AppArmor

AppArmor je bezpečnostní software, který vytváří ochrannou vrstvu mezi aplikací a systémem. Tím, že aplikaci přesně v profilu vymezíme, co smí a nesmí dělat, chráníme systém před případným využitím bezpečnostních nebo jiných chyb ještě před tím, než mohou být zjištěny a opraveny v aktualizacích.

Instalace

AppArmor je již nainstalován a připraven k použití ve výchozí instalaci Ubuntu. Pokud jej náhodou nemáte, nainstalujte balíky apparmor a apparmor-utils.

Spuštění

AppArmor se spouští automaticky při startu systému. Jestli běží a které profily jsou aktivní zjistíte např. v Terminálu pomocí

```
sudo aa-status
```

Ve výchozím nastavení je aktivních jen pár profilů, např. pro Evince nebo cups. Do budoucna by jich mělo postupně přibývat.

Jak to funguje

AppArmor při startu načte profily (textové soubory s nastavením pro jednotlivé aplikace), které jsou uloženy v adresáři */etc/apparmor.d*. Pokud při své činnosti daná aplikace překročí limity dané profilem, nebude jí umožněno danou akci provést, a *AppArmor* to zaznamená do logu (ve výchozím nastavení */var/log/kern.log*).

Příklad profilu

Toto je (krácený a zjednodušený) příklad profilu uloženého jako */etc/apparmor.d/usr.lib.thunderbird.thunderbird-bin*

```
/usr/lib/thunderbird-3.0.5/thunderbird-*bin {
  # [...]
  @{PROC}/filesystems r,
  /etc/mtab r,
  /etc/mime.types r,
  /etc/mailcap r,

  # browsing directories allowed
  / r,
  /**/ r,

  owner @{HOME}/.thunderbird/** rw,
  owner @{HOME}/.thunderbird/*/.parentlock k,
  owner @{HOME}/.thunderbird/**/*.sqlite* k,
  owner @{HOME}/Desktop/** rw,

  # [...]
  /usr/lib/thunderbird-3.0.5/** rw,
  /etc/thunderbird/** r,
  /usr/lib/thunderbird-3.0.5/components/** w,

  /usr/lib/gamin/** rix,
  /usr/share/applications/** r,
  /usr/share/mozilla/extensions/** r,
  /usr/lib/mozilla/extensions/** r,
  /usr/share/myspell/** rw,
  /usr/share/hunspell/** rw,

  # for PDFs
  /usr/bin/evince PUxr,

  # Openoffice.org
  /usr/bin/ooffice Uxr,

  # [...]
}
```

Pokud je tento profil aktivní, Thunderbird může pouze

- číst (**r**) základní systémové soubory v */etc* a */proc* a procházet adresáře,
- zapisovat a číst (**rw**) do vlastních adresářů a na plochu,
- spouštět (**x**) pouze aplikace nutné k chodu nebo otevření přílohy.

Vše ostatní je zakázáno. Pokud je útok na systém veden přes kompromitaci Thunderbirdu, jsou tímto možnosti útočníka velmi omezeny. Ostatní aplikace, jako např. Firefox, který je častějším terčem útoků, je možné nastavit podobným způsobem.

Na druhou stranu je patrné, že každá zvýšená bezpečnost s sebou může přinést nižší komfort pro uživatele. Např. v případě instalace nestandardního doplňku může být potřeba ručně doplnit profil. Z tohoto důvodu jsou nové profily zaváděny velmi pomalu a s relativně volnými omezeními, což je ovšem vždy bezpečnější než aplikace bez profilu.

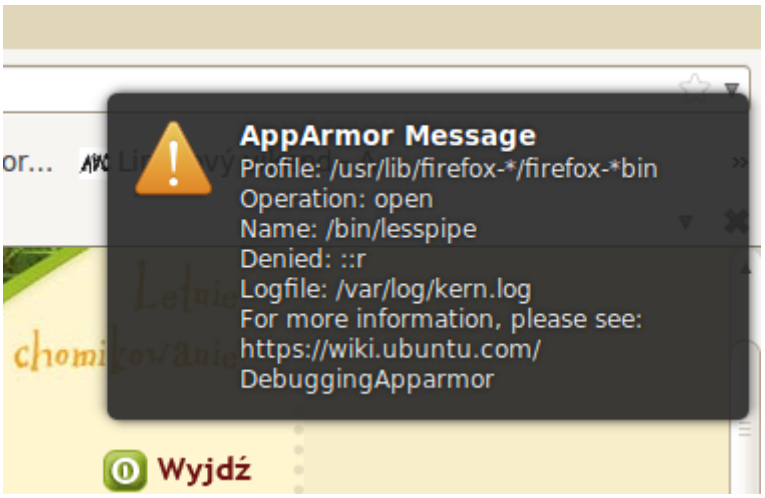
Příklad záznamu do logu

Výňatek z */var/log/kern.log*.

