bytemine

Entwicklungsmanufaktur für innovative Lösungen

Einführung in OpenBSD

OpenBSD

- freies, unixoides Betriebsystem
  - 4.4BSD-basierend
    - BSD = Berkeley Software Distribution
  - portabel
  - sicher
  - integrierte Kryptographie
  - BSD-Lizenz

Geschichte

- Ende 1995 entstanden
- erstes Release auf CD: OpenBSD 2.1 (Juni '96)
- aktuell OpenBSD 3.7
- bereits auf viele Architekturen portiert:
  - i386, vax, amd64, macppc, sparc, sparc64, alpha, cats, hp300, hppa, luna88k, mac68k, mvme68k, mvme88k, sgi, zaurus

Das OpenBSD Projekt

- Theo de Raadt, Kopf des Projekts
- hautpsächlich freiwillige Entwickler
- finanziert durch Spenden und den Verkauf der Releases, T-Shirts, etc.
- Release Zyklus von sechs Monaten
- Schwerpunkt: Frei und Sicher
- jährlicher Hackathon in Calgary

Bekannte Software

- OpenSSH
  - mittlerweile die Standard SSH Implementation
  - wird von vielen kommerziellen Herstellern verwendet
  - vorhanden im Grossteil der Linux-Distribution
- OpenNTPd
- OpenBGPd

OpenBSD

- excellente Dokumentation (man pages)
- kleine Basis-Installation
- keine unnützen Netzwerk-Daemons aktiv in der Basis-Installation
- 3rd Party Software verfügbar in Form von Ports bzw. Packages
- simple textbasierte Installationsroutine

Kryptographie

- OpenBSD kommt aus Kanada und unterliegt nicht den Export-Beschränkungen der USA
- Unterstützung von Hardware Krypto Beschleunigern, inkl. Load-Balancing
- IPSec integriert
- Kernel Entropy Pool
  - Erzeugung von Zufallszahlen
  - Verwendung an vielen Stellen im System

Sicherheit

- “Secure by default”
- “Proactive Security”
- nur ein Remote-Root Sicherheitsloch in der Default Installation in mehr als acht Jahren
- “This problem has been fixed in OpenBSD six months ago”

Sicherheit

- setuid Programme
  - Anzahl so gering wie möglich halten
  - Reduzierung der setuid Programme auf < 8
- permanente Code-Audits
  - aktive Suche nach Programmierfehlern
  - Sicherheitslücken eigentlich immer das Resultat von Programmierfehlern

Sicherheit

- W^X
  - memory pages sind entweder schreibbar ODER ausführbar, aber nicht beides
  - Hardware Architektur muss dies unterstützen
- non-exec stack
  - auf allen Architekturen ausser VAX und m68k-basierten
  - Grossteil der Buffer Overflows funktioniert dadurch nicht mehr

Sicherheit

- ProPolice
  - Stack-Smash-Protector
  - gcc-Erweiterung, stack smash handler in libc
  - Pointer stehen immer vor den Variablen auf dem Stack
  - Zur Laufzeit: Overflow-Checks mit magic cookies

Sicherheit

- strlcat und strlcpy
  - tradiotionelle String-Funktionen in der Programmiersprache C verleiten zu unsachgemässer Verwendung
  - sichere Alternative zu strcat und strcpy
  - nach Analyse vieler Buffer Overflows entwickelt

Sicherheit

- Privilege Seperation
  - viele Daemons in OpenBSD die ursprünglich mit root-Rechten liefen, legen diese nun nach dem Start ab
  - Daemons laufen in einem Chroot
    - named
    - apache
    - ntpd

Netzwerk

- PF - packet filter
  - entwickelt nach dem es Lizenzprobleme mit den IPF von Darren Reed gab
  - mittlerweile ist der PF der mächtigste Paket-Filter in der IT Landschaft
  - carp, pfsync
    - “Redundancy must be free”

OpenBSD 3.8

- erscheint am 1. November
- hostapd
- watchdogd
- ospfd
- OpenSSH 4.2
- bioctl, RAID Management für AMI-basierende Controller

Vielen Dank für Eure Aufmerksamkeit!

http://www.openbsd.org/
misc@openbsd.org