

Take a closer look at OpenBSD 4.3

Shift your focus to superior security

Skill Level: Intermediate

[John W. Fronckowiak \(john@idcc.net\)](mailto:john@idcc.net)

President

IDC Consulting, Inc.

12 Aug 2008

OpenBSD provides a UNIX® distribution with a primary emphasis on security and cryptography. If you're looking for a UNIX distribution to deploy in the most critical nexus in your network infrastructure, look no further than OpenBSD. The recent release of OpenBSD—version 4.3—includes several new features and bug fixes that this article reviews.

Berkeley Software Distribution (BSD) is one of the oldest and continues to be one of the most common flavors of UNIX available. There are three major flavors of BSD UNIX: *FreeBSD*, which focuses on performance and the Intel processor architecture; *NetBSD*, which focuses on portability and clean design; and *OpenBSD*, which focuses on portability, security, and integrated cryptography.

OpenBSD's motto—"free, functional, and secure"—says it all. In its default configuration, OpenBSD has proven one of the most secure operating systems available. Its recent version 4.3 release continues in that tradition.

The OpenBSD audit process

OpenBSD offers a high level of out-of-the-box security. In fact, only two security vulnerabilities have been identified in the default installation over the past 10 years. Although there may be some debate on this topic because of what is enabled in the default OpenBSD installation, it's clear that OpenBSD places a high degree of focus on enabling security.

Much of the security consistency is the result of the audit process found in its distributions. A team of experienced developers focused on auditing each piece of code entered into the source tree. Codes are analyzed for security flaws as well as bugs in general—bugs that might not affect general functionality but could be exploited as security flaws down the line. Every bug is taken seriously and immediately addressed. This proactive approach has kept OpenBSD from being susceptible to unknown exploits, which other distributions have to scramble to cover upon discovery.

OpenBSD: Where and when

Although OpenBSD may not see the same mass distribution as other UNIX flavors, because of its secure nature and focus on cryptography, it is generally found at the most crucial points of highly secure networks. In fact, many financial institutions responsible for corporate networks and customer record keeping place a high degree of confidence in their OpenBSD deployments.

Because of OpenBSD's relation to other BSD UNIX distributions, it is available on a wide variety of hardware platforms, including:

- **alpha**: Digital Alpha-based systems
- **amd64**: AMD64-based systems
- **armish**: Various ARM-based appliances
- **hp300**: Hewlett-Packard HP 9000 series 300 and 400 workstations
- **hppa**: Hewlett-Packard Precision Architecture (PA-RISC) systems
- **i386**: Standard computers based on the Intel® i386 architecture and compatible processors
- **landisk**: IO-DATA USL-5P, using a Hitachi/Renesas SH-4 CPU
- **luna88k**: Omron LUNA-88K and LUNA-88K2 workstations
- **mac68k**: Motorola 680x0-based Apple Macintosh with MMU
- **macppc**: Apple PowerPC-based machines, from the Apple iMac on
- **mvme68k**: Motorola 680x0-based VME systems
- **mvme88k**: Motorola 881x0-based VME systems
- **sgi**: SGI MIPS-based workstations
- **sparc**: Sun sun4-, sun4c-, and sun4m-class SPARC systems
- **sparc64**: Sun UltraSPARC systems

- **vax:** Digital VAX-based systems
- **zaurus:** Sharp Zaurus C3x00 Personal Digital Assistants (PDAs)

OpenBSD core packages and features

Now that you've determined whether OpenBSD is an option for your hardware platform, let's take a closer look at some OpenBSD highlights.

OpenSSH

The first package of note is OpenSSH, with which every UNIX and Linux® user is familiar. However, many people might not know that it comes from OpenBSD developers. OpenSSH was originally developed for OpenBSD and has since become the standard Secure Shell (SSH) package, ported for just about every version of the UNIX, Linux, and Microsoft® Windows® operating systems. OpenSSH includes `ssh` for secure logins, `scp` for secure copies, and `sftp`—a secure alternative to File Transfer Protocol (FTP). All source code falls into the open source BSD license, following OpenBSD's directive to keep all proprietary code and restrictive licensing schemes out of the distribution (which was the initial impetus to create a new version of SSH). Every piece of software included in OpenBSD is completely free, with no restrictions on use.

