OpenBSD 30th Anniversary

Celebrating Security and Freedom

Jiří Navrátil

Me in 2025

- System Architect at CGI
- Self-hosting domains, emails, and web sites using OpenBSD on physical hardware
- Personal laptop[1] running OpenBSD
- Unix lectures at the University of Ostrava utilizing OpenBSD on physical hardware
- Authoring a book on OpenBSD, virtualization, containerization, and Kubernetes

[1] https://openbsd.navratil.info/openbsd_on_laptop/tuxedo_aura_14_gen3/

Me and OpenBSD

- 1987 - first owned computer: Atari 1040ST
- 1995 - birth of OpenBSD[2]
- 1997 - first owned domain: navratil.cz
- 1997 - got hacked: Sendmail[3] on Red Hat Linux
- 1997 - D. J. Bernstein and Unix to rescue: qmail on FreeBSD
- 2002 - started using OpenBSD[4]
- 2015 - added OpenSMTPD: qmail and OpenSMTPD on OpenBSD
- 2015 - OpenBSD 20th birthday celebration in Tieto Ostrava
- 2023 - switched to OpenSMTPD on OpenBSD only
- 2023 - gave a talk at the OpenAlt conference about OpenBSD on my notebook
- 2025 - OpenBSD 30th birthday celebration in CGI Prague

[2] Wait for more details and evidence.
[3] http://cr.yp.to/maildisasters/sendmail.html
[4] Based on advice from Jan Fikar at University of Lausanne, Switzerland.

Unix history 1/3

- 1961 MIT created CTSS (Compatible Time Sharing System) - success
- 1965 MIT, General Electric and Bell Labs started work on Multics
  - too complex
  - too expensive
  - not a success
- 1969 Bell Labs pulled out their scientists
  - Ken Thompson find unused DEC PDP-7
  - Dennis Ritchie
  - proto-Unix (file system, shell, editor, assembler)
  - keep good ideas and make it simpler

Unix history 2/3

- 1970 better machine DEC PDP-11/20
  - Ken Thompson promised software for patent department
  - real version of Unix was developed on this machine
- 1st Edition Unix, late 1971
  - multiple independent and simultaneous users
  - well documented, man pages
- 2nd Edition Unix, June 1972 „The number of Unix installations has grown to 10, with more expected“.
- 6th Edition Unix, May 1975
  - hierarchical file system, flat files
  - programmable shell
  - regular expressions
  - pipes
  - tools and languages

Unix history 3/3

- The C programming language
  - BCPL - Martin Richards, Cambridge, UK
  - B - Ken Thompson
  - C - Dennis Ritchie, 1972 - 1973
- Sufficiently expressive and efficient[5]
- Portable C compiler - Steve Johnson
- Portable operating system $\rightarrow$ workstations from Sun Microsystems, Silicon Graphics (SGI), Hewlett-Packard (HP), Digital Equipment Corporation (DEC), IBM, NeXT Computer
- Split to two major branches: Berkeley Software Distribution (BSD) and AT&T System V
- Microsoft Xenix was considered the dominant variant of Unix during the mid-to-late 1980s
- Microsoft sold Xenix to SCO[6] and focused on PC market[7]
- „Unix Wars“ in the 1980s and early 1990s

[5] Limited resourced
[6] Santa Cruz Operation
[7] DOS, OS/2 and eventually Windows

Berkeley Software Distribution branch

- OpenBSD continues the lineage of BSD Unix.
- Besides OpenBSD, the BSD family also comprises of these open-source Unix-like operating systems
  - FreeBSD - Performance, advanced networking, and enterprise features like OpenZFS. More permissive about including proprietary or Binary Large Object (BLOB) drivers (sometimes requiring NDAs), which aids hardware compatibility.
  - NetBSD - Portability and supporting diverse hardware. Its motto is „Of course it runs NetBSD“.
  - DragonFly BSD - Scalability and modern multiprocessing/clustering. HAMMER2 file system.
- Commercial and proprietary macOS is also derived from the BSD Unix, and moreover is
  - UNIX 03 certified from The Open Group as compliant with the Single UNIX Specification
  - POSIX (Portable Operating System Interface) certified

UNIX System V branch

- Illumos - open-source OS that was forked from OpenSolaris after Oracle discontinued OpenSolaris.
- Proprietary, commercially licensed and certified UNIX® systems
  - IBM AIX
  - Oracle Solaris[8]
  - HP-UX

[8] The first generation of Sun's OS was BSD-based, but the famous Solaris line was based on System V Release 4.

GNU

- GNU is Not Unix
- 27.09.1983 - announced by Richard Stallman (RMS)
- software should be free (in the sense of liberty, not price) for users to study, modify, and share
- develop a complete, free operating system (like Unix, but entirely free)
- The GNU Toolchain (Development Tools): GNU Compiler Collection (GCC), GNU C Library (glibc), GNU Binutils (Binary Utilities), GNU Debugger (GDB), GNU make, GNU Autotools (Autoconf, Automake, Libtool)
- GNU Core Utilities (Coreutils)
  - File Utilities: ls, cp, mv, rm, mkdir, chmod, chown, chgrp
  - Text Utilities: cat, grep, sed, awk, head, tail
  - Shell Utilities: Bash, date, echo, hostname, pwd, who, man
- only missing piece for a complete free OS was the kernel[9]

