

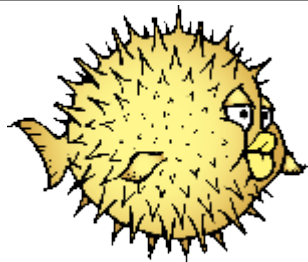
*Open***BSD**

O Sistema Operacional mais seguro do mundo
2 falhas de segurança remotas em mais de 10 anos

Semana da Informática - COTIL

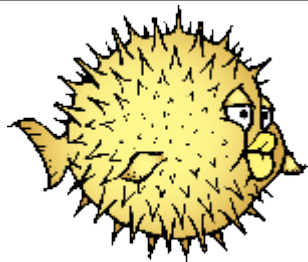
Renato Botelho

garga@FreeBSD.org



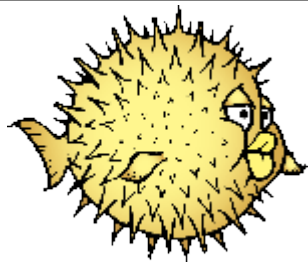
O nascimento do UNIX

- 1967 – Bell Labs, GE e MIT começam a desenvolver o MULTICS
- 1969 – Bell Labs abandona o projeto
- 1969 – Ken Thompson e Dennis Ritchie desenvolvem uma versão simplificada do MULTICS em um PDP-7. Brian Kernigham o batiza UNICS, e depois UNIX
- 1971 – Lançado o Unix V1 (assembly)
- 1973 – Ken Thompson e Dennis Ritchie criam a linguagem C
- 1973 – Unix é reescrito em C
- 1975 – Lançado o Unix V6, Berkeley compra os fontes e inicia o desenvolvimento do BSD
- 1978 – Lançado o 2BSD
- 1982 – Lançado o 2.11BSD, versão que trouxe o c shell



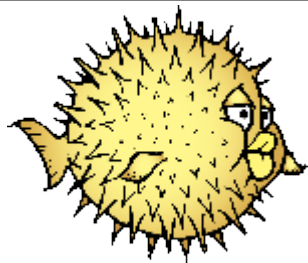
O nascimento do UNIX

- 1982 – Lançado o 3BSD, com suporte a memória virtual
- 1983 – Lançado o 4.2BSD, versão que trouxe o TCP/IP e sockets
- 1990 – Lançado o 4.3BSD
- 1992 – Lançado o 386BSD 0.0, baseado no 4.3BSD
- 1993 – O Projeto 386BSD muda o nome e é lançado o FreeBSD 1.0, foco em estabilidade
- 1993 – Lançado o 4.4BSD, muitas mudanças, versão muito estável
- 1993 – Lançado o NetBSD 0.8, foco em portabilidade
- 1994 – Novell compra o UNIX, e processa o FreeBSD 1.x por conter código proprietário do UNIX
- 1994 – 4.4BSD é totalmente reescrito e distribuído em formato opensource, nasce assim o 4.4BSD-Lite



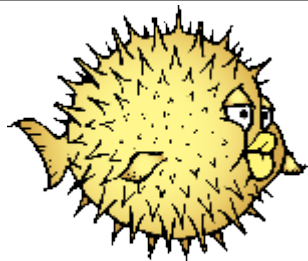
O nascimento do UNIX

- 1994 – Lançado o FreeBSD 2.0, removidos todos os códigos proprietários do UNIX
- 1994 – Lançado o NetBSD 1.0
- 1995 – Theo de Raadt não concorda com o rumo do NetBSD e quer lançar um Sistema Operacional focado em segurança, assim nasce o OpenBSD 1.0, baseado no NetBSD 1.0
- 1996 – Lançado o OpenBSD 2.0, primeira versão estável, desde então são lançadas versões à cada 6 meses, em 1º de Maio e 1º de Novembro. A versão atual é a 4.1.



