Bezpečný nebo použitelný?
Security or usability?

Is OpenBSD usable on a laptop?

OpenAlt 2023

Jiří Navrátil
https://www.navratil.cz

Me in 2023

- developer, sysadmin*, and dbadmin at Oracle
- Unix lectures at the University of Ostrava
  - two physical servers with OpenBSD
  - virtualisation with vmd(8), vmm(4), and vmctl(8)
  - web server with httpd(8)
  - databases with PostgreSQL and Redis
- freelancer with OpenBSD on physical amd64 and arm64 hardware
- running OpenBSD 7.4 amd64 on my personal laptop

* Oracle Linux and Solaris

Me and Brno

- 1989 - during the Velvet Revolution, as a UJEP student, used dial-up communication over modem to transfer documents between striking college students in Prague, Brno, and Bratislava
- 1990 - Informační Centrum Studentů, BBS / FidoNET
- 1991 - Burešova 20, ÚVT MU, EARN/BitNET
- 1992 - Kounicova 50, 1st dormitory in ČSFR connected to Internet
- 1993 - Decompositions of natural numbers in C/370 on IBM 3090
- 1993 - Kabátníkova 2, car sales over modems for AUTOMARKET
- 1996 - Kabátníkova 2, dial-up node for VOLNÝ (Czech On Line)
- 1998 - Internet against SPT Telecom monopol (www.bojkot.cz)
- 2000 - Aldiscon/Logica Dublin, Ireland; Logica Mobile Networks Prague

When and why OpenBSD?

- 1987 - first owned computer: Atari 1040ST
- 1997 - first owned domain: navratil.cz
- 1997 - got hacked for the first time: Sendmail* on Red Hat Linux
- 1997 - D. J. Bernstein and Unix to rescue: qmail on FreeBSD
- 2002 - started using OpenBSD
- 2015 - added OpenSMTPD: qmail and OpenSMTPD on OpenBSD
- 2015 - OpenBSD 20th birthday celebration in Tieto Ostrava
- 2023 - switched to OpenSMTPD on OpenBSD only

* http://cr.yp.to/maildisasters/sendmail.html

OpenBSD and security

- security* by default
- audit of code
- security bugs are fixed quickly
- security concepts: privilege separation, privilege revocation, W^X (write XOR execute), GOT and PLT protection, ASLR (Address Space Layout Randomization), PIE (position-independent executables), Static-PIE, random-data memory, SROP, library order randomization, fork+exec in privilege separated programs, trapsleds, kernel and sshd relinking at boot, MAP_STACK, MAP_CONCEAL, MAP_STACK, RETGUARD,
- security functions: arc4random(3), pledge(2), unveil(2), issetugid(2), bcrypt(3), strlcpy(3), strlcat(3), strtonum(3), imsg(3), timingsafe_bcmp(3), explicit_bzero(3), ohash(3), asr(3), reallocarray(3), getentropy(2), sendsyslog(2), timingsafe_memcmp(3), getpwnam_shadow(3), getpwuid_shadow(3), recallocarray(3), freezero(3), malloc_conceal(3), calloc_conceal(3), ober(3)

* https://www.openbsd.org/innovations.html

OpenBSD vs security disasters

- Heartbleed in OpenSSL
  - security expert Bruce Schneier „On a scale of 1 to 10, this is an 11“*
  - OpenBSD developers started LibreSSL as OpenSSL fork
  - I compiled OpenBSD from source code to follow development branch
- bash(1) Bashdoor (Shellshock) disclosed**
  - I already used ksh(1) as recommended default shell in OpenBSD

```
$ grep navratil /etc/passwd | awk -F: '{print $7}'
/bin/ksh
$ which ksh
/bin/ksh
$ which bash
/usr/local/bin/bash
```


* https://www.schneier.com/blog/archives/2014/04/heartbleed.html

** https://www.zdnet.com/article/shellshock-makes-heartbleed-look-insignificant/

What I like on OpenBSD

- secure, reliable, and stable
- free* and open-source
- documentation (FAQ, manual pages, papers, source code)
- simple configuration with examples
- daemons and services configured and controlled via rcctl(8)
- many supported platforms** (i386, sparc64, amd64, armv7, arm64, ...)
- support from community and developers
- lower hardware requirements than for Microsoft Windows

* https://www.openbsd.org/policy.html
** https://www.openbsd.org/plat.html

Already benefiting from OpenBSD?

