AppArmor crash course and workshop

Christian Boltz
openSUSE community
openSUSE AppArmor maintainer

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 Yast or 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:

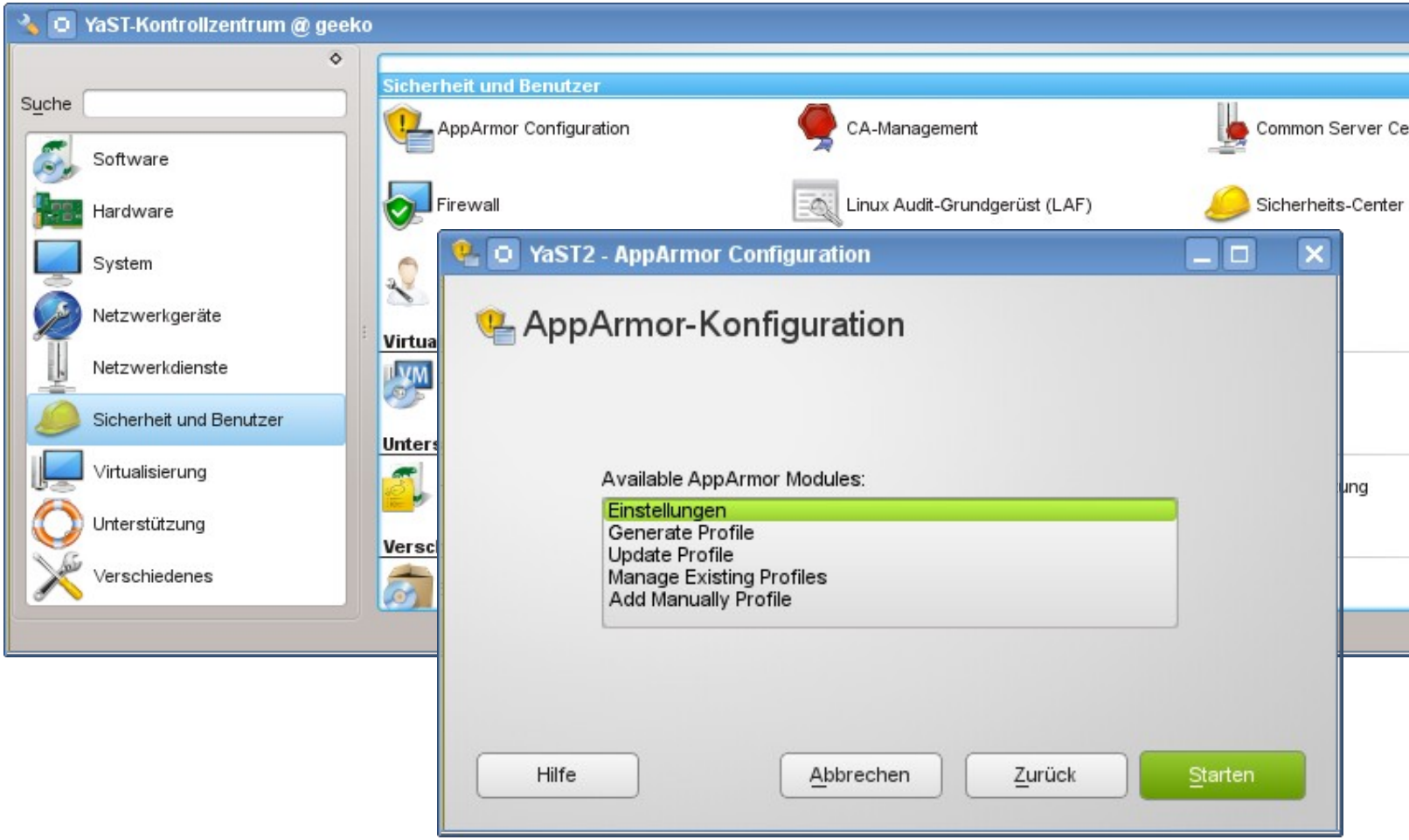
- restrict MySQL database permissions
  - one MySQL user per hosting and task
- validate user input
  - validate input
  - escape input
  - php5-suhosin

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 ;-)

