NetBSD 2003 — NetBSD 2004

Ignatios Souvatzis
Institut für Informatik, Abt. V
Universität Bonn
<ignatios@cs.uni-bonn.de>

Hubert Feyrer
The NetBSD Foundation
<hubert@feyrer.de>

12. März 2003

1 Einleitung

NetBSD ist ein frei verfügbares Unix-ähnliches „Open Source“ – Betriebssystem auf Grundlage der Codebasis der University of Berkeley. Kompatibiltät zu POSIX und der Single Unix Specification (SUS) werden weitgehend angestrebt. Im Unterschied zu Linux kommen Kernel und grundlegende Libraries und Programme einschliesslich X11 aus einer Hand. Die kompletten Kernel – Sourcen sowie große Teile der Userland – Quellen unterliegen der sogenannten BSD- Lizenz, und sind daher auch kommerziell ohne Probleme in Drittprodukten verwendbar.

2 Die Projektstruktur

Das NetBSD-Projekt entstand 1993 mit einer zunächst sehr informellen Struktur. Inzwischen wurde die „NetBSD Foundation“ als formeller Träger des Projekts gegründet.

Die NetBSD Foundation ist formeller Eigentümer von (einem Teil des) NetBSD – Codes, und verwaltet Spenden sowie die Server des Projekts (FTP, CVS, WWW, ...)

Die NetBSD Foundation hat etwa 300 Mitglieder in Form der Entwickler des Projekts. Sie sind weltweit verteilt und kommunizieren über das Internet, woher auch der Name des Projekts kommt. Die Satzung wurde im Jahr 2002 in einer elektronischen Abstimmung von den Mitgliedern angenommen, ebenfalls 2002 wurde gemäß der Satzung das erste fünfköpfige „Board of Directors“ in einer elektronischen Wahl von den Mitgliedern bestätigt. Im letzten Herbst wurden turnusgemäß zwei der Direktoren in einer Abstimmung ausgetauscht. Die Abstimmung erfolgte wieder auf elektronischem Wege.

Theorie und Praxis das Wahlverfahrens hat der Wahlleiter des Jahres 2002 in [12] beschrieben.

Die Projektstruktur sieht so aus (Abbildung 1):

- Board of Directors: Administrative Leitung
- Executive Committees (ECs): kleine Gruppen zur Kommunikation zwischen Project Management Committees und Board
  - administration-exec: Verwaltung der Rechendienste des Projekts
  - communications-exec: Public Relations
  - finance-exec: Spenden & Finanzen
  - membership-exec: Neue Mitglieder
  - technical-exec: Software Engineering
- Project Management Committees (PMCs): eigentliche Arbeits/Steuergruppen, kommunizieren über ECs mit Board
  - security officer: CERT – Kontakt

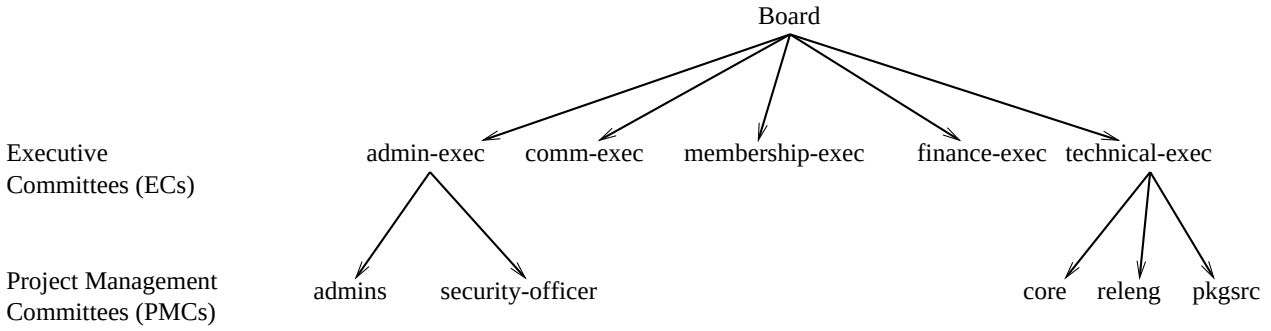

Abbildung 1: Projektstruktur der NetBSD Foundation

- admins: Systemverwaltung
- www: Dokumentation & Support
- releng: Release Engineering
- pkgsrc: 3rd Party Software
- core: Core Operating System

„The NetBSD Foundation, Inc.“ ist in den USA inzwischen als gemeinnützige Organisation nach Internal Revenue Code 501(c)(3) anerkannt und kann dort steuerlich wirksame Spendenbescheinigungen ausstellen. Die Registrierung von „NetBSD“ als eingetragenes Warenzeichen *(trademark)* wurde beantragt.

