BEZPEČNOSTNÍ MODUL V LINUXU APPARMOR

Vladimír Václavek

2010/2011

OSNOVA PREZENTACE

- Úvod
  - Základní informace, historie
- Popis
  - Jak to vlastně funguje
- Profily a správa profilů
  - Syntax
  - Vytváření a editace
- Výhody a nevýhody
  - Porovnání se SELinuxem
- Závěr
  - Použité zdroje

ZÁKLADNÍ INFORMACE

- Bezpečnostní modul pro linuxové jádro
- Software vytvářející ochrannou vrstvu mezi aplikacemi a systémem
- Vyvíjeno pod GNU licencí
- Napsáno v C a Perlu
- Alternativa SELinux

TROCHA HISTORIE

- 1998 – 2003
  - Immunix – poprvé zpřístupněn v SUSE
  - Známý jako SubDomain
- 2005 – 2007
  - Novell - CUPS, ale možnost rozšíření
  - Po 2007 pod GNU licencí
- 2009
  - Tak jak ho známe dnes

- Dnes dostupný v distribucích SUSE, Ubuntu, Gentoo, Debian, Red Hat, atd.

JAK TO VLASTNĚ FUNGUJE (1)

- Funguje na principu MAC
- Forma whitelistu – obsahuje „bezpečné“ aplikace
- Opakem blacklist – obsahuje všechny nepopsané aplikace
- Brání aplikacím přistupovat k nepovoleným zdrojům
- Základní nastavení pro jednotlivé aplikace (profily)
- Vše řeší na úrovni jádra OS s pomocí LSM

JAK TO VLASTNĚ FUNGUJE (2)

- Při startu načte profily (soubory v /etc/apparmor.d)

```
tifo@ubuntu:/etc$ ls apparmor.d/
abstractions      gdm-guest-session  usr.bin.evince
cache             local              usr.bin.firefox
disable           sbin.dhclient3     usr.sbin.cupsd
force-complain    tunables           usr.sbin.tcpdump
tifo@ubuntu:/etc$
```

- V rámci profilu umožněn přístup k souborům, adresářům a POSIXU
- Kontroluje činnosti aplikací a uživatelů
- Je transparentní (aplikace jej nevidí)
- Při překročení limitů dané aplikace, akce nepovolí a vše ukládá do logu (/var/log/kern.log)

VAR/LOG/KERN.LOG

- Ukázka neúspěšného pokusu Thunderbirdu o přečtení uložených hesel v klíčence

Nov 29 19:38:33 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**"

ZÁZNAMY V LOGU

- Proměnná type říká, jaký se vyskytl problém
- Type nabývá hodnot:
  - 1501 – AUDIT – záznamy s příkazem audit
  - 1502 – ALLOWED – povoleno
  - 1503 – DENIED – zakázáno
  - 1504 – HINT – informace k procesu
  - 1505 – STATUS – změny v konfiguraci
  - 1506 – ERROR – vnitřní chyba AppArmoru

PROFIL

- Prázdné řádky a řádky začínající na # AppArmor ignoruje
- Profil obsahuje:
  - Includy – obecná pravidla, předkompilovaná abstrakce -> již hotové profily
  - Určení síťové komunikace
  - Cesty, ke kterým má aplikace nějaká oprávnění a která
- Do profilu můžeme zahrnout základní proměnné jako jsou např. @{HOME}, @{PROC}

ČÁST PROFILU PRO FIREFOX

```
#include <tunables/global>

/usr/lib/firefox-3.5.*/firefox {
#include <abstractions/audio>
…

# povolí síťovou komunikaci protokolu IPv4 a IPv6
network inet stream,
network inet6 stream,
@{PROC}/[0-9]*/net/if_inet6 r,
@{PROC}/[0-9]*/net/ipv6_route r,
…

# oprávnění v pracovním adresáři
@{HOME}/ r,
@{HOME}/** rw,
@{HOME}/Desktop/** rw,
```

SYNTAX - SÍŤ

- Umožňuje nastavit pro každou aplikaci síťovou komunikaci

  network [[<doména>][<typ>][<protokol>]]

- Doména:
  - inet, ax25, ipx, appletalk, netrom, bridge, x25, inet6, rose, netbeui, security, key, packet, ash, econet, atmsvc, sna, irda, pppox, wanpipe, bluetooth
- Typ:
  - stream, dgram, seqpacket, rdm, raw, packet
- Protokol:
  - tcp, udp, icmp

SYNTAX – OPRÁVNĚNÍ (1)

