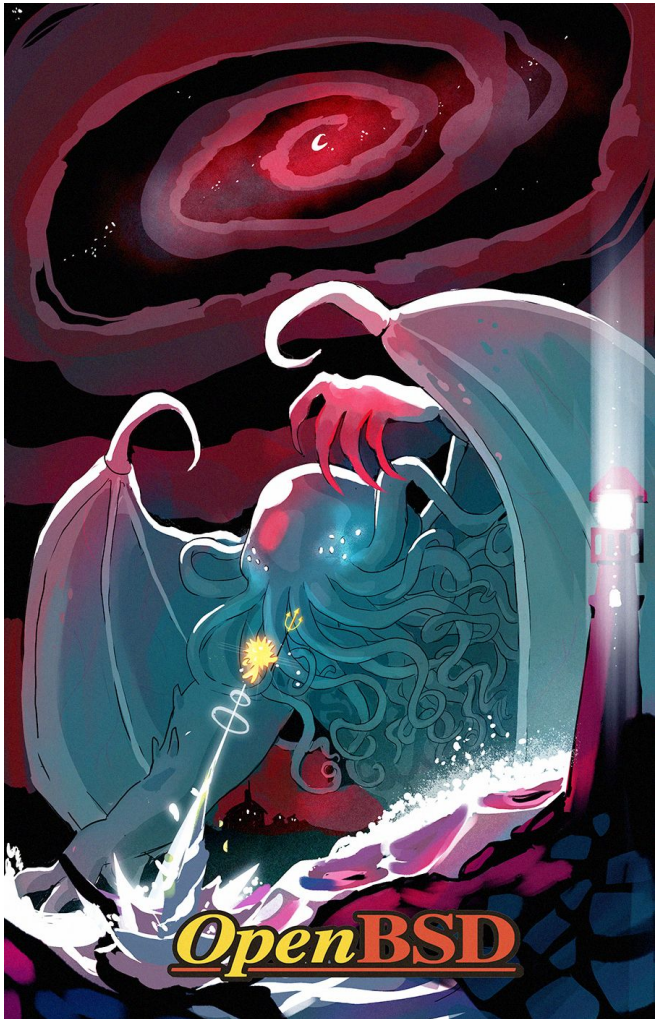
OpenBSD

Einblick, Überblick und Ausblick



Open**R**hein**R**uhr 2018
Rafael Sadowski <rsadowski@openbsd.org>

whoami(1)

- Erste Aktivität auf ports@
  - May 04, 2011; 1:18pm
  - NEW: graphics/opencv
- April 2017
  - Invitation
  - CVS commit rights
- Night-Job
  - OpenBSD ports (KDE5, CMake, Qt)
- Day-Job
  - IT Consultant - Computacenter AG & Co. oHG

- **FREIES** UNIX-like Betriebssystem
- Forked NetBSD. **Theo de Raadt** (October 18, 1995)
- amd64, i386, arm7, arm64, sparc64 …
- Wir sind die mit dem **Kugelfisch** und **Aluminiumhütten**!?

