AppArmor crash course

Christian Boltz
openSUSE AppArmor maintainer
AppArmor (utils) developer

cboltz@opensuse.org

What does AppArmor do?

The answer is simple ;-)

- allow applications to do only what they are supposed to do
- deny everything else

It isn't that easy! ;-)

- AppArmor must know what to allow

Why AppArmor?

- Bug-free and secure software would be ideal...

Why AppArmor?

- Bug-free and secure software would be ideal...

- Programmers can't perform magic...

Why AppArmor?

- Bug-free and secure software would be ideal...

- Programmers can't perform magic...

- so better keep an eye on what they are doing!
  - AppArmor monitors applications at the kernel level

Hands up! ;-)

- Who is using AppArmor?
- Who already created or updated a profile with the aa-* tools?
- Who already edited a profile with vi / $EDITOR?
- Cross-check: Who did not use AppArmor yet?

Hello world!

- The unavoidable Hello World...

```
#!/bin/bash
echo "Hello World!" > /tmp/hello.txt
cat /tmp/hello.txt
rm /tmp/hello.txt
```

- now I'll create an AppArmor profile for it...

Hello world!

- The unavoidable Hello World...

```
#!/bin/bash
echo "Hello World!" > /tmp/hello.txt
cat /tmp/hello.txt
rm /tmp/hello.txt
```

- Caution - hacker!

What does AppArmor do?

Monitor and restrict

- file access
- network access
- capabilities (chown, mknod, setuid, ...)
  - man 7 capabilities
- rlimit (aka ulimit)
- ...
- in general: restrict permissions

What DOESN'T AppArmor do?

- replace traditional file permissions
  - “chmod -R 777 /” is not a good idea
- replace user permissions
  - run as little as possible as root

for webservers:

- restrict MySQL database permissions
  - one MySQL user per hosting and task
- validate user input
  - validate input
  - escape input
  - php5-suhosin

Is my server secure now?

- Security consists of lots of small parts
- AppArmor protects you from lots of (but not all) exploits

- The server is definitely more secure than without AppArmor ;-)

aa-<tab><tab>: The AppArmor tools (I)

aa-status

  overview of loaded profiles and their usage

aa-unconfined

  overview of protected/confined applications

aa-notify

  provides desktop notifications and log summaries

aa-<tab><tab>: The AppArmor tools (II)

aa-complain

switch profile to complain (learning) mode (allow everything, log what would be denied)

aa-enforce

switch profile to enforce mode (deny everything not explicitely allowed and log denials)

aa-disable

disable and unload profile

aa-audit

set or remove audit flag for a profile (log everything)

aa-<tab><tab>: The AppArmor tools (III)

aa-logprof

update existing profiles based on logfile

aa-genprof

create a new profile

aa-autodep

create a very basic new profile
(better use aa-genprof!)

aa-easyprof

template-based profile generation

aa-<tab><tab>: The AppArmor tools (IV)

aa-mergeprof

merge two profiles into one

aa-cleanprof

cleanup profile, remove superfluous rules

aa-decode

translate log entries for filenames with special chars to human-readable

aa-exec

execute a binary with the specified profile

aa-unconfined: check the status

```
# aa-unconfined
1552 /usr/lib/postfix/smtpd confined by
'/usr/lib/postfix/smtpd (enforce)'
2879 /usr/sbin/avahi-daemon confined by
'/usr/sbin/avahi-daemon (enforce)'
2955 /usr/sbin/clamd confined by
'/usr/sbin/clamd (enforce)'
3541 /usr/bin/perl (amavisd (master))
confined by '/usr/sbin/amavisd (complain)'
3839 /usr/sbin/vsftpd not confined
...
```

aa-unconfined: check the status

General rule of thumb: all daemons that are accessible from the internet should be protected

```
3839 /usr/sbin/vsftpd not confined
```

It's time to fix this!

aa-genprof: create a profile

Use two xterms:

- first xterm: aa-genprof /usr/sbin/vsftpd
- second xterm: use the application

Tactics for creating the profile:

- rcvsftpd start / stop
  - gets the basics and keeps the log small
- use the application
- when finished, you might want to run the profile in complain mode for some time
  - especially when it comes to complex applications
  - use aa-logprof to update the profile