Ukazuje neúspěšný (*denied_mask=„r::“*) pokus Thunderbirdu (*profile=„/usr/lib/thunderbird-3.0.5/thunderbird-*bin“*) o přečtení (*requested_mask=„r::“*) uložených hesel v klíčence (*name=„/home/arrange/.gnome2/keyrings/default.keyring“*).

```
Jul 27 13:25:20 lucid-lean kernel: [ 8142.886121] type=1503
audit(1280229920.037:145):  operation="open" pid=25252 parent=25209
profile="/usr/lib/thunderbird-3.0.5/thunderbird-*bin" requested_mask="r::"
denied_mask="r::" fsuid=1000 ouid=1000
name="/home/arrange/.gnome2/keyrings/default.keyring"
```

Tip: výpisy je možné sledovat pomocí grafického prohlížeče logů, nebo si nainstalujte balík apparmor-notify. Po restartu budete o hláškách *AppArmoru* automaticky informováni systémovou notifikací vpravo nahoře.



Doplňkové informace

Výhody

- vynikající způsob aktivní ochrany před napadením
- relativně jednoduchá administrace (pro mírně pokročilého uživatele)
- možnost měnit profil za běhu systému i programu (ručně)
- možnost spouštět neznámé programy v „bezpečném módu“ a sledovat, co dělají (viz třeba Odkazy - „restrikce viru“)

Nevýhody

- obtížný pro začátečníka - pokud něco nefunguje, může být těžké nalézt příčinu
- menší uživatelská přívětivost - občas může být potřeba aktualizovat profil
- v Ubuntu neexistuje grafická nadstavba (aplikace, kde by se dalo nastavení „naklikat“)
- nenabízí samo možnosti při běhu programu - vždy je potřeba se podívat do logů a upravit profil *ex post*

Alternativy

- SELinux

Odstranění

 Odeberte balík `apparmor`.

Odkazy

- Ubuntu stránky o programu
- článek, který obsahuje i stručný popis aplikace v češtině
- hrátky s AppArmor na ubuntuforums.org od bodhi.zazen
- zevrubná dokumentace z dílny OpenSUSE
- ukázka využití AppArmoru při restrikci viru - video

Technické detaily

Dostupné příkazy

aa-status

```
arrange@lucid-lean:~$ sudo aa-status
[sudo] password for arrange:
apparmor module is loaded.
14 profiles are loaded.
12 profiles are in enforce mode.
   /etc/cron.daily/logrotate
   /sbin/dhclient3
   /usr/bin/evince
```

```
   /usr/bin/evince-previewer
   /usr/bin/evince-thumbnailer
   /usr/bin/passwd
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/connman/scripts/dhclient-script
   /usr/lib/cups/backend/cups-pdf
   /usr/lib/firefox-3.6.7/firefox-*bin
   /usr/lib/thunderbird-3.0.5/thunderbird-*bin
   /usr/sbin/cupsd
2 profiles are in complain mode.
   /usr/bin/skype
   /usr/bin/transmission
4 processes have profiles defined.
4 processes are in enforce mode :
   /sbin/dhclient3 (701)
   /usr/lib/firefox-3.6.7/firefox-*bin (1504)
   /usr/lib/firefox-3.6.7/firefox-*bin (1902)
   /usr/sbin/cupsd (1041)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
```

- *AppArmor* je aktivní
- existuje 14 profilů, 2 z nich jsou v módu *complain* (tréninkový mód - AA zapisuje do logů, ale aplikaci neomezuje - užitečné při tvorbě profilů)
- 4 profily mají odpovídající běžící proces

apparmor_parser

```
sudo apparmor_parser -r -T -W /etc/apparmor.d/usr.bin.firefox
```

Přehraje původní nastavení profilu novým (**-r** - *reload*) bez toho, že bychom museli restartovat celý *AppArmor*. Užitečné při tvorbě profilu a jeho úpravách.

```
sudo apparmor_parser -R /etc/apparmor.d/usr.bin.skype
```

Vymaže profil z modulu v kernelu, takže již není aktivní. Pokud se chcete profilu zbavit úplně, vymažte jej pak i z adresáře */etc/apparmor.d*.