[9] Search or ask for „GNU Hurd“

Linux kernel, GNU/Linux, Distributions

- 1991 first version of Linux kernel by Linus Torvalds
- GNU + Linux = tools + kernel = GNU/Linux free OS (often shortened as Linux)
- Linux Distributions (Debian, Red Hat, ...) bundle of the kernel, GNU tools and applications
- Android and Alpine Linux use Linux kernel, but non-GNU tools
- Dominance on servers, containers, high performance computing, IoT and Edge Computing
- Small percentage on desktop market
- Unix-like dominance as mobile OS (Android + iOS)

OpenBSD birthday

```
$ cd $HOME/OpenBSD/src/src
$ cat CVS/Root
anoncvs@anoncvs.eu.openbsd.org:/cvs
$ cvs log bin/cat/cat.c | tail -14
----------------------------
revision 1.2
date: 1996/06/23 14:19:02;  author: deraadt;  state: Exp;  lines: +2 -1;
update rcsid
----------------------------
revision 1.1
date: 1995/10/18 08:37:01;  author: deraadt;  state: Exp;
branches:  1.1.1;
Initial revision
----------------------------
revision 1.1.1.1
date: 1995/10/18 08:37:01;  author: deraadt;  state: Exp;  lines: +0 -0;
initial import of NetBSD tree
=============================================================================
```

OpenBSD and security

- security[10] 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)

[10] 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“[11]
  - OpenBSD developers started LibreSSL as OpenSSL fork
  - I compiled OpenBSD from source code to follow development branch
- bash(1) Bashdoor (Shellshock) disclosed[12]
  - 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
```

[11] https://www.schneier.com/blog/archives/2014/04/heartbleed.html
[12] https://www.zdnet.com/article/shellshock-makes-heartbleed-look-insignificant/

What I like on OpenBSD

- secure[13], reliable, and stable
- free[14] and open-source
- simple configuration with examples
- comprehensive documentation (FAQ, manual pages, source code, papers)
- daemons and services configured and controlled via rcctl(8)
- many supported platforms[15] (i386, amd64, armv7, arm64, sparc64, ...)
- support from community and developers

[13] https://www.openbsd.org/innovations.html
[14] https://www.openbsd.org/policy.html
[15] https://www.openbsd.org/plat.html

You and OpenBSD?

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

```
ssh -V
OpenSSH_10.0, LibreSSL 4.1.0
```

- **hackathon** type of events come from OpenBSD (or Sun Microsystems)
- many firewalls use **pf** from OpenBSD
- ~~OpenSSL~~ → LibreSSL
- ~~sudo~~ → doas
- ~~screen~~ → tmux
- ~~rsync~~ → openrsync[16]
- ~~git~~ → Got: https://gameoftrees.org/

[16] Search or ask for „openrsync on macOS“

How to install and upgrade OpenBSD

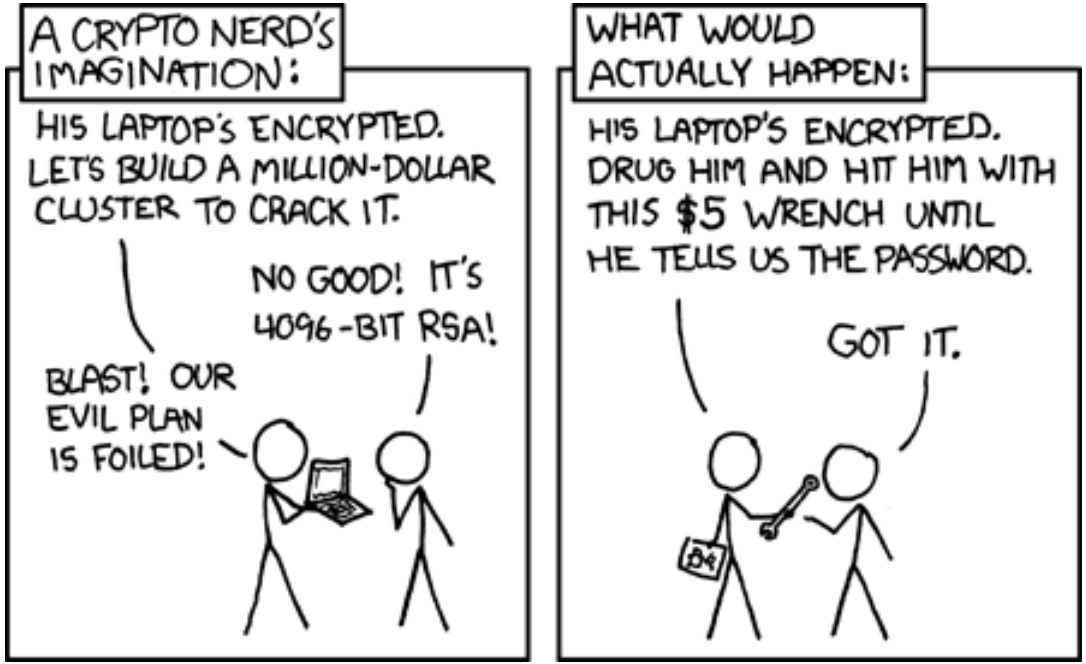
- to get and install OpenBSD for amd64: https://www.openbsd.org/amd64.html
- to upgrade existing installation

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

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[17]
- 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/

[17] https://engineering.berkeley.edu/bill-joy-co-founder-of-sun-microsystems/



https://xkcd.com/538/

Thank you for your attention

https://openbsd.navratil.info/