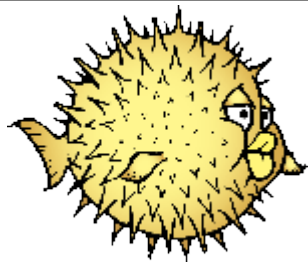
OpenBSD

- É um Sistema Operacional
 - Livre, licença BSD
 - Multiplataforma
 - Baseado em 4.4BSD-Lite
 - Foco em segurança e criptografia
 - Desenvolvido e mantido por voluntários de todo o mundo
 - Fundado e liderado até hoje por Theo de Raadt
 - Sediado no Canadá, pois não existem restrições ao uso e comercialização de software criptográfico



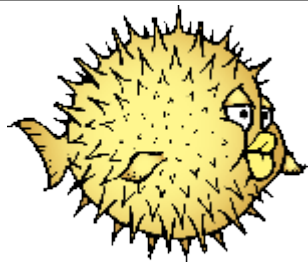
Arquiteturas Suportadas

- **Alpha** - Sistemas baseados em Digital Alpha
- **Amd64** - Sistemas baseados em AMD64
- **Armish** - Appliances baseados em ARM (Thecus, IO-Data, e outros)
- **Hp300** - Workstations Hewlett-Packard HP 9000 series 300 e 400
- **Hppa** - Sistemas Hewlett-Packard Precision Architecture (PA-RISC)
- **I386** - Plataforma PC e clones baseadas na arquitetura Intel i386 e processadores compatíveis
- **Landisk** - Sistemas Landisk IO-DATA (como os USL-5P) baseados na cpu SH4
- **Luna88k** - Workstations Omron LUNA-88K e LUNA-88K2
- **Mac68k** - Baseada no Motorola 680x0 Apple Macintosh com MMU
- **Macppc** – Computadores Apple do *Novo Mundo* baseados no processador PowerPC, da base do iMac
- **Mvme68k** - Sistemas VME baseados no Motorola 680x0
- **Mvme88k** - Sistemas VME baseados no Motorola 881x0
- **Sgi** - Workstations SGI baseadas em MIPS
- **Sparc** - Sistemas classe SPARC sun4, sun4c e sun4m
- **Sparc64** - Sistemas Sun UltraSPARC
- **Vax** - Sistemas baseados em VAX da Digital
- **Zaurus** - Sharp Zaurus C3x00 PDAs



Segurança

- Como manter a segurança?
 - Serviços não essenciais vem desabilitados por padrão
 - chroot em todos os serviços possíveis
 - Alterações no compilador
 - Ex: Para evitar *Buffer Overflow* funções como strcpy não compilam por padrão, é necessário usar strncpy, com tamanho máximo definido
 - Criptografia, até mesmo no swap
 - Quando uma nova falha é descoberta, ela é anunciada e corrigida rapidamente
 - Toda alteração é revisada por pelo menos 2 outros desenvolvedores
 - Segurança pró-ativa, da mesma maneira que os invasores sempre procuram novas brechas, os desenvolvedores também o fazem, para tentar encontrar antes e corrigir



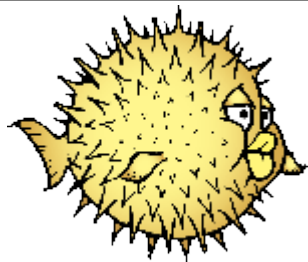
Versões

■ Sistema Base

- Lançadas a cada 6 meses
- 2 versões anteriores são mantidas
- Correções de falhas de segurança lançados imediatamente
- Current x Stable

■ Packages

- Árvore acompanha a versão
- Correções e atualizações importantes são feitas em todas as versões mantidas
- Pacotes compilados disponíveis para download
- Ports disponível no sistema para compilação e instalação local



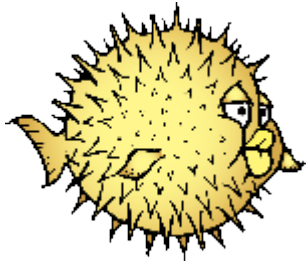
Prós e Contras

■ Prós

- Segurança
- Portabilidade
- Padronização
- Correção
- Segurança pró-ativa
- Criptografia integrada
- Requer pouco hardware

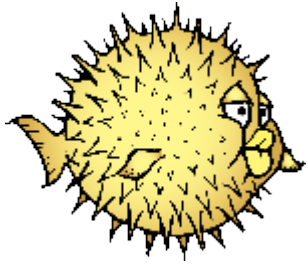
■ Contras

- Curva de aprendizado
- Sistema de arquivos lento
- Alguns fabricantes de hardware não provêem suporte