Cryptography

Because the OpenBSD project is based in Canada, no United States export restrictions on cryptography apply, allowing the distribution to make full use of modern algorithms for encryption. Encryption can be found almost everywhere in the operating system, from file transfers to file systems to networking. Pseudo-random number generators are also included in OpenBSD, which ensures that random numbers cannot be predicted based on the system state. Other features include cryptographic hash functions, cryptographic transform libraries, and cryptographic hardware support.

Another heavily exported piece of OpenBSD is the IP Security Protocol (IPSec), which the operating system uses rather than relying on the inherently insecure TCP/IP version 4 (IPv4). (IPv4 chooses to trust just about everybody and everything.) IPSec encrypts and validates packets to protect the privacy of data and to ensure that no changes are made to packets during the delivery process. IPSec became an integral piece of the standard Internet Protocol with the introduction of TCP/IP version 6 (IPv6), making the future of the Internet more secure by default.

OpenBSD as firewall

Because OpenBSD is both thin and secure, one of the most common OpenBSD

implementation purposes is as a firewall. Firewalls operate at the ground level of most secure locations, and OpenBSD's implementation of packet filtering is top notch. Packet Filter (PF)—an open source solution designed by the OpenBSD development community—is the OpenBSD method of choice. Like many other pieces of OpenBSD software, its success has prompted the other BSD variants to port it into their own distributions.

OpenBSD is set up to be secure by default, so there aren't too many services that you must turn off to set up a rock-solid firewall. You will have to enable a second Ethernet interface and configure PF to your needs. See [Resources](#) for links to articles on how to set up an OpenBSD server as a firewall.

OpenBSD 4.3: What's new

OpenBSD version 4.3 introduces several new features and improvements. The most important of these include:

- A fix for a buffer overflow problem in `dhcpcd(8)`. Shortly after OpenBSD version 4.2 was released, an error was discovered with carefully crafted Dynamic Host Configuration Protocol (DHCP) requests resulting in a buffer-overflow condition, making `dhcpcd(8)` much more robust.
- `hoststated(8)` and `hoststatectl(8)` were renamed to `relayd(8)` and `relayctl(8)`, respectively. `relayd(8)` is a fully featured TCP/IP relay, or Application Layer Gateway (ALG), in which the health checking of hosts is just a part of the functionality. It currently supports TCP, Hypertext Transfer Protocol (HTTP), and Domain Name System (DNS) relaying; Secure Sockets Layer (SSL) "acceleration," or termination; and the traditional layer 3 redirections. `relayd(8)` is now also able to send Simple Network Management Protocol (SNMP) traps through `snmpd(8)` when the state of a monitored host changes. This includes a feature to monitor load balancers in existing Network Monitoring Systems (NMS).
- The configuration of the `carp(4)` load balancer has been simplified. One `carp` interface can now contain up to 32 virtual host instances. Rather than creating multiple interfaces with the same address, you can create a single `carp` interface and assign it multiple `carpnodes` with their respective `advskews`.
- Four new drivers for 802.11 wireless devices in version 4.3, including `bwi(4)` for Broadcom AirForce devices, `upgt(4)` for Conexant PrismGT USB devices, `iwn(4)` for Intel Wireless WiFi Link 4965AGN devices, and `ral(4)` RT2860 for Ralink Technology devices.
- Improvements in the speed of flash drives.