File permissions

r – read

w – write

a – append

l - link

k - lock

m – mmap (for libraries), typically also requires r

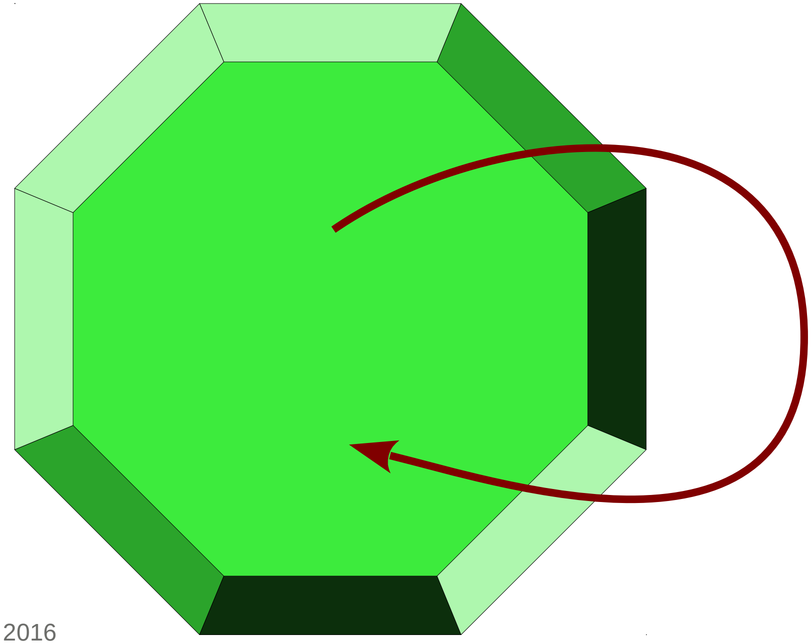
ix, Px, Cx, Ux, … - execute

```
/etc/vsftpd.conf r,
/srv/www/** rwk,
```

Execute options: ix

inherit (ix)

- run program with the same profile
- for helper applications and shells (cat, grep, rm, bash)
- also useful for rbac style confinement

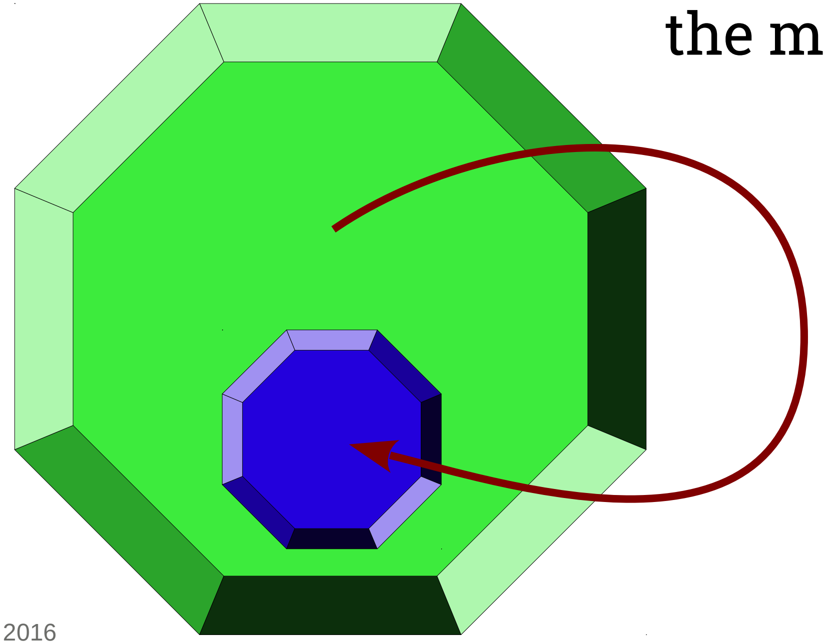


/bin/grep ix,

Execute options: Cx

child (Cx)

- used for “foo called by bar”
- doesn't confine standalone calls of foo
- for helpers that need more or less permissions than the main application