YaST AppArmor module



aa-<tab><tab>: The AppArmor tools

- aa-unconfined
  - overview of protected/confined applications
- aa-genprof
  - create a new profile
- aa-logprof
  - modify an existing profile
- aa-complain
  - switch profile to learning (complain) mode
  - policy violations are logged, but not blocked
- aa-enforce
  - switch profile to enforce mode
  - policy violations are blocked (and logged)
- aa-notify

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 accessable 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:

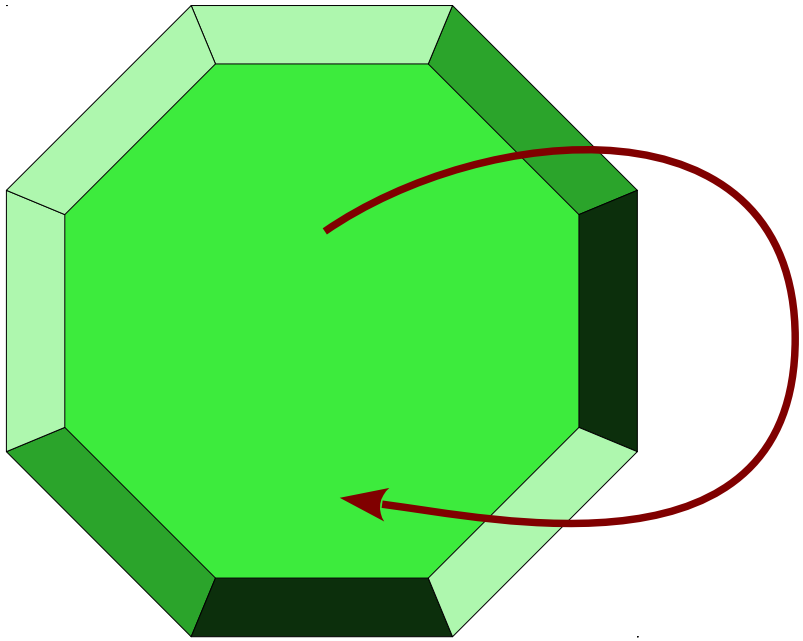
- first xterm: aa-genprof /usr/sbin/vsftpd
- second xterm: use the application

Tactics for creating the profile:

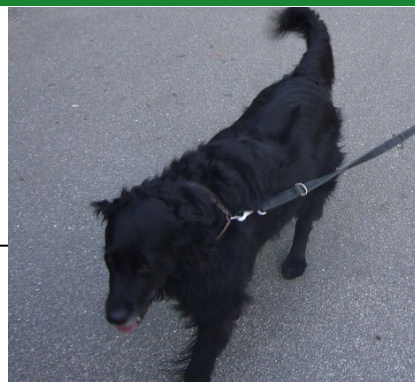
- rcvsftpd start / stop
  - gets the basics
  - keeps the log small
- use the application
- when finished, you might want to run the profile in complain mode for some time
  - especially when it comes to complex applications
  - use aa-logprof to update the profile

Execute options: ix

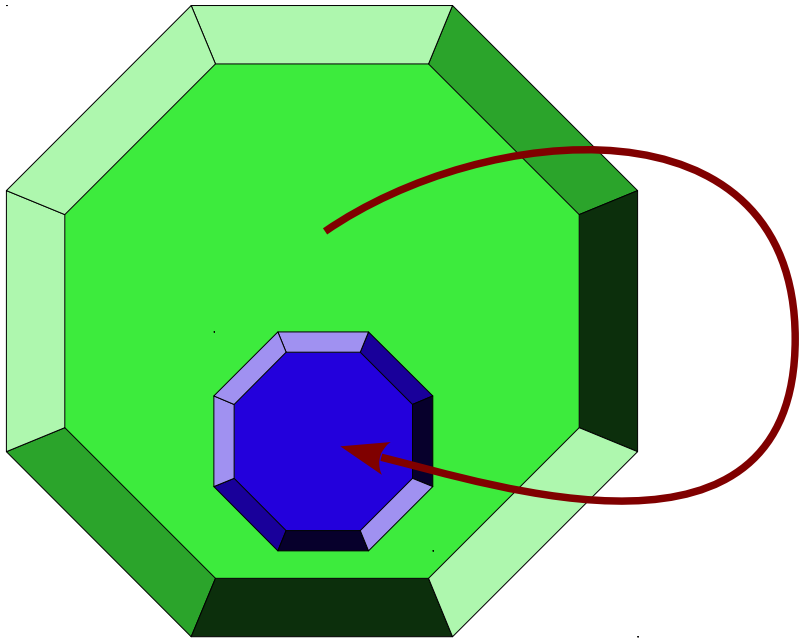
- inherit (ix)
  - run program with the same profile
  - for helper applications and shells (cat, grep, rm, bash)