- Very large disk support for volumes with more than 2 terabytes (TB) of storage.
- On the sparc64 platform, support for symmetric multiprocessing (SMP) and new eeprom(8) updates allow the firmware to be queried for installed devices.
- A new M_ZERO flag for malloc allows for memory allocation and zeroing in a single operation.
- OpenSSH version 4.8 includes security releases to fix a bad policy and an X11 hijacking problem. The big new feature is `chroot` support for `sshd(8)`. An in-process SSH over FTP (SFTP) server, which links `sftp-server(8)` into `sshd(8)` rather than forking and executing it as a separate process, particularly helps `chroot` setups, because no special support files (for example, `/dev` nodes) are required.
- `Cwm(1)` has undergone a major code clean up. Several new features have been included: the ability to resize windows and move the pointer with keyboard bindings; default key bindings can now be overridden by user-defined bindings while also allowing users to "unmap" a key binding; and "exec window manager" allows you to either restart `cwm(1)` or switch to another window manager—namely, another version if `cwm(1)`—without restarting the X server.
- Support for more than 5000 packages, with several small bug fixes and improvements for OpenBSD version 4.3.

For a list of major machine-independent changes, visit the [OpenBSD site](#).

Installing OpenBSD 4.3

The OpenBSD installation process can be intimidating and confusing to new users, especially those used to easier installation processes in other UNIX distributions. There are several installation methods, and steps vary by platform. Here are the basic steps to get started with a basic CD-ROM-based installation for the i386 architecture. (For information for other platforms, see the [OpenBSD FAQ](#).)

Step 1. Get the distribution

First, visit the [OpenBSD.org download page](#), choose any mirror on the list, and then go to `/4.3/i386/`. This is the first place you'll notice something different, if you're used to installing Linux distributions. The only `.iso` file is a 5 MB file called `cd43.iso`. Can this be right? Don't worry: With an OpenBSD installation, the boot CD is a bare-bones kernel; the rest is extracted from files that you can download and burn to an additional CD (or purchase a CD set from OpenBSD.org to help support the project). Make sure you download `cd43.iso`, all the `.tgz` files, `bsd`, `bsd.rd`, and

bsd.mp. (Or, to make things easy, just download everything in the directory.)

Step 2. Create the installation media

Create a boot CD from `cd43.iso` and label it **Disk 1**. Create a regular CD with all the other files in a directory called `/4.3/i386/`, and label it **Disk 2**. Other options include purchasing a CD set, performing a network installation, or building a custom `.iso` file, but I find the two-CD method easiest.

Step 3. Start the installation

After you've created the installation CDs, boot the new server from Disk 1. Command prompts guide you through the installation process. You can find detailed instructions in Section 4 of the OpenBSD FAQ.

The most complicated part is the "Setting up disks" section, but you can skip a lot of this information by choosing to use the entire disk for OpenBSD (if you don't have any other partitions you would like to retain). Regardless of your partitioning decision, make sure you follow the "Creating a disklabel" section step by step, with the only deviation being to create larger `/usr` and `/home` partitions, if you desire. Note the two-layer partitioning system in OpenBSD: The first step sets up traditional `fdisk`-viewable partitions, while the second `disklabel` step sets OpenBSD sub-partitions.

Other than this, the only adjustment (to use your two-CD installation set) is to swap CDs at this step:

```
Let's install the sets!  
Location of sets? (cd disk ftp http or 'done') [cd]  
Switch from Disk 1 to Disk 2 (the CD with all the files in  
/4.3/i386/).
```

Step 4. Start computing!

With everything set up, you're ready to start computing.

Getting started with OpenBSD 4.3

You might want to be aware of some steps before you start administering your system as a new OpenBSD user. First, by default, no users are included in the `wheel` group, which means that an attempt to use the `su` command will fail. Create new users from the command line with the `adduser` command, which leads you through a simple question-and-answer session to set up defaults (a one-time process) and to create your first user.

Say, for example, that you created a user called `bsdadmin`. If `bsdadmin` is going to

be your primary administrative account, you want to be able to use the `su` command to access the root account quickly. To do this, log in under the root account, and then edit the `/etc/group` file to include `bsdadmin` in the wheel group. Simply append `bsdadmin` to the first line (the one that says `wheel:*:0:root`).