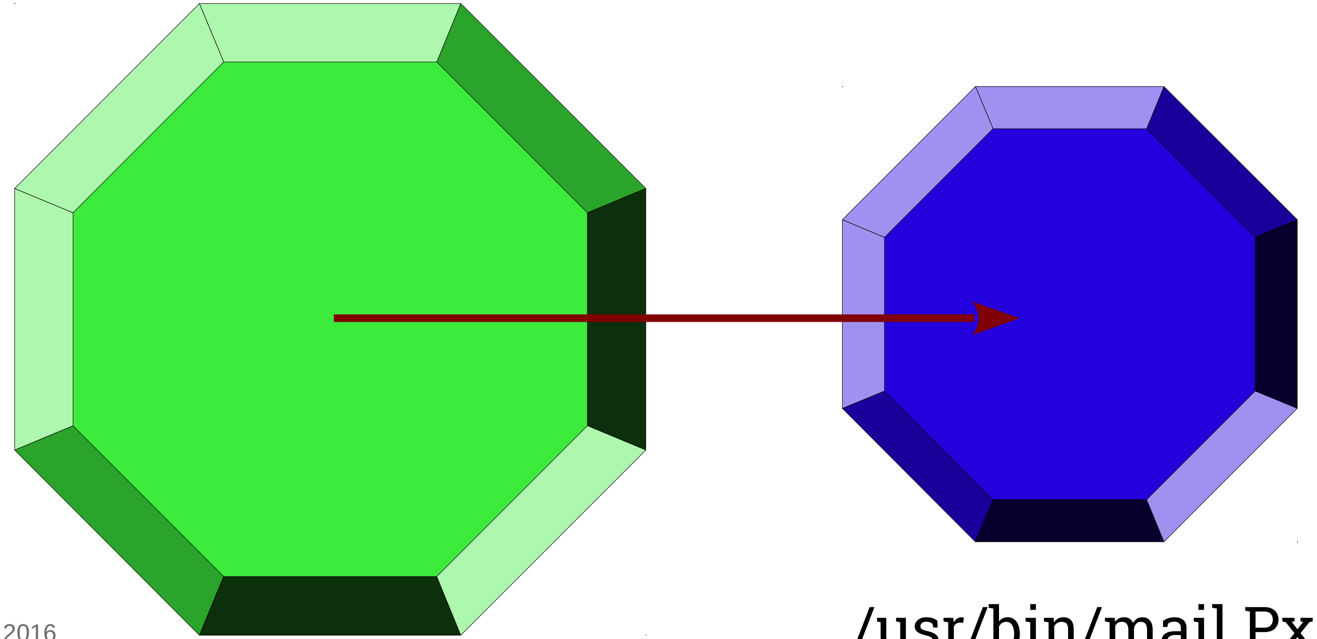


/bin/bash Cx,

Execute options: Px

profile (Px)

- separate profile for helpers
- also used if the helper is called standalone
- not a good idea for /bin/bash ;-)

