Software security

Aleksey Cheusov
vle@gmx.net

Minsk, Belarus, 2012

Secure string functions

- strlcat, strlcpy (*BSD, Solaris, AltLinux, Cygwin, Interix)
- getline (POSIX 2008)
- snprintf (C99)
- scanf (%Ns)
- ...

Stack smashing protection (SSP)

- Canary
- Available since gcc-4.1 (-fstack-protector, -fstack-protector-all)
- "Base system" compiled with SSP: OpenBSD, NetBSD (partially), AltLinux...
- SSP always enabled in gcc: OpenBSD, AltLinux... (-fno-stack-protector)

Address Space Layout Randomization (ASLR)

- Shared libraries
  - Enabled: Hardened Gentoo, OpenBSD, AltLinux ...
  - Disabled by default: NetBSD (sysctl, paxctl)
- Stack segment
  - Enabled: Hardened Gentoo, OpenBSD, AltLinux ...
  - Disabled by default: NetBSD (sysctl, paxctl)
- Data segment, mmap, PIC (Position Independent Executable)
  - Enabled: Hardened Gentoo, OpenBSD ...

“Chroot is not and never has been a security tool.” ©

Problems

- Unprivileged user: fchdir(2), ptrace(2), getcwd(3)
- Root: mknod(2), mount(8), chroot(2) ...

Solutions

- Unprivileged user: Hardened Gentoo, NetBSD
- Root: Hardened Gentoo, NetBSD (patch)

Non-executable stack and heap (NX bit)

- PaX: Hardened Gentoo, NetBSD (original implementation)
- W^X: OpenBSD
- Exec Shield: Linux kernel (patch), Fedora(?), RHEL(?)

PaX MPROTECT

- Hardened Gentoo
- NetBSD (disabled y default, sysctl, paxctl)

PaX Segvgard

- Hardened Gentoo
- NetBSD (disabled y default, sysctl, paxctl)

Veriexec, a file integrity subsystem

- NetBSD

Per-user directory for temporary files

- NetBSD (/tmp)
- AltLinux (/tmp/.private/$USER, tempnam(3) and others)

Information filtering

- NetBSD (sysctl security.curtain, secmodel_securelevel(9))
- Linux (virtualization technics only (vserver, openvz, lxc etc.)?)

No SUID executables

- Openwall Linux (no SUIDs at all)
- AltLinux (PAM tcb, su and sudo executable by wheel)

Capsicum

- FreeBSD-9 (partially)

File systems in userspace

- FUSE: Linux, FreeBSD, Solaris, OpenBSD
- PUFFS, FUSE over PUFFS: NetBSD

GNU ld: -z,relro -z,now

- Hardened Gentoo
- Source-base packaging systems (pkgsrc)

Hardened Gentoo = grsecurity + PaX

- Enormous amount of features (http://grsecurity.org)

secmodel_securechroot(9) restrictions (NetBSD, p.1)

- chroot(2) and fchroot(2)
- Setting the CPU state using cpuctl(8)
- Debugging-related operations using ipkdb(4)
- Quota operations on file systems
- Using the file system reserved space
- Creating devices using mknod(2)
- Loading and unloading modules
- Processor-set manipulation
- Rebooting the system
- Changing coredump settings for set-id processes
- swapctl(2) modifying operations

secmodel_securechroot(9) restrictions (NetBSD, p.2)

- Mounting new file systems, unmounting, and changing existing mounts
- Access to a process using ptrace(2) and ktrace(2) if it doesn't belong to the same chroot
- Access to a process using procfs if it doesn't belong to the same chroot
- Sending signals to a process if it doesn't belong to the same chroot
- Only processes belonging to the same chroot are visible by, for example, ps(1)
- Decreasing process nice
- Setting the scheduler affinity, policy, and parameters
- Setting the process corename

secmodel_securechroot(9) restrictions (NetBSD, p.3)

- Setting the process resource limits
- Firewall-related operations such as modification of packet filtering rules or modification of NAT rules
- Network interface-related operations such as setting parameters on the device or setting privileged parameters
- Adding and enabling network interfaces
- Modification of network routing tables
- Changing privileged settings of Bluetooth devices.
- Hardware passthru requests and user commands passed directly to the hardware
- Changing the entropy pool and privileged settings of rnd(4)
- Modifying machine-dependent requests
- Access to kmem(4) files /dev/mem and /dev/kmem