Overview and Recent Developments

AppArmor

2018 Linux Security Summit – Europe

Presentation by
John Johansen
john.johansen@canonical.com
www.canonical.com
October 2018
Now hosted on gitlab

AppArmor

AppArmor gives you network application security via mandatory access control for programs, protecting against the exploitation of software flaws and compromised systems.

Filter by name... Last created

- **apparmor**
  The AppArmor user space development project.
  - 14
  - 2 weeks ago

- **apparmor-profiles**
  The AppArmor profiles project, for sharing developed profiles.
  - 3
  - 2 months ago

- **apparmor-kernel**
  Development for the apparmor kernel module. The official tree use.
  - 0
  - 2 months ago
CII Best Practices

AppArmor

Projects that follow the best practices below can voluntarily self-certify and show that they've achieved a CII Infrastructure Initiative (CII) badge. If this is your project, please show your badge status on your project page! The badge status looks like this:

These are the 12/12 level criteria. You can also view the 12/12 or 12/12 level criteria.

Identification

What is the human-readable name of the project? Show details.

AppArmor

What is a brief description of the project?

AppArmor is an effective and easy-to-use Linux application security system. AppArmor proactively protects the operating system and applications from external or internal threats, even zero-day attacks, by enforcing good behavior and preventing unknown application files from being exploited.

AppArmor security policies completely define what system resources individual applications can access, and with what privileges. A number of default policies are included with AppArmor, and using a combination of advanced static analysis and learning-based tools, AppArmor policies for even very complex applications can be deployed successfully in a matter of hours.

What is the URL for the project (as a whole)?

https://github.com/apparmor/apparmor/wiki/home

What is the URL for the version control repository (if you have one as the project URL)?

https://github.com/apparmor

What programming language(s) are used to implement the project? Show details.

C, C++, Python, bash, perl, Make

What is the Common Platform Enumeration (CPE) name for the project (if it has one)? Show details.

(Optional) CPE name
Overview
What is AppArmor

A Modified Domain Type Enforcement (DTE)
What is AppArmor

A Modified Domain Type Enforcement (DTE) + Capability System*
AppArmor Design

- Start with a target policy
  - Make it easy to confine applications
  - Controlled sharing
    - Allow sandboxes to be built on top
    - Allow confining more than just applications
- The user is the biggest problem
  - Try to make it easy to use
    - Let tooling do the work
  - Get out of the way of admin or any improvements will get turned off
    - Unconfined
- Work towards supporting strict confinement
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,^[s][^h]} flags=(complain) {
    include <abstractions/audio>
    include <abstractions/cups-client>
    include <abstractions/dbus-strict>
    include <abstractions/dbus-session-strict>

    allow file r /etc/firefox*/,
    allow file r /etc/firefox*/**,
    allow ixr /usr/bin/basename,

    dbus bus=system path="/org/freedesktop/UPower"
    interface=org.freedesktop.Upower
    member="{Device,}Changed",

    ...

}
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,^[s]^h} flags=(complain) {
    include <abstractions/audio>
    include <abstractions/cups-client>
    include <abstractions/dbus-strict>
    include <abstractions/dbus-session-strict>
    allow file r /etc/firefox*/,
    allow file r /etc/firefox*/**,
    allow ixr /usr/bin/basename,
    dbus bus=system path="/org/freedesktop/UPower"
    interface=org.freedesktop.Upower
    member="{Device,}Changed",
    ...
}
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,[^s][^h]} flags=(complain) {
    include <abstractions/audio>
    include <abstractions/cups-client>
    include <abstractions/dbus-strict>
    include <abstractions/dbus-session-strict>

    allow file r /etc/firefox*/,
    allow file r /etc/firefox*/**,
    allow ixr /usr/bin/basename,

    dbus bus=system path="/org/freedesktop/UPower"
    interface=org.freedesktop.Upower
    member="{Device,}Changed",