3 Das Betriebssystem

In diesem Abschnitt wird über wichtige Neuerungen in 2.0 berichtet.

3.1 Zeitplan

- Release-Zweig: Das aktuelle Release ist 1.6.1, ein Bugfix Release zu 1.6. 1.6.2, ein weiteres Bugfix Release ohne wesentliche neue Features, wird im 1. Quartal 2004 erwartet (siehe Abb. 2).

- Das nächste Major Release wird 2.0 heißen. Es kommt wie üblich “when it is done” — voraussichtlich im 2. oder 3. Quartal 2004.

3.2 Systembau

Das Grundsystem von NetBSD ist schon im 1.6-Zweig für alle Plattformen crosscompilierbar (Kernel wie Userland).

Das führt dazu, das wöchentlich mehrere Snapshots des Systems sowohl für den Releasezweig als auch für den Entwicklungszweig zur Verfügung stehen.[autobuild]. Gleichzeitig werden so CPU- und maschinenspezifische Fehler schneller aufgedeckt, die durch Änderungen an zentraler Stelle ausgelöst wurden.

Für die meisten CPU-Architekturen wird in 2.0 die neueste GNU-Toolchain benutzt: gcc 3.3.x, gdb 5.3, binutils 2.13.2.1.

3.3 Geräteunterstützung

Hier eine Auswahl von Geräten, die in 2.0 neu unterstützt werden:

- Die amd64-CPU (Opteron). Damit steht nach DEC Alpha, Sparc64 und SuperH-5 die vierte 64-Bit-Architektur zur Verfügung.

- Die IDE-Treiber sind nach Chipsätzen aufgeteilt.

- Treiber für Serial ATA

- Es gibt eine Infrastruktur für IEEE-802.11-Access-Points.

- Unterstützung für RAID-Controller, Wireless-Karten, Gigabit-Ethernet

- Ein TCPA-Treiber ist in Entwicklung.

- Ein HPPA- (hp700-) Port ist in Entwicklung.

- Nach wie vor lässt der FireWire-(IEEE1394-) Support einiges zu wünschen übrig. IP over FireWire soll aber funktionieren.

