Az Apache webszerver biztonsági és egyéb kiegészítései

NetWorkShop 2009

Vincze Dávid
Miskolci Egyetem Számítóközpont

Szeged, 2009

Webkiszolgálók és szkriptek

- Webkiszolgálók
  - **Apache** (61%, 88% HU), Zeus, SunONE, MS IIS, Caudium, lighttpd, TUX, thttpd, stb.
- Weben használt szkript nyelvek
  - **PHP** (40%), Perl, Python, JSP, stb.

- Kiszolgálási mód
  - Statikus
    - HTML, kép, dokumentum, CSS, JS, stb.
  - Dinamikus
    - CGI (**C**ommon **G**ateway **I**nterface) – közös ID
    - suexec CGI / suphp – változtatható ID
    - mod_php (mod_perl, mod_python) – közös ID

Felhasználói azonosító megváltoztatása

- POSIX kompatibilis op. rendszereken
- Azonosító váltás **aktuális** processzen
  - felhasználói: setuid(), ... , setresuid()
  - csoport: setgid(), ... , setresgid()
- **Csak a rendszergazdának van hozzá jogosultsága**

- Capabilites rendszer (POSIX.1e)
  - Felosztja a rendszergazdai jogkört
- CAP_SETUID/CAP_SETGID
  - futó processz képessége a saját azonosítóinak megváltoztatásához

CAP_SETUID/GID + setuid() I.

- Az Apache fő processze rendelkezik minden képességgel
- A gyermek processzeket felruházza CAP_SETUID és CAP_SETGID képessé-gekkel, így azok bármikor válthatnak
- setuid()/setgid()/setgroups() hívásokkal megtörténik a váltás
- Eldobja a képességeket
- Végrehajtja magát a szkriptet

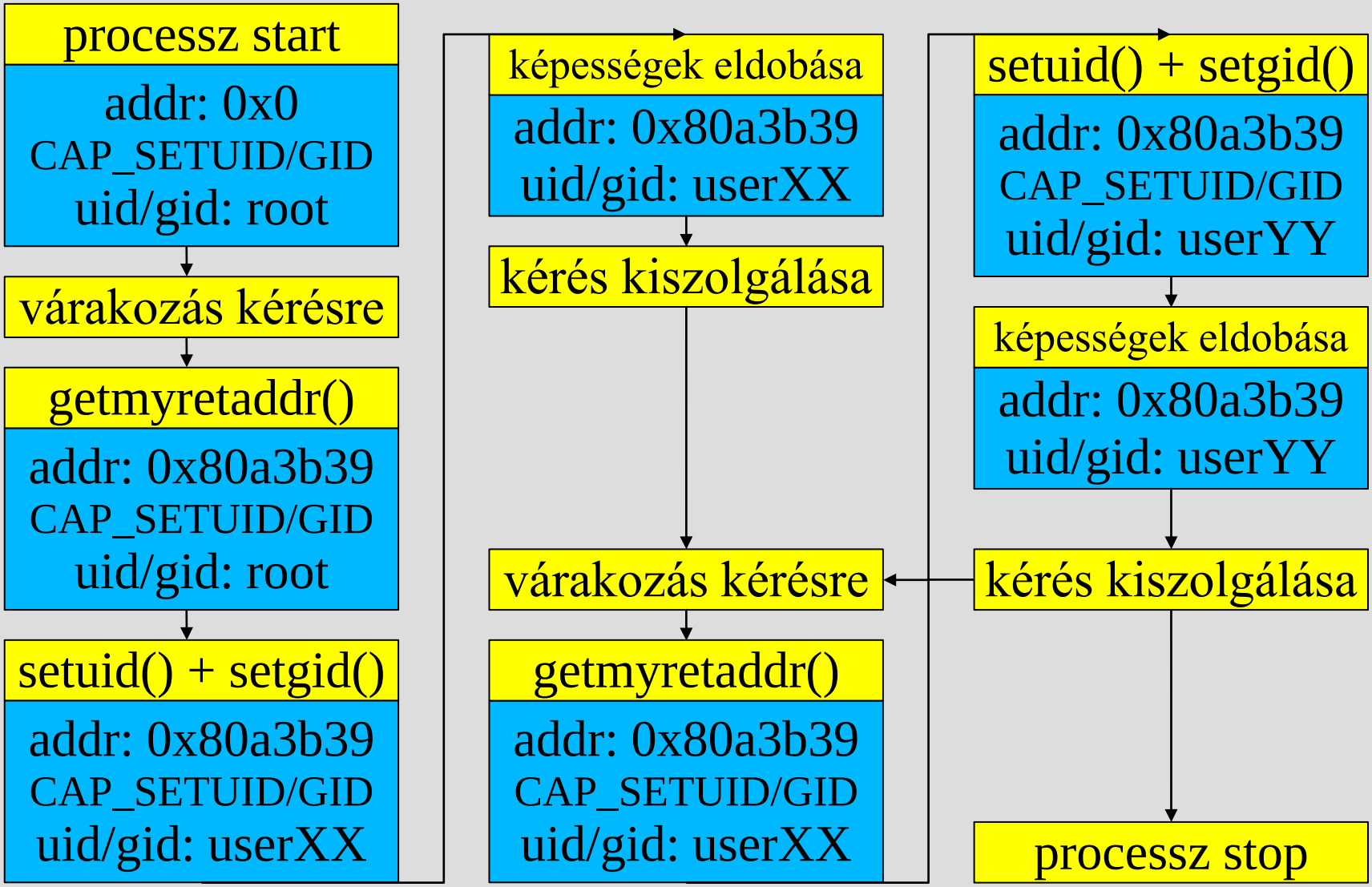
CAP_SETUID/GID + setuid() II.

