



Vlastnosti hardened kernelu pro každého paranoika

Tomáš Chvátal <scarabeus@gentoo.org>

2013/06/01



Kdo je Tomáš Chvátal

- Vývojář Gentoo od podzima 2008
- Člen councilu od ledna 2010
- Člen KDE týmu (chvilí jim i šéfoval než se objevilo akonadi)
- Správce/vývojář LibreOffice
- Dříve také v Gentoo pracoval na X11, Overlays, Clustering, QA, ...
- Pracuje v SUSE jako L3/QA Maintenance

To byl nápad tu prezentaci dělat česky. Složitější odborné termíny budou v angličtině jinak bysme se z toho zbláznili.



Základní informace

- Projekt pro zvýšení zabezpečení počítače pomocí různých patchů (viz další slide)
- Snahou je co nejvíce těchto vlastností integrovat přímo do hlavního profilu Gentoo
- Z důvodu snížení výkonu některých aplikací a zamezení funkčnosti některých funkcí pro desktop je to stále oddělený projekt

<http://www.gentoo.org/proj/en/hardened/>



Dostupné funkce

- Nastavení toolchainu (kompilér, linker, ..) jako vynucení PIE, kontrola zásobníků při kompilaci, nebo ochrana proti stack-smashingu
- Rozšíření jádra PaX, poskytující non-executable memory, address space layout randomization, ...
- Rozšíření jádra grSecurity, umožňující restrikce chrootu, dodatečný audit, omezení procesů, ...
- Rozšíření jádra SELinux, MAC (Mandatory Access Control) rozšiřující běžná omezení linuxových práv
- Technologie komem Integrity, jako Integrity Measurement Architecture, která chrání systém proti nevídaným změnám



Zabezpečení při kompilaci

PIE a FORTIFY_SOURCE jsou i v základním profilu

- `-DFORTIFY_SOURCE=2`: zabezpečení proti jednoduchým přetečením zásobníků
- `PIE/PIC`: kód nezávislý na pozici v paměti, většina skoků je počítána tedy relativně místo abs. odkazů
- `SSP`: ochrana proti stack-smashing z GCC, přidá na konec (lze i náhodně) zásobníku kanárka který informuje o pokusu o přetečení ať náhodným či cíleným (srandá sledovat s nepomukem)



Zabezpečení při linkování

- -Wl,-z,relro: označí části knihovny pouze pro čtení a znemožní úpravy (GOT, PLT)
- -Wl,-z,now: přeloží všechny symboly a vynutí načtení knihoven při spuštění aplikace (spadne když nejsou všechny splněny) a neznatelně zpomalí první spuštění aplikace



grSecurity

- RBAC část: rozšíření unixových přístupových práv o další možnosti, např. ochrana před brute-force, skrytí ptace vybraným procesům, ...
- Omezení chroot: ochrana proti priv-esc a další omezení/zábrany: zamezený přístup do sdílené paměti z chrootu, nemožnost videt procesy mimo chroot, omezený kill/sgid/...
- Audit: logování činností uživatelů, mount, změny času, použití chdir, zaznamenání příkazů Exec, nezdařené fork...



grSecurity - nastavení

grSecurity obsahuje spoustu možností a vyplatí se je nastudovat s webových stránek projektu.

Gentoo se snaží proti výchozím možnostem (Nízké/Vysoké zabezpečení) přidat ještě možnost desktop/server, kdy jsou ty nejzajímavější možnosti povoleny.

Mimo jádro už se moc věcí pro grSec dělat nemusí, spíše se jedná o nastavení pro PaX.



Technicky vzato se jedná o část grSecurity, která není vyvíjena upstreamem a umožňuje následující činnosti.

- ASLR: náhodné rozmístění adresového prostoru a proto útočník neodhadne rozvržení paměti
- Vynucení stavu paměti: buď je ke čtení nebo pouze k zápisu. VELICE zpomalí systém, zato ho zatraceně dobře zabezpečí (binární drivery pláčou)
- Trampolínky: runtime rozšíření pro SSP dá se říct, protože dělá téměř to samé. Bohužel runtime ovládá PaX a tedy díra v PaX kompromituje celý systém



PaX - ovládání

Doporučuji na testování stáhnout soubor `checksec.sh` a nainstalovat `paxtest`.

- `paxctl -flagy binarka / paxctl-ng -flagy binarka`
- Paxctl zapisuje přímo do elf a nefunguje např. nefunguje na Skype
- Paxctl-ng používá `xattr` (v Gentoo myslím to používá i starý `pax`)

```
root@desktopik: ~ # paxctl-ng -v /usr/lib64/libreoffice/program/  
/usr/lib64/libreoffice/program/soffice.bin:
```

```
PT_PAX      : -em--
```

```
XATTR_PAX: not found
```



PaX - výstup checksec.sh

...