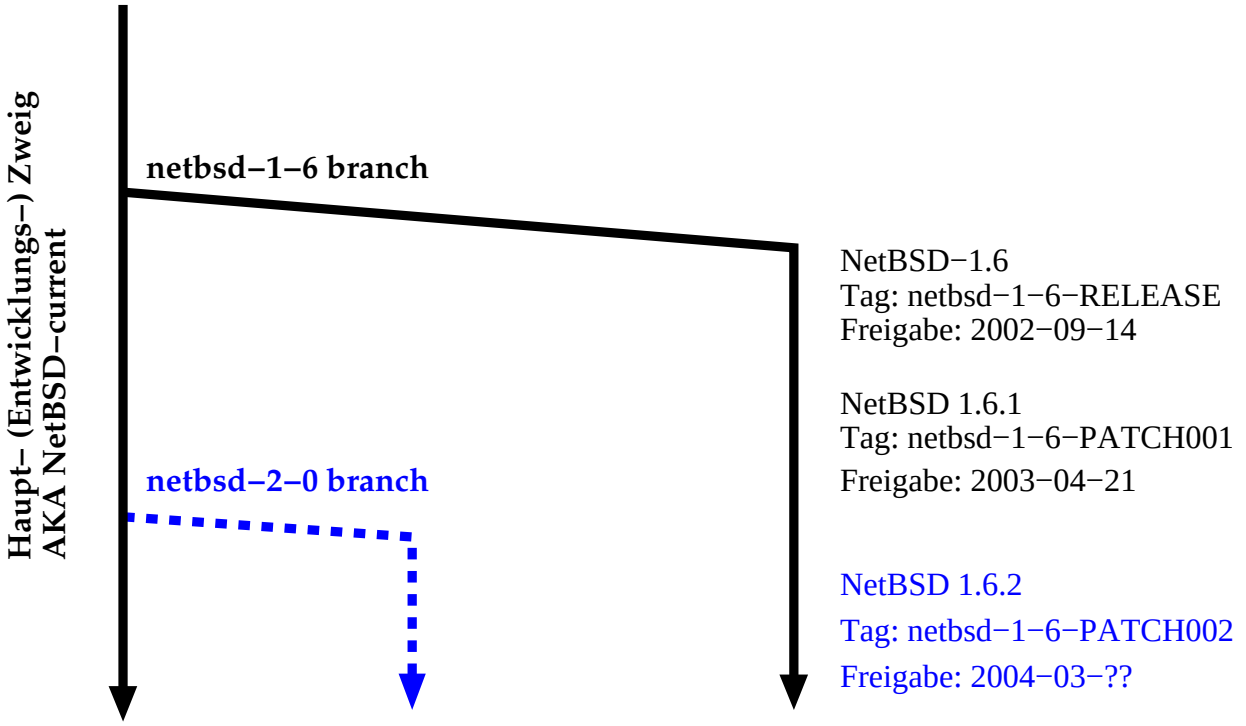

Abbildung 2: NetBSD-Entwickler- und Releasezweig.

3.4 Storage

- Filesystemcode für das Apple-UFS (MacOS-X) und Kirk McKusicks UFS2 wurde hinzugefügt. Ersteres wird Benutzer von PowerPC-Mac-Maschinen erfreuen, die beide Betriebssysteme benutzten; letzteres hat vor allem Vorteile bei sehr grossen Filesystemen ($> 1TB$ bei 512 Bytes Blockgröße).
- Es gibt jetzt ein SMB-Dateisystem (`mount -t \\server\share /mnt`)
- Der Volume Manager „VINUM“ wurde integriert.
- fss(4) ist ein neues Pseudogerät zum Anfertigen von Schnappschüssen eines Filesystems, etwa für Backups im laufenden Betrieb.

3.5 Kernel-Interna

Im folgenden werden einige wichtige Hardwareunabhängige Neuerungen bei NetBSD beschrieben:

3.5.1 Multiprozessorunterstützung

Multiprozessorunterstützung wurde für die Architekturen amd64, i386, MacPPC, 32- und 64bit- Sparc hinzugefügt. Bereits in 1.6.* vorhanden war sie für VAX und Alpha.

3.5.2 Multithreading

Während NetBSD bis zum 1.6-Zweig einschließlich kein kernel-unterstütztes Multithreading kannte, wurden danach „Scheduler Activations“ im Kernel implementiert[13] und eine darauf basierende N:M-POSIX-Thread-Bibliothek hinzugefügt.

3.5.3 Kqueue

Bei kqueue(2) handelt es sich um ein Interface, mit dem der Kernel Ereignisse an Userland-Prozesse melden kann. Es wurde ursprünglich von Jonathan Lemon für FreeBSD geschrieben[7]. Bei NetBSD werden von kqueue sowohl Geräte- als auch Filesystem-Ereignisse geliefert. Melden von USB- und Netzwerkinterface-Ereignissen ist geplant.

3.5.4 Log-structured Filesystem (LFS) mit Unified Buffer Cache (UBC)

Nach anderen Filesystemen benutzt jetzt auch NetBSD's Log-Structured Filesystem (LFS) den Unified Buffer Cache[10], so dass zum einen der gesamte Arbeitsspeicher als Buffer Cache benutzt werden kann und andererseits mmap(2) und read(2)/write(2) auch hier synchronisiert sind.

3.6 Performance Tuning

In diesem Bereich gibt es folgende Neuigkeiten:

- Ein neues API zum Zugriff auf Performancezähler (pmc).
- Checksumming von TCP und IP - Paketen einiger Netzwerkkarten wird genutzt.
- Das nicht mehr ganz so neue Virtual-Memory-System UVM in NetBSD erlaubt es, relativ effektiv Speicherseiten an einen anderen Adressraum auszuleihen *(page loanout)*[1]. Dieser Mechanismus wird in NetBSD-current ausgenutzt, um ein senderseitiges „Zero Copy TCP“ (und UDP) zu implementieren.

