HardenedBSD Internals

shawn.webb@hardenedbsd.org
Twitter: @lattera

Agenda

- About Me
- Definitions
- About HardenedBSD
- Features
- Weather Report
- Digging In

About Me

- Cofounder of HardenedBSD
- Security enthusiast
- Opensource advocate
- Evangelist of FreeBSD
- ZFS fanboy

Definitions

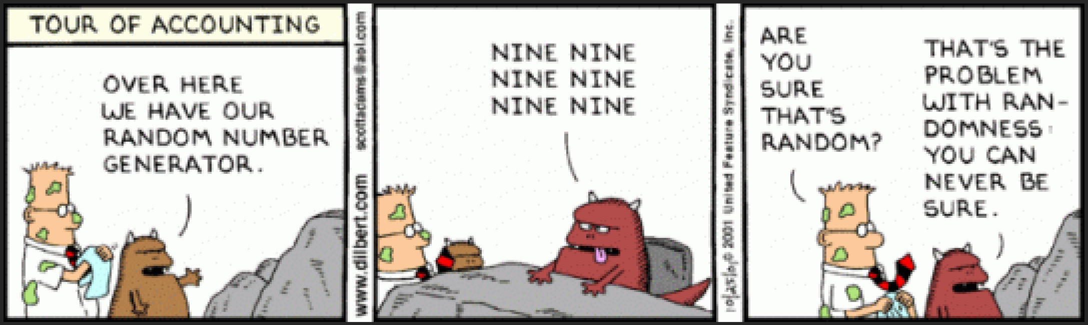
Security

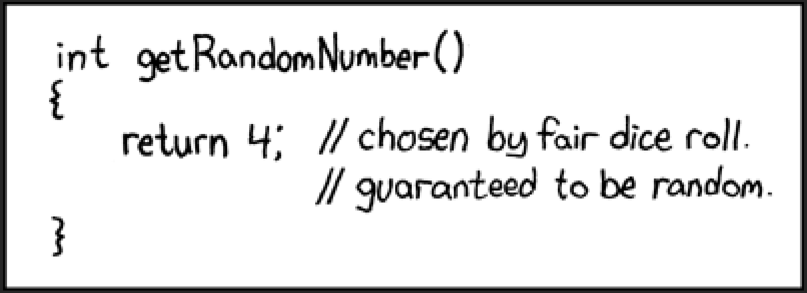
Definitions

Exploit Mitigation

Definitions

Address Space Layout Randomization (ASLR)


TOUR OF ACCOUNTING
OVER HERE WE HAVE OUR RANDOM NUMBER GENERATOR.
www.dilbert.com scottadams@aol.com
NINE NINE NINE NINE NINE NINE
© 2001 United Feature Syndicate, Inc.
ARE YOU SURE THAT'S RANDOM?
THAT'S THE PROBLEM WITH RANDOMNESS: YOU CAN NEVER BE SURE.



```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

About HardenedBSD

About HardenedBSD

- Officially launched April 2014
- Implementing and upstreaming ASLR is hard
- Single repository for FreeBSD exploitation mitigation development
- Full fork of FreeBSD

About HardenedBSD

- Many contributors
- Four developers. Two active daily.
- Incoming contributions from universities
- Four dedicated servers. One fully funded via IndieGogo.
- Potentially even more servers on their way

About HardenedBSD

- Three-year game plan:
  - ASLR, mprotect(exec) restrictions, w^x upstreamed
  - UDEREF
  - [lin]procfs restrictions upstreamed
  - Official releases
  - Commercial support

About HardenedBSD

- Five-year game plan:
  - 501(c)3 non-profit organization
  - And for-profit arm
  - Official hardware appliances (firewalls, IDS/IPS, etc.)
  - Windows SBS-like tool

Features

- ASLR
- NoExec – AKA w^x, AKA PaX PAGEEXEC
- [lin]procfs protections (lolwut? Yeah, really)
- PTrace restrictions
- mmap(map_32bit) hardening

Features

- Complete removal of mmap(NULL, MAP_FIXED) support
- Removal of many image activators
- getentropy
- Boot hardening

Features

- PaX-inspired SEGVGUARD
- Intel Supervisor Mode Access Protection (SMAP)
- The secadm application

Weather Report

- ASLR
  - Version 0
    - Being upstreamed
  - Version 0.5
    - Shared object load order randomization
      - Will upstream after v0 is accepted

Weather Report

- ASLR
  - Version 1
    - Research phase
    - VDSO randomization
    - True stack randomization
      - PS_STRINGS
      - Breaks a whole ton of ABI/API

Weather Report

- NoExec – AKA w^x, AKA PaX PAGEEXEC
  - Inspired by PaX
  - Prevent pages from being both writable and executable
  - Problem: Dynamic code (IE, Java, Javascript, JIT engines)
  - More research being done

Weather Report

- [lin]procfs hardening
  - Inspired by the Linux procfs attack vector
    - “OpenSSH <=6.6 SFTP misconfiguration exploit for 64bit Linux”
  - Completed

Weather Report

- Userland Enhancements
  - Recursive setfacl

Weather Report

- secadm – Security Administration
  - Version 0.1 - Released
    - Toggle ASLR, mprotect, PAGEEXEC, SEVGUARD per-binary
  - Version 0.2 – In progress
    - Executable File Integrity Enforcement
      - Enforce file hash before exec
      - Known as Integriforce

Weather Report

- secadm – Security Administration
  - Version 0.3 – Long-Term Research
    - Full binary signing, with x509 certs

Weather Report

- Infrastructure
  - Nightly build automation with Jenkins
    - Release targets signed with GPG
  - Package builds with Poudriere
    - Packages are signed
    - Stress testing!
  - All running HardenedBSD

ASLR Implementation

- Based off of PaX
  - Deltas for execution base, mmap, and stack
  - Stack is gap-based
- Code dive!

mprotect Implementation

- Inspired by PaX and OpenBSD
  - Enforce when PROT_EXEC is enabled on a mapping, PROT_WRITE is disabled
- Code dive!

[lin]procfs Implementation

- Cannot write to /proc/pid/mem and /proc/pid/*regs
- Code dive!

mmap Implementation

- On amd64: Disable MAP_32BIT support
  - Ties into ASLR implementation a bit
- Code dive!

secadm Implementation

- Three moving parts:
  - Kernel module
    - MAC framework
    - sysctl control channel
  - Shared library
  - Application
- Code dive!

Putting it all Together

- Lots of work done
- Lots of work to do
  - Especially with ASLR
- Combine multiple exploitation mitigations for best security

Next Milestones

- ASLRv2
- W^X/NoExec/PAGEEXEC
- UDEREF
- Executable file integrity enforcement
- Official release

https://www.hardenedbsd.org

https://github.com/HardenedBSD

https://twitter.com/HardenedBSD

http://jenkins.hardenedbsd.org

https://www.soldierx.com/