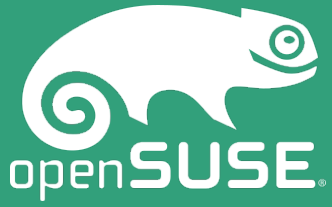


AppArmor

Co to je, k čemu slouží a jak jej používat.

Zdeněk Kubala
Senior QA Engineer
zkubala@suse.com
@n1djz88

Co to AppArmor je a obecné informace

Co to je AppArmor?

- **Wiki definice**

  AppArmor je rozšíření jádra Linuxu o mandatorní řízení přístupu sloužící ke zvýšení počítačové bezpečnosti.

  AppArmor umožňuje definovat oprávnění k provedení určité operace na úrovni jednotlivých procesů v závislosti na umístění spustitelného souboru tím, že na kritická místa jádra umisťuje volání svých kontrolních rutin. Tím dochází ke zvýšení režie systému, avšak je možné zabránit programu, aby provedl potenciálně nebezpečnou akci, která může vést k narušení bezpečnosti (včetně elevace oprávnění).

Obecné informace

- open source
- LSM v linuxovém jádře od verze 2.6.36 (Říjen 2010)
- proaktivní ochrana systému a aplikací

  (interní, externí a dokonce i zero-day útoky)
- uplatňování politik(soubor pravidel) se provádí přes profily, které definují jaká má aplikace oprávnění

  (přístupy k adresářům, socketům či síťi)
- nejpoužívanější profily jsou obsažené v distribučních kanálech

K čemu slouží a proč jej používat?

K čemu slouží a proč jej používat?

- přidává další vrstvu zabezpečení a tím snižuje riziko kompromitace systému, tlumí dopady úspěšného průniku
- ochrana systému před zdivočelými aplikacemi
- je možné měnit profily za běhu systému
- lze zjistit, co "*dělají*" neznámé aplikace, pustíme-li je v "*bezpečném módu*"

Kde AppArmor najdeme?

Kde AppArmor najdeme?

- lze nalézt v různých distribucích
  - Debian
  - Gentoo
  - (open)SUSE
  - Ubuntu
- nejen RPM balíčky a nejen pro (open)SUSE lze nalézt/vytvořit na openSUSE Build Service [https://build.opensuse.org/]
- nebo na Launchpad.net [https://launchpad.net/apparmor/]

Rozdíly mezi AppArmor a SELinux

Rozdíly mezi AppArmor a SELinux

- Pro někoho může být práce s SELinux politikami obtížnější - větší komplexita
- Apparmor je součástí výchozí instalace např. v distribucích (open)SUSE nebo Ubuntu. SELinux Redhat či CentOS
- AppArmor pracuje s cestami, SELinux se štítky(labels) a inodami
- AppArmor hledí na aplikace, SELinux na systém jako celek

Komponenty a nástroje AppArmor

Komponenty AppArmor

- kernelový modul
- parser
- ovládací utilitky

Jak to funguje?

Jak to funguje?

- AppArmor načte při startu modul a dostupné profily z /etc/apparmor.d
- profily se roztřídí dle módu, do kterého patří
  - disabled
  - complain(learning)
  - enforce(confined)
- implicitní politika AppArmor
  - zakazující s "*whitelistem*
  - povolující s "*blacklistem*"

Určení módu - příklad

- z hlavičky profilu „*complain*“

  /usr/lib/colord flags=(attach_disconnected,complain)

- adresář pro profily v módu „disable“

  /etc/apparmor.d/disable

Jak AppArmor začít používat?

Instalace na open(SUSE)

- při standardní instalaci jsou AppArmor balíčky automaticky nainstalovány
- manuální instalace - názvy balíčků

libapparmor
apparmor-profiles
apparmor-utils
apparmor-parser
yast2-apparmor
apparmor-docs

Kontrola, zda AppArmor běží

- `systemctl status apparmor.service`
- `aa-status`
- `ps axuwZ | head`

Verze apparmoru

- /sbin/apparmor_parser -V

Jak AppArmor ovládat?