* Does the CPU support NX: Yes

| COMMAND | PID | RELRO | STACK CANARY | NX/PaX | PIE |
|-----------------|------|---------------|-----------------|------------|-------------|
| init | 1 | Full RELRO | Canary found | NX enabled | PIE enabled |
| udev | 2583 | Full RELRO | Canary found | NX enabled | PIE enabled |
| dbus-daemon | 3176 | Full RELRO | Canary found | NX enabled | PIE enabled |
| rsyslogd | 3190 | Full RELRO | Canary found | NX enabled | PIE enabled |
| console-kit-dae | 3209 | Full RELRO | Canary found | NX enabled | PIE enabled |
| polkitd | 3283 | Full RELRO | Canary found | NX enabled | PIE enabled |
| wpa_supplicant | 3520 | Full RELRO | Canary found | NX enabled | PIE enabled |
| wpa_cli | 3527 | Full RELRO | Canary found | NX enabled | PIE enabled |
| smartd | 4089 | Full RELRO | No canary found | NX enabled | PIE enabled |
| X | 3564 | Partial RELRO | Canary found | NX enabled | PIE enabled |

...



PaX

PaX - výstup paxtest

```
# paxtest
Executable anonymous mapping      : Killed
Executable bss                    : Killed
Executable data                   : Killed
Executable heap                   : Killed
Executable stack                  : Killed
Executable anonymous mapping (mprotect) : Killed
Executable bss (mprotect)         : Killed
Executable data (mprotect)        : Killed
Executable heap (mprotect)        : Killed
Executable stack (mprotect)       : Killed
Executable shared library bss (mprotect) : Killed
Executable shared library data (mprotect) : Killed
Writable text segments           : Killed
Anonymous mapping randomisation test : 16 bits (guessed)
Heap randomisation test (ET_EXEC)  : 13 bits (guessed)
Heap randomisation test (ET_DYN)   : 25 bits (guessed)
Main executable randomisation (ET_EXEC) : 16 bits (guessed)
Main executable randomisation (ET_DYN) : 17 bits (guessed)
Shared library randomisation test   : 16 bits (guessed)
Stack randomisation test (SEGMEEXEC) : 23 bits (guessed)
Stack randomisation test (PAGEEXEC) : No randomisation
Return to function (strcpy)        : Vulnerable
Return to function (memcpy)       : Vulnerable
Return to function (strncpy)       : Vulnerable
```



Tomáš Chvátal

Vlastnosti hardened kernelu pro každého paranoika



SELinux

- O SELinuxu nevím téměř nic a zvládl jsem to nastavit pouze jednou
- Doporučuji přečíst si dokumentaci a Svenův blog

<http://www.gentoo.org/proj/en/hardened/selinux/selinux-handbook.xml>

<http://blog.siphos.be/category/gentoo/hardened/>



Advanced Intrusion Detection Environment

- Jedná se o metodu detekce průniku (AIDE).
- V Gentoo je balíček dostupný jako `app-forensics/aide`.
- Je důležité si správně nastavit co vše sledovat (ani málo ani moc)
- Nastavení musí být read-only pokud možno externě (nfs?)
- Skenování by se mělo provádět offline z livecd/memory-sticku



AID - ukázkový výstup

```
AIDE found differences between database and filesystem!!  
Start timestamp: 2013-05-30 16:41:02
```

Summary:

| | |
|------------------------|-----|
| Total number of files: | 625 |
| Added files: | 0 |
| Removed files: | 0 |
| Changed files: | 2 |

Changed files:

```
changed: /etc/pam.d/  
changed: /etc/pam.d/sudo
```





AID - ukázkový výstup - page 2

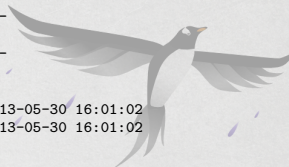
Detailed information about changes:

Directory: /etc/pam.d

| | | |
|-------|-----------------------|-----------------------|
| Mtime | : 2013-05-11 21:09:20 | , 2013-05-30 16:01:02 |
| Ctime | : 2013-05-11 21:09:20 | , 2013-05-30 16:01:02 |

File: /etc/pam.d/sudo

| | | |
|-------|--------------------------------|-------------------------------|
| Size | : 135 | , 80 |
| Mtime | : 2013-05-11 21:09:20 | , 2013-05-30 16:01:02 |
| Ctime | : 2013-05-11 21:09:20 | , 2013-05-30 16:01:02 |
| Inode | : 328303 | , 464053 |
| MD5 | : 239be3ac285c0860e5e81a== | , eLUrP2BKw43eExAZX+d1BA== |
| SHA1 | : e7d7393f0768ed2dbebdBne5V6E= | , KwQ42poukMiqEjKQ7e9xkBNZB8= |

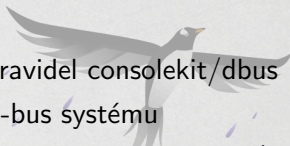




Nejpravděpodobnější možnosti útoků

Nejpravděpodobnější možnosti útoků na desktop v dnešní době

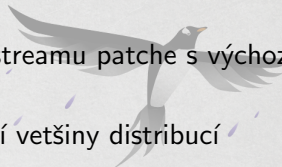
- Zneužití špatně nastavených pravidel consolekit/dbus
- Zneužití špatně nastaveného d-bus systému
- SUID binárka liknovaná s kreativníma knihovnama (Xlib, ...), přecijen suid dává kernel
- pomocí podvržení balíčku (distro od distra podle toho jak mají řešené podpisy)





Obrana

- Přinucení distribucí vracet upstreamu patche s výchozím chováním, které je bezpečné
- Díky předchozímu zabezpečení většiny distribucí
- Odebírání suid bitů kde jen to jde
- Více paranoiků kteří pomáhají s položkou číslo 1





Souhrn

Dotazy

Otázky a odpovědi.





Poděkování

Děkuji za pozornost

