Zabezpečenie pracovnej stanice s OS Linux

Peter Vašut

Školiteľ: RNDr. Jaroslav Janáček PhD.

.

Úvod

- AppArmor

AppArmor

- povinné riadenie prístupu (`MAC` vs `DAC`)
- *Selective confinement*
- zakázanie prístupu, štandardná *DAC* stále funguje
- žiadne značky v súborovom systéme

AppArmor

- povinné riadenie prístupu (`MAC` vs `DAC`)
- *Selective confinement*
- zakázanie prístupu, štandardná *DAC* stále funguje
- žiadne značky v súborovom systéme

AppArmor

- povinné riadenie prístupu (`MAC` vs `DAC`)
- *Selective confinement*
- zakázanie prístupu, štandardná *DAC* stále funguje
- žiadne značky v súborovom systéme

AppArmor

Možnosti konfigurácie

- /etc/apparmor.d
-
```
/usr/bin/subor {
    /path/to/file  rw,
    rw /path/to/file2,
    /path/to/file3
         r,
}
```

AppArmor

Možnosti konfigurácie

- /etc/apparmor.d
- ```
  /usr/bin/subor {
      /path/to/file  rw,
      rw /path/to/file2,
      /path/to/file3
           r,
  }
  ```
  ```

Možnosti konfigurácie

Sieť

- permissions: create, shutdown, listen, bind, connect, accept, read/receive, write/send, getname, getpeer, setopt
- domain (inet, bluetooth, ..., často vynechaný)
- type: stream, dgram, ...
- protocol: tcp, udp, icmp, ...
- delegate

Možnosti konfigurácie

Pripájanie súborových systémov

- `mount options=nastavenia /dev/foo -> /cesta /,`

Možnosti konfigurácie

Signály

