Petr Krčmář

AppArmor: brnění pro váš systém

3. listopadu 2012
LinuxAlt, Brno

ROOT.CZ

Problém: hrubé řízení práv

- Jsi buď uživatel = můžeš jen něco
- Nebo jsi root = můžeš všechno
- Nemožnost rozlišení pro jednotlivé aplikace
- Obzvlášť nebezpečné pro setuid binárky
  - Ale nejen pro ně
- Možnost zneužití třeba u buffer overflow
- Má třeba ping mít právo něco spouštět?
- Klasický systém práv to neumožňuje

Řešením je LSM

- LSM = Linux Security Module
- Framework pro bezpečnostní rozšíření jádra
- Univerzální vyvedení patřičných volání jádra
- V jádře v současné době čtyři řešení:
  - AppArmor
  - SELinux
  - Smack
  - TOMOYO Linux

ROOT.CZ

Proč právě AppArmor

- Je velmi uživatelsky přívětivý – hlavní vlastnost
- Můžete se jej naučit velmi rychle
- Nijak dramaticky nezasahuje do systému
  - Nevyžaduje integraci v userspace
- Možnost správy za běhu systému
- Možnost sandboxíngu libovolné aplikace
- Má výborný poměr cena/výkon
  - Aneb za málo práce bude hodně muziky

Nevýhody AppArmor

- Běžným uživatelem nespravovatelné
- Neumí práva přidávat, jen ubírat
  - K tomu jsou tu capabilities nebo setuid
- Nemůže hlídat aplikace spuštěné před AA
- Nemá automat „Aplikace chce tohle. Povolit?“
- Může zkomplikovat správu systému
  - Může v něm začít „strašit“ - Proč to nejede?

ROOT.CZ

Jakýsi jaderný firewall

- Síťový firewall blokuje nevhodnou komunikaci
- AppArmor je postaven mezi jádro a aplikaci
- Také mu nastavujeme pravidla filtrace
  - Tedy kterou akci aplikaci dovolíme a kterou ne
- Nastavení probíhá dle binárky a cesty
- Každá binárka má svůj profil
- Jednoduchý textový soubor, popisující pravidla

ROOT.CZ

Chování AppArmor

- Výchozí chování je „nedělám nic“
  - AppArmor se tedy většiny aplikací nedotkne
- Pokud existuje profil, pak „všechno zakaž“
  - Prázdný profil znemožní komunikaci s okolím
- S výjimkou toho, co je výslovně povoleno
- Nepovolené akce se logují
  - Sledujte log - často odhalíte zdroj problémů

Bezpečnostní profily

- Uloženy v /etc/apparmor.d/
- V Ubuntu doplňkový balíček apparmor-profiles
  - Dále budeme potřebovat apparmor-utils
- Pojmenované podle cesty, místo / je .
- Jednoduchý textový soubor
- Možno editovat libovolným editorem
- Nebo pomocí speciálních nástrojů

Jak vypadá profil

```
/bin/foo {
        /etc/fstab r,
        /bin/ping rx,
        owner @{HOME}/.config/foo rwa,
        network inet stream,
        network inet6 stream,
        owner /tmp/** rwa,
        capability net_raw,,
}
```

ROOT.CZ

Co je možné regulovat

- Soubory (čtení, zápis, spouštění, tvorba...)
- Síť (IPv4, IPv6, TCP, UDP, RAW, adresy...)
- Mount (kam, co, zápis/čtení, fs...)
- Práva (chmod, chown, kde, maska...)
- Capabilities (jako v jádře)
- Další (DBUS, rlimit, IPC...)
- (http://wiki.apparmor.net/index.php/ProfileLanguage)

Praktická ukázka...

- Prozkoumání adresářů
- Vytvoření prázdného profilu
- Manuální vytvoření profilu
- Automatické vytvoření profilu
- Prohlédnutí logů
- Otestování funkčnosti AppArmor

ROOT.CZ

Otázky na závěr

- Kdo to...?
- Co to...?
- Je to pravda...?
- Proč je to...?
- A jak je to s...?
- Komu je...?
- S kým je to...?
- Proč proboha...?
- Kdo to má...?
- To už vážně tohle...?
- Na mou duši...?
- Žádná legrace...?
- A proč bych měl...?
- Nebo neměl...?

ROOT.CZ

Děkuji za pozornost

Petr Krčmář
www.root.cz, www.debian-linux.cz
petr.krcmar@iinfo.cz

ROOT.CZ