    ...
}

Profile – attachment specification

include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
    include <abstractions/audio>
    include <abstractions/cups-client>
    include <abstractions/dbus-strict>
    include <abstractions/dbus-session-strict>

    allow file r /etc/firefox*,
    allow file r /etc/firefox*/**,
    allow ixr /usr/bin/basename,

    dbus bus=system path="/org/freedesktop/UPower"
        interface=org.freedesktop.Upower
        member="{Device,}Changed",
    ...
}
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
    include <abstractions/audio>
    include <abstractions/cups-client>
    include <abstractions/dbus-strict>
    include <abstractions/dbus-session-strict>

    allow file r /etc/firefox*/,
    allow file r /etc/firefox*/**, 
    allow ixr /usr/bin/basename, 

    dbus bus=system path="/org/freedesktop/UPower" 
    interface=org.freedesktop.Upower 
    member="{Device,}Changed",

    ...

}
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
   include <abstractions/audio>
   include <abstractions/cups-client>
   include <abstractions/dbus-strict>
   include <abstractions/dbus-session-strict>

   allow file r /etc/firefox*/,
   allow file r /etc/firefox*/**,
   allow ixr /usr/bin/basename,

   dbus bus=system path="/org/freedesktop/UPower"
   interface=org.freedesktop.Upower
   member="{Device,}Changed",
   ...
}

include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
  include <abstractions/audio>
  include <abstractions/cups-client>
  include <abstractions/dbus-strict>
  include <abstractions/dbus-session-strict>
  allow file r /etc/firefox*/*,
  allow file r /etc/firefox*/**,
  allow ixr /usr/bin/basename,
  dbus bus=system path="/org/freedesktop/UPower"
      interface=org.freedesktop.Upower
      member="{Device,}Changed",
      ...
}
Profile – class rules

include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,[^s][^h]} flags=(complain) {
  include <abstractions/audio>
  include <abstractions/cups-client>
  include <abstractions/dbus-strict>
  include <abstractions/dbus-session-strict>

  allow file r /etc/firefox*/
  allow file r /etc/firefox*/**
  allow ixr /usr/bin/basename,

  allow dbus bus=system path="/org/freedesktop/UPower"
    interface=org.freedesktop.Upower
    member="{Device,}Changed",

  ...
}

Profile – domain transition

```plaintext
include <tunables/global>

profile firefox /usr/lib/firefox/firefox{,*[^s][^h]} flags=(complain) {
    include <abstractions/audio>
    include <abstractions/cups-client>
    include <abstractions/dbus-strict>
    include <abstractions/dbus-session-strict>

    allow file r /etc/firefox*/,
    allow file r /etc/firefox*/**,
    allow ixr /usr/bin/basename,

    dbus bus=system path="/org/freedesktop/UPower"
    interface=org.freedesktop.Upower
    member="{Device,}Changed",
    ...
}
```
Policy

profile ping /{usr/,}bin/ping {
    #include <abstractions/base>
    #include <abstractions/consoles>
    #include <abstractions/nameservice>

    capability net_raw,
    capability setuid,
    network inet raw,
    network inet6 raw,

    /{,usr/}bin/ping mixr,
    /etc/modules.conf r,

    ...
}

/sbin/dhclient {
    #include <abstractions/base>
    #include <abstractions/nameservice>
    #include <abstractions/openssl>

    capability net_bind_service,
    capability net_raw,
    capability dac_override,
    capability net_admin,

    network packet,
    network raw,

    @PROC)/[0-9]*/net/ r,
    @PROC)/[0-9]*/net/** r,

    /sbin/dhclient mr,

    ...
}

profile syslogd /{usr/,}sbin/syslogd {
    #include <abstractions/base>
    #include <abstractions/nameservice>
    #include <abstractions/consoles>

    capability sys_tty_config,
    capability dac_override,
    capability dac_read_search,
    capability setuid,
    capability setgid,
    capability syslog,