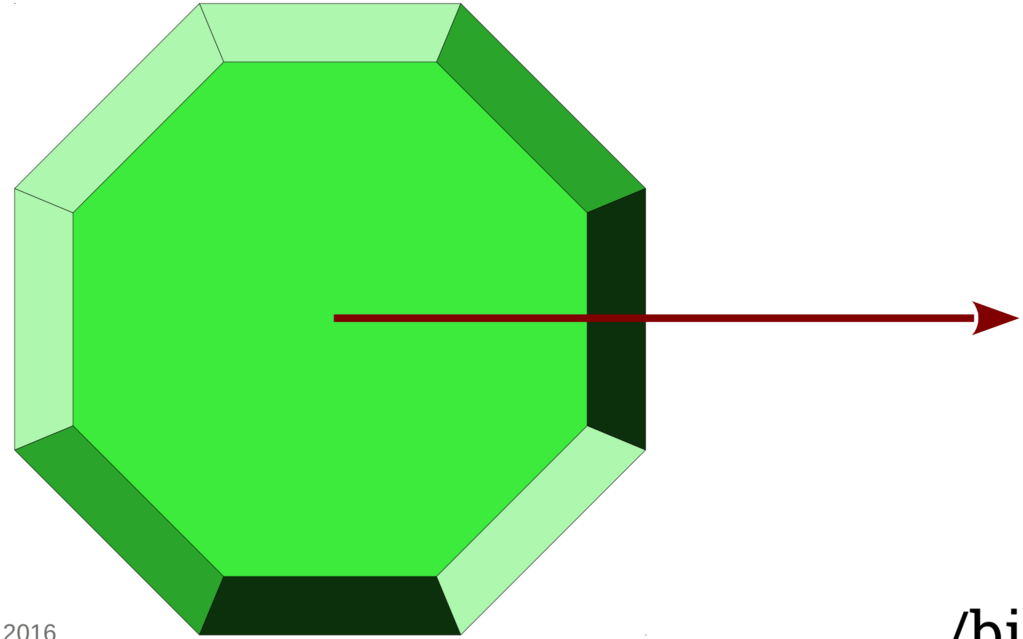


/usr/bin/mail Px,

Execute options: Ux

unconfined (Ux)

- execute helper applications without AppArmor protection
- example: protect sshd, unrestricted shell after login

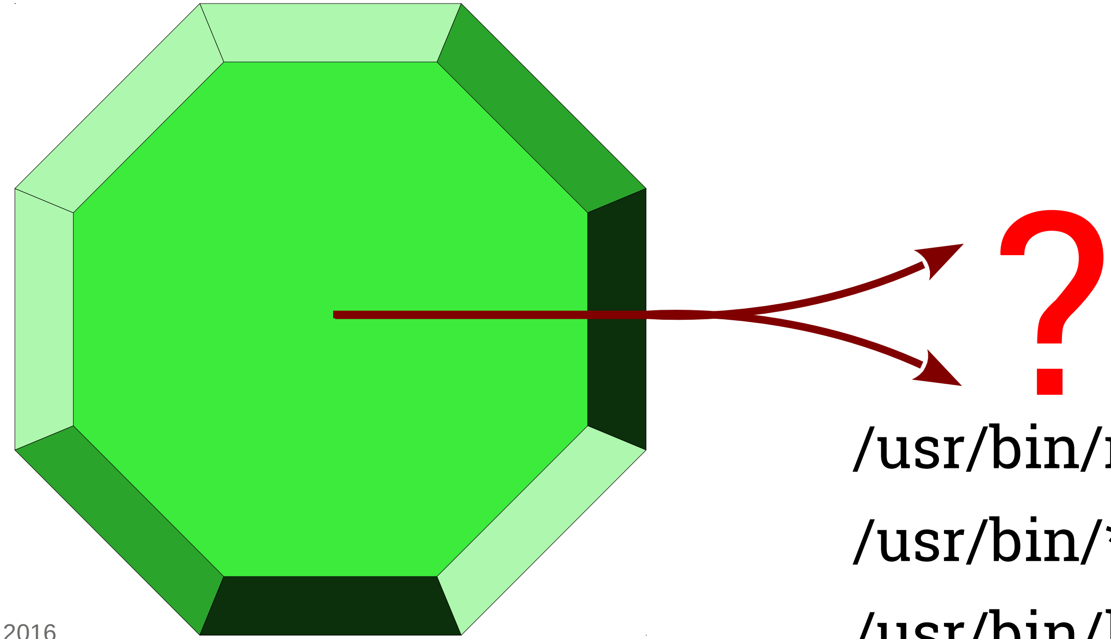


/bin/bash Ux,

Execute options

Fallback rules if a profile doesn't exist

- Pix
- PUx
- Cix
- CUx



```
/usr/bin/mail Pix,
/usr/bin/* Cix,
/usr/bin/lpr PUx,
```

Execute options

named profile (Cx -> ..., Px -> ...)

- allows specifying the target profile
- multiple helper applications can use a common abstract profile

```
profile ping /{usr/,}bin/ping {
   # ...
}
```

```
/bin/ping Px -> ping,
/usr/bin/* Cx -> helpers,
```

Execute options

Cleanup the environment?

- In general: yes
  Rules: Cx, Px, Ux (uppercase)
- In exceptional cases keep all environment variables
  Rules: cx, px, ux (lowercase)

Other rules

- link (see also: file rules)
- set rlimit
- capability – see capabilities(7)
- network
- dbus
- mount
- signal
- ptrace
- pivot_root
- unix

require kernel patches
(Ubuntu contains all patches,
openSUSE supports network)

Details: apparmor.d(5)

audit.log

```
type=AVC msg=audit(1438886688.987:169160):
apparmor="DENIED" […]
```

- add /var/log/audit/audit.log to logdigest
  (or let cron mail you the aa-notify summary)
- “translate” the timestamp:
  date -d @1438886688.987

- DENIED – (blocked) violations of profiles
  in enforce mode
- AUDIT – logging of audit rules
- ALLOWED – profiles in complain mode

Apache mod_apparmor

- global configuration:

```
AADefaultHatName default_vhost
```

  - otherwise AppArmor proposes a hat per file (!)

