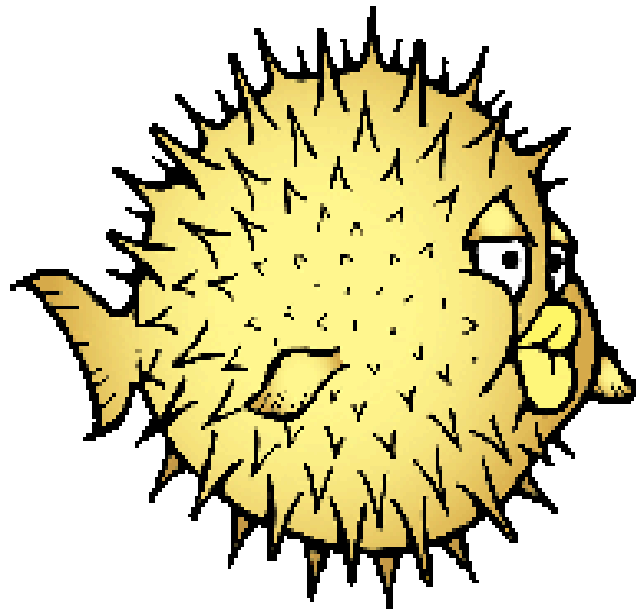


Breve introduzione al
Sistema Operativo
OpenBSD



***Open*BSD**

OpenBSD

La storia

GNU/Linux & BSD

Il progetto

Applicativi

Firewalling

Installazione

OpenBSD: La storia

OpenBSD nasce da un'idea di Theo de Raadt il 14 ottobre 1995.

OpenBSD si può considerare un *figlio* di NetBSD (Theo al tempo era uno degli sviluppatori di NetBSD).

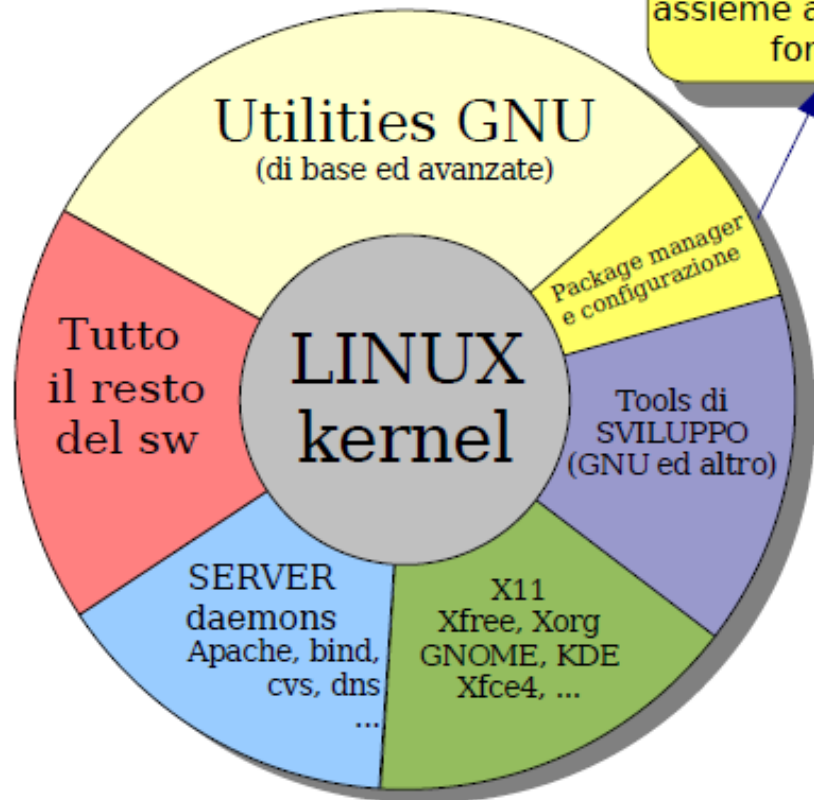
OpenBSD, come tutta la famiglia *BSD, nasce dalla versione UNIX sviluppata presso l'università di Berkeley (*Berkeley Software Distribution*)