```
signal,  # Povolí prístup ku všetkým signálom.
deny signal (send) set=(hup, int),
 # Explicitne zakáže prístup k signálom HUP 1 a INT 2 .
signal (receive) peer=unconfined,
 # Povolí príkazom z ktoré unconfined aby mi posielali príkazy
signal (send) peer=/usr/bin/foo,
 # Posielanie signálov procesu pod profilom /usr/bin/foo
signal (receive, send) set=("exists"),
# Povolí kontrolovanie či existuje PID procesu.
signal peer=@{profile_name},
# Povolí posielanie signálov sebe.
```

Možnosti konfigurácie

Ďalšie

- capabilities
- ptrace
- dbus
- aliasy
- kvalifikátory pravidiel: audit, deny, **owner**
- include

Ciele práce

- navrhnúť a popísať spôsob zabezpečenia *používateľského* počítača
  - vytvorenie profilov pre jednotlivé kategórie (všeobecne)
  - možnosti prispôsobenia špecifickým potrebám
- kategorizácia aplikácií
- definícia požiadaviek bezpečnosti
- implementovať pomocné nástroje

Ciele práce

- navrhnúť a popísať spôsob zabezpečenia *používateľského* počítača
  - vytvorenie profilov pre jednotlivé kategórie (všeobecne)
  - možnosti prispôsobenia špecifickým potrebám
- kategorizácia aplikácií
- definícia požiadaviek bezpečnosti
- implementovať pomocné nástroje

Ciele práce

- navrhnúť a popísať spôsob zabezpečenia *používateľského* počítača
  - vytvorenie profilov pre jednotlivé kategórie (všeobecne)
  - možnosti prispôsobenia špecifickým potrebám