- per VirtualHost:

```
<VirtualHost 1.2.3.4>
    AADefaultHatName vhost_someone
```

  - restricts each virtual host to itself

- for specific directories:

```
<Directory /some/where>
    AAHatName something
```

  - recommended if multiple different software (CMS, Forum, ...) is used in one virtual host

Hats?

- Hats are similar to subprofiles
- An application can switch between them (change_hat)
- My typical usecase: Apache with a hat per virtual host
- Syntax inside a profile:

```
^hatname {
  ...
}
```

mod_apparmor base configuration

/etc/apparmor.d/abstractions/vhost_cboltz:

```
#include <abstractions/apache2-common>

/home/www/cboltz.de/conf/htpass-webstat r,
/home/www/cboltz.de/httpdocs/** r,
/home/www/cboltz.de/statistics/logs/access_log w,
/home/www/cboltz.de/statistics/logs/access_log-20?????? w,
/home/www/cboltz.de/statistics/logs/error_log w,
/home/www/cboltz.de/statistics/logs/error_log-20?????? w,
/home/www/cboltz.de/statistics/zugriffe/* r,
/home/www/cboltz.de/tmp/ r,
/home/www/cboltz.de/tmp/** rwk,
/usr/share/zoneinfo/ r,
```

mod_apparmor specialities

- Generate abstractions/vhost_someone automatically
  - saves lots of time compared with manually creating a profile/hat per virtual host
- ^HANDLING_UNTRUSTED_INPUT tends to do more than planned
  - this hat wants write access to the access_logs and error_logs of all virtual hosts
- “Tightness” of the profile is relevant
  - real world example: a forum allowed to upload avatar photos – including *.php...
- “deny owner /**.php rw” can protect against freshly uploaded exploits, but also blocks valid scripts if owned by wwwrun, and self-updating web applications

Creative usage of AppArmor

- AppArmor as inventory list:
  - which vHost uses which scripts in the server-wide shared directory?
  - which vHost sends mails? (by calling sendmail)
  - ...
- AppArmor as debugging tool:
  - which files does application foo read?
  - just let aa-genprof create a summary ;-)
- AppArmor as load monitor
  - “ps Zaux” shows which vHost is using/blocking an apache process
- read-only root access for backups

Backup: read-only for root

Two component solution:

- SSH key in /root/.ssh/authorized_keys:
  command="/root/bin/rsync-shell" ssh-dss 7j1ntgRx...
- /root/bin/rsync-shell:

```
#!/bin/bash
echo "cmd=$SSH_ORIGINAL_COMMAND" |
    logger -t rsync-backup
echo "$SSH_ORIGINAL_COMMAND" |
    grep "^rsync --server --sender" \
    >/dev/null \
    && exec $SSH_ORIGINAL_COMMAND
```

