(TENTAR) (DE VERDADE)
COMO USAR O APPARMOR NO DEBIAN?

Moisés Santos Farias
moisesmsf@proton.me
https://github.com/moisesmsf
https://www.linkedin.com/in/moisesmsf

ABOUT ME

Piaçabuçu – AL

Moisés Santos Farias
moisesmsf@proton.me
https://github.com/moisesmsf
https://moisesmsf.github.io
https://www.linkedin.com/in/moisesmsf/

Privacy + Anonimity + Security
Monero + Anti-forensics

MiniDebConf MACEIÓ 2025

AppArmor?

QUESTIONS

(a) Who has used or is using AppArmor?

(b) Who has already created\changed an AppArmor profile?

(c) Who has had problems with AppArmor?

Moisés Santos Farias | https://github.com/moisesmsf

AppArmor?

MISCONCEPTIONS

- Focus on server
- Focus on processes that face users or Internet
- Focus on breaking things

Moisés Santos Farias | https://github.com/moisesmsf

AppArmor?

DOESN’T

- Doesn’t replace traditional file permissions
- Doesn’t restrict database permissions
- Doesn't validate user inputs (webpages, etc)
- Doesn’t solve all problems

Moisés Santos Farias | https://github.com/moisesmsf

Let's enable AppArmor by default (why not?)

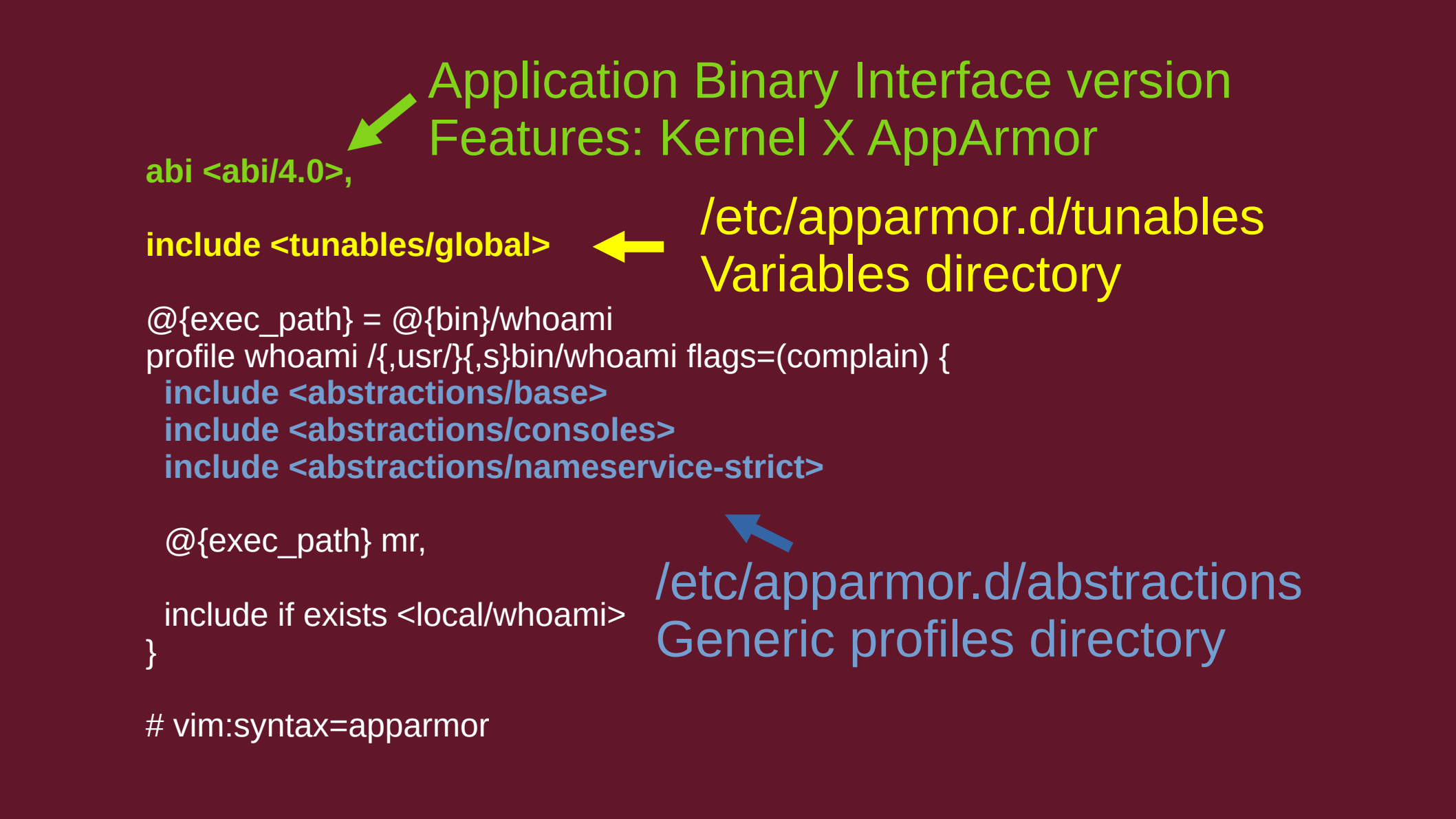
- *To*: debian-devel@lists.debian.org
- *Subject*: Let's enable AppArmor by default (why not?)
- *From*: intrigeri <intrigeri@debian.org>
- *Date*: Fri, 04 Aug 2017 19:31:36 -0400
- *Message-id*: <[🔎] 857eyij4fb.fsf@boum.org>
- *Reply-to*: debian-devel@lists.debian.org

```
Hi!

tl;dr: I hereby propose we enable AppArmor by default in testing/sid,
and decide one year later if we want to keep it this way in the
Buster release.

My goals when initiating this discussion are:

 - Get a rough idea of what amount of effort the Debian project is
   happy (and able) to invest into such proactive security measures.

 - Learn about any relevant social & technical concerns I am not
   aware of.

I don't expect we'll make a decision based on this very proposal:
I expect the proposal will need to be refined, or abandoned, to take
into account what we will learn during this preliminary discussion.
```