- kategorizácia aplikácií
- definícia požiadaviek bezpečnosti
- implementovať pomocné nástroje

Ciele práce

- navrhnúť a popísať spôsob zabezpečenia *používateľského* počítača
  - vytvorenie profilov pre jednotlivé kategórie (všeobecne)
  - možnosti prispôsobenia špecifickým potrebám
- kategorizácia aplikácií
- definícia požiadaviek bezpečnosti
- implementovať pomocné nástroje

Graf

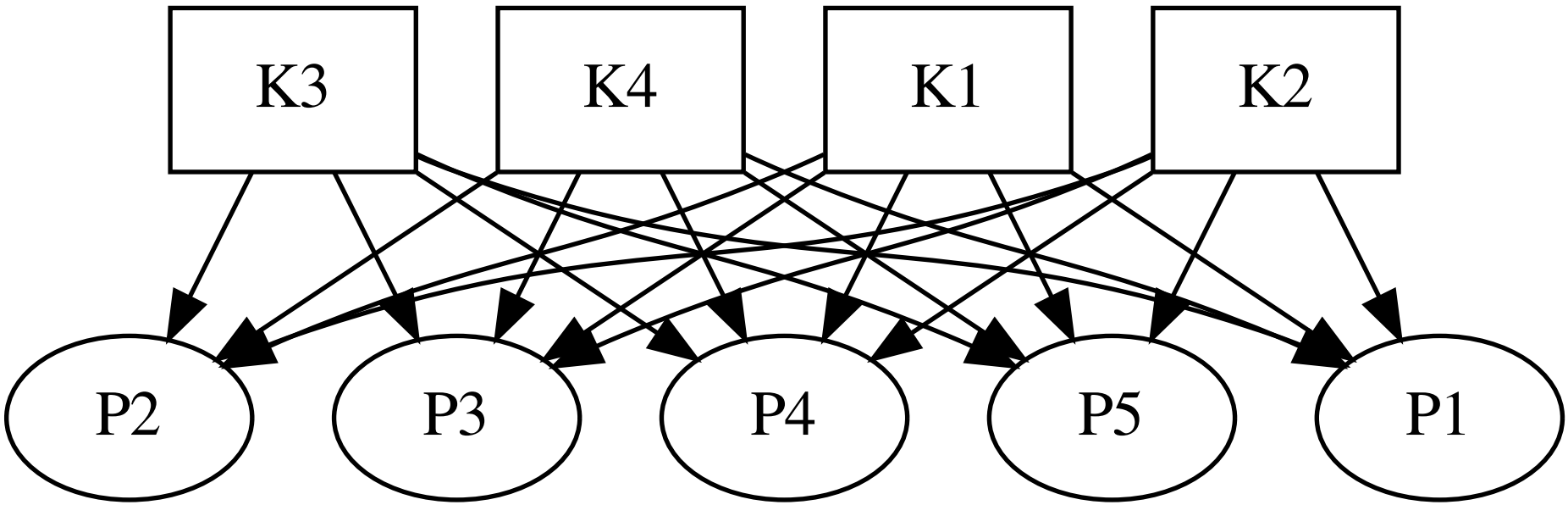
- DAG
- vrcholy:
  - typy aplikácií: 

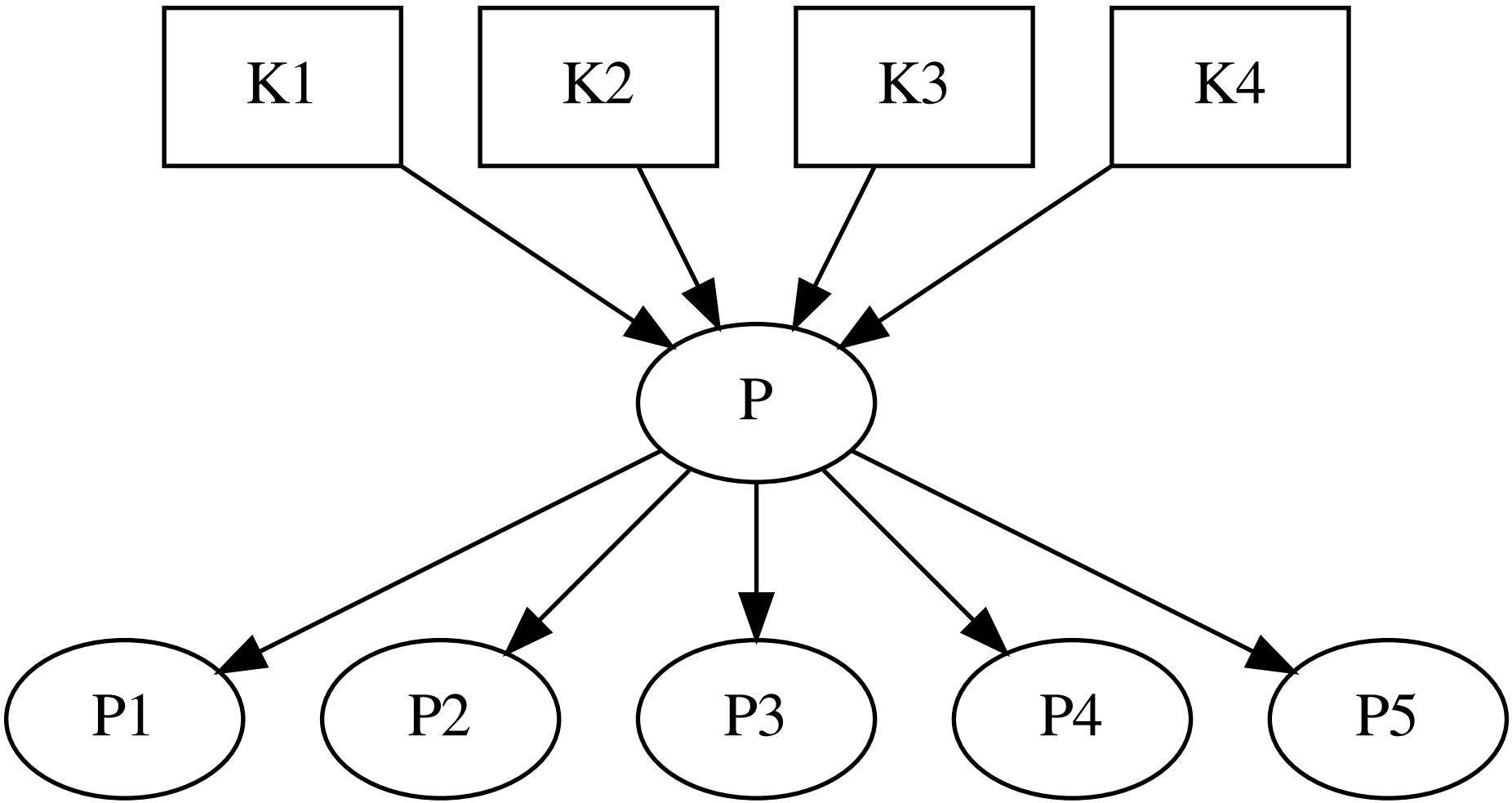
  - požiadavky: 

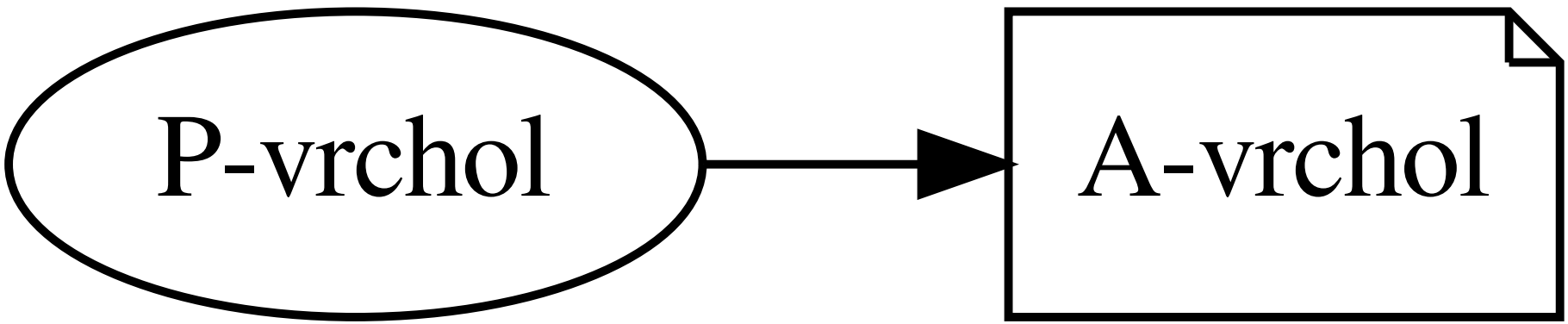
  - možnosti: 

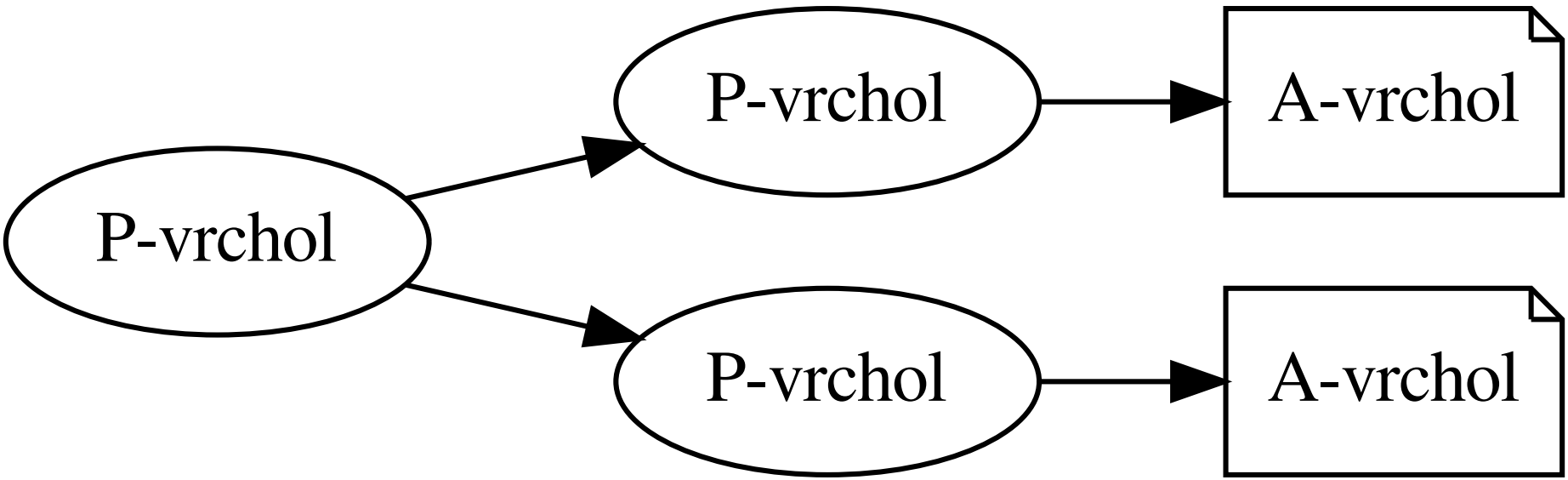
  - implementácia: 

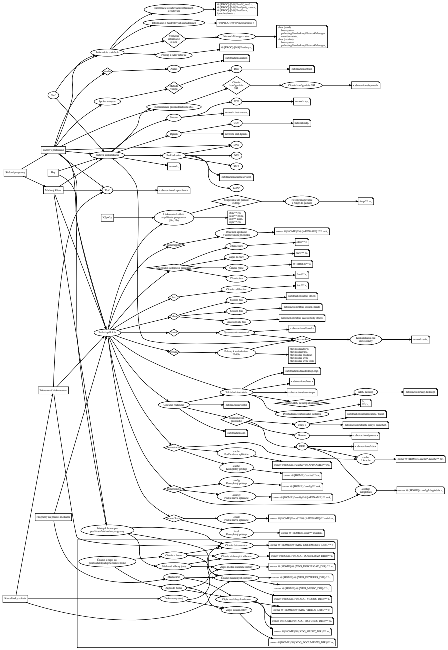
- hrany


K3
K4
K1
K2
P2
P3
P4
P5
P1


K1
K2
K3
K4
P
P1
P2
P3
P4
P5


P-vrchol
A-vrchol


P-vrchol
P-vrchol
P-vrchol
A-vrchol
P-vrchol
A-vrchol



Sieťové programy
Webový prehliadač
Hry
Mailový klient
Sieť
Informácie o sieťach
Informácie o sieťových rozhraniach a routovaní
@{PROC}/[0-9]*/net/if_inet6 r,
@{PROC}/[0-9]*/net/ipv6_route r,
@{PROC}/[0-9]*/net/dev r,
/proc/net/route r,
Informácie o bezdrôtových zariadeniach
@{PROC}/[0-9]*/net/wireless r,
Voliteľné informácie o sieti
NetworkManager - stav
Prístup k ARP tabuľke
@{PROC}/[0-9]*/net/arp r,
Audio
<abstractions/audio>
Správa vstupov
Metóda vstupu
Ibus
<abstractions/ibus>
Komunikácia prostredníctvom SSL
Čítanie konfigurácie SSL