- if you use ssh, then it might be OpenSSH from OpenBSD

```
ssh -V
OpenSSH_9.5, LibreSSL 3.8.2
```

- hackathon type of events come from OpenBSD (or Sun Microsystems)
- many firewalls use pf from OpenBSD

OpenBSD replacements

- ~~sudo~~ - doas
- ~~screen~~ - tmux
- ~~rsync~~ - openrsync
- ~~git~~ - Got: `https://gameoftrees.org/`

„Old“ workstation requirements

- before age of web applications, I had to use Microsoft Windows for
  - editing local documents in Microsoft Office
  - communication with Czech government via IE*
  - communication with Komerční banka via their KB_DATA proprietary software
  - software updates for diving computer Aeris F-10
  - software updates for Garmin watch
  - used dual boot
  - used virtualisation
  - tested GNU/Debian Linux, Ubuntu Linux, Linux from Scratch, Gentoo Linux with compilation from stage 1, OpenSolaris

* the only supported web browser was Internet Explorer running on Microsoft Windows

Apple MacBook with Mac OS X

- bought a refurbished white MacBook for half price
- bought Microsoft Office for Mac OS X
- installed applications from source code (MacPorts, later Homebrew)
- found and reported four bugs in iPhoto application
- no response from Apple
- wrote email to Steve Jobs*
- got call and email** from Maria Deffense, Executive Relations EMEA, Apple Sales International, Cork, Ireland
- the received attention and support prolonged my time with Mac OS X
- still own other Apple MacBook - Air 13-inch, but with OpenBSD***

* Message-Id: 20100501113846.GA18444@navratil.cz, Date: Sat, 1 May 2010
** Message-Id: aea6e5e2-f073-4e7a-9a9a-e2300961cb14@euro.apple.com, Tue, 4 May 2010
*** https://www.nocloud.cz/pub/Apple_is_slowing_down_old_MacBook.pdf

Which laptop for OpenBSD?

- Lenovo ThinkPad laptops are well supported
- I prefer TrackPoint with three buttons*
- older generations (even refurbished) are better**
- supported Wi-Fi card
- touchscreen not needed
- avoid nVidia (too proprietary)
- newer HW may have issues with S3 suspend (try BIOS option)
- Joshua Stein articles: `https://jcs.org/openbsd-laptops`
- repository with BSD dmesg files: `https://dmesgd.nycbug.org/`
- mailing lists with shared details about supported HW or particular issues

* middle button for „paste“

** drivers, discount for refurbished or old generation

My preferred laptop specification

- size 13 or 14 inches
- integrated network card
- matte display
- silent

The X Window System

- no configuration* needed
- `xenodm(1)` - X Display Manager enabled during install

```
grep xenodm /etc/rc.conf.local
xenodm_flags=
```

- I'm removing `xconsole` and adding czech keyboard

```
grep setxkbmap /etc/X11/xenodm/Xsetup_0
setxkbmap cz
```

- `cwm(1)` - X Window Manager**
- config `~/.cwmrc` based on EXAMPLES section in `cwmrc(5)`
- focus follows the mouse
- `redshift` to reduce the amount of blue light
- `termbar.sh` for status bar

* neither Xconfigurator or xf86config is required
** tested also KDE, GNOME, i3, dwm, xmonad

Network

- one line with `ifconfig`

```
doas ifconfig iwx0 nwid OxfordTube -wpakey autoconf
```

- or `hostname.if` and `doas sh /etc/netstart`

```
$ tail -7 /etc/hostname.iwx0
join OxfordTube
join CDWiFi
join "Regiojet - zluty"
join OpenAlt wpakey Open2023
inet autoconf
inet6 autoconf
up
```

- for eduroam with WPA2 Enterprise is required `wpa_supplicant`

```
doas ifconfig iwx0 -wpakey -bssid
doas ifconfig iwx0 nwid eduroam wpa wpaakms 802.1x up
doas wpa_supplicant -c /etc/wpa_supplicant.conf \
  -D openbsd -i iwx0
```

Text editing and processing

```
$ which ed
/bin/ed
$ which vi
/usr/bin/vi
$ which vim
/usr/local/bin/vim
$ which mg
/usr/bin/mg
$ pkg_info emacs | head -1 | cut -c 56-
7.4/packages/amd64/emacs-29.1p0-gtk2.tgz
$ echo $EDITOR
/usr/local/bin/vim
```