    /dev/log                      wl,
    /var/lib/*/dev/log            wl,

    ...
}
Handling Pattern matching

A
/**a** r,

B
/**b** w,

C
/**c** mr,

[^a]
[a/b/c]
[^b]
[^a/b/c]
[^c]
[^a/b/c]
Basic Policy Summary

```
profile Backend {
  allow file rw
  allow ipc Intermediary
  bind service address
  ...
}

Trusted context

Trusted Helper

profile Application {
  allow ipc intermediary
  ent=foo rw,
  ...
}

Policy Compiler

Active Policy

Audit Subsystem

Audit Subsystem

Trusted Helper

Application context

unconfined context

obj label

Application

unconfined context

Application context

Trusted context

Trusted Helper
Policy Namespaces
Policy Namespaces

Namespace 1
/usr/sbin/libvirtd (enforce)
/usr/sbin/mdnsd (complain)
/usr/sbin/ippusbxd (enforce)
/usr/sbin/dovecot (complain)
/usr/lib/snapd/snap-confine (enforce)
/usr/lib/telepathy/telepathy-ofono (enforce)
/usr/lib/telepathy/telepathy-* (enforce)
/usr/lib/telepathy/mission-control-5 (enforce)
/usr/sbin/identd (complain)
/usr/sbin/cupsd (enforce)

Namespace 2
/usr/sbin/libvirtd (enforce)
/usr/sbin/mdnsd (complain)
/usr/sbin/identd (complain)
/usr/sbin/cupsd (enforce)
firefox (enforce)
firefox//sanitized_helper (enforce)
firefox//lsb_release (enforce)
firefox//browser_openjdk (enforce)
firefox//browser_java (enforce)
Policy Namespaces

:ns:profile

:ns://profile
Policy Namespaces - Hierarchical

```
System
  nscd
dnsmasq

:ns1:
  nscd
dnsmasq

:ns2:

:ns3:

:ns4:

