# *OpenBSD and Soekris*

UUASC meeting
June 3, 2004

Presented by
Arild Jensen

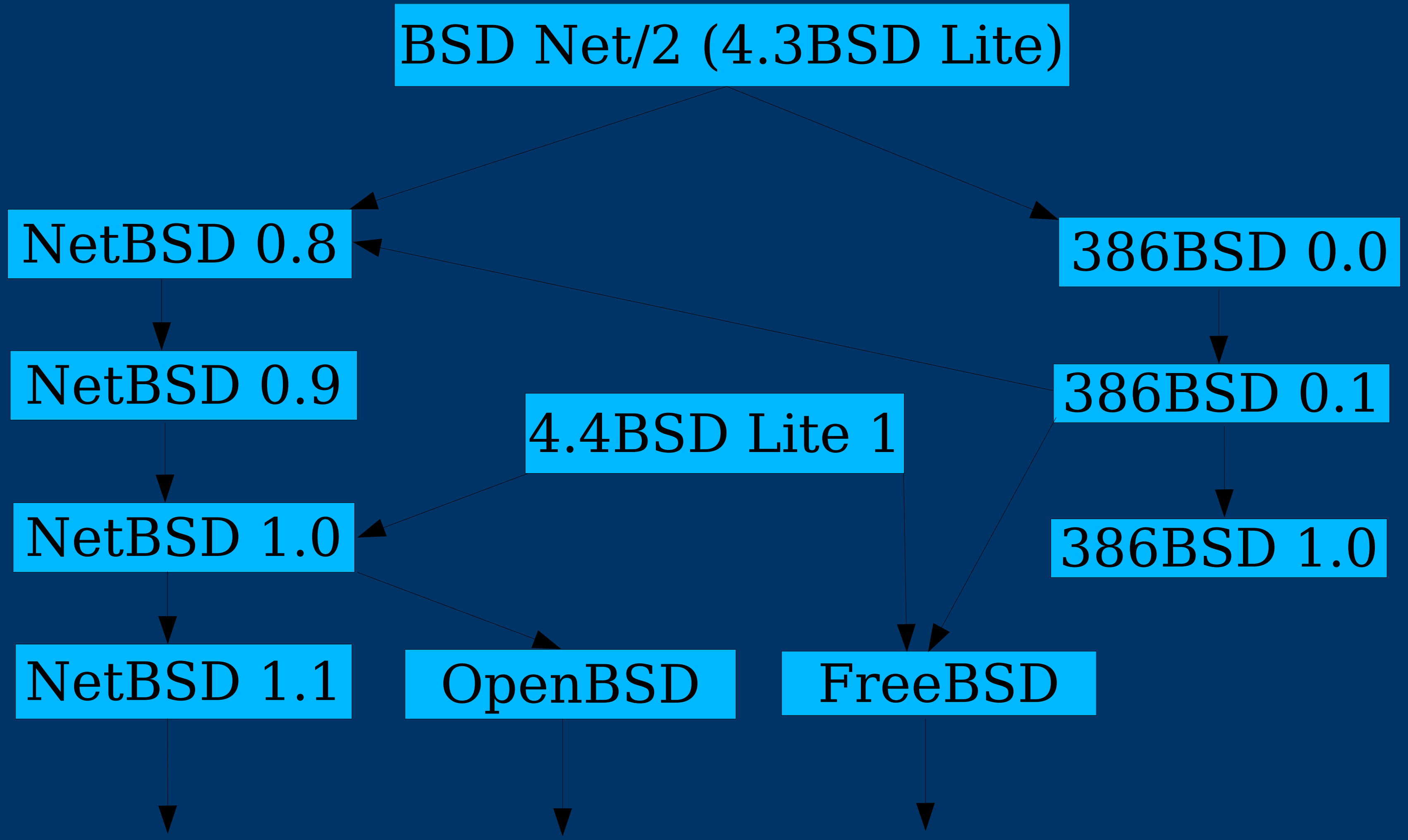
# Outline

- What is OpenBSD and where do I get it?
- Built-in security features
- Maintaining an OpenBSD system
- The PF packet filter

# Outline (cont'd)

- What is Soekris and where do I get it?
- Different models and accessories
- Getting OpenBSD onto a Soekris box
- Maintaining a Soekris/OpenBSD solution

# What is OpenBSD?
# History



BSD Net/2 (4.3BSD Lite)

NetBSD 0.8

386BSD 0.0

NetBSD 0.9

386BSD 0.1

4.4BSD Lite 1

NetBSD 1.0

386BSD 1.0

NetBSD 1.1

OpenBSD

FreeBSD

# What is OpenBSD?

From the creators: "...freely available, multi-platform 4.4BSD-based UNIX-like OS."

Emphasis on:

- Portability
- Standardization
- Correctness
- Proactive Security
- Integrated Cryptography

# *...and where do I get it?*

www.openbsd.org

CD sales only
No .iso downloads
$40

# *Portability*

- i386
- Sparc
- Sparc64
- HP300
- Mac68k
- MacPPC
- MVME68k
- MVME88k
- AMD64
- CATS (ARM)
- HPPA

# Standardization

The Story of CARP

- Firewall failover desired
- IEEE VRRP (Virtual router redundancy protocol)
- Cisco patents involved, HSRP protocol
- Cisco and Alcatel dispute
- Birth of CARP (Common address redundancy protocol
- Early implementation included in OpenBSD 3.5

# Correctness

## The Audit Process

- 6-12 member security team
- Continuous audit of code multiple times by different people
- Security holes *and* common errors
- Result: Newly discovered bugs often already fixed in OpenBSD

