Aktuelles in OpenBSD

Sebastian Benoit <benno@openbsd.org>
Stefan Sperling <stsp@openbsd.org>

Schwerpunkte des Projekts

- UNIX-artiges Betriebssystem [1]
- offener Quellcode
- freie Lizenz (ISC)
- Fokus auf Korrektheit und Sicherheit
- hochwertige Dokumentation auf dem laufenden System

[1] basierend auf 4.4BSD-lite von UC Berkeley

Aktuelle Daten

- Oktober 2015: 20 Jahre OpenBSD, Release 5.8
- Aktueller Release: 6.2
  - Wir bringen 2 Releases im Jahr raus.
  - Wir patchen Bugs in den letzten 2 Releases.
  - -current ist derzeit bereits 6.3-beta
- ca. 70 aktive bis semi-aktive Entwickler (base + ports)
- ca. 5 Hackathons jedes Jahr, einer davon gross (ca. 40 Entwickler)

Entwicklergemeinschaft

Anwendergemeinschaft

https://xkcd.com/349/

- Technische Experten
- Individuen
- Firmen und Konzerne
- Spenden an die OpenBSD Foundation (Geld)
  - Reisekosten Hackathons, Stromrechnung Infrastruktur, Hardware
- Spenden an individuelle Entwickler (Hardware, Bier, ...)

Releasezyklus

- zwei Releases im Jahr (ca. alle 6 Monate)
- Sicherheits-Patches für 1 Jahr
- Fokus auf Stabilität bevor ein Release geschnitten wird
- Invasive und experimentelle Änderungen warten bis nach dem Release
- Snapshots
- Zum Release passende Bildmaterialien und Lieder

Basissystem versus Ports

- vollfunktionales und konsistentes Basissystem
- vernünftige Voreinstellungen vereinfachen die Systemkonfiguration
- Der Quellcode des Basissystems wird kontinuierlich gesichtet
- Applikationen von Dritten werden separat verpackt
  - Desktop Umgebungen, Firefox, LibreOffice, ...
  - Programmiersprachen, Datenbanken, wissentschaftliche Werkzeuge, ...
  - Multimedia, Videospiele, ...

