OpenBSD Security Model

Nenad Merdanovic
<nenad.merdanovic[at]carnet[dot]hr>
FSec, Varazdin, 23.09.2011.

Only two remote holes in the default install, in a heck of a long time!

- What is OpenBSD?
- Goals of the OpenBSD project?
- Means to achieve those goals?
- How does it compare to Linux?
- Criticism!
- Other operating systems slowly followed

Development model

- Relatively small group of developers governed by one person – Theo De Raadt
- Fixed milestone release cycle – how do they do it?
- Security is just one side of the coin

Auditing process

- Largest audit happened at the end of 1996 and numerous (general) bugs were fixed
- Code regularly audited
- Developer meetings – large number of commits to the code
- Recent large audit of the OpenSSH code

Security mechanisms

- Secure by default!
- Buffer overflow protection
- Privilege separation
- Packet filter (pf)
- Network stack modifications
- Cryptography

Buffer overflow basics

- Basic types of BO attacks:
  - Rewrite return address
  - Rewrite frame pointer
  - Rewrite function arguments
- OpenBSD gonna give you hell!

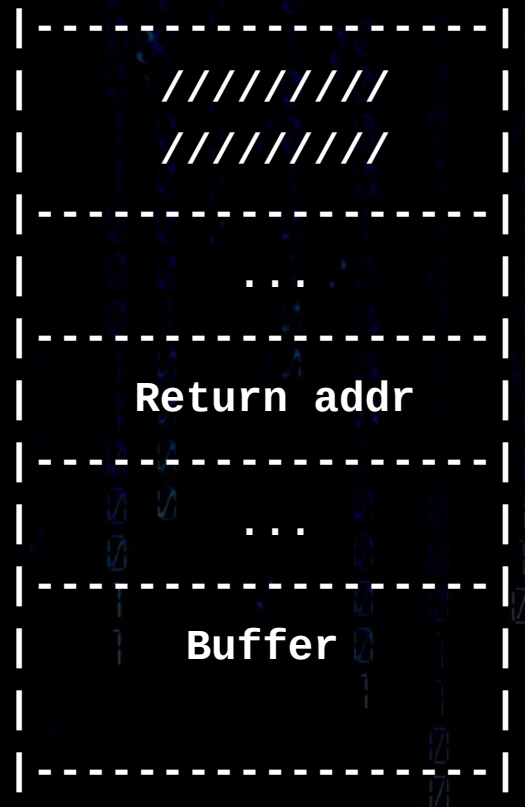
W xor X

- Memory based attacks often rely on a memory page being writeable and executable
- Mutual exclusion: A page is either writeable or executable, but never both
- Hardware support

Stackgap

- 3 line change to the kernel
- Random 64-256KB offset at the beginning of the stack
- 8KB aligned
- 1/32768 chance of getting it right
- You're doomed!

StackGap stack



ProPolice

- Based on StackGuard
- Altered stack order
- Guard variable inserted on the stack
- Compile time function altering

ProPolice stack

Additions to the C library

- While auditing, a lot of strcpy/strcat function usage found
- strncpy/strncat misused
- Developed two new functions: strlcpy and strlcat
- Simple usage, more security

PF – packet filter

- L3/L4 filter
- Appeared in OpenBSD 3.0
- Human readable syntax
- Support for NAT/PAT, HA, load balancing, etc.

ICMP based attacks

- First to deploy protection
- Types of attack:
  - Blind connection-reset
  - Blind performance-degrading
  - Blind throughput-reduction
- Other operating systems followed

Questions?