# *Pro-active Security*

## Source Code

- ProPolice
  - Buffer overflow protection
  - Similar to Stackguard
- W^X
  - Write xor Execute
  - Fine-grained memory permission layout
  - Only on some architectures

## Run Time

- Privilege Separation
  - Avoid running as root
  - Dual-process setup
  - Daemons being converted
- Chroot
  - Apache /var/www
  - BIND /var/named

# Cryptography

- Based outside of U.S.
- Kerberos V (Heimdal)
- OpenSSH
- PRNG
- Hash Functions
  - MD5
  - SHA1
  - RIPEMD-160
- Transforms
  - DES/3DES
  - AES
  - Blowfish
  - Cast
- Hardware
  - Ipsec crypto dequeue
  - 3DES at 130 Mbps
  - VIA C3 AES-128 at 780 Mbyte/s
  - OpenSSL automatic support

# *Maintenance*

- Updates via source code
  - CVS checkouts
  - Diff patches
- Ports via port tree
  - Updates same as OS source tree
  - "make install" builds *or*
  - pkg-add via ftp
- Upgrades
  - Reinstall recommended
  - Upgrade supported, but req. interaction

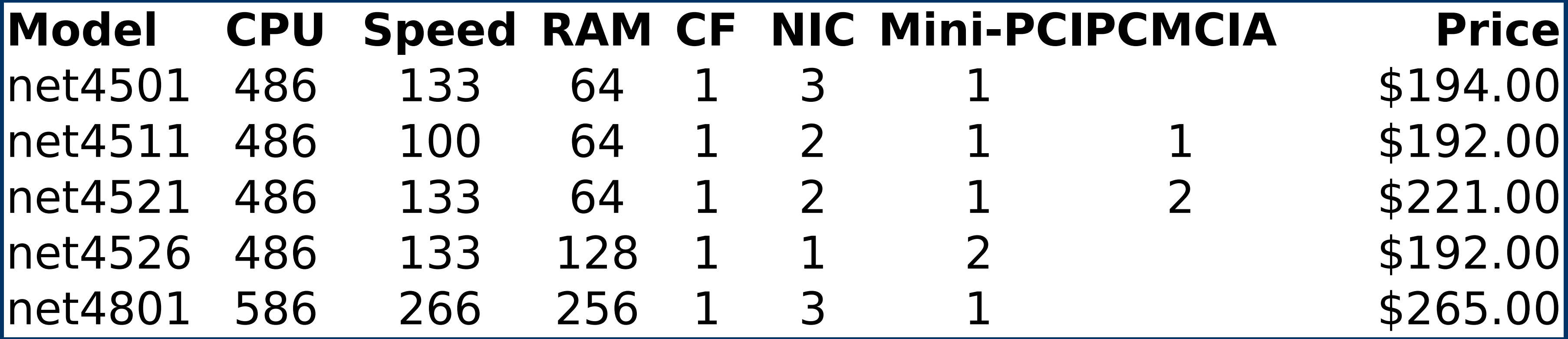
# *The PF Packet Filter*

- Stateful packet filter with
  - NAT and redirection
  - Packet normalization
  - Bandwidth management and prioritization
  - Passive OS fingerprinting
  - Load-balancing
  - Logging
  - Authpf
- Replacement of IPF in 3.0 (Nov. 2001)
- Ported to FreeBSD, NetBSD

# What is Soekris?

- Soekris Engineering of Santa Cruz
- Embedded computers and communication devices
- Selection of x86-based small 5”x6” PC's and encryption accelerators

# Soekris Models



| Model | CPU | Speed | RAM | CF | NIC | Mini-PCI | PCMCIA | Price |
|---|---|---|---|---|---|---|---|---|
| net4501 | 486 | 133 | 64 | 1 | 3 | 1 |  | $194.00 |
| net4511 | 486 | 100 | 64 | 1 | 2 | 1 | 1 | $192.00 |
| net4521 | 486 | 133 | 64 | 1 | 2 | 1 | 2 | $221.00 |
| net4526 | 486 | 133 | 128 | 1 | 1 | 2 |  | $192.00 |
| net4801 | 586 | 266 | 256 | 1 | 3 | 1 |  | $265.00 |

# OpenBSD onto Soekris Solutions

- OpenSoekris
- Flashdist
- PXE boot (remote filesystem)

# OpenBSD onto Soekris Hardware

- Null-modem cable
- OpenBSD PC
- Use a supported USB/CF adapter, or
- Use an IDE/CF bridge
- Record CHS

# OpenBSD onto Soekris Software

- Compile Soekris kernel
- Combine kernel and subset of userland files onto image (using script)
- Copy image to CF module
- Two scripts:
  - OpenSoekris
  - flashdist

# *OpenBSD onto Soekris End Result - flashdist*

- Two partitions:
  - Root (/), which is read-only and stored on CF media
  - Temp (/tmp), which is read-write and stored in RAM
- No man pages
- 27 commands in /sbin. Default 86.
- 10 commands in /usr/sbin. Default 201.
- 21 commands in /bin. Default 42.
- 20 commands in /usr/bin. Default 383.
- All configuration takes place in /etc/rc file.

# OpenBSD onto Soekris Maintenance

**Solutions 1**

- Use reference system
- Run cvs update and build
- Use “find” to list new binaries
- Copy new files over
- Reboot
- Short downtime

**Solution 2**

- Use reference system
- Run cvs update and build
- Create new image, move onto CF media
- Replace CF media in Soekris box
- Slightly longer downtime

# The End