Hardwareunterstützung

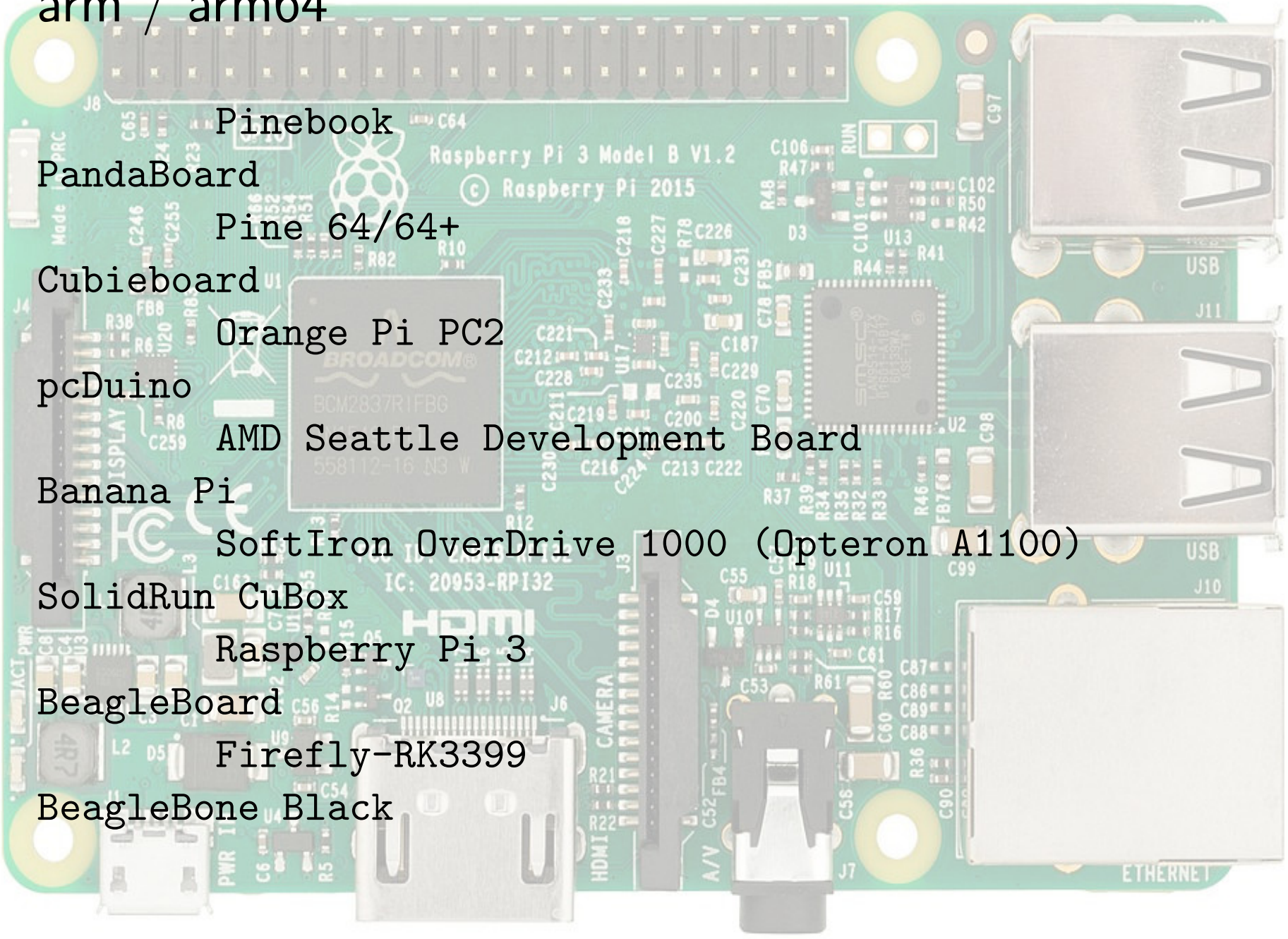
- Architekturen (amd64, i386, sparc64, arm, powerpc, ...)
- Clang als Compiler für arm64 importiert
  inzwischen auch amd64, sparc64 und i386.
- aktuelle Laptops
- Grafikkarten (Intel und AMD, kein Nvidia Treiber)
- Netzwerk Geräte (Ethernet, WLAN, UMTS)
- ACPI inkl. Ruhemodus (suspend-to-RAM, suspend-to-disk)

Blobs

- Wir haben keine Blobs (Binary Large Objects)
- Mit “Blobs” meinen wir Gerätetreiber mit geschlossenem Quellcode
- Firmware läuft auf einen Peripheriegerät, nicht auf der CPU
- Firmware läuft oft mit hohen Privilegien; die Risikoabwägung liegt beim Nutzer
- Firmware wird vermieden, in dem man die entsprechende Hardware nicht kauft
- Wir sind Softwareentwickler, wir bauen keine Hardware
- Wir unterschreiben keine NDAs (im Gegensatz zu den meisten anderen Projekten)
- Wir wünschen uns, dass dieses Problem in der Industrie mehr diskutiert wird, da die aktuelle Situation insgesamt sehr schlecht für Freie Software ist

arm / arm64

- Pinebook
- PandaBoard
- Pine 64/64+
- Cubieboard
- Orange Pi PC2
- pcDuino
- AMD Seattle Development Board
- Banana Pi
- SoftIron OverDrive 1000 (Opteron A1100)
- SolidRun CuBox
- Raspberry Pi 3
- BeagleBoard
- Firefly-RK3399
- BeagleBone Black