<abstractions/openssl>
Sieťová komunikácia
Stream
TCP
network tcp,
network inet stream,
Dgram
UDP
network udp,
network inet dgram,
DNS
Preklad mien
NIS
SMB
<abstractions/nameservice>
LDAP
network,
Tlač
<abstractions/cups-client>
Výpočty
Linkovanie knižníc a spúšťanie programov (bin, lib)
Mapovanie do pamäte z /tmp/
Povoliť mapovanie z /tmp/ do pamäte
/tmp/** m,
/bin/** rix,
/usr/** rixm,
/lib/** rixm,
/opt/** rix,
Priečinok aplikácie v domovskom priečinku
owner @{HOME}/*@{APPNAME}*/** rwk,
Špecifické systémové priečinky
Čítanie /dev
/dev/** r,
Zápis do /dev
/dev/** w,
Čítanie /proc
@{PROC}/** r,
Čítanie /run
/run/** r,
/etc
Čítanie celého /etc
/etc/** r,
D-bus
System bus
<abstractions/dbus-strict>
Session bus
<abstractions/dbus-session-strict>
Accessibility bus
<abstractions/dbus-accessibility-strict>
Bežná aplikácia
dconf
Spravovanie nastavení
<abstractions/dconf>
Unix socket
Komunikácia cez unix sockety
network unix,
Nvidia
Prístup k zariadeniam Nvidia
Zobrazovač dokumentov
Základné abstrakcie
<abstractions/freedesktop.org>
<abstractions/base>
<abstractions/user-tmp>
XDG desktop
<abstractions/xdg-desktop>
Grafické rozhranie
<abstractions/fonts>
Prechádzanie súborového systému
Používateľské prostredie
Unity 7
<abstractions/ubuntu-unity7-base>
<abstractions/ubuntu-unity7-launcher>
<abstractions/X>
Gnome
<abstractions/gnome>
KDE
<abstractions/kde>
home/cache