  Eine Applikation muss dazu wie folgt vorgehen: mmap(2) (oder direktes Erzeugen von Daten in einem lokalen Pufferspeicher des Programms) gefolgt von write(2). Dabei muss darauf geachtet, dass der geschriebene Puffer nicht mehr verändert wird, da sonst ein copy-on-write page fault ausgelöst wird, solange die Daten nicht endgültig gesendet sind. [11]
- Im Kernel wurden insgesamt einige Performance- und besonders Skalierbarkeits-Verbesserungen durchgeführt, demonstriert und teilweise angeregt im Herbst 2003 durch die Benchmarks von Felix von Leitner[6]. Siehe auch Abbildung 3.

3.7 Security

Folgende neue Features geben dem Systemadministrator Werkzeuge zum Aufbau sichererer Systeme in die Hand:

- In der Default-Installation sind (wie schon in 1.6) keine Netzwerkdienste aktiviert, sondern müssen via `inetd.conf` bzw. `rc.conf` bei Bedarf von der Systemadministration freigegeben werden.
- Auf einigen Architekturen, wo dies von der CPU/MMU her möglich ist, sind Stack und Heap per Default nicht ausführbar.
- NetBSD unterstützt jetzt „verified exec“ — Ausführen nur von Code mit bekannter Prüfsumme.
- Systrace[9] erlaubt, einzelnen Programmen bzw. Prozessen die Zugriffsrechte auf einzelne System Calls — und sogar in Verbindung mit bestimmten Parametern — zu erlauben bzw. zu verweigern. Damit kann z.B. verhindert werden, dass unbekannter Code ausserhalb eines bestimmten Verzeichnisses liest oder schreibt (ähnlich wie chroot(2), aber feiner einstellbar). Es können aber auch bestimmte Netzwerkzugriffe verhindert werden.
- Der cgd(4) – Pseudotreiber stellt eine Verschlüsselungsschicht auf Geräte (Partitions) – Ebene zur Verfügung. Dies kann sowohl zum Verschlüsseln von Datenpartitionen als auch (mit Zufallsschlüssel) zum Verschlüsseln der Swap-Partition benutzt werden.

Natürlich wurden im Entwicklungs- wie im Releasezweig die integrierten Versionen von OpenSSL, OpenSSH, BIND, Sendmail etc. mit Sicherheitsfixes versehen.

3.8 Verschiedenes

- Die Binäremulation von Linux wurde zugunsten von Java und OpenOffice auf der i386- und der PowerPC-Architektur verbessert.
- Auf PowerPC-Architekturen steht eine MacOS X - Emulation zur Verfügung.

