AppArmor:
Alkalmazásbiztonság Linuxon

Papp Zsolt
Rendszermérnök, Novell PSH
zpapp@novell.com

Novell®

Szoftver-biztonság kérdése

Probléma: nem tökéletes programok

- A megbízható szoftver azt teszi, ami a dolga
- A biztonságos szoftver azt teszi, ami a dolga *és semmi mást*

Megoldás: csak **tökéletes** programok használata

... abból nincs túl sok :-)

AppArmor

Kényszeríteni az alkalmazásokat, hogy csak azt tehessék, ami a feladatuk

Mi is egy alkalmazás feladata?

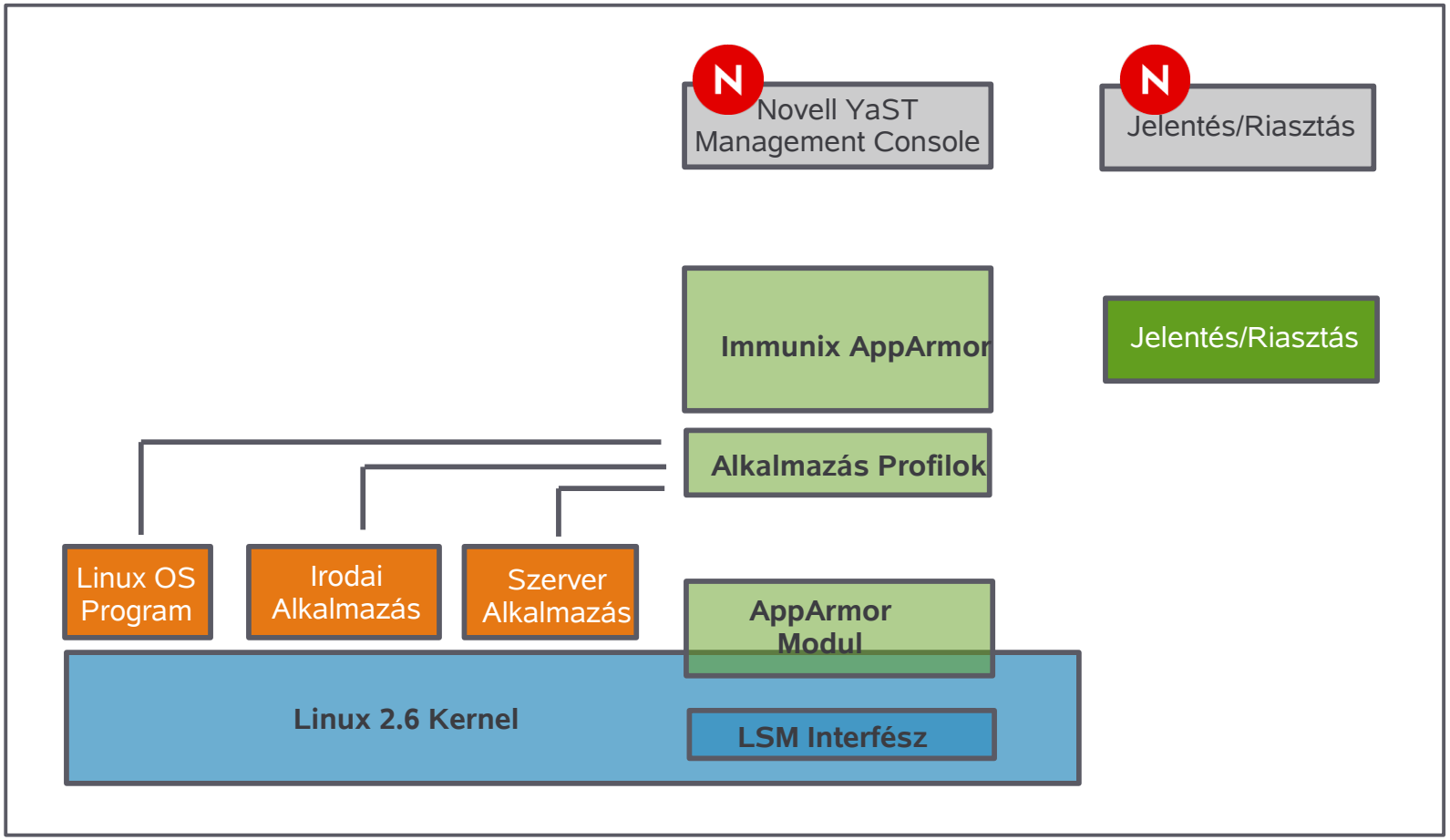
- Azt a kódból tudjuk csak meg
- Azért ezt mégsem :-)
- Kell valami egyszerűbb, valami absztrakt

Erőforrások:

- Korlátozni az alkalmazást, hogy csak olyan erőforrásokat érjen el, amiket szabad neki