.cache: Podľa názvu aplikácie
owner @{HOME}/.cache/*@{APPNAME}** rw,
.cache: Kompletný prístup
owner @{HOME}/.cache/** rw,
.cache: *.kcache
home/config
.config: Kompletný prístup
owner @{HOME}/.config/** rwk,
.config: Podľa názvu aplikácie
owner @{HOME}/.config/*@{APPNAME}** rwk,
.config: kdeglobals
home/.local
.local: Podľa názvu aplikácie
.local: Kompletný prístup
owner @{HOME}/.local/** rwixkm,
Programy na prácu s médiami
Prístup k home pre používateľské online programy
Čítanie a zápis do používateľských priečinkov home
Čítanie z home
Stiahnuté súbory (rw)
Médiá (rw)
Zápis do home
Dokumenty (rw)
Čítanie dokumentov
owner @{HOME}/@{XDG_DOCUMENTS_DIR}/** r,
Čítanie stiahnutých súborov
owner @{HOME}/@{XDG_DOWNLOAD_DIR}/** r,
Zápis medzi stiahnuté súbory
owner @{HOME}/@{XDG_DOWNLOAD_DIR}/** w,
Čítanie mediálnych súborov
owner @{HOME}/@{XDG_PICTURES_DIR}/** r,
owner @{HOME}/@{XDG_MUSIC_DIR}/** r,
owner @{HOME}/@{XDG_VIDEOS_DIR}/** r,
Zápis mediálnych súborov
owner @{HOME}/@{XDG_VIDEOS_DIR}/** w,
owner @{HOME}/@{XDG_PICTURES_DIR}/** w,
owner @{HOME}/@{XDG_MUSIC_DIR}/** w,
Zápis dokumentov
owner @{HOME}/@{XDG_DOCUMENTS_DIR}/** w,
Kancelársky softvér

Kategorizácia aplikácií

- sieťové programy (webový prehliadač, mailový klient)
- zobrazovač dokumentov
- výpočty
- kancelársky softvér
- hry
- programy na prácu s médiami

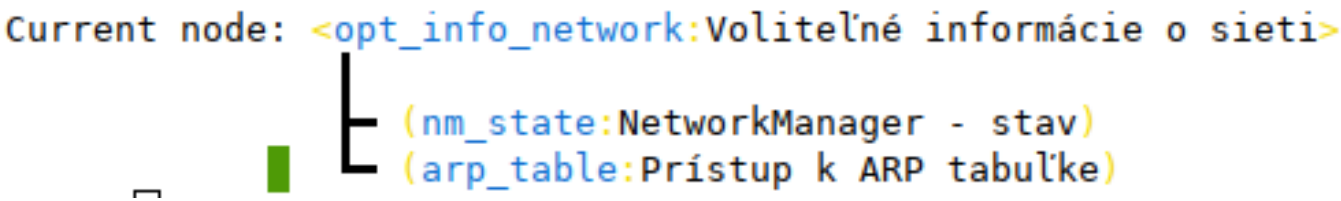
Konfigurátor