:ns5:
```
Policy Stacking & Dynamic Policy
Stacking - System View

System
ns1:
nscd
dnsmasq

ns2:

ns3:

ns4:

ns5:

Task
Stacking Across Policy NS can Reduce View

System
nscl
dnsmasq

:ns1:
nscd
dnsmasq

:ns2:

:ns3:

:ns4:

:ns5:

Task
Policy NS & Stacking – Scope & View

- View
- Scope
- Admin

System
nsdc
dnsmasq

:ns1:
nsdc
dnsmasq

:ns2:

:ns3:

:ns4:

:ns5:

Task
Policy NS & Stacking – Scope & View* - NOT yet available

- View
- Scope
- Admin

System
nsdrv
 dnsmasq

:ns1:
nsdrv
dnsmasq

:ns2:

:ns3:
nscd

:ns4:

:ns5:
nscd

Task

User sees:
nsdv
:ns5:nscd

CANONICAL
Application and User Defined Policy* - NOT yet available
Stacking – not just across namespaces

Image description:
- Diagram shows a hierarchical structure with a central label "System" connected to "nscd dnsmasq".
- Four namespaces are named: :ns1:, :ns2:, :ns3:, :ns4:, :ns5:.
- Each namespace is connected to the system via arrows.
- A box labeled "Task" is connected to the system.
Delegation of Authority* - NOT yet available

Targeted Task Profile
rmPx /usr/bin/evince, px /usr/bin/bug-buddy, ...

Profile
file r /etc/firefox*/,
file r /etc/firefox*//**,
...

Delegated Authority
&

Delegated Rules
file rw /**,
...

CANONICAL
Stacking – Domain Label

firefox//&evince
Recent Developments
Everything except

af_unix
Upstreaming cont.

- Secids – 4.18
- audit rule filtering (SUBJ_ROLE) – 4.18
- socket mediation – 4.17
- Profile attachment – 4.17
  - EVM
  - Improved overlapping exec attachment resolution
  - np np subset test
Policy tagged with ABI info

profile ping /{usr/,}bin/ping 
  include <abstractions/base>
  include <abstractions/consoles>
  include <abstractions/nameservice>

capability net_raw,
capability setuid,
network inet raw,
network inet6 raw,

file mixr /{,usr/}bin/ping,
file r /etc/modules.conf,
abi=<features/upstream-4.18>

profile ping /{usr/,}bin/ping {
    include <abstractions/base>
    include <abstractions/consoles>
    include <abstractions/nameservice>

    capability net_raw,
    capability setuid,
    network inet raw,
    network inet6 raw,

    file mixr /{,usr/}bin/ping,
    file r /etc/modules.conf,
Single Binary Policy Cache

/etc/apparmor.d/cache

- bin.ping
- sbin.klogd
- sbin.syslogd
- sbin.syslog-ng
- skype
- usr.bin.evience
- usr.bin.firefox
- usr.bin.pidgin
- usr.sbin.cupsd
- usr.sbin.dnsmasq
- usr.sbin.dovecot
- ...

CANONICAL
Per Kernel binary policy

\$\text{location}/7f01cf2e.0$

- bin.ping
- sbin.klogd
- sbin.syslogd
- sbin.syslog-ng
- skype
- usr.bin.evince
- usr.bin.firefox
- usr.bin.pidgin
- usr.sbin.cupsd
- usr.sbin.dnsmasq
- usr.sbin.dovecot
- ...

\$\text{location}/cache/7f01cf2e.1$

- bin.ping
- sbin.klogd
- sbin.syslogd
- sbin.syslog-ng
- skype
- usr.bin.evince
- usr.bin.firefox
- usr.bin.pidgin
- usr.sbin.cupsd
- usr.sbin.dnsmasq
- usr.sbin.dovecot
- ...

\$\text{location}/cache/a035ea11.0$

- bin.ping
- sbin.klogd
- sbin.syslogd
- sbin.syslog-ng
- skype
- usr.bin.evince
- usr.bin.firefox
- usr.bin.pidgin
- usr.sbin.cupsd
- usr.sbin.dnsmasq
- usr.sbin.dovecot
- ...

43
### Binary Policy Overlay

<table>
<thead>
<tr>
<th>$(loc1)/7f01cf2e.0</th>
<th>$(loc2)/7f01cf2e.0</th>
<th>$(loc1)/a035ea11.0</th>
<th>$(loc2)/a035ea11.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>skype</td>
<td>bin.ping</td>
<td>skype</td>
<td>bin.ping</td>
</tr>
<tr>
<td>usr.bin.evince</td>
<td>sbin.klogd</td>
<td>usr.bin.evince</td>
<td>sbin.klogd</td>
</tr>
<tr>
<td>usr.bin.firefox</td>
<td>sbin.syslogd</td>
<td>usr.bin.firefox</td>
<td>sbin.syslogd</td>
</tr>
<tr>
<td>usr.sbin.cupsd</td>
<td>sbin.syslog-ng</td>
<td>usr.bin.pidgin</td>
<td>sbin.syslog-ng</td>
</tr>
<tr>
<td></td>
<td>skype</td>
<td>usr.sbin.cupsd</td>
<td>skype</td>
</tr>
<tr>
<td></td>
<td>usr.bin.evince</td>
<td>usr.sbin.dnsmasq</td>
<td>usr.bin.evince</td>
</tr>
<tr>
<td></td>
<td></td>
<td>usr.sbin.dovecot</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- $(loc1)/7f01cf2e.0
- $(loc2)/7f01cf2e.0
- $(loc1)/a035ea11.0
- $(loc2)/a035ea11.0
WIP
Current WIP

- Internal cleanups and improvements
- Rework early policy loading
  - Systemd integration
  - Default profile
  - initrd/initramfs hooks
- Fine grained networking
  - af_unix
  - ipv4/ipv6
- Improved mount mediation
- Missing mediation
  - Keys mediation
  - ioctl mediation
  - ...
WIP continued

• Improvements to auditing
  • Get audit data off the stack
  • Caching and grouping

• Improvements to complain/learning
  • Caching of recently audited events
  • Direct to daemon logging
  • Daemon interaction, similar to the seccomp notify work

• Further attachment conditionals (user, ...)

• Extended conditionals, and permissions

• Policy namespaces
  • Separate scope & view work
  • Open up policy to users and applications

• Delegation
WIP continued

• no_new_priv improvements
• pam_apparmor
• Interaction with system namespaces
• Documentation
Questions please
Thank you

John Johansen
john.johansen@canonical.com
www.canonical.com