Részletesebben

Hogyan működik az AppArmor



Megkerülhetetlen

Nem szabad, hogy megkerülhető legyen a HIPS

- Kernel-szinten kell működnie

Az AppArmor a 2.6-os kernel LSM interfészét használja

- LSM (Linux Security Module) egy kernel-szintű közvetítő réteget kínál, nem kell a kernelt patchelni
- Nyílt szabványú API-t nyújt a hozzáférést vezérlő modulnak
- Pontos információ az alkalmazások viselkedéséről, teljesítményéről
- Jól működő, megkerülhetetlen réteget kínál

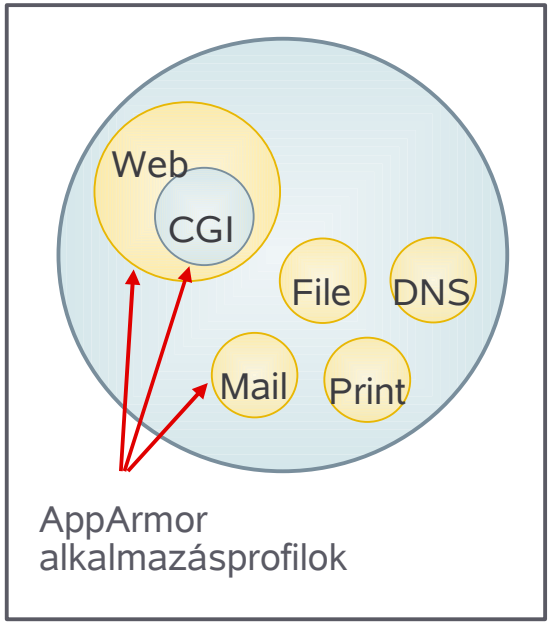
Biztonsági modell

Helytelen használat vs. szabálytalan működés megakadályozása

- Helytelen használat (vírus, trójai) megakadályozását könnyebb kezelni
- Szabálytalan működés megakadályozása sokkal biztonságosabb de jóval nehezebb elérni

Az AppArmor a két modellt ötvözi

- Hangsúly az alkalmazásbiztonságon van
- Név-alapú hozzáférés-vezérlés a szabályok könnyebb megértéséért
- Hibrid engedélyező/tiltó lista
  - Engedélyező lista az alkalmazás profilban
  - Rendszerszintű tiltólista



Alkalmazás-alapú hozzáférés-vezérlés

Védett program futásakor az AppArmor UID-tól függetlenül szabályozza a hozzáférést:

- A használható POSIX képességek (még akkor is, ha root-ként fut)
- A könyvtárak/fájlok, melyek írhatóak/olvashatóak/ futtathatóak

Példa profil az **ntpd** programhoz

```
/usr/sbin/ntpd {
  #include <abstractions/base>
  #include <abstractions/nameservice>

  capability ipc_lock,
  capability net_bind_service,
  capability sys_time,
  capability sys_chroot,
  capability setuid,

  /etc/ntp.conf                r,
  /etc/ntp/drift*                          rwl,
  /etc/ntp/keys                r,
  /etc/ntp/step-tickers                    r,
  /tmp/ntp*                                rwl,
  /usr/sbin/ntpd               rix,
  /var/log/ntp                 w,
  /var/log/ntp.log             w,
  /var/run/ntpd.pid            w,
  /var/lib/ntp/drift           rwl,
  /var/lib/ntp/drift.TEMP      rwl,
  /var/lib/ntp/var/run/ntp/ntpd.pid        w,
  /var/lib/ntp/drift/ntp.drift             r,
  /drift/ntp.drift.TEMP        rwl,
  /drift/ntp.drift             rwl,
}
```

Natív Unix szintaxis és szemantika

Az AppArmor profilok a klasszikus Unix jogosultsági mintát tükrözik

- Kiegészíti a Unix jogokat nem lecseréli azokat

Reguláris kifejezések az AppArmor szabályokban

- /dev/{,u}random a /dev/random-ra és a /dev/urandom-ra illeszkedik
- /lib/ld-*.so* a /lib-ben az ld osztott könyvtárra illeszkedik
- /home/*/.plan minden felhasználó .plan fájlja
- /home/*/public_html/** minden felhasználó public_html könyvtárstruktúrájára illeszkedik

Profilok

Alapvető szabályok, melyekre a profilokban lehet hivatkozni

- **base**: majdnem minden programnak szükséges
- **authentication**: felhasználók azonosítása
- **console**: a program ír a TTY konzolra
- **kerberos**: Kerberos titkosítás használata
- **nameservice**: DNS névfeloldás
- **wutmp**: felhasználói belépés rögzítése