```
(Cmd) current
0 nodes to check after this one
Current node: ROOT
                ├─ [net:Sieťové programy]
                ├─ [turing:Výpočty]
                ├─ [media:Programy na prácu s médiami]
                ├─ [game:Hry]
                ├─ [office:Kancelársky softvér]
                ├─ (network:Sieť)
                └─ (home_all_rw:Čítanie a zápis do  používateľských priečinkov home)
```

Konfigurátor

```
(Cmd) current
0 nodes to check after this one
Current node: ROOT
                ├ [net:Sieťové programy]
                ├ [turing:Výpočty]
                ├ [media:Programy na prácu s médiami]
                ├ [game:Hry]
                ├ [office:Kancelársky softvér]
                ├ (network:Sieť)
                └ (home_all_rw:Čítanie a zápis do  používateľských priečinkov home)
(Cmd) search net
(Cmd)
0 nodes to check after this one
Current node: [net:Sieťové programy]
                ├ [web:Webový prehliadač]
                └ [mail:Mailový klient]
```

```
(Cmd) keep web
(Cmd)
13 nodes to check after this one
Current node: <opt_xdgdesktop:Použiť XDG-desktop abstrakciu>
                └ (xdgdesktop:XDG desktop)
(Cmd) keep xdgdesktop
(Cmd)
12 nodes to check after this one
Current node: <opt_de:Používateľské prostredie>
                ├ (gui_kde:KDE)
                ├ (unity7:Unity 7)
                └ (gui_gnome:Gnome)
(Cmd)
11 nodes to check after this one
Current node: <opt_etc:/etc>
                └ (etc_all:Čítanie celého /etc)
(Cmd) keep etc_all
```


Current node: <opt_info_network:Voliteľné informácie o sieti>
(nm_state:NetworkManager - stav)
(arp_table:Prístup k ARP tabuľke)