Execute options: Cx

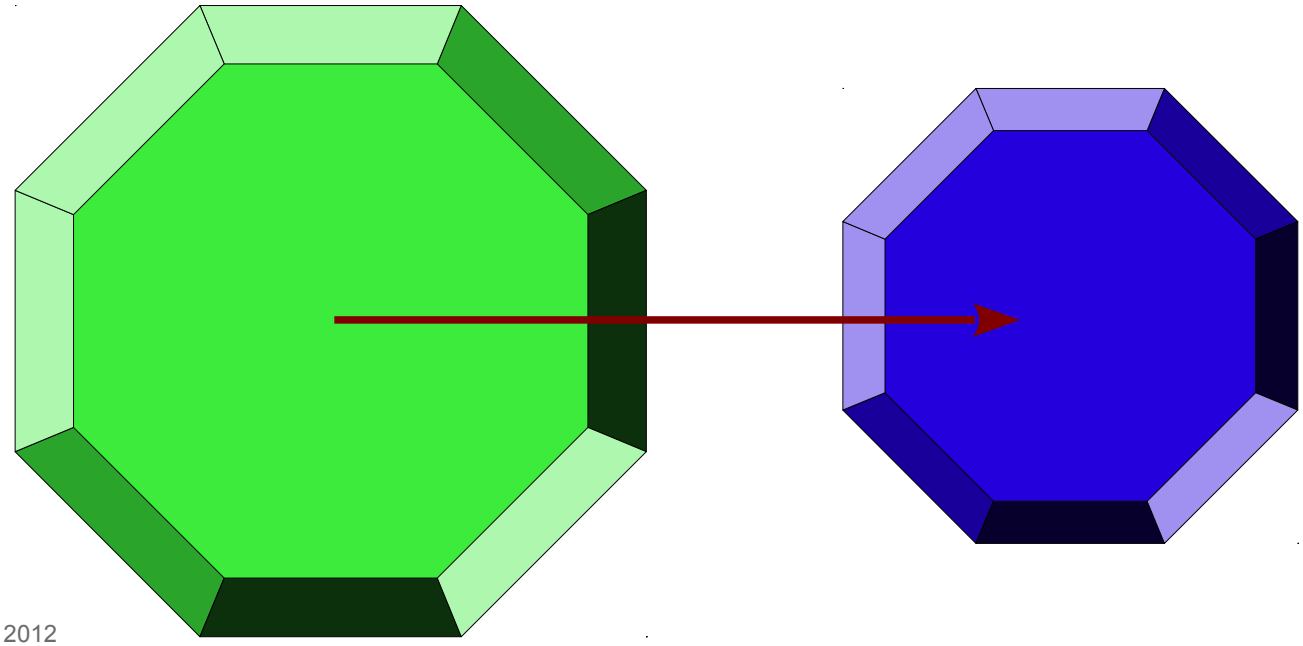


- child (Cx)
  - used for “foo called by bar”
  - doesn't confine standalone calls of foo
  - for helpers that need more or less permissions than the main application