- plain TEX with OPmac* macros from RNDr. Petr Olšák

* https://petr.olsak.net/opmac-e.html

Emails

- getmail
- mutt
- mutt_oauth2.py
- signing and encryption with GPG and S/MIME
- Maildir (not mbox)

```
$ ls -1 ~/Maildir | head -1
2002/
$ date; find ~/Maildir -type f | wc -l
Thu Nov  9 17:18:12 CET 2023
  432998
```

- mu for searching in shell

```
$ mu find "openalt.cz" --fields "d s l" --sortfield=date
```

Development

```
$ as -v 2>&1 | cut -c -26
GNU assembler version 2.17
$ nasm -v
NASM version 2.16.01 compiled on Oct  5 2023
$ ld.bfd -v
GNU ld version 2.17
$ ld.lld -v
LLD 13.0.0 (compatible with GNU linkers)
$ cc -v 2>&1 | head -1
OpenBSD clang version 13.0.0
$ rustc -V | cut -c -35
rustc 1.72.1 (d5c2e9c34 2023-09-13)
$ cargo -V
cargo 1.72.1
$ python3.11 --version
Python 3.11.5
```

Web browsers

- surf
- luakit
- w3m

```
w3m -T text/html -dump URL > article.txt
```

- firefox

```
ls /etc/firefox/
pledge.content  pledge.rdd      unveil.content  unveil.rdd
pledge.gpu      pledge.socket   unveil.gpu      unveil.socket
pledge.main     pledge.utility  unveil.main     unveil.utility
```

- chromium(1)

```
iridium --enable-unveil
chrome --enable-unveil --proxy-pac-url=http://wpad/wpad.dat
```

- `doas usermod -L staff $USER`

Packages management

```
$ pkg_info nix | head -1 | cut -c 56-
7.4/packages/amd64/nix-2.3.16p3.tgz
$ pkg_info -Q emacs | wc -l
      13
$ doas pkg_add emacs
$ doas pkg_add -u emacs
$ doas pkg_delete emacs
$ doas pkg_add -u
```

How to install and upgrade OpenBSD

- to get and install OpenBSD for amd64:
  https://www.openbsd.org/amd64.html
- to upgrade existing installation

```
sysupgrade -n
cd /home/_sysupgrade/
rm x* # only for servers without X Window System
reboot
fw_update
sysmerge
syspatch
pkg_add -u
```

My laptop with OpenBSD

- no dual-boot (and even no virtualisation)
  - entire hard drive for OpenBSD
  - replacing Microsoft Windows*
- both swap (by default) and data encrypted - softraid(4)
- soundless fan (`apmd(8)` or `obsdfreqd`)
- buttons „just work“
  - volume mute: F1, down: F2, up: F3
  - brightness decrease: F5, increase: F6
  - keyboard backlight dimming: FN+SPACE
- HDMI external video, USB-A, USB-C

* Can’t buy without Microsoft Windows licence or get refund for not used Microsoft OS

My 2023 laptop configuration 1/3

```
pfetch
      _____          navratil@curufin.navratil.lan
    \-     -/        os      OpenBSD 7.4
 \_/         \       host    ThinkPad E14 Gen 4
 |         O O |     uptime  1d 21h 18m
 |_  <   )  3 )     pkgs    400
 / \         /       memory  2438M / 7852M
    /-_____-\

dmesg | grep iwx0 | head -1 | cut -f1 -d","
iwx0 at pci0 dev 20 function 3 "Intel Wi-Fi 6 AX211" rev 0x01

dmesg | grep em0 | cut -f1 -d","
em0 at pci0 dev 31 function 6 "Intel I219-V" rev 0x01: msi
```

My 2023 laptop configuration 2/3

```
sysctl hw | grep -v sensors | head -12
hw.machine=amd64
hw.model=12th Gen Intel(R) Core(TM) i3-1215U
hw.ncpu=8
hw.byteorder=1234
hw.pagesize=4096
hw.disknames=sd0:4c4c2cc9a93fd2ac,sd1:41524463baee8440
hw.diskcount=2
hw.cpuspeed=2501
hw.setperf=100
hw.vendor=LENOVO
hw.product=21E3005HCK
hw.version=ThinkPad E14 Gen 4

sysctl hw.smt
hw.smt=0
```

My 2023 laptop configuration 3/3

- encrypted hard (NVMe) drive
- resolution 1920x1080, 32bpp

```
dmesg | grep sd0
sd0 at scsibus1 targ 1 lun 0: <NVMe, Micron MTFDKCD51, 7003>
sd0: 488386MB, 512 bytes/sector, 1000215216 sectors

dmesg | grep sd1
sd1 at scsibus3 targ 1 lun 0: <OPENBSD, SR CRYPTO, 006>
sd1: 488126MB, 512 bytes/sector, 999682111 sectors
root on sd1a (41524463baee8440.a) swap on sd1b dump on sd1b

dmesg | grep "^inteldrm0"
inteldrm0 at pci0 dev 2 function 0 "Intel Graphics" rev 0x0c
inteldrm0: msi, ALDERLAKE_P, gen 12
inteldrm0: 1920x1080, 32bpp
```