- Příklad aplikace, která má povoleno pouze čtení v Tmp adresáři

```
/ Tmp / r,          tmp
/ Tmp / * r,        všechny soubory přímo
/ Tmp / * / r,      všechny adresáře přímo
/ Tmp / ** r,       všechny soubory a adresáře
/ Tmp / ** / r,     všechny adresáře
```

- Pozn:
  - * jakýkoli počet znaků mimo /
  - ** jakýkoli počet znaků včetně /
  - ? jakýkoli jeden znak mimo /

SYNTAX – OPRÁVNĚNÍ (2)

- Oprávnění jednotlivých cest k souborům

r	čtení
w	zápis
a	připojení
ix	spuštění programu (zděděná oprávnění)
m	mapuje spustitelná data do paměti
l	vytváří pevný odkaz
ux	bezpodmínečné spuštění programu
px	spuštění programu (s aktivním profilem)
k	zamknutí souboru

DALŠÍ MOŽNOSTI

- owner – povolí přístup jen pokud je uživatel vlastníkem souboru
  - owner /home/*/** rw,
- audit – zapíše zprávu do logu vždy (nejen v případě, že došlo k zákazu)
  - audit /etc/shadow w,
- deny – zakáže určitou činnost, aniž by se zpráva zapsala do logu
  - deny @{HOME}/.ssh/** rw,

MÓDY PROFILŮ (1)

- Complain/Learning Mode
  - Porušení profilu je pouze zapisováno do logu, není omezena funkčnost aplikace
  - Používá se při vytváření a ladění profilů
- Enforce Mode
  - Funguje podle našeho nastavení

MÓDY PROFILŮ (2)

```
tifo@ubuntu:~$ sudo aa-status
apparmor module is loaded.
10 profiles are loaded.
10 profiles are in enforce mode.
   /sbin/dhclient3
   /usr/bin/evince
   /usr/bin/evince-previewer
   /usr/bin/evince-thumbnailer
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/connman/scripts/dhclient-script
   /usr/lib/cups/backend/cups-pdf
   /usr/sbin/cupsd
   /usr/sbin/tcpdump
   /usr/share/gdm/guest-session/Xsession
0 profiles are in complain mode.
2 processes have profiles defined.
2 processes are in enforce mode :
   /sbin/dhclient3 (1257)
   /usr/sbin/cupsd (1002)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
tifo@ubuntu:~$
```

PŘÍKAZY PRO SPRÁVU (1)

- sudo aa-genprof
  - vytvoří profil pro aplikaci a umístí aplikaci do complain módu
- sudo aa-status
  - vypíše existující profily v jejich módech
- sudo aa-complain
  - umístí profil do complain módu
- sudo aa-enforce
  - umístí profil do enforce módu

PŘÍKAZY PRO SPRÁVU (2)

- sudo apparmor_parser
  - přehraje původní nastavení profilu novým
- sudo aa-logprof
  - povolí logovat do profilu
- sudo /etc/init.d/apparmor reload
  - aktualizuje profily