Alle Details gibt es auf
https://www.OpenBSD.org

OpenBSD - Projektziele

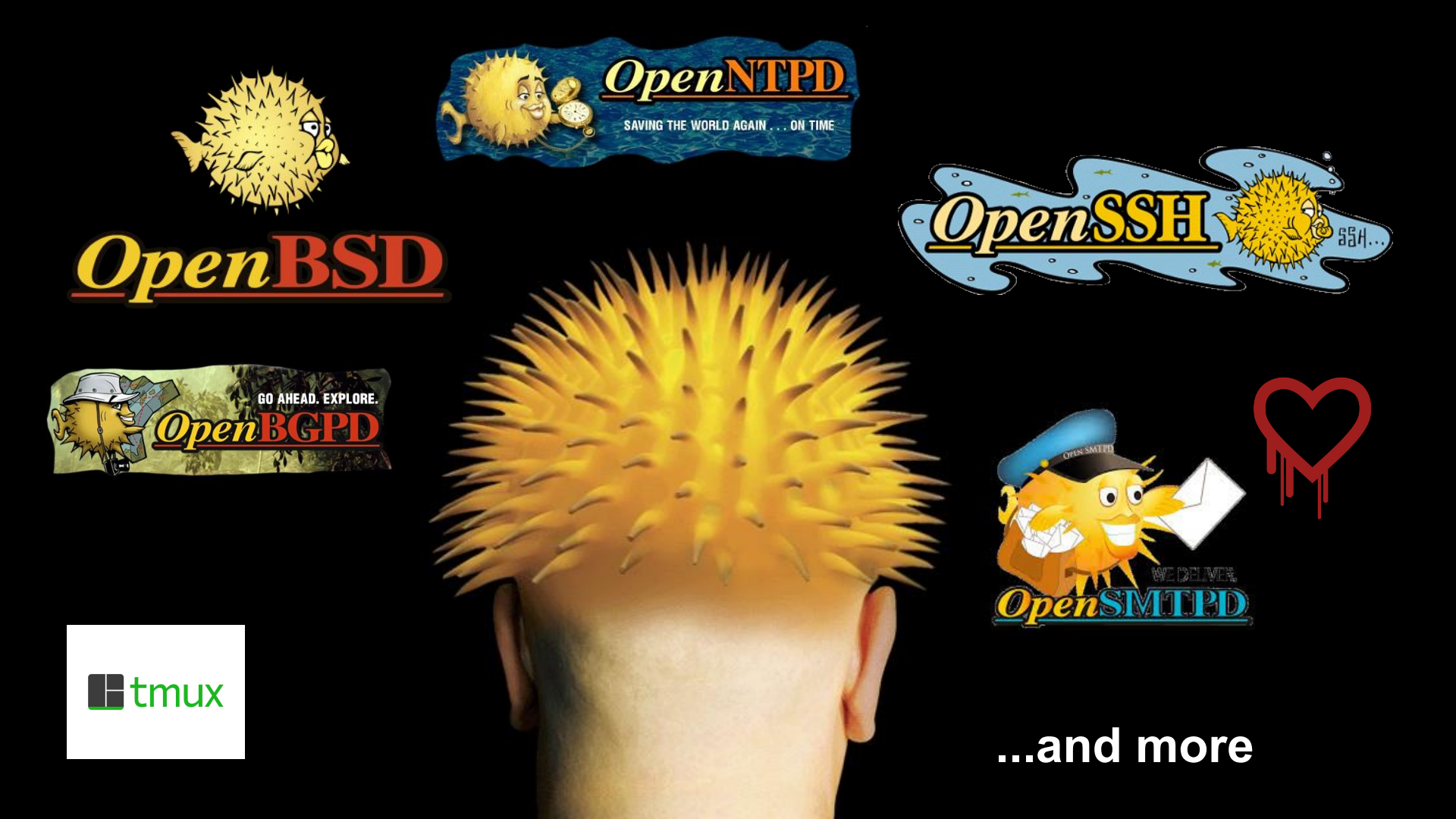
- “Try to be the #1 **most secure o**perating **s**ystem.”
- Bereitstellung der bestmöglichen **Entwicklungsplattform**.
- Ausschließlich Software verwenden, die **freien Lizenzen** unterliegt
- **Standards** (ANSI, POSIX, parts of X/Open, etc.)
- Politikfreie dafür **technische Entscheidungen**
- **Releases** in regelmäßigen Abständen ~6 Monate

Release Zyklus

-release, ca. Alle 6 Monate
-stable, *Release*, und patches (Support für **6.3** und **6.4**)
-current, Entwicklungszweig (rolling release)

OpenBSD-Entwicklungskultur

- Theo ist: **Chef**, Koordinator und Motivator
  - Trotzdem ist **OpenBSD ein Team**, mittlerweile ca. 80 Entwickler weltweit
- Wer viel an einem bestimmten **Subsystem** entwickelt wird dafür **verantwortlich.**
- Richtig, sauber und langfristig als schnell.
  - **Evolution statt Revolution**
- Aufteilung
  - **src (Kernel und Userland)**
  - **ports**
  - **xenocara (X11)**
    - Xenocara ist die OpenBSD-Build-Infrastruktur für den angepassten X.Org-Server des Projekts
  - **www**
- "**In-tree**"-Entwicklung
- **Mehraugenprinzip**
- **Hackathons**


OpenNTPD
SAVING THE WORLD AGAIN . . . ON TIME
OpenBSD
OpenSSH
SSH...
GO AHEAD. EXPLORE.
OpenBGPD
OpenSMTPD
tmux
...and more

Open**BSD** innovations

Software und Ideen entwickelt oder betreut vom OpenBSD Projekt:
https://www.openbsd.org/innovations.html

- ypbind(8), ypset(8), ypcat(1), ypmatch(1), ypwhich(1)
- ypserv(8)
- mopd(8)
- AnonCVS
- aucat(1)
- OpenSSH
- mg(1)
- m4(1)
- pf(4), pfctl(8), pflogd(8), authpf(8), ftp-proxy(8)
- systrace(4), systrace(1)
- spamd(8)
- dc(1)
- bc(1)
- sensorsd(8)
- pkg_add(1)
- carp(4)
- OpenBGPD including bgpd(8) and bgpctl(8)
- dhclient(8)
- dhcpd(8)
- hotplugd(8)
- OpenNTPD including ntpd(8) and ntpctl(8):
- dpb(1)
- ospfd(8), ospfctl(8
- ifstated(8)
- bioctl(8)
- hostapd(8)
- watchdogd(8):
- sdiff(1)
- dvmrpd(8), dvmrpctl(8)
- ripd(8), ripctl(8)
- pkg-config(1)
- relayd(8) with relayctl(8)
- cwm(1)
- ospf6d(8), ospf6ctl(8)
- libtool(1)
- snmpd(8), snmpctl(8)
- sysmerge(8)
- ypldap(8)
- OpenSMTPD including smtpd(8), smtpctl(8), makemap(8)
- mandoc including mandoc(1), man(1), apropos(1), makewhatis(8), man.cgi(8)
- ldapd(8), ldapctl(8)
- OpenIKED including iked(8) and ikectl(8)
- iscsid(8), iscsictl(8)
- rc.d(8), rc.subr(8)
- tftpd(8)
- npppd(8), npppctl(8)
- ldomd(8), ldomctl(8)
- sndiod(8)
- cu(1)
- identd(8)
- slowcgi(8)
- signify(1)
- htpasswd(1)
- LibreSSL
- httpd(8)
- rcctl(8)
- file(1)
- doas(1)
- radiusd(8)
- eigrpd(8), eigrpctl(8)
- rebound(8):
- vmm(4), vmd(8), vmctl(8).
- pdisk(8)
- mknod(8)
- audioctl(1)
- switchd(8), switchctl(8)
- acme-client(1)
- syspatch(8)
- xenodm(1)
- ocspcheck(8)
- slaacd(8)
- rad(8)
- tmux, tmux(1)
- ldpd(8), ldpctl(8)