OpenBSD: alcune note

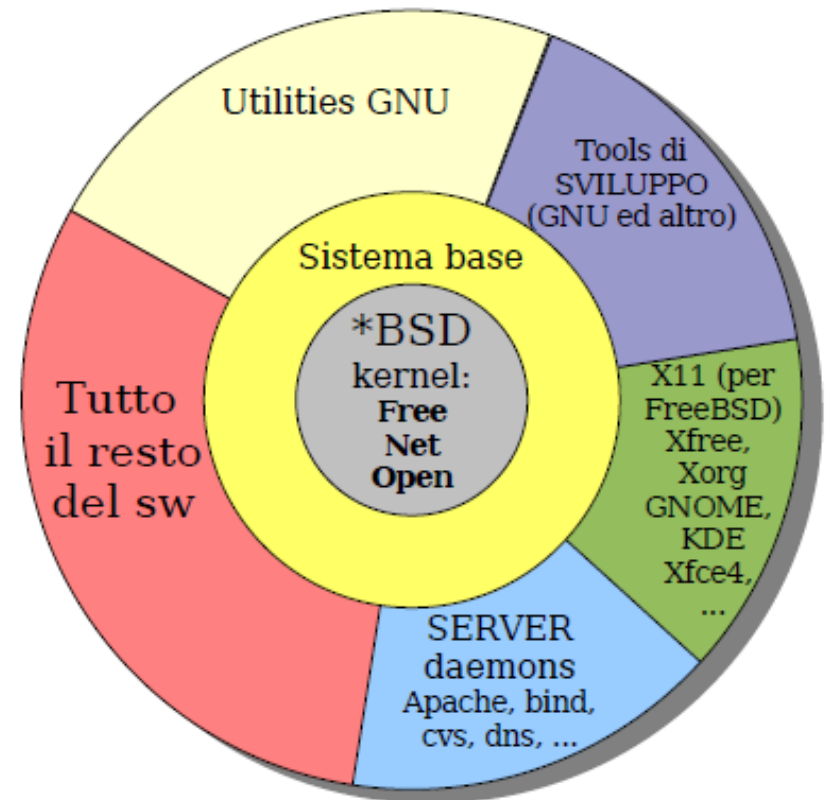
Attualmente, la comunità degli sviluppatori conta circa 80 sviluppatori nella sua parte core (di cui solo 1 italiano – Michele *mydecay* Marchetto)

Sistemi: GNU/Linux e *BSD

Linux



*BSD



Varie "distribuzioni" Linux:
Debian, *buntu, Gentoo,
Slackware, Mandriva, Fedora,
SuSe, LFS, LRP, Knoppix, ...

Principali *BSD:

- FreeBSD (stabilità, velocità, semplicità)
- NetBSD (portabilità, innovazione, eleganza)
- OpenBSD (sicurezza)
- DragonFly BSD (scalabilità, robustezza)

Scopi del progetto

Fornire completo accesso ai sorgenti.

Avere una licenza libera e permissiva.

Codice scritto in maniera leggibile e ben commentato.

Avere crittografia libera ed integrata (è uno dei motivi per cui OpenBSD è in Canada e non negli U.S.A. - non permettono la ri-esportazione libera dei protocolli di crittografia).

Essere proattivi nella sicurezza e fornire correzioni in maniera rapida e chiara.

Scopi del progetto

Totale audit del codice per prevenire errori che portino a compromissioni (solo 2 falle di sicurezza nel sistema di base)!

(ok... molti obietteranno che il sistema base permette ben poco; ma, io, non amo attivare servizi che non uso).

Se escludiamo il sistema base (che è l'unica vera parte del S.O., gli altri bug affliggono anche tutte le altre varianti unix!)

Scopi del progetto

Il modello di sviluppo aperto, soprattutto tendente ad uno standard definito, permette di tenere una linea guida piuttosto rigida, specialmente nella stesura del codice. La comunità OpenBSD è molto orientata alla sicurezza (a volte in maniera paranoica).

