What's New with OpenBSD

Brian Callahan <bcallah@openbsd.org>

Intro

- Recap talk
- 10 things in the last year (really 10 months) that have happened in OpenBSD that I think are cool and you should too
- Roughly reverse chronological order

- Ask questions during the talk!

Intro

- About me
  - OpenBSD developer since 2013
  - Ph.D. student at RPI
  - 4-time NYC*BUG talk giver
  - 1-time BSDCan talk giver
  - CDBUG

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

doas(1)

- New userland program that allows you to run a command as another user.
  - Sounds familiar…
- By tedu@

doas(1)

- sudo:

  sudo -h | -K | -k | -V

  sudo -v [-AknS] [-a type] [-g group] [-h host] [-p prompt] [-u user]

  sudo -l [-AknS] [-a type] [-g group] [-h host] [-p prompt] [-U user]
  [-u user] [command]

  sudo [-AbEHnPS] [-a type] [-C num] [-c class] [-g group] [-h host]
  [-p prompt] [-r role] [-t type] [-u user] [VAR=value] [-i | -s]
  [command]

  sudoedit [-AknS] [-a type] [-C num] [-c class] [-g group] [-h host]
  [-p prompt] [-u user] file …

- doas:

  doas [-ns] [-C config] [-u user] command [args]

doas(1)

- Requires an /etc/doas.conf file in order to run.
- pf-inspired syntax
  - Last match wins.
- A basic rule starts with permit or deny and specify a user or group.
  - You can also specify things like nopass, which user you are allowed to run a command as, and which command the rule applies to.

doas(1)

- Let's try it out.

doas(1)

- Caveats
- doas does not do everything sudo does, intentionally.
- If you need something that sudo does that doas does not, the proper solution is:
  - pkg_add sudo
  - You still have reason to buy mwl's book!
- Ports to other operating systems.

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

sudo in ports

- sudo in OpenBSD was quite old.
- It was also lacking some things that might be useful to some people (such as the ability to work with ldap).
- doas pkg_add sudo

sudo in ports

- “Won't sudo be less secure now that it's not in the base system?”

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

tame(2)

- tame(2) restricts what syscalls can be used by a program.
- This is not necessarily an easy thing, as it requires you to study what the program is doing to figure out what syscalls it's using.
- tame(2) is to address similar attacks as FreeBSD's Capsicum, but is able to do so without major program rewrites.

tame(2)

- There's about 30 userland programs that have tame(2) diffs to them to demonstrate how it works.
  - cat pax ps dmesg ping ping6 dc diff finger from id kdump logger script sed signify uniq w wc whois arp authpf bgpd httpd ntpd relayd syslogd tcpdump traceroute

tame(2)

- How hard is it to use?

tame(2)

```
Index: bin/cat/cat.c
===================================================================
RCS file: /cvs/src/bin/cat/cat.c,v
retrieving revision 1.21
diff -u -p -u -r1.21 cat.c
--- bin/cat/cat.c 16 Jan 2015 06:39:28 -0000    1.21
+++ bin/cat/cat.c  24 May 2015 01:03:25 -0000
@@ -35,6 +35,7 @@

 #include <sys/types.h>
 #include <sys/stat.h>
+#include <sys/tame.h>

 #include <ctype.h>
 #include <err.h>
@@ -65,6 +66,8 @@ main(int argc, char *argv[])
    int ch;

    setlocale(LC_ALL, "");
+
+  tame(TAME_STDIO | TAME_RPATH);

    while ((ch = getopt(argc, argv, "benstuv")) != -1)
    switch (ch) {
```

tame(2)

- Debuts in 5.8, but still in active development.
- Follow -current if you want to test/use.

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

SMP steroids for PF

Hello,

attached is SMP patch for PF. consider it as toxic proof of concept as it has paniced my amd64 system (see attached phone-shot). I have to figure out how to debug it yet. The problem is the USB keyboard has died, so I had no chance to type anything. fortunately the issue is 100% reproducible.

The patch compiles in .MP and non-MP version. As you'll see more work is needed to stabilize it and get full SMP support of PF. Those PF features are not covered by SMP changes:

- packet queues
- packet logging
- pf-sync

patch is attached.

Regards
sasha

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

c2k15 highlights

- Mandoc internal jump targets (Ingo)
  - Test drive
- Building softraid volumes with 4K disks, and mixing/matching 4K and 512B in one volume (krw@)
- tcpdump now understands 11n metadata (stsp@)
- Assorted wifi fixes (stsp@)
- UTF-8 in, single-byte locales out (tedu@/stsp@)
  - Possible hackathon for this
- rcctl improvements (ajacoutot@)
  - Future of sysmerge

c2k15 highlights

- Octeon improvements (pirofti@)
- sed -i (jasper@)
- Ruby finds bugs (jeremy@)
- Virtual Private LAN Service (rzalamena@)
- libdrm and Mesa updates (jsg@)
- HTTP Strict Transport Security (HSTS) for httpd(8) (florian@)
- Coffee (afresh1@)

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

OpenSSH everywhere

- Microsoft to integrate OpenSSH into Powershell
- Oracle to drop SunSSH for OpenSSH

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

LibreSSL improvements

- Removal of SSLv3
- More platforms (AIX, Cygwin)
- Routine CVE fixes

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

Autoinstall improvements

- New disklabel(8) flag, -T file (henning@)
  - Partition disk using a file
  - Flat file, one partition per line
    - Partition Minsize(-Maxsize) (Percentage)

Autoinstall improvements

/	1G	
swap	256M-512M	
/var	2G-4G	10%
/tmp	1G-2G	5%
/usr	50G-80G	35%
/home	1G-*	

Autoinstall improvements

- Autoinstall can take advantage of disklabel -T
  - Patch by henning@, tweaked by rpe@
- URL to autopartioning template for disklabel = 127.0.0.1/mytemplate

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

OpenNTPD

- Portable is back (bcook@)
- Using HTTPS headers (NOT TLS timestamp) as a constraint
  - Not for time itself, but to provide a range
  - Mitigates some unauthenticated ntp MITM attacks

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

groff is dying

- Well, USE_GROFF at least…
  - 309 ports still need groff to format their manual pages
  - There are 9144 ports total
  - 3.4%

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

Static PIE

- Self-relocating static binaries
- Demonstration

Topics

- doas(1)
  - sudo in ports
- tame(2)
- MP Networking
  - pf
- c2k15 highlights
- OpenSSH everywhere
- LibreSSL improvements
- Autoinstall improvements
- OpenNTPD
- groff is dying
- Static PIE
- Others...

Others...

- W^X in amd64 kernel
- Portroach
- USB 3.0

Questions?

- Questions/Comments/Flames/Encouragement
  - bcallah@openbsd.org
  - @__briancallahan

The End

- To the bar!