Alfolyamat korlátozás

Apache mod_perl és mod_php szkriptek

- Lehetőség van profilt definiálni egyes szkriptekhez
- A szkripthez tartozó profil használata, ha van
- Egyébként alapértelmezett szkript-profil használata
- Nem szükséges minden CGI-t Apache jogokkal futtatni
- Az egyetlen ismert módszer PHP szkriptek védelmére

Jogosultság szétválasztás

- Bejelentkezés előtti része az OpenSSH szolgáltatásnak egy szigorú profilt használ
- Bejelentkezés után pedig teljes hozzáférést kaphat

Teljesítmény

Rendkívül hatékony, alacsony teljesítménycsökkenés

- Apache kb. 0-2% teljesítménycsökkenést mutat a Webstone terhelési tesztjei alatt
- **általános eset**: a teljesítménycsökkenés nem mérhető (megközelítőleg 0%)
- **rendkívüli eset**: 2%-al nagyobb terhelés

Működő minta-profilokat tartalmaz

Elterjedt szolgáltatásokhoz és alkalmazásokhoz alapvető profilokat tartalmaz :

- Apache Web kiszolgáló
- Postfix levelező kiszolgáló
- Sendmail levelező kiszolgáló
- OpenSSH
- Squid proxy
- Network Time Protocol Daemon (ntpd)
- Name Service Cache Daemon (nscd)
- egyéb

Felhasználási területek

AppArmor célközönsége

Bármely cég, akinek hálózati szerverei kritikus alkalmazásokat futtatnak

Bármely értékes adatokkal rendelkező szervezet

Minden Linux alkalmazás ami támadásoknak lehet kitéve

AppArmor célközönsége

Hálózati kiszolgálók

- Elszigetelni a külvilággal érintkező programokat
- Auto-scan eszköz megtalálja azokat a szolgáltatásokat, amiket szabályozni kell

Üzleti alkalmazások

- Összetett, nehezen auditálható
- Esetleg zárt forrású
- Megakadályozza, hogy egy támadás más komponensekre, vagy rendszerekre továbbterjedjen

Asztali környezet

- Küslő adatokkal dolgozó asztali alkalmazások védelme
- Elkülöníteni ezeket a programokat más asztali alkalmazásoktól
- Nagyon kockázatos programok védelme

POS terminálok, Kioszkok

- Elszigetelni a külvilággal érintkező programokat
- Teljes szolgáltatáslistát átölelő profilkészlet
- Hibás felhasználás korlátozása
- Felhasználó munkamenetét szabályozó profil

Fejlesztési tervek

Rövid távú tervek

- **Hálózati hozzéáférés-vezérlés** – TCP/UDP-alapú hálózati hozzáférés-vezérlés az egyes folyamatok számára
- **Profilok összefésülése** – két profilból egy harmadik létrehozása
- **Profil megosztás** – eszközök és közösségi portál kialakítása az AppArmor profilok könnyű megosztásához
- **Tomcat/JBoss támogatás** – Java konténerben futó servletek kezelése
- **pam_apparmor modul** – megerősített biztonság (change_hat funkció) a szerep-alapú shell funkcióknak, melyek PAM-ot használnak (pl.: sshd, gdm)
- **CIM Providers** – szabványos CIM-alapú csatolók jelentések készítéséhez, riasztások kezeléséhez és profil állapot lekérdezéséhez

További tervek

- **DBArmor** – hozzáférés-vezérlés egyes táblákhoz az adatbázisban
- **Alapértelmezett szabály** – olyan rendszererőforrások listája, melyeket *kizárólag* AppArmor profilokon keresztül lehet elérni
- **DBUS** – események jelentése DBUS-on keresztül
- **IPC elszigetelés** – folyamatok közötti kommunikáció kezelése
- **Profile Lint** – profil analizálása, veszélyes szabályok kiszűrése
- **Erőforrás limitáció felügyelete**
- **Központosított profilfejlesztés**

Elérhetőség

Elérhetőség

A következő disztribúciókban az alaptelepítés része:

- SLES10
- SLED10
- openSUSE 10.1, 10.2 ...

Az AppArmor nyílt forrású: GPL

- http://opensuse.org/AppArmor
- Levelezési listák: apparmor-announce, apparmor-general, apparmor-dev
- IRC irc.oftc.net/#apparmor

AppArmor az Ubuntuban

Magnus Runesson portolta az AppArmort Ubuntura

- http://www.linuxalert.org/ubuntu/apparmor/
- Megtalálható a Feisty Fawn Universe repóban
- Hamarosan bekerül a Gutsy Gibbon Main repóba is

További információk

http://opensuse.org/Apparmor

http://www.novell.com/apparmor

Levelezési listák:

- apparmor-announce
- apparmor-general
- apparmor-dev

IRC

- irc.oftc.net/#apparmor


Novell®