Il codice è sotto costante controllo da parte del gruppo per identificare errori.

Tutto il codice viene testato nella sua totale integrità e funzionalità durante il processo di release.

Alcuni esempi di prodotti.

La comunità OpenBSD ha prodotto alcuni software che sono usati su base quotidiana:

OpenSSH

OpenCVS

OpenNTPd

OpenBGPd

OpenBSD

Spesso, questi software sono nati dall'esigenza di rendere realmente sicuri i protocolli/applicativi in questione. Per la comunità ha avuto più senso svilupparli ex novo che non cercare di sistemare prodotti esistenti.

OpenBSD: le caratteristiche

Oltre alla sicurezza, agli standard e alla coerenza, il progetto ha tenuto conto anche della portabilità.

Attualmente sono supportate pienamente le seguenti piattaforme:

- [alpha](#) Digital Alpha-based systems
- [amd64](#) AMD64-based systems
- [armish](#) ARM-based appliances (by Thecus, IO-DATA, and others)
- [hp300](#) Hewlett-Packard HP 9000 series 300 and 400 workstations
- [hppa](#) Hewlett-Packard Precision Architecture (PA-RISC) systems
- [i386](#) Standard PC and clones based on the Intel i386 architecture and compatible processors
- [landisk](#) IO-DATA Landisk systems (such as USL-5P) based on the SH4 cpu
- [macppc](#) Apple *New World* PowerPC-based machines, from the iMac onwards
- [mvme68k](#) Motorola 680x0-based VME systems
- [mvme88k](#) Motorola 881x0-based VME systems
- [sgi](#) SGI MIPS-based workstations
- [socppc](#) Freescale PowerPC SoC-based machines
- [sparc](#) Sun sun4, sun4c and sun4m class SPARC systems
- [sparc64](#) Sun UltraSPARC systems
- [vax](#) Digital VAX-based systems
- [zaurus](#) Sharp Zaurus C3x00 PDAs

OpenBSD: le caratteristiche

Affiancare al progetto una documentazione il più possibile omogenea, esaustiva e comprensibile.

Produrre delle FAQ più esaustive possibile.

Cercare di mantenere la configurazione il più semplice possibile.

Sviluppo

L'albero cvs di OpenBSD è diviso in varie categorie, di cui 4 sono le principali:

- src: i sorgenti del sistema vero e proprio

- xenocara: l'interfaccia grafica (X server)

- ports: tutti gli applicativi non inclusi nel sistema base (in questi possiamo trovare anche applicazioni con licenza diversa da BSD)

- www: il sito web (per chi voglia avere una copia del medesimo, o lo voglia pubblicare)

Sviluppo

Ogni 6 mesi viene rilasciata una nuova versione (la prima fu la 2.0).

Ogni versione ha un ciclo di supporto di un anno (ovvero il sistema è supportato nella versione corrente e la precedente).

Esistono 3 '*versioni*' di ogni Release di OpenBSD:

-release: ovvero la versione creata allo snapshot e che determina la nuova release

-stable: la release con correzioni di sicurezza e di migliorie all'esistente

-current: tutte le nuove features, che in buona parte confluiranno nella nuova release

Sviluppo

Il sistema non ha una proprio piano di sviluppo:

questo implica che si procede passo per passo migliorando l'esistente ed aggiungendo porzioni di codice da parte di volontari.

Se quindi volete del supporto per uno specifico prodotto avete solo 2 scelte:

Scrivere il Vostro codice e sottometterlo al comitee

Assoldare qualcuno che lo faccia per voi

Sicurezza del sistema

La sicurezza del sistema, a livello di codice, è ottenuta attraverso vari modi:

Massima riduzione dell'uso di eseguibili con il flag di suid/sgid abilitato

Ricorso alla 'privilege separation'

Audit del codice

StackGap

ProPolice (GCC)

W^X

Gestione casuale dell'immagine per librerie condivise (ld.so)

mmap() con allocazione casuale

malloc() con allocazione casuale

Ricorso all'uso dei dati in modalità ROM (.rodata)

Gli applicativi: ports

OpenBSD, come molti altri sistemi unix based, propone una cospicua serie di applicazioni di terze parti.