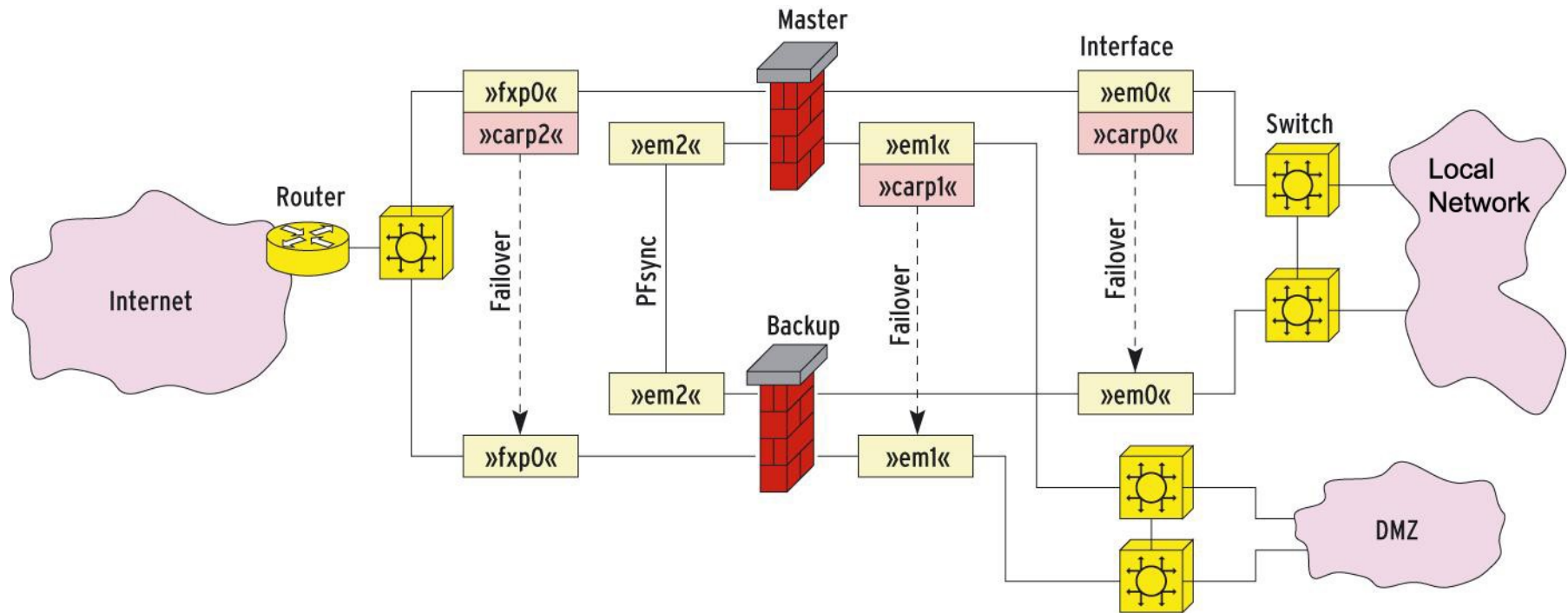
Aplicações

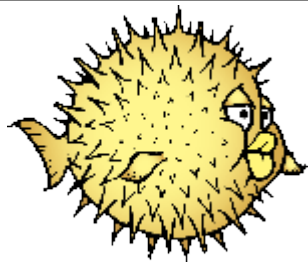
- Gateway (inclusive redundantes)
 - Firewall
 - Firewall autenticado
 - Roteadores
 - Sistemas embarcados
 - VPN
 - Balanceamento de carga (entrada e saída)
 - Criptografia via hardware
 - Servidor www
 - Servidor de arquivos
 - Proxy
-



Gateway redundante

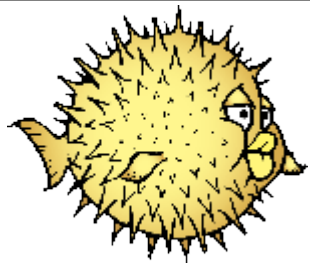
- CARP (Common Address Redundancy Protocol)
- pfsync





Quem usa?

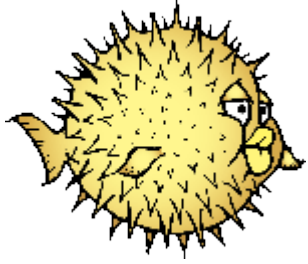
- Adobe Systems
 - Nasa
 - Network Security
 - Alteon
 - Comitê Gestor da Internet
 - Muitas universidades
 - Governo de países como Austrália, Chile, México e Colômbia
 - Usado como base em sistemas embarcados, firewalls comerciais
-



Informações

■ Sites:

- ❑ www.openbsd.org
 - ❑ www.openbsd.org/pt
 - ❑ www.openbsd-br.org
 - ❑ www.openbsd101.com
-



OpenBSD

Perguntas???