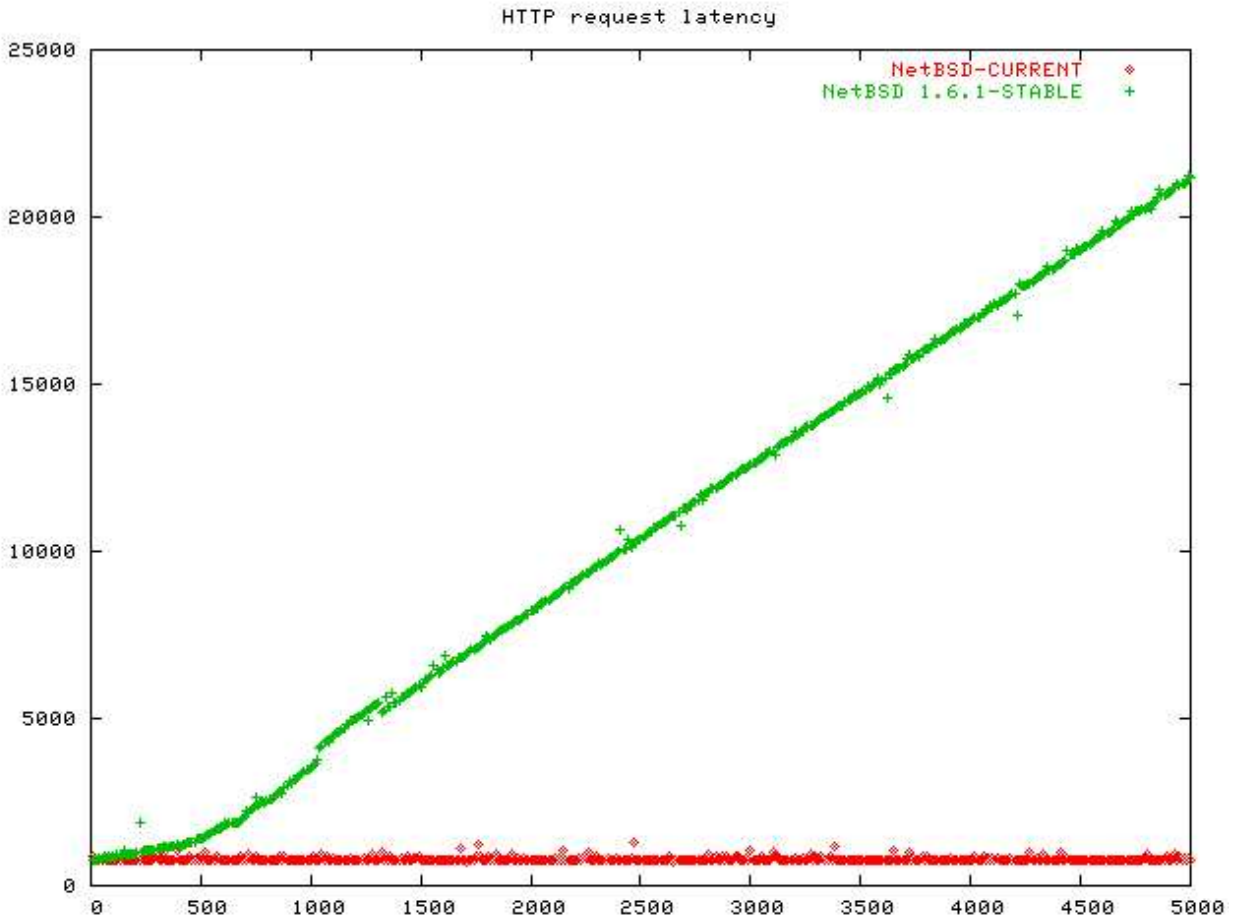

Abbildung 3: Skalierbarkeit eines einfachen HTTP-Servers (Latenzzeit in Mikrosekunden gegen Anzahl der gleichzeitigen Anforderungen, ohne connect(2)-Zeit. Für NetBSD-1.6.1 wurde poll(2) benutzt, für NetBSD-current das neue kqueue(2). Entnommen aus [6]

- Das Sysctl-Interface wird dynamisch generiert. Es ist jetzt neuen Kernelmodulen möglich, neue Knoten in den Sysctl-Baum einzuhängen, ohne dass für deren Verwendung wie bisher `/sbin/sysctl` neu compiliert werden muss.

- `pkg_add` kann Abhängigkeiten (inklusive Wildcards) bisher von der lokalen Festplatte und über FTP laden; jetzt ist HTTP hinzugekommen.

- Unterstützung für lange Rechnernamen in `utmpx`, `wtmpx`, `lastlogx`.

- Die Systembinaries (inklusive /bin und /sbin) sind komplett dynamisch. Für den Notfall steht ein kleines Verzeichnis `/rescue` zur Verfügung (2.5 MB).

- Diverse Upgrades von externer (aber integrierter) Software haben stattgefunden, wie pppd, tcpdump, file, named, gcc, binutils (as, ld, etc.), postfix, sendmail, cvs, routed, texinfo , diff, grep, amd, openssh, openssl, less ...

4 Das pkgsrc-System

Das pkgsrc-System dient dazu, Fremdsoftware einfach installieren und wieder deinstallieren zu können. Es wurde ursprünglich vom FreeBSD-Ports-System abgeleitet, seitdem aber stark verbessert. Heute stehen etwa 4400 Packages zur Verfügung und können automatisch, einschließlich weiterer benötigter Pakete, aus den Quelltexten (die dann automatisch bezogen werden) gebaut oder als Binärpaket installiert werden. Da-