Virtualisierung

- Unterstützung als Gast von Xen, Vmware, KVM, Hyper-V
  - Entwickler: mikeb@, reyk@, sf@
  - man pages: pvbus(4)
- Gastgeber und Gast für Sparc T1 / T2 “Logical Domains”
  - Multi-host Sparc Server ohne Solaris :-) vvrrrm vrrrmmmmm...
  - Entwickler: kettenis@, stsp@ (Bugfixes)
  - man pages: ldomd(8), ldomctl(8)
- Gastgeber und Gast für Intel VT mit vmm(4)
  - inklusive Live-Migration des Gasts (mit kurzem Schlaf)
  - Entwickler: mlarkin@, pd@
  - man pages: vmm(4), vmd(8), vmctl(8)
- Tools für Cloud-Netzwerke: switch(4), switched(8), vxlan(4)

WLAN

OpenBSD unterstützt die 802.11a/b/g/n Standards

- WLAN Entwickler: reyk@ (2004-2009), damien@ (2004 - 2011), stsp@, kevlo@
- Treiber für Atheros, Intel, Ralink/Mediatek, Realtek
- 802.11n derzeit eingeschränkt
  - Tx-Aggregation und 40-MHz Kanäle fehlen noch
- Neu in OpenBSD 6.3:
  - Roaming zwischen Access Points mit Intel WLAN (stsp@)
  - Atheros USB Treiber nutzt Open Source Firmware[2] (stsp@)
  - Neuer Treiber für Broadcom 802.11ac ist in Arbeit (patrick@)

[2] `https://github.com/qca/open-ath9k-htc-firmware`

Sicherheit

spielt eine Rolle bei Entscheidungen, z.B. “sane defaults”.

- Verlässliche Zufallszahlen[3]
- Separation von Privilegien
- pledge
- Schutz vor Stapelüberlauf
- ASLR
- W^X
- Entwickler: deraadt@, und viele andere je nach Thema
- Meltdown fix seit letzter Woche (guenther@, mlarkin@)

[3] getrandom, https://lwn.net/Articles/711013/

Mitigations

- Mitigations: dafür sorgen, dass Bugs nicht zu Sicherheitslücken führen
- Software wird nie perfekt sein, deshalb: “Fail closed”.
- Einzelne Massnahmen sind immer ein Kompromiss: Effektiv, Effizient, Verständlich, Benutzbar (vom Entwickler)
- fork + exec
- KARL / relinking von ld.so, libcrypto (deraadt@)
- trapsleds (mortimer@, deraadt@)

Pledge

- Einschränkung der Systemcalls die nutzbar sind von einem Prozess
- SE Linux, systrace, seccomp, Capsicum

```
if (pledge("stdio sendfd rpath cpath", NULL) == -1)
    fatal("pledge");
```

- harmoniert mit privsep
- Programmcode umstrukturieren: Initialisierung vs. normaler Programmablauf, meist Event-Loop

Entfernen oder Deaktivieren von ungenutzten oder unsicheren Features

Beispiele:

- Bluetooth Support wurde im Juli 2014 komplett gelöscht (tedu@)
- LibreSSL (beck@, jsing@, tedu@, bcook@, ...)
- sudo, ersetzt durch doas (tedu@)
- OpenSSH entfernt alte Ciphers mit einem lang angekündigten Zeitplan
- WPA1 Verschlüsselung seit Ende 2016 standardmässig deaktiviert (stsp@)

Weniger Code, weniger Bugs

Netzwerk

- pf(4) Firewall kann jetzt Syncookies (henning@)
- mgre(4) Multi-point GRE Tunnel (dlg@)
- slaacd(8) IPv6 autoconf im Userland (florian@)
- Netzwerk-Stack MP: Packet-Forwarding ohne Big-Lock
  - Am unlocking des socket-layers wird gearbeitet
  - Auch für pf gibt es Pläne
  - Auf aktueller Hardware 1.75 Mpps
  - Entwickler: mpi@, bluhm@, guenther@, kettenis@, sashan@, claudio@, henning@, ...

Ressourcen

- Projekt Webseite: `https://www.openbsd.org`
  - FAQ
  - Manuals: `https://man.openbsd.org`
  - Mailinglisten
- Aktuelle Neuigkeiten zum Projekt: `https://www.undeadly.org`
  - Artikel zu besonderen Änderungen
  - Hackathon Reports von einzelnen Entwicklern