Syntax profilového souboru

Prázdné řádky a řádky začínající na **#** jsou ignorovány (kromě `#include*` - viz níže).

Include

Do profilu je možné přidat pomocí `include` již hotové profily, které najdete v */etc/apparmor.d*.

```
#include <tunables/global>
```

```
#include <abstractions/base>
```

V prvním případě do profilu zahrnete základní proměnné (např. `@{HOME}` a `@{PROC}`), v druhém základní profil, který využije téměř každý program (přístup k `/etc/ld.so.cache`, `/dev/null` apod).

Nastavení cest a zástupných znaků

AppArmor rozlišuje soubory a adresáře: adresář končí vždy na **/**, tzn., že `/etc/apparmor != /etc/apparmor/`.

∗ - zástupný znak pro libovolný počet jakýchkoliv znaků kromě*/*

∗∗ - zástupný znak pro libovolný počet jakýchkoliv znaků **včetně***/*

? - zástupný znak pro libovolný jeden znak kromě*/*

Příklady

/tmp/*

soubory přímo v adresáři /tmp

/tmp/*/

adresáře přímo v adresáři /tmp

/tmp/**

vše (=adresáře i soubory) v libovolné hloubce pod /tmp

/tmp/**/

adresáře (pouze) v libovolné hloubce pod /tmp

Nastavení přístupových práv

r

čtení

w

zápis (nelze použít zároveň s *a*)

a

připojení (*append*) dat (nelze použít zároveň s *w*)

k

zamknutí (*lock*) souboru

px

spuštění programu, ale jen v případě, že má aktivní profil (v opačném případě je spuštění zakázáno). Předává systémové proměnné.

Px

stejně jako *px*, ale nepředává systémové proměnné

ux

bezpodmínečné spuštění programu, předává proměnné

Ux

bezpodmínečné spuštění programu, nepředává proměnné

ix

spuštění programu ve stejném prostředí a se stejnými omezeními jaké má původní program

m

umožňuje mapovat spustitelná data do paměti (`mmap(2)`, `PROT_EXEC flag`)

l

vytváření pevných odkazů (*hardlink*)

Sítě

`network <domain>][<type>][<protocol>`

`domain` může být typu: `inet, ax25, ipx, appletalk, netrom, bridge, x25, inet6, rose, netbeui, security, key, packet, ash, econet, atmsvc, sna, irda, pppox, wanpipe, bluetooth`

`type`: `stream, dgram, seqpacket, rdm, raw, packet`

`protocol`: `tcp, udp, icmp`

Příklady použití

```
network,
network inet,
network inet stream,
network inet tcp,
```

```
network tcp,
```

- povolí veškerou síťovou komunikaci
- povolí veškerou síťovou komunikaci protokolu IPv4
- povolí síťovou komunikaci IPv4 přes TCP
- totéž co v předchozím
- povolí TCP komunikaci přes IPv4 i IPv6.

Další příkazy

owner

povolí přístup jen tehdy, pokud je uživatel zároveň vlastníkem souboru

```
owner /home/*/** rw,
/home/*/foo rw,
```

V prvém případě je přístup povolen jen pro vlastní soubory, v druhém i pro soubor, který vlastní někdo jiný.

audit

zapíše zprávu do logu v každém případě, ne jen tehdy, pokud došlo k zákazu přístupu

```
audit /etc/shadow w,
/etc/shadow r,
```

Můžeme vždy v logu zkontrolovat otevření souboru */etc/shadow* pro zápis.

deny

zakáže určitou činnost. To je užitečné v případě, že potřebujete

- něco zakázat, a přitom nechcete, aby se zpráva o tom pořád vyskytovala v logu (zakáže, ale potlačí zprávu)
- vymezit konkrétní zakázanou oblast v širším pravidle

```
@{HOME}/** rw,
deny @{HOME}/.ssh/** rw,
```

Povolí čtení a zápis v celém domovském adresáři kromě *~/.ssh*.

capability

viz `man capabilities`

```
capability chown
```

Může měnit UID a GID.

Záznamy v logu

type

Proměnná *type* může nabývat hodnot 1501-1506. Nejběžnější je *type=1503* - DENIED (přístup odepřen).

- 1501 - AUDIT - záznamy související s příkazem `audit`
- 1502 - ALLOWED - povoleno
- 1503 - DENIED - zakázáno
- 1504 - HINT - informace k procesu
- 1505 - STATUS - změny v konfiguraci
- 1506 - ERROR - vnitřní chyba *AppArmor*