Second, check the system default settings in the `/etc/` directory. Tread carefully here, as most services are turned off by default for a reason. OpenBSD uses `rc.conf` to launch most startup daemons. You'll see that services, such as `httpd` and `nfs`, are turned off by default—even PF is off. As an example, you can turn Apache (`httpd`) on by adding the line `httpd=YES` to `/etc/rc.conf`.

Although OpenBSD might not have graphics-based tools to help in system administration, the OpenBSD developers have given extra attention to providing extensive, accurate man pages for each component of the operating system. I recommend that you make liberal use of the stalwart `man` command any time you're confused or simply want to learn about a new tool.

Packages

A large number of packages are available for the most common architectures. You can find the complete list of available packages at the [OpenBSD packages site](#).

To install packages, you use the `pkg_add(1)` utility. You can make things really easy by using the `PKG_PATH` environment variable. Just point it to your favorite location, and `pkg_add(1)` automatically looks there for any package you specify as well as fetches and installs the necessary dependencies of this package. You can just call `pkg_add(1)` with the package name, as in the following basic example:

```
$ sudo pkg_add -i screen
```

Conclusion

The new OpenBSD version 4.3 UNIX distribution continues its tradition of providing a highly secure operating system that can be deployed in the most critical areas of your infrastructure. Design principles, such as code auditing, extensive use of encryption, and careful configuration choices, combine to ensure that OpenBSD's secure-by-default philosophy holds true. Although it's most common to find OpenBSD installations in secure servers and firewalls, its wide hardware and software support make the operating system suitable for a large range of purposes. UNIX and Linux gurus alike will find many parts of OpenBSD familiar, and they will likely appreciate the areas in which it purposely strays from the pack.

Resources

Learn

- [OpenBSD home page](#): See what OpenBSD is all about.
- [Documentation and FAQ](#): This page provides answers to common and not-so-common OpenBSD questions.
- "[Cryptography in OpenBSD: An Overview](#)": For more information about how cryptography works in his system, read this paper by Theo de Raadt, et al.
- "[Firewalling with OpenBSD's PF packet filter](#)": For more information about using OpenBSD as a firewall, read through this detailed guide by Peter N. M. Hansteen.
- "[OpenBSD's network stack](#)": Get more information on OpenBSD's network security capabilities.
- "[A Cryptographic File System for UNIX](#)": Read this paper by Matt Blaze for more information about the Cryptographic File System (CFS).
- [AIX and UNIX zone](#): Visit the developerWorks AIX and UNIX zone to get the resources you need to advance your skills.
- [New to AIX and UNIX](#): New to IBM® AIX® and UNIX? Visit the this page to learn more.
- [Technology bookstore](#): Browse the technology bookstore for books on these and other technical topics.

Get products and technologies

- [OpenBSD mirrors](#): Download OpenBSD now.
- [OpenBSD online ordering](#): Purchase OpenBSD CDs and other goods, or just contribute to the cause.
- [IBM trial software](#): Build your next development project with software for download directly from developerWorks.

Discuss

- [Podcasts](#): Tune in and catch up with IBM technical experts.
- [developerWorks blogs](#): Check out developerWorks blogs and get involved in the [developerWorks community](#).
- Participate in the AIX and UNIX forums:
 - [AIX Forum](#)
 - [AIX forum for developers](#)

- [Cluster Systems Management](#)
- [IBM Support Assistant Forum](#)
- [Performance Tools Forum](#)
- [Virtualization Forum](#)
- [More AIX and UNIX forums](#)

About the author

John W. Fronckowiak

John Fronckowiak is president and founder of [IDC Consulting Inc.](#) and also a Clinical Assistant Professor in Information Systems at [Medaille College, at the School of Adult and Graduate Education](#). He is the author of several books and articles about Web application development, programming, database design and development, and networking. You can reach John at john@idcc.net.

Trademarks

UNIX is a registered trademark of The Open Group in the United States and other countries.

Intel is a registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.