- A szkript lefutása után visszakapják a képességeket
- Hogyan?
- **Probléma:** van-e jogosultsága visszakapni a processznek a képességeket?
- Mikor legyen?

Jogosultságkezelés a hívó memóriacím alapján

- Nem állapítható meg egyértelműen, hogy a felhasználó váltást maga a webszerver, vagy egy éppen végrehajtott szkript kéri
- Lehetséges megoldás: a kernelbe lépéskor ellenőrzésre kerül, hogy a rendszerhívás honnan lett meghívva
- A rendszerhívás első meghívásakor állítódik be a processz kontextusában, hogy melyik memóriacím lesz “megbízható”
- Ha a “megbízható” címről jött a hívás, akkor kaphat kiemelt jogokat, egyéb esetben nem

Jogosultságkezelés a hívó memóriacím alapján



Apache bővítések

- processzor idő naplózása
  - egy lekérdezés kiszolgálási ideje és az igénybe vett processzor ideje nem feltétlen egyezik meg
  - lekérdezésenként az elhasznált processzor idő user space-ben és kernel space-ben
- processz nevének megváltoztatása
  - alaphelyzetben minden Apache processznek ugyanaz a neve
  - lekérdezés metódusának és az URI-nak a megjelenítése a processz névben
- terhelés függő kiszolgálás
  - ha a rendszerterhelés elér egy bizonyos értéket, a kéréseket ideiglenesen visszautasítja

Futás közben - előtte

Az Apache processzeinek listája a módosítások nélkül, néhány próba lekérdezés közben:

```
$ ps awx -o user,pid,%cpu,%mem,args|grep httpd|grep -v grep

root     5121  0.0 1.2 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
www-data 5122  0.0 1.2 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
www-data 5123  0.1 1.2 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
www-data 5124 33.9 1.2 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
www-data 5125  0.0 1.2 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
www-data 5126 31.0 1.2 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
www-data 5127  0.0 1.1 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
www-data 5128  0.0 1.1 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
www-data 5129  0.0 1.1 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
```

USER PID CPU% MEM% ARGUMENTUM LISTA (PROCESSZ NÉV)

Futás közben - utána

Az Apache processzeinek listája a módosításokkal, néhány próba lekérdezés közben:

