Securing Kopano with Apparmor

Kopano Conference 2017, Arnhem NL

Guido Günther

2017-09-28

Outline

About me

- Debian Developer (libvirt et al., gbp, LTS, ...)
- GNOME contributor
- FSFE Fellow
- Freelancing Free Software Developer

Topic

What is Apparmor

- pathname based Mandatory access control (MAC)
- Linux LSM, userspace tools and profiles
- Confines application to a limited set of resources via profiles
- These control
  - file read, write, execute, lock
  - Network access
  - raw socket access
  - allowed capabilities
  - rlimits
  - tracing
  - (dbus, signals)

Apparmor Policy Example I

```
/usr/sbin/kopano-server {
  #include <abstractions/base>
  #include <abstractions/nameservice>
  #include <abstractions/user-tmp>

  capability chown,
  ...
  capability setuid,

  network tcp,

  /etc/kopano/debian-db.cfg r,
  /etc/kopano/server.cfg r,

  @{PROC}/@{pid}/task/@{tid}/comm rw,
  ...
```

Apparmor Policy Example II

```
  ...
  /run/kopano/prio.sock rw,
  /run/kopano/server.pid rw,
  /run/kopano/server.sock rw,

  /usr/lib/x86_64-linux-gnu/kopano/*.so m,

  ...
  profile kopano_userscripts {
    file,
    network,
  }
  ...
}
```

Building and Debugging profiles

- Denials are logged in kernel log, use dmesg
- aa-complain <program>
- aa-genprof <program>

Apparmor Distro Support

Apparmor Distro Support

Enabled by default in

- Ubuntu (lots of code upstreamed in 4.13)
- OpenSuSE

Apparmor Distro Support

Enabled by default in

- Ubuntu (lots of code upstreamed in 4.13)
- OpenSuSE

Installation on Debian

https://wiki.debian.org/AppArmor/HowToUse

```
sudo apt install apparmor apparmor-{utils,profiles}
mkdir /etc/default/grub.d
echo 'GRUB_CMDLINE_LINUX_DEFAULT="'       \
        '$GRUB_CMDLINE_LINUX_DEFAULT'     \
        'apparmor=1 security=apparmor"' \
    > /etc/default/grub.d/apparmor.cfg
update-grub && reboot

aa-enabled && sudo aa-status
```

Topic

Security Precautions in Kopano

- Services run as user kopano nowadays
- Built with hardening support (in Debian)
- But all services run as the same user

Why is MAC useful

- Webapp listens on the internet
- Z-Push listens on the internet
- e.g. kopano-dagent and kopano-search process untrusted input
- ...

Restricting the MariaDB/Mysql I

Add and activate the profile

```
wget 'https://raw.githubusercontent.com/MariaDB/' \
     'server/10.2/' \
     'support-files/policy/apparmor/usr.sbin.mysqld'
touch /etc/apparmor.d/local/usr.sbin.mysqld
apparmor_parser -a /etc/apparmor.d/usr.sbin.mysqld
```

Needs current git version

Output

```
1 processes are unconfined but have a profile defined.
   /usr/sbin/mysqld (592)
```

Restricting the MariaDB/Mysql II

Restart the service

```
/etc/init.d/mysql restart
```

Output

```
1 processes are in complain mode.
   /usr/sbin/mysqld (2461)
```

Restricting the MariaDB/Mysql III

Enforce the policy

```
aa-enforce /usr/sbin/mysqld
```

Output

```
1 processes are in enforce mode.
   /usr/sbin/mysqld (2461)
```

Restricting kapano-server

- new profile created from scratch

Add the apparmor policy

```
cd /etc/apparmor.d
cp profiles/usr.sbin.kopano-server .
touch local/usr.sbin.kopano-server
apparmor_parser -a usr.sbin.kopano-server
systemctl restart kopano-server
```

Restricting kopano-dagent

kopano-dagent

- Reads untrusted network traffic
- Similar to the server but far less permissions
- New profile created from scratch

Add the apparmor policy

```
cp profiles/usr.sbin.kopano-dagent /etc/apparmor.d/
touch /etc/apparmor.d/local/usr.sbin.kopano-dagent
apparmor_parser -a /etc/apparmor.d/usr.sbin.kopano-dagent
```

Restricting kopano-search

- Indexes untrusted data
- Basic profile

Kopano Search

```
touch local/usr.sbin.kopano-search
cp profiles/usr/sbin.kopano-search /etc/apparmor.d
apparmor_parser -a /etc/apparmor.d/usr.sbin.kopano-search
```

Other core services and helpers

kopano-archiver, kopano-backup, kopano-gateway, kopano-ical, kopnao-monitor, kopano-spooler

Restricting Webapp (Apache)

Restricting Apache itself

```
apt-get install libapache2-mod-apparmor
rm /etc/apparmor.d/disable/usr.sbin.apache2
apparmor_parser -r /etc/apparmor.d/usr.sbin.apache2
aa-status
```

Restricting Webapp (Webapp)

- New profile created from scratch
- Add AAHatName to /etc/kopano/apache2.conf
- Enable profile

Restricting Webapp

```
cp profiles/kopano-webapp /etc/apparmor.d/apache2.d/
apparmor_parser -r /etc/apparmor.d/usr.sbin.apache2
a2enmod apparmor
systemctl restart apache2
```

Other Kopano Components

- ~~Z-Push~~
- ~~Deskapp~~ (but see `http://bugs.debian.org/742829` for chromium)
- ~~Mattermost~~

How you can help

See above

Upstreaming Status

- ⊟ mariadb profile fixes
  - ☒ `https://github.com/MariaDB/server/pull/447`
  - ☐ `https://bugs.debian.org/875890`
- ☐ apache2 profile fixes
  - ☐ `https://code.launchpad.net/~intrigeri/apparmor/apache2-attach_disconnected/+merge/331065`
  - ☐ `http://bugs.debian.org/875892`
- ⊟ kopanocore profiles
  - ☐ Upstream `https://github.com/Kopano-mirror/kopano-core/pull/1`
  - ☒ Debian Package
- ☒ kopano-webapp profile
  - ☐ Upstream not yet submitted
  - ☒ Debian: Pushed to git
- ☐ dh-apparmor
  - Support *etc/apparmor.d/apache*: `http://bugs.debian.org/876647`

Thanks

- Send profile updates to <pkg-giraffe-discuss@lists.alioth.debian.org>
- Questions?

Links

- http://wiki.apparmor.net/index.php/AppArmor_Core_Policy_Reference

Status of Kopano in Debian

- kopanocore 8.3.4 is in Buster/testing
- z-push 2.3.8 is in experimental
- Webapp 3.3.1 in waiting in new