Battery

```
apm
Battery state: high, 99% remaining, unknown life estimate
AC adapter state: connected
Performance adjustment mode: auto (2501 MHz)

apm
Battery state: high, 99% remaining, 408 minutes life estimate
AC adapter state: not connected
Performance adjustment mode: auto (400 MHz)

expr 408 / 60
6

bc
scale=2
408/60
6.80
```

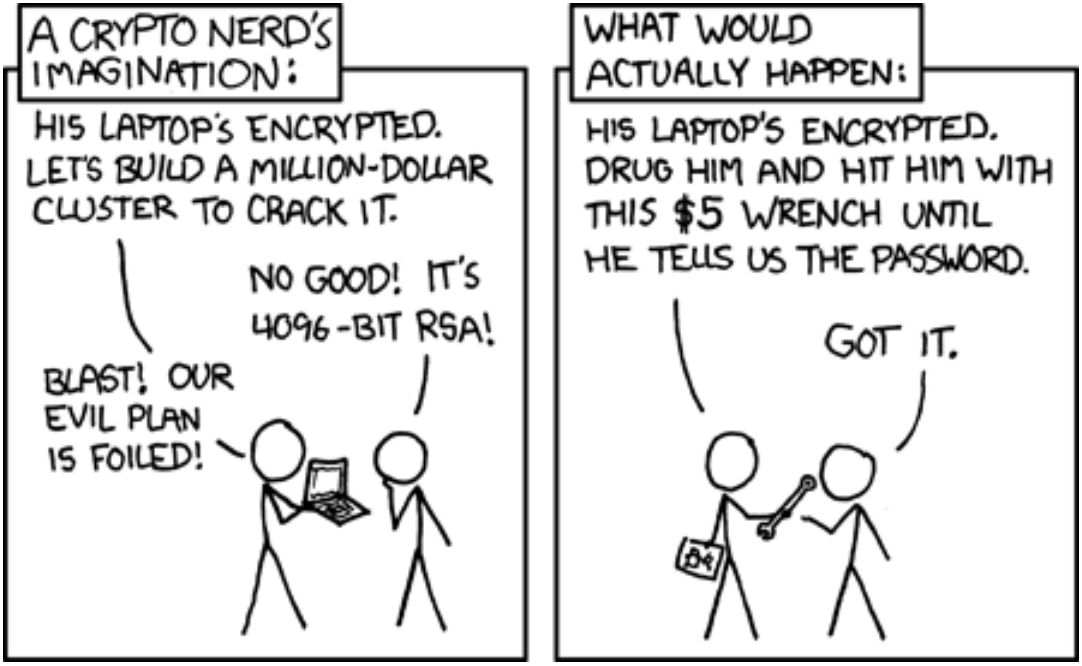
I own my data

- my shell history, emails, source code and notes are stored on my laptop
- only big files like audio/video recordings and photos are stored in different places
- some files are just placed in home directory, some are sorted into particular directories and some are also versioned in Fossil SCM or Git
- I use two locations connected via IPsec as my LAN
- I can connect laptop to LAN from Internet via ssh with ed25519 key
- my web sites, domains and emails are hosted on my hardware with OpenBSD

OpenBSD urls, Unix&GNU/Linux names

- OpenBSD FAQ (Handbook) https://www.openbsd.org/faq/
- OpenBSD Events and Papers https://www.openbsd.org/events.html
- OpenBSD Innovations https://www.openbsd.org/innovations.html
- Brian Kernighan https://www.cs.princeton.edu/~bwk/
- Dennis Ritchie https://www.bell-labs.com/usr/dmr/www/
- Ken Thompson http://cs.bell-labs.co/who/ken/
- Bill Joy*
- Theo de Raadt https://www.theos.com/deraadt/
- Steve Jobs https://www.apple.com/stevejobs/
- Linus Torvalds https://github.com/torvalds
- Richard Stallman https://stallman.org/

* https://engineering.berkeley.edu/bill-joy-co-founder-of-sun-microsystems/



https://xkcd.com/538/

Thank you for your attention

https://openalt.navratil.cz/