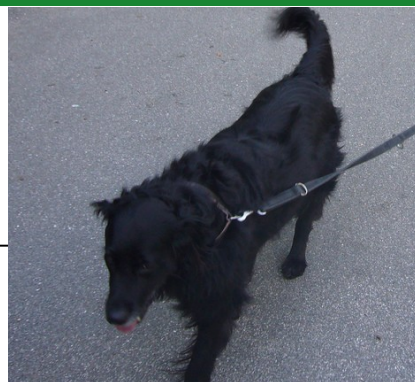


Execute options: Px

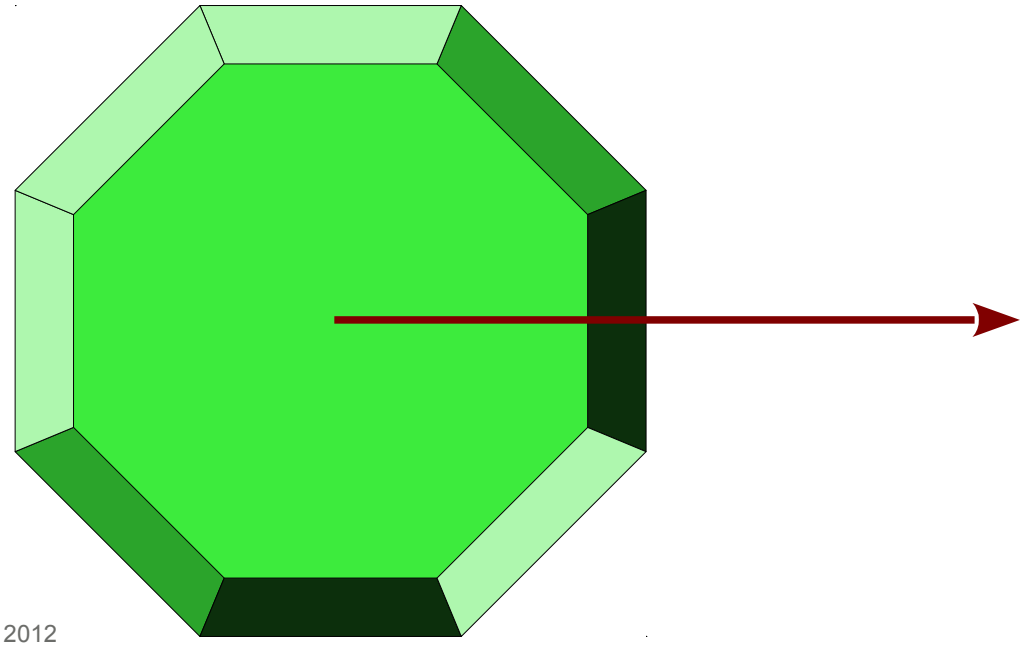
- profile (Px)
  - separate profile for helpers
  - also used if the helper is called standalone
  - not a good idea for /bin/bash ;-)



Execute options: Ux



- unconfined (Ux)
  - execute helper applications without AppArmor protection
  - example: protect sshd, and provide an unrestricted shell after login

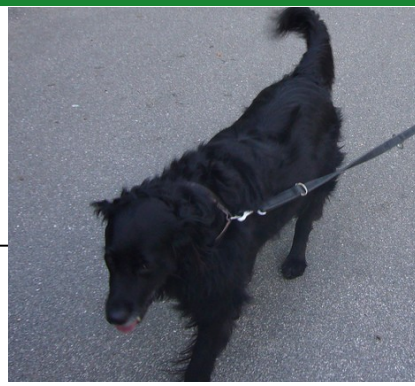


Execute options

Fallback rules if a profile doesn't exist

- Pix
- PUx
- Cix

Execute options



- named profile (Cx -> …, Px -> …)
  - allows specifying the target profile
  - multiple helper applications can use a common abstract profile

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)

audit.log

```
type=APPARMOR_ALLOWED
msg=audit(1245789190.902:123): [...]
```

- add /var/log/audit/audit.log to logdigest
- “translate” the timestamp:
  date -d @1245789190.902
- APPARMOR_DENIED – (blocked) violations of profiles in enforce mode
- APPARMOR_AUDIT – logging of audit rules
- APPARMOR_ALLOWED – profiles in complain mode
- APPARMOR_HINT … operation="ptrace" – an application in complain mode forked

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 itsself
- 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
- 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:

```
/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,
/dev/urandom r,
/proc/*/attr/current w,
/usr/share/apache2/error/** r,
/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
  - also blocks valid scripts if owned by wwwrun

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 7j1ntgRxts8X...
- /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,
}
```

More information...

- http://en.opensuse.org/SDB:AppArmor
- http://apparmor.net/

- openSUSE Security Guide
  http://doc.opensuse.org/documentation/html/openSUSE/opensuse-security/part.apparmor.html

- Mailinglist: apparmor@lists.ubuntu.com

- Download the profiles I use on servers at
  http://blog.cboltz.de/plugin/tag/apparmor
  (slightly outdated)

Questions?

Get your hands dirty!

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/