysop

maciek@lasyk.info

@docent-net