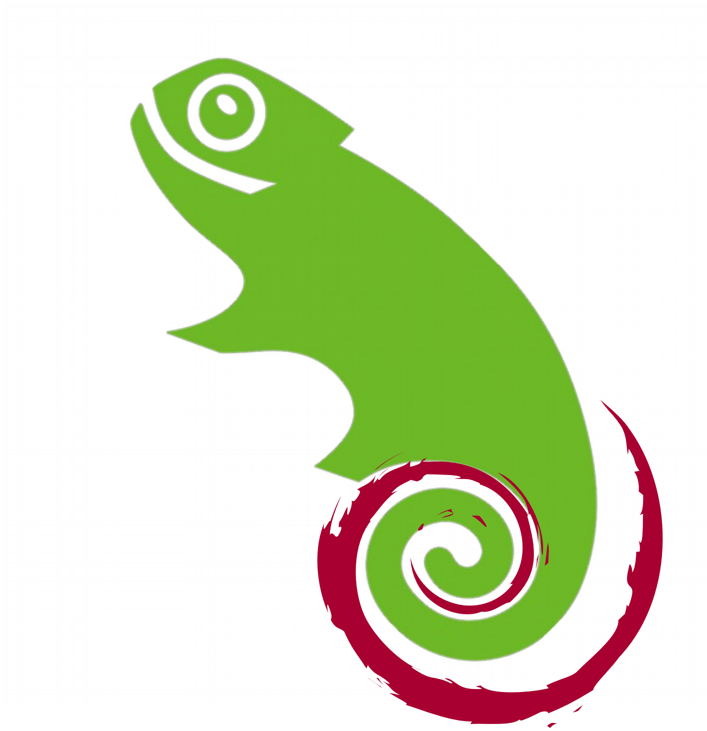
Backup: read-only for root

- The corresponding AppArmor profile (slightly shortened):

```
/root/bin/rsync-shell {
  #include <abstractions/base>
  #include <abstractions/bash>
  #include <abstractions/consoles>
  #include <abstractions/nameservice>
  capability dac_override,
  capability dac_read_search,
  /bin/bash rix,                       /etc/ r,
  /bin/grep rix,                       /etc/** r,
  /bin/logger Px,                      /home/ r,
  /root/bin/rsync-shell mr,            /home/** r,
  /usr/bin/rsync rix,
}
```

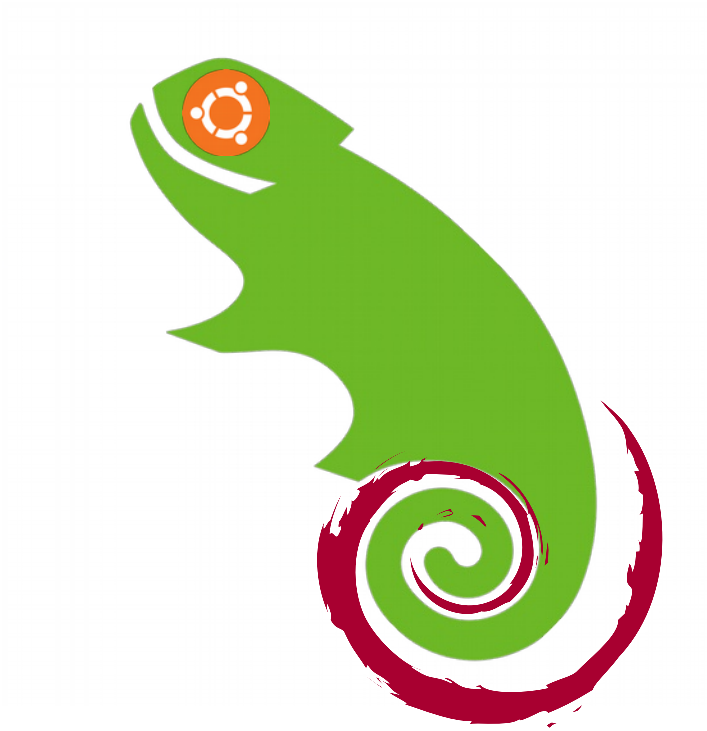
Any relation between Debian and openSUSE?

Depends on how you turn it ;-) *



* does not comply with the logo guidelines ;-)

Depends on how you turn it ;-) *



* does not comply with the logo guidelines ;-)