Nel nostro caso, queste applicazioni sono state 'testate' per garantire il massimo livello di sicurezza (nel limite dell'applicativo stesso, senza doverlo o riscrivere o limitarne troppo le sue funzionalità).

Alla data odierna vi sono 5068 pacchetti disponibili (senza considerare le varianti).

Ports 2

I ports sono strutturati per categorie.

archivers, astro, audio, benchmarks, biology, books, cad, chinese, comms, converters, databases, devel, editors, education, emulators, games, geo, graphics, infrastructure, inputmethods, japanese, java, net, korean, lang, mail, math, misc, multimedia, news, palm

Ports 3

Il gruppo di sviluppo di OpenBSD rende disponibili sempre i ports aggiornati in formato binario.

(lo stesso gruppo ne consiglia l'utilizzo)

Vi sono però delle eccezioni.

Queste sono essenzialmente dovute a 2 cause:

Licenza (non è permessa la distribuzione del binario compilato)

FLAVORS.

Ports 4

I sorgenti dei ports sono presenti (o scaricabili via cvs o ftp/http all'ultimo snapshot) nella cartella /usr/ports.

I pacchetti vengono sempre installati, anche per mantenere una buona 'pulizia' del filesystem, in /usr/local.

Una delle cose più interessanti del sistema dei ports è che risolve da solo le eventuali dipendenze (pkg_add -r)

Ports 5

La compilazione dei pacchetti prevede l'eventuale installazione di tutte le dipendenze (sia di compilazione che di runtime).

Per compilare un port, basta mettersi nella cartella dell'applicativo che ci interessa e digitare

make install (qui possiamo aggiungere anche eventuali opzioni/flavour di compilazione)

Quando compiliamo un port, troveremo sia questo che le eventuali dipendenze nel percorso

`/usr/ports/package/{architettura}/<nome_port.tgz>`

PacketFilter (pf)

PacketFilter fa la sua comparsa con la versione 3.0.

La nascita di PF è stata generata dalla modifica introdotta alla licenza di ipf (il firewall precedentemente utilizzato, sviluppato da Darren Reed).

Il suo sviluppo è iniziato in maggio 2001.

Ha iniziato a sostituire ipf già nel giugno 2001.

PacketFilter 2

Tra le caratteristiche più interessanti di pf vi sono:

Stateful inspection

Packet tagging

Utilizzo di macro

Utilizzo di tabelle (sia dinamiche che statiche)

Syntax validation

Queueing

Load balancing

Transparent mode

Authpf

Ridondanza

NAT

Redirection

PacketFilter 3

La configurazione è contenuta in un unico file */etc/pf.conf*.

pf può esser controllato per mezzo del comando *pfctl*.

Questo tool permette di abilitare, modificare, verificare il funzionamento e la modifica delle regole e delle tabelle in esso contenute.

PacktFilter 4

Tabelle, liste e macro

Liste:

Sono oggetti che contengono definizioni (porte, indirizzi, liste - è ammesso l'annidamento delle liste -, etc)

Le liste sono contrassegnate da oggetti contenuti tra { }.

Macro:

Le macro sono definizioni di altri oggetti (interfacce, liste, indirizzi, porte, etc)

Sono contrassegnate da una assegnazione =” “.

PacketFilter 5

Tabelle:

Possono essere di vari tipi:

Dinamiche, statiche e persistenti.

Le tabelle contengono liste di indirizzi IP (sia singoli ip che sequenze)

Sono contrassegnate da <>

PacketFilter 6

NAT

Le operazioni di NetworkAddressTranslation sono integrate in pf. Con ipf, il filtering ed il NAT erano gestiti da 2 applicativi distinti, con relative configurazioni.

