



NetBSD

— Introducing NetBSD —



What is the NetBSD Project?

The NetBSD Project gives you a complete Unix-like operating system that is up to today's Open Source and security standards, supporting industry-standard APIs, communication protocols, and a huge variety of hardware platforms. NetBSD is suited to a wide range of applications, from servers and workstations to PDAs and embedded systems.

NetBSD is often chosen to control newly developed hardware and to drive such products as network computers, single-board computers, internet appliances, firewalls, printers, copiers and even web-cams. NetBSD is used in network development all over the world. ISPs use NetBSD because of the wide spectrum of network possibilities, and enthusiasts choose NetBSD for its excellent hardware support.

Why is NetBSD so special?

Since NetBSD was founded in 1993 as a successor of the BSD-line, it has always been at the forefront of Open Source operating system development. NetBSD has been the complete foundation or reference for other projects. Many of NetBSD's advantages are not found in any other open source operating system.

- NetBSD offers support for 55 different hardware platforms and 17 CPU architectures. And even more will follow.
- POSIX threads implementation based on Scheduler Activations
- Cross compiling of the kernel and userland supported by the standard toolchain - build NetBSD almost anywhere, out of the box!
- Kernel events notification framework provides a stateful and efficient event notification, including socket, file, directory, fifo, pipe, tty and device changes
- Many security-specific features, including Verified Exec and the systrace framework are implemented in the base system.
- Complete source, including the history of the development, available via anonymous CVS, rsync, SUP and CVSweb
- Support for various network technologies including ATM, HIPPI, FDDI, HSSI, IEEE 802.11, Token-Ring, ARCnet and Ethernet (up to 10Gbps!)
- NetBSD was the first open source operating system to support USB, USB2, and PCMCIA audio.

Use Your Favorite Tools and Applications

NetBSD contains all the features you would expect in an open source operating system today, including X11, tools for firewalls, and software RAID. With NetBSD's package tools you can install more than 5500 freely available software packages easily.

Ideal for Embedded Environments

NetBSD is designed to minimize the effort needed to make it run on new hardware. As a result, you are able to concentrate on the development of the hardware.

NetBSD is particularly well suited to embedded environments. It supports many lower-power CPUs, such as ARM, MIPS, PowerPC, Xscale, and Hitachi SH 3/4/5. By removing optional components, NetBSD can be trimmed down to fit comfortably on very small systems. And of course tools are available to do cross-development. Both the toolchain and compilers support cross-compiling. Cross-compiling the kernel and the whole operating system is easily possible, as is cross-building whole distribution sets.

Make the decision—joining many Fortune 100 and Fortune 500 companies—to use NetBSD, the world's most portable operating system, for your product.

Security for Paranoids

With integrated firewall tools and tools that can be easily installed from our software archives—including IPsec, Kerberos 5, SSH, SSL, and encryption tools such as PGP—you have access to a modern security system.

NetBSD enforces non-executable mappings on many platforms. Stack and heap mappings are non-executable by default, making exploitation of potential buffer overflows harder. NetBSD also supports PROT_EXEC permission via mmap(2) for all platforms where the hardware differentiates execute access from data access.

In the public forums related to Security issues, such as the Bugtraq mailing list, NetBSD has always had fewer known security problems than the alternative solutions. One more reason security consultants choose NetBSD!

Help is only an e-mail away!

In case of trouble you can find fast and unbureaucratic help through our mailing lists and the bug-tracking system. For more professional help, you'll find many consultants listed at our website.

Don't miss the connection

NetBSD has been growing since March 1993, longer than any other alternative solutions in the field of open source, and is today stronger than ever. We won't disappear and leave you alone or stop supporting your platform. You can put your mind at ease knowing that the future development of your OS is in the hands of capable experts.

www.NetBSD.org



NetBSD

— Secure by default —



Secure by default

The NetBSD Project adopts the same approach to security as it does to the the rest of the system: *Solutions and not hacks*. Security issues in NetBSD are handled by the NetBSD security officer and the NetBSD security alert team. As well as investigating, documenting and updating code in response to newly reported security issues, the team also performs periodic code audits to search for and remove potential security problems.

NetBSD has integrated Kerberos IV (KTH-KRB), Kerberos 5 (Heimdal), and ssh. In addition, all services default to their most secure settings, and insecure services are disabled by default for new installations. NetBSD also contains full support for IPSEC for both IPv4 and IPv6.

Security Advisories

When security problems are discovered and corrected, we issue a security advisory, describing the problem and containing a pointer to the fix. These are announced to our netbsd-announce mailing list as well as to various other mailing lists and websites.

Checking for Vulnerabilities in Installed Packages

The NetBSD Security-Officer and Packages Groups maintain a list of known security vulnerabilities to packages which are (or have been) included in pkgsrc. Through audit-packages, this list can be downloaded automatically, and a security audit of all packages installed on a system can take place. One can set up audit-packages to download the vulnerabilities list and run a package audit in the daily security script.

File Flags and Security Levels

File flags allow the administrator and users to protect programs and data from being altered even by root. If a file is marked with the *sappnd* flag, data can only be appended to the file, but it cannot be altered anymore. The *schg* flag protects a file from being altered even by root.

Security levels restrict several system functions, according to the level. The system can be set to a stricter level, but not to a lower level, while running in multiuser mode. So the system is protected even against an intruder with superuser access.

Checking for Manipulated Files

The mtree utility compares a file hierarchy against a specification read from a file. By using a specification that collected sufficient attributes of files like ownership, mode and cryptographic message digests, any manipulation of a file can be revealed – uncovering threats like rootkits or trojans.

Non-Executable Stack and Heap

NetBSD supports non-executable mappings on platforms where the hardware allows it. Process stack and heap mappings are non-executable by default. This makes exploiting potential buffer overflows harder. When the hardware has a larger granularity, the rule is that if any page in the larger unit is executable, then the entire larger unit is executable, otherwise the entire larger unit is not executable.

No compile-time option is needed to enable this software support, it's always available.

Locking Out Trojans

Veriexec adds a new function to the exec-Path of the kernel, thus allowing the kernel to check a cryptographic hash for a binary. With this feature, it is almost impossible to run manipulated binaries like a rootkit or a trojan.

Encrypted Partitions

The cryptographic device driver (cgd) provides functionality which allows you to use disks or partitions for encrypted storage. After providing the appropriate key, the encrypted partition is accessible using cgd pseudo-devices just like a normal data partition. Cgd can also be used to encrypt /tmp and swap-space or file systems residing in a file, creating an encrypted container.

Controlling System Calls

Niels Provos' systrace provides a way to monitor, intercept, and restrict system calls. Systrace acts as a wrapper to the executables, controlling their access of system calls.

File System Extended Attributes

Extended Attributes allow one to add meta data to vnodes of files and directories. This can be used to keep user defined information (eg. a checksum) connected to a file/directory.

Daily Security Checks

NetBSD comes with two shell scripts, *daily.conf* and *security.conf*. The scripts are used to do daily maintenance and security checks of the system. They can be started via cron each night and generate a verbose report of the system's security status.

Packet Filter

NetBSD comes with two mature TCP/IP packet filters in the base system. Ipf or pf enable any NetBSD machine to work as a well-engineered and sophisticated firewall.