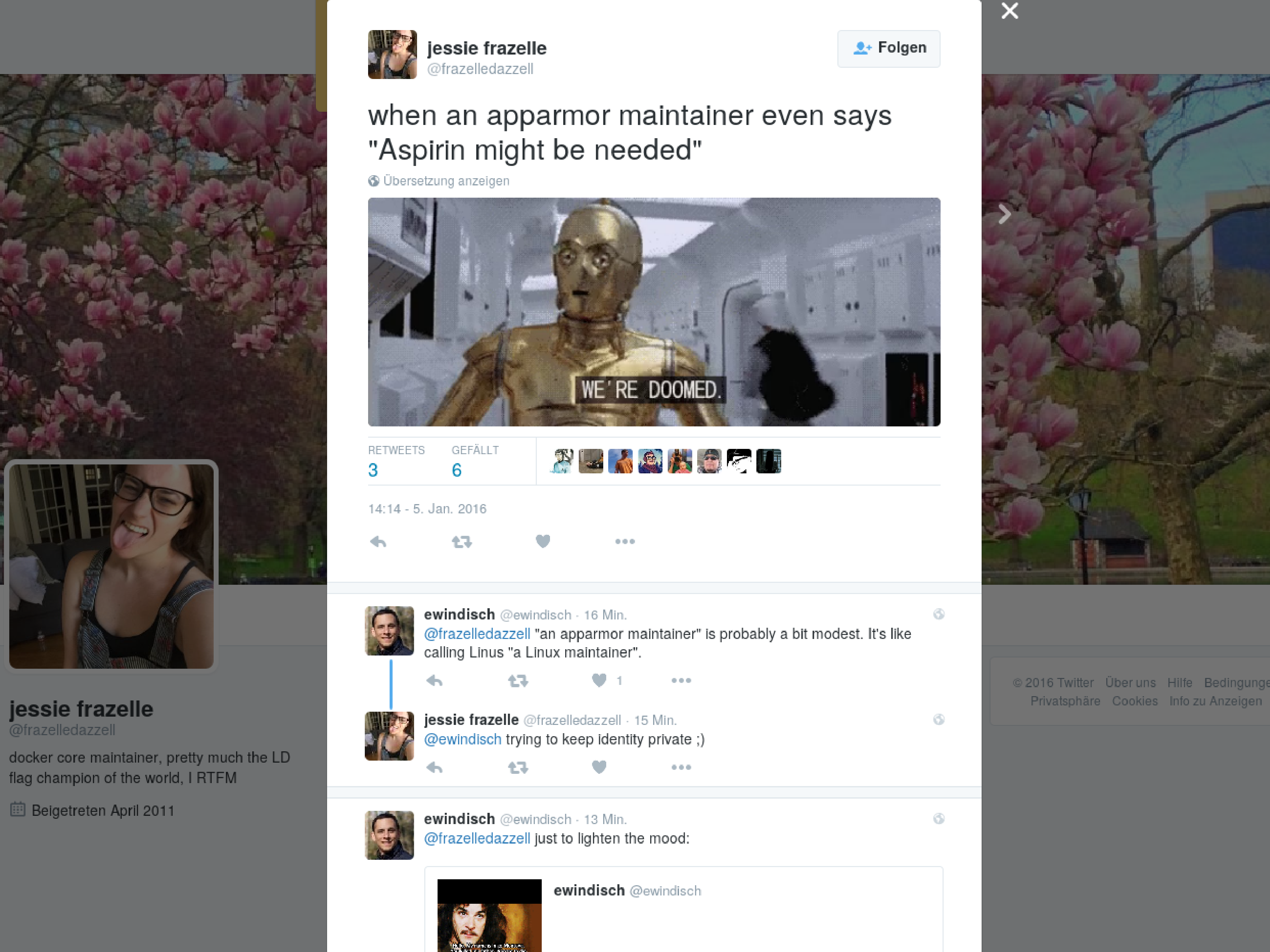
How to make things interesting[tm]

```
file,

deny @{PROC}/* w,



deny
  @{PROC}/{[^1-9],[^1-9][^0-9],[^1-9s][^0-9y][^0-9s],[^1-9][^0-9][^0-9][^0-9]*}/** w,

deny @{PROC}/sys/[^k]** w,

deny @{PROC}/sys/kernel/{?,??,[^s][^h][^m]**} w,
```

How to make things interesting[tm]

```
# allow access to all files (mrwlkix mode)
file,  # <---- bad idea!

# deny write for all files directly in /proc/ (not in a subdir)
deny @{PROC}/* w,

# deny write to files not in /proc/<number>/** or /proc/sys/**
# (/proc/sys/kernel/shm* is what would really be needed, but that
# would be a monster regex)
deny
  @{PROC}/{[^1-9],[^1-9][^0-9],[^1-9s][^0-9y][^0-9s],[^1-9][^0-9][^0-9][^0-9]*}/** w,

# deny /proc/sys/ except /proc/sys/k* (effectively /proc/sys/kernel)
deny @{PROC}/sys/[^k]** w,

# deny everything except shm* in /proc/sys/kernel/
deny @{PROC}/sys/kernel/{?,??,[^s][^h][^m]**} w,
```

(unfortunately a real-world example!)



jessie frazelle @frazelledazzell

when an apparmor maintainer even says "Aspirin might be needed"

RETWEETS 3 GEFÄLLT 6

14:14 - 5. Jan. 2016

ewindisch @ewindisch · 16 Min.
@frazelledazzell "an apparmor maintainer" is probably a bit modest. It's like calling Linus "a Linux maintainer".