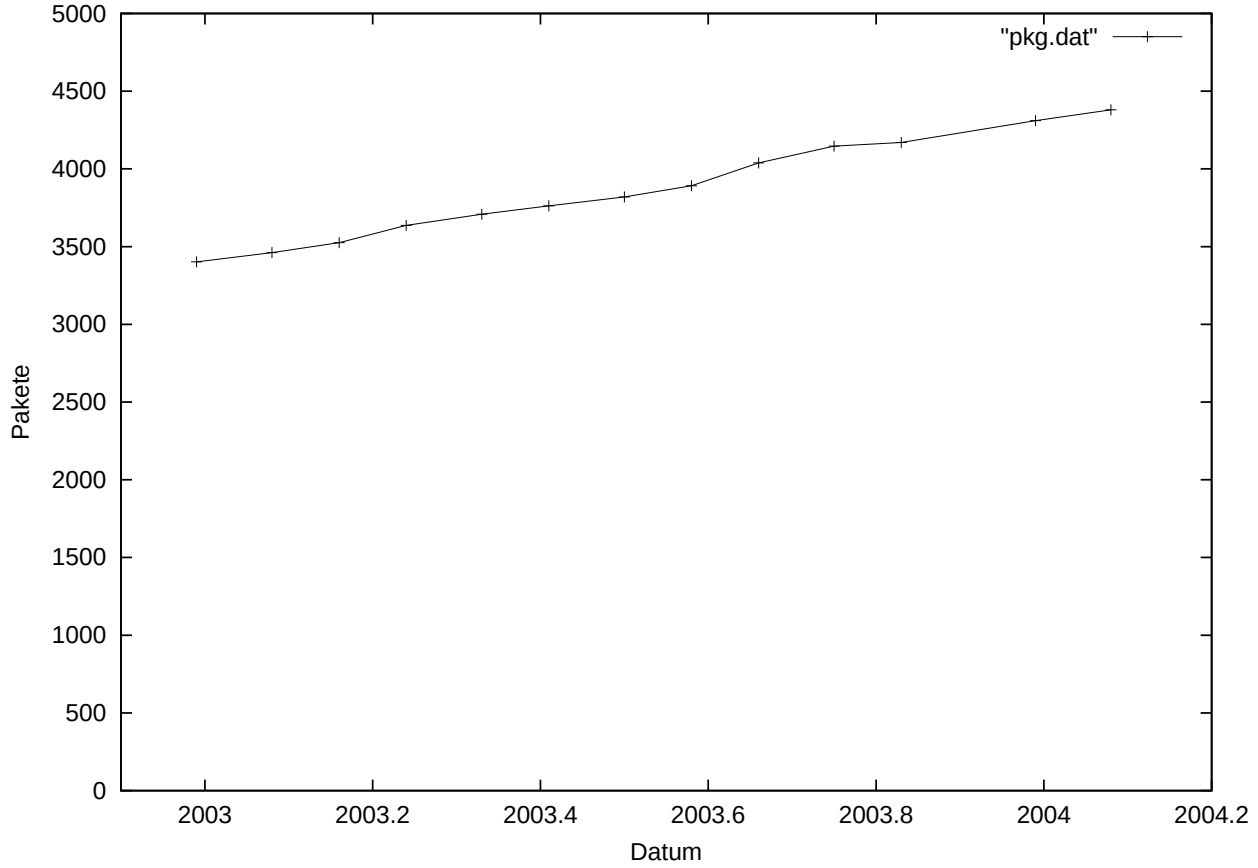

Abbildung 4: Das Wachstum der `pkgsrc`-Sammlung 2003–2004.

bei werden definierte Anpassungen, z.B. an die NetBSD-Verzeichnisstruktur oder zur schnellen Fehlerbehebung bis zur Korrektur des Originalpakets, hinzugefügt.

Das pkgsrc-System steht aber nicht nur für NetBSD zur Verfügung, sondern auch für Solaris, Linux, Darwin/MacOS-X, FreeBSD, OpenBSD, IRIX. In Arbeit sind CygWin, Tru64 und HP/UX.

4.1 Packages und Sicherheit

Eigene Sicherheitsbulletins für Drittpakete werden von NetBSD nicht herausgegeben. Stattdessen steht inzwischen das Paket [audit-packages] zur Verfügung. Es besteht aus zwei Komponenten:

- `download-vulnerability-list` führt einen Abgleich der Vulnerability-Datenbank durch
- `audit-packages` vergleicht diese mit der Liste der installierten Pakete und gibt Übereinstimmungen aus.

Beide Skripte sollten regelmäßig (z.B. im `/etc/daily` - Skript) ausgeführt werden. Angezeigt werden je Übereinstimmung die installierte verwundbare Version, eine kurze Charakterisierung der Verwundbarkeit, und eine URL, die das Problem näher beschreibt. `audit-packages` mahnt ein Update der Datenbank an, wenn diese zu alt ist (siehe Abb.5).