(affinchè NAT possa funzionare è necessario attivare il packet forwarding a livello di kernel)

Il NAT può essere anche escluso per uno specifico host e/o porta

PacketFilter 7

CARP e pfsync

In pf, con la sua evoluzione costante, sono comparsi *pfsync* e *CARP*.

CARP e *pfsync* permettono a due o più host di scambiarsi gli aggiornamenti di stato delle connessioni (abbiamo quindi una propagazione di tutte le connessioni che transitano per un pool di host).

PacketFilter 8

Authpf

Altro elemento interessante, introdotto in pf è *authpf*.

Si tratta, sommariamente, di una shell utente che permette di ottenere un nuovo set di regole per pf.

Installazione ed upgrade

Installare OpenBSD può risultare strano o ostico per molti che siano abituati alle moderne installazioni grafiche.

OpenBSD si installa (e probabilmente si installerà sempre in modalità testuale).

I prerequisiti sono pochi (specie in termini di spazio).

Ogni nuova release è accompagnata da un file di istruzioni e di hardware supportato.

OpenBSD non ha un supporto hardware esteso come quello di GNU/Linux.

Se quindi volete utilizzarlo su una vostra macchina, prima verificate bene che quello che vi serve sia supportato (verificate nel sito o nel file `INSTALL.xxx`).

Installazione ed upgrade 2

È anche buona norma non basarsi su hardware di scarsa qualità.

Un tipico esempio di hardware povero in tal senso sono le schede di rete della RealTek

- * The RealTek 8139 PCI NIC redefines the meaning of 'low end.' This is*
- * probably the worst PCI ethernet controller ever made, with the possible*
- * exception of the FEAST chip made by SMC. The 8139 supports bus-master*
- * DMA, but it has a terrible interface that nullifies any performance*
- * gains that bus-master DMA usually offers.*

(tratto da if_rl.c, The FreeBSD Project)

Ricorrere ad hardware di qualità può apparire un costo, ma alla fine, darà solo vantaggi in termini di affidabilità e performance.

Installazione ed upgrade 3

Una delle peculiarità di OpenBSD è permettere l'upgrade sia partendo da sorgenti (ma richiede, in tal caso, spazio e CPU) che da binari.

È quindi possibile aggiornare da remoto una macchina.

È indispensabile però verificare cosa sia cambiato (specie negli utenti e elementi sensibili - esempio pf).

(uno dei relatori all'OpenCon del 2006 ha tenuto in talk su tale argomento, mostrando, dati alla mano, come sia _quasi_ impossibile avere problemi... ma egli stesso dichiarava: tenete 'just in case' un biglietto aereo a portata di mano, se operate su una macchina non ridondata o non in cluster).

Installazione ed upgrade 4

OpenBSD può essere installato da molteplici supporti, anche da hardware headless (anche il pc di casa vostra, se supporta il boot senza bios video).

Eseguire l'installazione da cd, ftp, http, floppy, tftp o altri protocolli/media dipende molto dalla vostro senso d'avventura, dall'hardware o dalla vostro modo di vedere il mondo.

I passi richiesti per l'installazione sono semplici:

Definire una serie di parametri (video, tastiera, target device, eventuale configurazione della rete)

Definire cosa vogliate installare (quali elementi)

Installazione ed upgrade 5

.OpenBSD è diviso in sezioni:

.bsd/bsd.mp

.bsd.rd

.basexx.tgz

.compxx.tgz

.etcxx.tgz

.gamexx.tgz

.manxx.tgz

.miscxx.tgz

.X Server:

- ❖ xbasexx.tgz

- ❖ xetcxx.tgz

- ❖ xfontxx.tgz

- ❖ xsharexx.tgz

- ❖ xservxx.tgz

Credits

Tutto il materiale presentato è stato tratto da sito di OpenBSD.org

La slide *Sistemi: GNU/Linux e BSD* è tratta da una presentazione di Massimo Masson del BLUG

La porzione di codice dell'interfaccia di rete per le RealTek813x è tratta dai sorgenti di FreeBSD.