https://lists.debian.org/debian-devel/2017/08/msg00090.html

A very brief overview about AppArmor profiles

Moisés Santos Farias | https://github.com/moisesmsf


Application Binary Interface version
Features: Kernel X AppArmor
abi <abi/4.0>,
include <tunables/global>
/etc/apparmor.d/tunables
Variables directory
@{exec_path} = @{bin}/whoami
profile whoami /{,usr/}{,s}bin/whoami flags=(complain) {
include <abstractions/base>
include <abstractions/consoles>
include <abstractions/nameservice-strict>
@{exec_path} mr,
include if exists <local/whoami>
}
# vim:syntax=apparmor
/etc/apparmor.d/abstractions
Generic profiles directory

```
abi <abi/4.0>,

include <tunables/global>

@{exec_path} = @{bin}/nmap
profile nmap /{,usr/}{,s}bin/nmap flags=(complain) {
  ...
  capability net_bind_service,
  capability net_raw,

  network inet dgram,
  network inet6 dgram,
  network inet stream,
  ...
  signal (receive) set=(term, kill) peer=zenmap,
  ...
  owner @{tmp}/zenmap-stdout-* rw,
  owner @{tmp}/zenmap-*.xml rw,
  ...
```

Variable definition

Attachment specification
Attach profile to app

Profile name

Profile flags:
- enforce (default if not specified)
- complain, unconfined, etc

```
abi <abi/4.0>,

include <tunables/global>

@{exec_path} = @{bin}/sudo
profile sudo /{,usr/}{,s}bin/sudo flags=(attach_disconnected,complain) {
  include <abstractions/base>
  include <abstractions/app-launcher-root>
  include <abstractions/app/sudo>

  capability chown,
  capability fowner,
  capability mknod,
  capability sys_ptrace,

  network inet dgram,
  network inet6 dgram,

  ptrace read,

  signal send set=(winch, hup, term),
  ...
```

Capability rules

Network rules

Ptrace rules

Signal rules

```
...
@{exec_path} = @{bin}/sshd
profile sshd /{,usr/}{,s}bin/sshd  flags=(attach_disconnected,complain) {
  ...
  @{exec_path} mrix,

  @{bin}/@{shells}                rux,
  @{bin}/false                   rix,
  @{bin}/nologin                  rpx,
  @{bin}/passwd                   rpx,
  @{lib}/{openssh,ssh}/sftp-server  rpx,
  @{lib}/{openssh,ssh}/sshd-session rix,
  ...
  /var/lib/lastlog/ r,
  /var/lib/lastlog/* rwk,
  /var/lib/wtmpdb/ r,
  /var/lib/wtmpdb/* rwk,

  # For scp
  owner @{user_download_dirs}/{,**} rwl,
  owner @{user_sync_dirs}/{,**} rwl,
  ...
```

File access modes

AppArmor + SystemD

[Service]
...
AppArmorProfile=profilename

Moisés Santos Farias | https://github.com/moisesmsf

AppArmor + Containers

https://kubernetes.io/docs/tutorials/security/apparmor/

https://docs.docker.com/engine/security/apparmor/

Demo

Moisés Santos Farias | https://github.com/moisesmsf

apparmor.d

https://github.com/roddhjav/apparmor.d
https://apparmor.pujol.io/

~1600 profiles
aa-log
Full System Policy

Demo

AppArmor Play
https://play.pujol.io
ssh root@play.pujol.io
Password: apparmor

Moisés Santos Farias | https://github.com/moisesmsf

AppArmor + Demo

AuthPass privacy issues?

https://github.com/authpass/authpass/issues/391

Moisés Santos Farias | https://github.com/moisesmsf

AppArmor + Demo

LibreOffice - CVE-2024-12425

https://codeanlabs.com/blog/research/exploiting-libreoffice-cve-2024-12425-and-cve-2024-12426/

Moisés Santos Farias | https://github.com/moisesmsf

AppArmor + Future

- Permission Prompting
- Apparmor extension file
- Object delegation
- many others

https://gitlab.com/apparmor/apparmor/-/issues/510

Moisés Santos Farias | https://github.com/moisesmsf

Thanks!

https://moisesmsf.github.io/awesome-apparmor

Moisés Santos Farias | https://github.com/moisesmsf