Bei mehreren Verwundbarkeiten kann ein Paket durchaus mehrfach genannt werden.

4.2 Package Views: Abhängigkeiten besser verwalten

Das gegenwärtige Packagesystem hat einen großen Nachteil für Produktionssysteme: ein Paket kann nicht mitten im Betrieb ohne zumindest ein paar Sekunden von Nichtverfügbarkeit ausge-

```
Script started on Wed Feb 25 10:19:49 2004

% audit-packages
** /usr/local/pkgsrc/distfiles/pkg-vulnerabilities more than a week old
** run download-vulnerability-list
% download-vulnerability-list
Trying 2001:4f8:4:7:2e0:81ff:fe21:6563...
Connected to ftp.NetBSD.org.
220 ftp.NetBSD.org FTP server (NetBSD-ftpd 20020615) ready.
331 Guest login ok, type your name as password.
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Type set to I.
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
250 CWD command successful.
local: pkg-vulnerabilities.12006 remote: pkg-vulnerabilities
229 Entering Extended Passive Mode (|||58370|)
150 Opening BINARY mode data connection for 'pkg-vulnerabilities' (41766 bytes).
226 Transfer complete.
41766 bytes received in 00:01 (37.14 KB/s)
221-
    Data traffic for this session was 41766 bytes in 1 file.
    Total traffic for this session was 46091 bytes in 1 transfer.
221 Thank you for using the FTP service on ftp.NetBSD.org.
Package vulnerabilities file has been updated
% audit-packages
Package unzip-5.50 has a weak-path-validation vulnerability, see
        http://www.securityfocus.com/archive/1/334070/2003-08-18/2003-08-24/2
Package screen-3.9.13 has a remote-code-execution vulnerability, see
        http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0972
Package gnupg-1.2.3 has a weak-authentication vulnerability, see
        http://lists.gnupg.org/pipermail/gnupg-announce/2003q4/000276.html
Package rsync-2.5.5 has a remote-user-shell vulnerability, see
        http://www.mail-archive.com/rsync@lists.samba.org/msg08782.html
Package audit-packages-1.23 has a
        no-exploit-but-less-integrity-so-please-upgrade vulnerability, see
        http://mail-index.netbsd.org/tech-pkg/2003/11/30/0001.html
Package libtool-base-1.4.20010614nb12 has a local-symlink-race vulnerability,
        see http://www.securityfocus.com/archive/1/352519
Package mutt-1.4.1nb2 has a remote-code-execution vulnerability, see
        http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0078
% exit

Script done on Wed Feb 25 10:20:42 2004
```

Abbildung 5: Anwendung von audit-packages

tauscht werden; und wenn andere Pakete von ihm Abhängen, wird das Problem noch verschärft.

Dies bewog Alistair Crooks, das *Package-Views*-System[2] zu entwerfen. Hier wird jedes Paket in sein eigenes Verzeichnis (einschließlich Versionsnummer!) installiert. Außerdem stehen Tools zur Verfügung, die ein „View“ (implementiert als eine Symlink-Farm) auf die installierten Pakete erzeugen. Eins dieser Views kann der normale Baum sein, den die Anwender benutzen, während in einem neuen View neue Versionen installiert und getestet werden.

Package Views ist inzwischen im NetBSD-pkgsrc-Baum integriert und kann schon optional benutzt werden. Jedoch ist es noch als experimentell deklariert.[5] Unter anderem fehlt bei vielen Paketen noch Support für PkgViews.

5 (Nicht nur) Neue Dokumentation

NetBSD enthält die üblichen Manual Pages. Zu den von Unix bekannten acht Kapiteln kommt bei NetBSD ein neuntes über Kernel-Funktionen und -Interfaces hinzu.

Weiterhin wird Federico Lupis „NetBSD Guide“ jetzt vom NetBSD-Projekt gepflegt[8].

Im Entstehen begriffen ist ein NetBSD Device Driver Writing Guide[4] (Englisch/Deutsch).

Beide Dokumente sind - wie viele weitere Designdokumente und HOWTOs, auf dem NetBSD-WWW-Server im Unterverzeichnis *Documentation* zu finden.

Die NetBSD-WWW-Seiten stehen in mehreren Sprachen zur Verfügung, die auf der Hauptseite auswählbar sind.