```
(Cmd)
Nothing left in the queue.
(Cmd) save /tmp/pokus1
(Cmd) export /tmp/firerox_pokus1
Enter possible names of app separated by space:
firefox Firefox
(Cmd) exit
```

Ďalšie nástroje

- zobrazovanie dokumentácie
- generovanie dokumentácie

Časti práce a prínosy

- Popis AppArmoru
- Rámec na zvýšenie bezpečnosti počítača
- Konkrétny graf a definície vrcholov
- Konfiguračný nástroj pre tvorbu profilu
- Príklady použitia a vyhodnotenie
- Záver

Záver

Problémy

- príliš špecifické požiadavky aplikácie
  - riešenia: väčšie zovšeobecnenie, zablokovanie
- vopred neznáme požiadavky (názvy priečinkov)

Záver

Problémy

- príliš špecifické požiadavky aplikácie
  - riešenia: väčšie zovšeobecnenie, zablokovanie
- vopred neznáme požiadavky (názvy priečinkov)

Záver

Problémy

- príliš špecifické požiadavky aplikácie
  - riešenia: väčšie zovšeobecnenie, zablokovanie
- vopred neznáme požiadavky (názvy priečinkov)

Záver

Problémy

- príliš špecifické požiadavky aplikácie
  - riešenia: väčšie zovšeobecnenie, zablokovanie
- vopred neznáme požiadavky (názvy priečinkov)

Záver

Do budúcna

- zlepšenie používateľského zážitku
- čiastočná automatizácia pomocou strojového učenia
- rozširovanie grafu/špecializované grafy
- štandardizácia tvorby programov

Ďakujem za pozornosť

- Navyše, nie je celkom jasné, prečo je užitočné vysvetľovať syntax konfiguračných súborov v práci, ktorej cieľom a výsledkom je de-facto odstrániť potrebu manipulácie s konkrétnou syntaxou a namiesto nej pracovať na vyššej úrovni abstrakcie.

- Niektoré tvrdenia [...] vyvolávajú pochybnosti o svojej pravdivosti (napríklad tiež v časti 1.2 “AppArmor je pomerne nová technológia” – keďže do hlavnej vetvy jadra bol zaradený už viac ako 9 rokov dozadu).

- D-vrchol

- Bolo by možné vytvoriť aplikáciu, ktorá by používateľovi prehľadne vizualizovala efekty konkrétnej vybranej politiky aj bez jej aplikovania? Napríklad by používateľ mohol vidieť strom priečinkov a súborov a v ňom by mal vyznačené, kam všade daná aplikácia smie alebo nesmie pristupovať.

- V operačnom systéme Android sú aplikácie pomerne silne izolované a majú svoje používate- ľom pridelené oprávnenia. Tieto sú dostatočne vysokoúrovňové na to, aby boli pre bežného človeka pochopiteľné, ale pritom dostatočne silné, aby aplikácii neumožili robiť nepovolené operácie. Je možné niečo podobné implementovať pomocou AppArmorovej politiky? T.j. zredukovať konfiguráciu profilu pre aplikáciu do podoby niekoľkých áno-nie otázok namiesto zložitého grafu?

- Potrebuje očakávaný používateľ Vášho nástroja čítať kapitoly 1 a 2 a porozumieť im, pokiaľ chce iba používať graf prezentovaný v kapitole 3?