1

jessie frazelle @frazelledazzell · 15 Min.
@ewindisch trying to keep identity private ;)

ewindisch @ewindisch · 13 Min.
@frazelledazzell just to lighten the mood:

ewindisch @ewindisch

jessie frazelle
@frazelledazzell

docker core maintainer, pretty much the LD flag champion of the world, I RTFM

Beigetreten April 2011

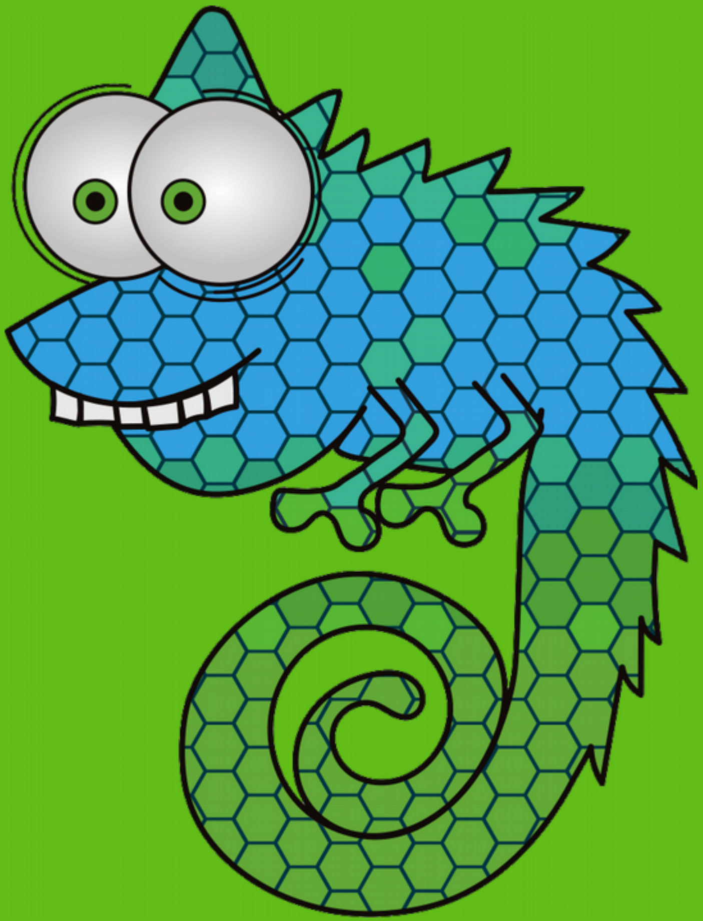
© 2016 Twitter Über uns Hilfe Bedingunge
Privatsphäre Cookies Info zu Anzeigen

More information…

- apparmor.d(5)
- http://apparmor.net/
- http://en.opensuse.org/SDB:AppArmor
- https://wiki.debian.org/AppArmor
- https://wiki.ubuntu.com/AppArmor
- http://doc.opensuse.org/
  → Security Guide → AppArmor

- #apparmor on OFTC
- upstream: apparmor@lists.ubuntu.com
- Debian: pkg-apparmor-team@lists.alioth.debian.org

Questions?



License

Pictures taken from:

www.flickr.com/photos/carbonnyc/2294144289/
www.landjugend-rheinhessenpfalz.de/theater-berlin.html
www.flickr.com/photos/polaroidmemories/2626967595/
www.oldskoolman.de/bilder/technik_und_bau/werkzeug-baumaterial/axt-klotz/
www.manufactum.de/Produkt/0/1443290/NistkastenWolfgangS.html
www.flickr.com/photos/vrogy/514733529/
www.flickr.com/photos/ida-und-bent/248684278/
www.flickr.com/photos/kosin-germany/2898566898/
www.flickr.com/photos/78428166@N00/5895968782/
www.flickr.com/photos/gotshoo/2336903636/