Jak AppArmor ovládat - nástroje

- `aa-status`
- `aa-complain`
- `aa-enforce`
- `aa-disable`
- `apparmor_parser`
- `aa-autodep`
- `aa-logprof`

Jak AppArmor ovládat - konfiguráky

- /etc/apparmor/

  `easyprof.conf

  logprof.conf

  notify.conf

  parser.conf

  reports.conf

  reports.crontab

  subdomain.conf`

Logování

Logovaní

- log operací se nachází ve */var/log/audit/audit.log*
- výchozí logování *DENIED* operací
- logují se typy
  - DENIED
  - ALLOWED
  - STATUS
- logují se operace
  - mkdir
  - profile_load
  - profile_remove
  - profile_replace

Abstrakce a dynamické profily

Abstrakce – základní informace

- jedná se o profily, které definují „chování“
- umístění ve složce `/etc/apparmor.d/abstractions`
- možné použít ke „seskupení“ profilů např.:

  imaginarní profil `abstractions/profilx`

  #include <abstractions/base>

  #include <abstractions/consoles>

  #include <abstractions/nameservice>

Dynamické profily - lokální

- Lokální profily vs vytvoření ze šablony
- lokální profil
  - umožňuje definovat rozdílná práva(sub-profily)
  - vhodné např. pro forknutí potomka

```
/parent/profile {
    ..
    profile local/profile {
```

  - slouží pro uvěznění procesů, které mohou mít rozdílné parametry

Dynamické profily - šablony

- spolupráce aplikace
- vytvoření/modifikace či odstranění dle potřeby
- povolí se nezbytně potřebné přístupy(šité na míru)

AppArmor a Kontejnery

AA a kontejnery

- kontejnery stejně jako VM mohou běžet ve svázaném režimu
- podobný princip jako u VM
  - kontejnerizační démon má vlastní nesdílený profil
  - dále existuje základní profil pro kontejnery
  - musí být načten v jádře
- podpora tzn. `profile namespace`

Co AppArmor nedělá?

:)

Co AppArmor nedělá

- nevyvenčí za Vás psa :)
- **nejedná se o 100% ochranu proti všem útokům**
- není možné naráz používat AppArmor a SELinux nebo jinou alternativu
- konverze mezi AppArmor profily a SELinux politikami aktuálně není možná
-

Jaké jsou nevýhody?

- neaplikuje se na „už běžící“ procesy
- absence kvalitního grafického rozhraní
- úprava profilů probíhá ex-post
- z počátku může být obtížnější vytváření/administrace profilů

Bonus: soubor(profil) AppArmor politiky i abstrakce

Bonus: soubor(profil) AppArmor politiky

- konvence pojmenování profilu, avšak nemusí být vždy dodržována
  `usr.bin.firefox` interpretuje profil /usr/bin/firefox
- příklad souboru politiky
  `

```
/tmp/ls flags=(complain) {
 # executable needs 'r' and mmap PROT_EXEC 'm'
 /tmp/ls rm,
 /lib/ld-2.5.so rmix,
 /etc/ld.so.cache rm,
 /lib/lib*.so* rm,
 /dev/pts/*    w,
 /proc/meminfo r,
 /var/run/nscd/socket w,
 /var/run/nscd/passwd r,
 /var/run/nscd/group  r,
 /tmp/ r,
}
```

  `

Bonus: Příklad užití abstrakce AppArmor politiky

```
#include <tunables/global>
/{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,
  # Site-specific additions and overrides. See local/README for details.
  #include <local/bin.ping>
```

Bonus: práce s politikami(ukázka)

Bonus: práce s politikami(ukázka)

- přepnout profil(proces) do módu *complain*
- přepnout profil(proces) do módu *enforce*
- zakázat profil(procesu) - aplikace je nespoutaná

Bonus: snadné vytvoření profilu

Bonus: snadné vytvoření profilu

- Vytvořím si program test_bash.sh
  `
  #!/bin/bash
  echo "Toto je testovací prográmek apparmoru."
  echo "Nacházím se v adresaři: "
  pwd
  echo "A jsou zde soubory: "
  ls -l `pwd`
  echo "Zmenim si práva: "
  chmod u+x /root/test_bash.sh
  echo "A toto se nachazi v /etc: "
  ls -l /etc/ | head -4
  `

- pustím `aa-autodep /root/test_bash.sh`
- zkontroluji profil `vim /etc/apparmor.d/root.test_bash.sh`
- pustim aplikaci s profilem v módu "complain"
- zkontroluji log, zda-li tam není něco podezřelého a případně přidám do profilu
- prepnu do *enforce* `aa-enforce root.test_bash.sh`