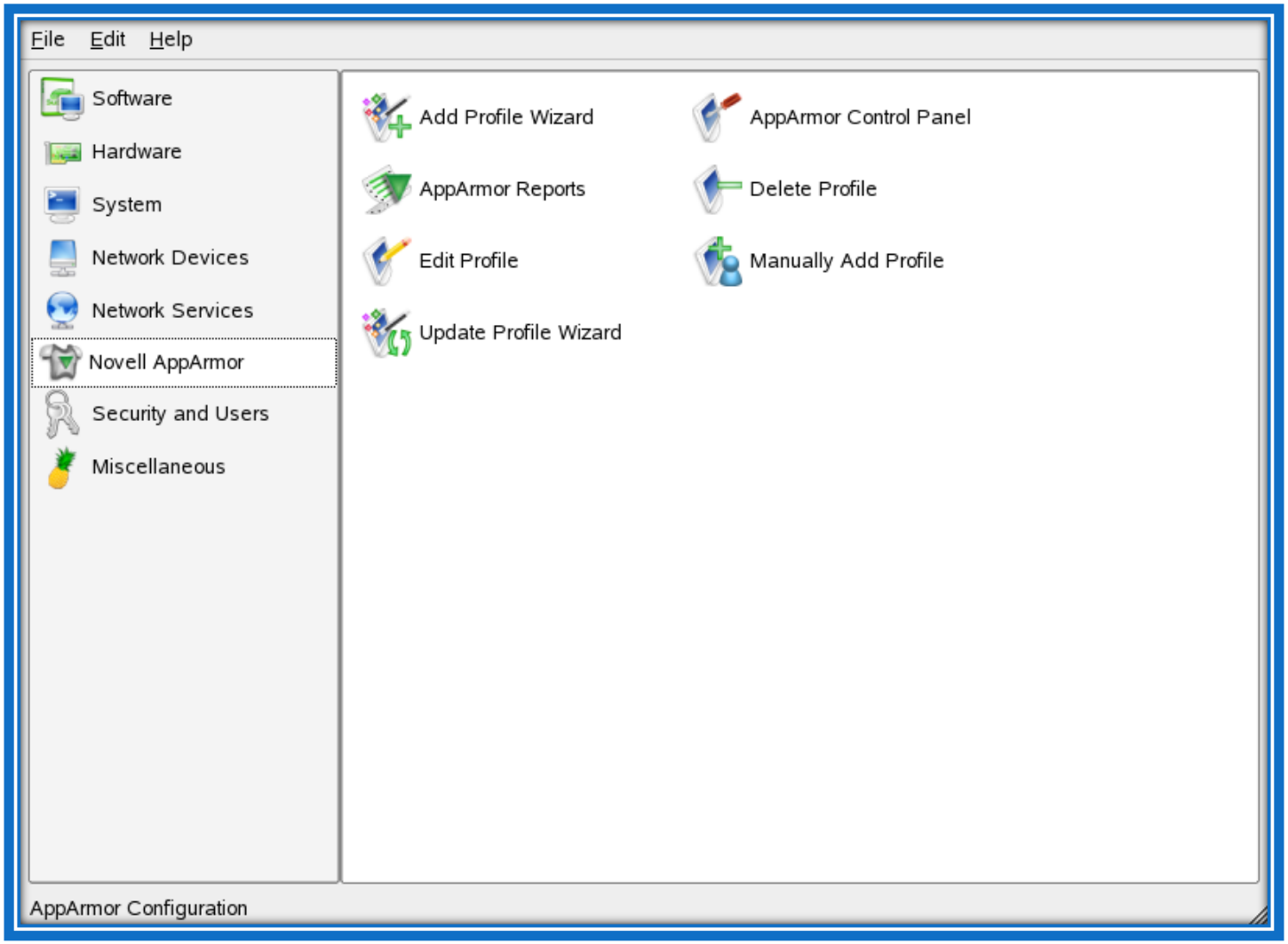
MOŽNOSTI TVORBY PROFILŮ

- Profily podporovaných standardních aplikací jsou již v souboru /etc/apparmor.d (netstats, ping, traceroute, atd.)
- Profily pro některé další aplikace jsou k dispozici na internetu (firefox, opera, gam, atd.)
- Profily pro ostatní soubory můžeme sami vytvořit

VHODNÉ DOPLŇKY

- AppArmor Notify
  - Informuje uživatele systémovou notifikací o zablokování některé aplikace
- YaST
  - Součástí distribuce SUSE
  - Možnost spravovat (nejen) profily přes jednoduché GUI

YAST (1)


File
Edit
Help
Software
Hardware
System
Network Devices
Network Services
Novell AppArmor
Security and Users
Miscellaneous
Add Profile Wizard
AppArmor Control Panel
AppArmor Reports
Delete Profile
Edit Profile
Manually Add Profile
Update Profile Wizard
AppArmor Configuration

VÝHODY A NEVÝHODY

- Výhody:
  - Aktivní ochrana před napadením
  - Vcelku jednoduchá administrace
  - Možnost ručně měnit profily za běhu
- Nevýhody:
  - Složitější nalezení příčiny, proč něco nefunguje
  - Menší uživatelská přívětivost – potřeby aktualizace profilu
  - V některých systémech bez grafické nadstavby
  - Sám nenabízí možnosti upravovat oprávnění při výskytu problému

POROVNÁNÍ SE SELINUXEM

- Rozhodnout, co je lepší je nemožné
- Hlavní rozdíl je v identifikaci objektů souborů – podle jména cesty / pomocí inode

- AppArmor neovlivňuje programy, které chrání (SELinux nutnost re-kompilace)
- AppArmor je snazší z hlediska spravování a bezpečnostní politiky, programový kód je čitelnější a kratší
- Naopak je prý méně bezpečný kvůli absolutním cestám

ZDROJE

http://www.novell.com

http://raygen.info

http://wiki.ubuntu.cz/AppArmor

http://www.linuxtopia.org

http://fei.abba.cz

Děkuji za pozornost!

Nějaké otázky?