pledge(2)

```
if (pledge("rpath dns audio proc", NULL) == -1) {
        err(1, "pledge");
}
```

- **rpath**
  - A number of system calls are allowed if they only cause read-only effects on the filesystem: chdir(2), getcwd(3), openat(2), fstatat(2), faccessat(2), readlinkat(2), lstat(2), chmod(2), fchmod(2), fchmodat(2), chflags(2), chflagsat(2), chown(2), fchown(2), fchownat(2), fstat(2), getfsstat(2)
- **dns**
  - Subsequent to a successful open(2) of /etc/resolv.conf, a few system calls become able to allow DNS network transactions: sendto(2), recvfrom(2), socket(2), connect(2)
- **proc**
  - Allows the following process relationship operations: fork(2), vfork(2), kill(2), getpriority(2), setpriority(2), setrlimit(2), setpgid(2), setsid(2)
- **audio**
  - Allows a subset of ioctl(2) operations on audio(4) devices (see sio_open(3) for more information): AUDIO_GETPOS, AUDIO_GETPAR, AUDIO_SETPAR, AUDIO_START, AUDIO_STOP

OpenBSD - Standard installation

- **5 min** erledigt (KISS)
- Security by default
- Aktuelle Software
  - Firefox
  - Xfce
  - Chromium
- Vollständiges Betriebssystem
  - Kernel
  - Userland
  - Xenocara (based on X.Org 7.7 with xserver 1.19.6 …)
- LLVM/Clang/LLD 6.0.0
- Perl 5.24.3, NSD 4.1.25, Unbound 1.8.1
- ...

- syspatch(8)
- vmm(4), vmd(8), vmctl(8)
- httpd(8)
- pf(4)
- ipsec(4)
- rcctl(8)
- ifconfig(8)
- doas(1)
- tmux(1)
- cwm(1)
- ...

OpenBSD 6.4

- Simultaneous MultiThreading (~~SMT~~)- ~~Hyper-Threading~~
  - **(Fri, 2 Nov 2018) CVE-2018-5407**: new side-channel vulnerability on SMT/Hyper-Threading architectures
- OpenBSD/**arm64 mit ACPI**
- Mehr Hardware Support
- Mehr **OpenBSD-Hypervisor** vmm(4)
- **radeondrm**(4) driver was updated to code based on Linux 4.4.155
- IEEE 802.11 **'join'** feature … alles über **ifconfig(8)**
- Mehr **Security** (New RETGUARD, MAP_STACK ... Meltdown, SpectreRSB Intel L1 mitigations...)
- Mehr OpenSMTPD OpenBGPD, OpenSSH und LibreSSL 2.8.2
- **unveil**(2) und mehr **pledge**(2)

unvail(2)

```
if (unveil("/etc/pf.os", "r") == -1) {
        err(1, "unveil");
}
```

- R -Make path available for **read** operations, corresponding to the pledge(2) promise rpath.
- W -Make path available for **write** operations, corresponding to the pledge(2) promise wpath.
- X - Make path available for **execute** operations, corresponding to the pledge(2) promise exec.
- C - Allow path to be **created** and **removed**, corresponding to the pledge(2) promise cpath.

Ausblick auf OpenBSD 6.5

Das kann niemand zu 100% sagen. Wieso? OpenSource!

- OpenSMTPD, OpenBGPD**!**
- unveil(2)**!**
- Mehr Hardware Support**!**
- SMP network**!**
- SMP syscalls**!**
- Mehr KDE5 Applikationen**!**
- GitLab**!?**
- X11 Security**?**

OpenBSD ist nicht perfekt!

Pros

- Security - “Secure by default”
- Stabilität
- Dokumentation
- Ein OS aus einem Guss
- Benutzerfreundliche Konzepte
- Stabile, moderne Software (packages)
- Server und Desktop OS
- Kein systemd

Cons

- Security kostet
- SMP
- Filesystem
  - ZFS?
- Keinen grafischen Installer
- NVidia
- Wayland
- Docker

Wir sollten reden ...

Fragen?

Vielen Dank

für Eure Aufmerksamkeit und an die Organisatoren des ORR 2018

https://www.rsadowski.de

rs@rsadowski.de, rsadowski@openbsd.org