Otázka pro bystré posluchače

\o_ |o, _o/

Otázka pro bystré posluchače

- mám bashový skript(#!/bin/bash)
- skript má `enforced` AppArmor profil
- Profil zakazuje použití /bin/bash
- při puštění `./bashovy_skript.sh` je přístup k bashi **správně zakázán**
- Ale při `bash bashovy_skript.sh` se vykoná jako by se nechumelilo :‘(

Bonus: ukázka lokálních změn

Bonus: ukázka lokálních změn

- soubor profilu je distribuční z balíčku, chceme drobnou úpravu či něco vyzkoušet
- obětní beránek `/usr/bin/ping`
- skript má AppArmor profil
- soubor změn je v `local/bin.ping`

Bonus: práce s apparmor_parser

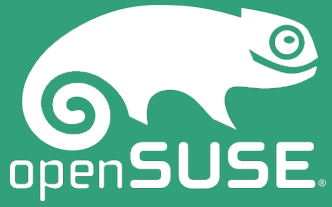
Bonus: práce s apparmor_parser

- některé příkazy nepotřebují oprávnění
  - výpis sad politik z daného adresáře či profilu `-N`

    apparmor_parser -N /path/to/your_profile
- zbytek privilegovaných zvýšená oprávnění chce
  - manipulace s profily `-a` `-r` `-R`

    apparmor_parser -r /path/to/your_profile

    apparmor_parser -R /path/to/your_profile



Otázky?

Zdroje:

https://www.suse.com/documentation/sles-12/book_security/data/part_apparmor.html

http://wiki.ubuntu.cz/bezpe%C4%8Dnost/apparmor?redirect=1

https://cs.wikipedia.org/wiki/AppArmor

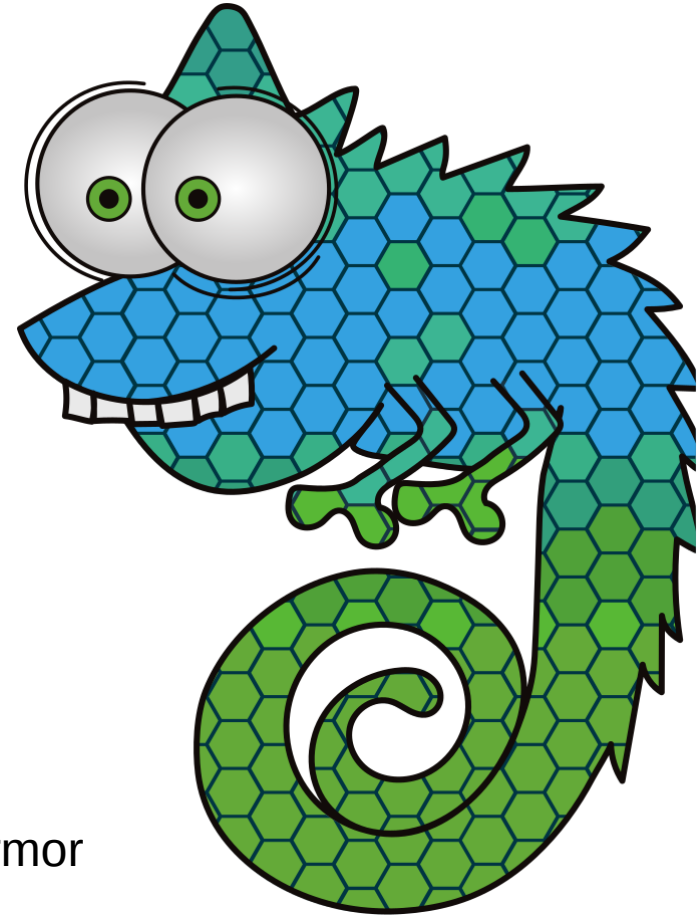
https://en.wikipedia.org/wiki/AppArmor

http://wiki.apparmor.net/index.php/Main_Page

https://en.opensuse.org/SDB:AppArmor

Zdeněk Kubala
Senior QA Engineer
zkubala@suse.com
@n1djz88

Děkuji za pozornost



Zdeněk Kubala
Senior QA Engineer
zkubala@suse.com
@n1djz88

GITHUB:
djz88/docs/tree/master/apparmor

Join Us at www.opensuse.org

License

General Disclaimer

Credits

Template
Richard Brown
rbrown@opensuse.org

Design & Inspiration
openSUSE Design Team
http://opensuse.github.io/branding-guidelines/