Schliesslich ist schon im letzten Jahr ein Buch über NetBSD-1.6-Systemadministration und -Anwendung erschienen[3], das genauso für NetBSD-1.6.1 und -1.6.2 zu gebrauchen ist. Es richtet sich nicht nur an den Heimanwender, sondern auch an professionelle Systemadministratoren, die eine Einführung in den Umstieg auf NetBSD gebrauchen können.

6 Ausblick

Der gemachte Überblick deckt die kommenden Releases 1.6.2 und besonders 2.0 ab, vor allem bei letzterem kann sich bis zum Release aber noch einiges tun. Wer mehr über den Fortschritt des NetBSD-Projektes wissen will, kann diesen auf der Homepage des NetBSD-Projekts unter http://www.NetBSD.org/ und auf den dort genannten Mailinglisten tun. Interessierte finden diese unter http://mail-index.NetBSD.org archiviert.

URLs

[netbsd]	NetBSD – Homepage: http://www.NetBSD.org/
[changes]	NetBSD – Änderungen: http://www.NetBSD.org/Changes/
[pkgsrc]	Pkgsrc – Homepage: http://www.pkgsrc.org/
[audit-packages]	Automatisiertes Sicherheitsbulletin für installierte Drittpakete: ftp://ftp.NetBSD.org/pub/NetBSD/packages/pkgsrc/security/audit-packages/-README.html
[autobuild]	Binäre Schnappschüsse von NetBSD-current und dem Releasezweig von der Autobuild-Maschine: http://releng.netbsd.org/ab/

Literatur

[1] Charles D. Cranor und Gurudatta M. Parulkar, *The UVM Virtual Memory System,* in: Proceedings of the USENIX Annual Technical Conference, Monterey, CA, USA 1999, http://www.usenix.org/events/usenix99/-full_papers/cranor/cranor.pdf

[2] Alistair G. Crooks, *PkgViews — ,* 2nd Eu-

ropean BSD Conference, Amsterdam 2002, http://www.NetBSD.org/Documentation/-software/pkgviews.pdf

[3] Redaktion freeX (Hrsg.): *NetBSD 1.6,* C&L Verlag, Böblingen 2003, ISBN 3-936546-00-2

[4] Jochen Kunz, *NetBSD Device Driver Writing Guide*, http://www.unixag-kl.fh-kl.de/-~jkunz/NetBSD/

[5] Johnny C. Lam, *User's Guide to PkgViews*, http://mail-index.netbsd.org/tech-pkg/2004/01/06/0004.html

[6] Felix v. Leitner, *Unix Scalability Benchmarks,* work in progress, http://bulk.fefe.de/scalability/

[7] Jonathan Lemon, *Kqueue: A generic and scalable event notification facility,* in: Proceedings of the FREENIX track, 2001 USENIX Technical Conference, Boston, MA, USA, http://www.usenix.org/events/usenix01/-freenix01/full_papers/lemon/lemon.pdf

[8] Federico Lupi et al., *The NetBSD Operating System: A Guide* (6 Sprachen), http://www.netbsd.org/Documentation/-#netbsd-guide

[9] Niels Provos, *Improving Host Security with System Call Policies*, 12th USENIX Security Symposium, Washington, DC, USA, August 2003.

[10] Chuck Silvers, *UBC: An Efficient Unified I/O and Memory Caching Subsystem for NetBSD,* in: Proceedings of FREENIX Track: 2000 USENIX Annual Technical Conference, San Diego, CA, USA, http://www.usenix.org/publications/-library/proceedings/usenix2000/freenix/-full_papers/silvers/silvers.pdf

[11] Jason Thorpe, *Experimental zero-copy for TCP and UDP transmit-side*, http://mail-index.netbsd.org/current-users/2002/05/02/0016.html

[12] Alexandre Wennmacher, *Electronic Voting,* 26. DECUS Symposium, Bonn 2003, http://www.decus.de/slides/sy2003/-09_04/2f04.pdf

[13] Nathan J. Williams, *An Implementation of Scheduler Activations on the NetBSD Operating System*, in: Proceedings of the FREENIX Track, 2002 Usenix Annual Technical Conference, Monterey, CA, USA, http://www.usenix.org/events/usenix02/-tech/freenix/williams.html

□