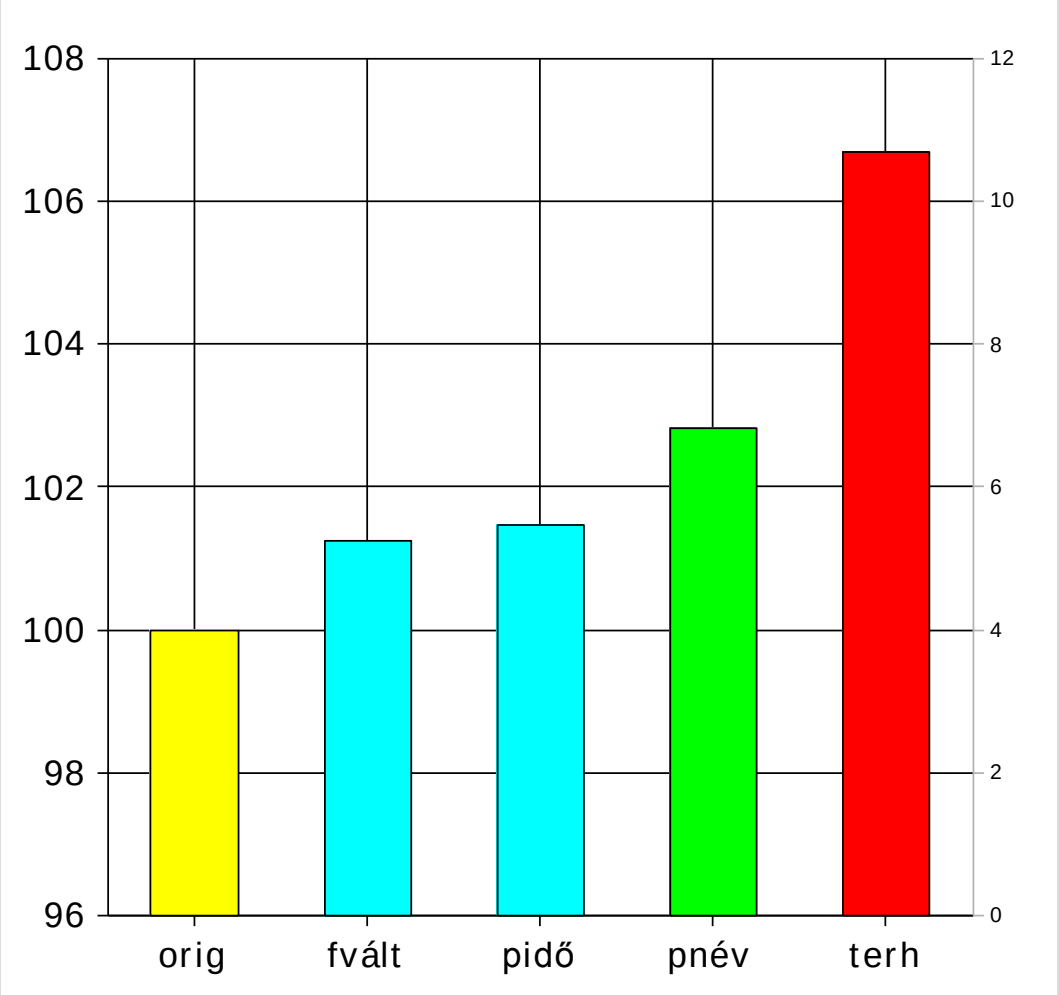
```
$ ps awx -o user,pid,%cpu,%mem,args|grep httpd|grep -v grep

root     4733  0.0 1.2 /mnt/work/nws/apache-2.0.63/bin/httpd -k start
walsh    4734  0.0 1.2 httpd: GET www.host1.hu/aludj.php
kirby    4735 28.3 1.2 httpd: GET www.host2.hu/szamolj.php
charlie  4736  0.0 1.2 httpd: GET www.charlie.hu/aludj.php
david    4737  0.0 1.2 httpd: GET www.david.hu/aludj.php
charlie  4738 26.0 1.2 httpd: GET www.charlie.hu/szamolj.php
www-data 4739  0.0 1.1 httpd: ready
www-data 4740  0.0 1.1 httpd: virgin
www-data 4741  0.0 1.1 httpd: virgin
```

USER PID CPU% MEM% ARGUMENTUM LISTA (PROCESSZ NÉV)

Teljesítmény

- 100.000 megegyező lekérdezés
- 1, 2, 4 párhuzamossági szintekkel
- mindez 3x

- felhasználó váltás: **1,25%<<500-1000%**



Az Apache webszerver biztonsági és egyéb kiegészítései

Köszönöm a figyelmet!