State of the Hardened Union

vBSDcon

06 Sep 2019

Shawn Webb
Senior Security Engineer

Technical Solutions Division

whoami

- Senior security engineer and development team lead for Huntington Ingalls Industries
- Cofounder of HardenedBSD
- President of the HardenedBSD Foundation
- Open source offensive and defensive work
- Human rights and anti-censorship work
- Perpetual newb

Agenda

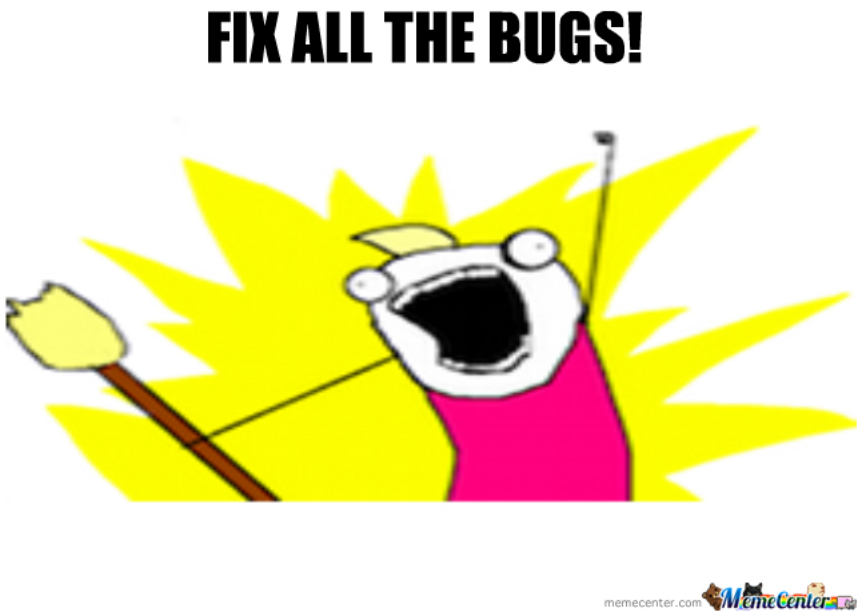
- Background
- Introduction to various exploit mitigations, focus on userland
  - W^X, PaX NOEXEC, DEP
  - ASLR
  - PaX SEGVGUARD
  - Control Flow Integrity
  - Code Pointer Integrity (chiefly: SafeStack)
  - CHERIBSD (primarily hardware-based)
- Security postures
- Call for participation
- Questions / comments

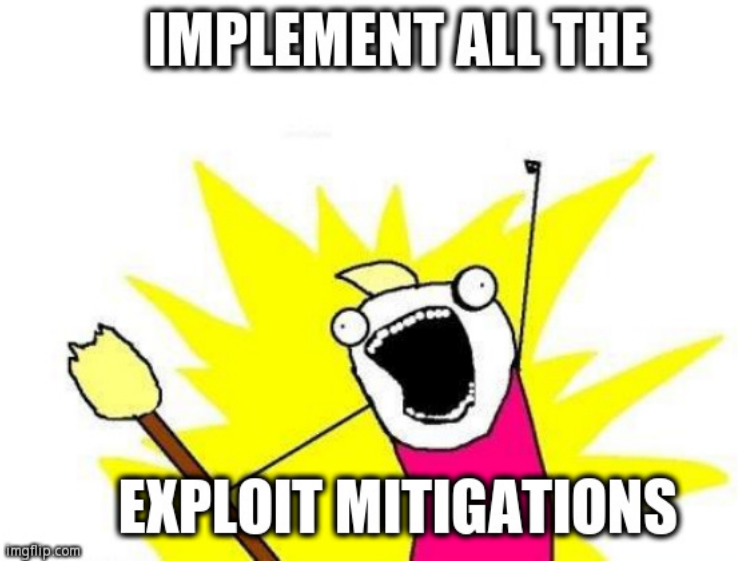
Background

- Back in my day...

Background

- Humans write code
- Humans are imperfect
- Imperfect code causes imperfect human
  - ...Or is it the other way around?





Intro to PaX NOEXEC

- PaX model:
  - At mmap time (PaX PAGEEXEC):
    - When page is writable, it can never be executable
    - When page is executable, it can never be writable
    - When page is both, silently drop executable
  - At mprotect time (PaX MPROTECT):
    - When page is writable, it can never be executable
    - When page is executable, it can never be writable
  - (PAGEEXEC + MPROTECT) = NOEXEC
  - Commonly breaks JITs. Implementors of the PaX model usually (always?) provide toggles for those very few applications violating PaX NOEXEC.
  - NetBSD and HardenedBSD
    - Interesting HardenedBSD commit: 0b951237eee70314b6d40f8fc7ea7fd77d312466

Intro to W^X (W xor X)

- OpenBSD model (aka, W^X):
  - Cannot create RWX pages
  - Can toggle between writable and executable
  - User-visible toggle: wxneeded for filesystem and binary
- FreeBSD model:
  - Application opt-in via new PROT_MAX macro added 30 Jun 2019
    - Do not allow page to have permissions not set in maxprot
    - Requires source-level modifications
    - procctl
- PaX model most strict
  - Breaks JITs, needs toggles
  - Provides highest level of security
- Windows term: Data Execution Prevention (DEP)
- “W^X” now generic term

Defeating W^X

- Assuming lack of AS[L]R
- 1997 saw ret2libc
  - NX stack defeat
  - Variants on a theme: ROP (2008), SROP, JOP, BROP
    - Code reuse attacks
- Shows need for AS[L]R and SEGVGUARD
- If attacker knows address space, game over

Address Space [Layout] Randomization

- Probabalistic defense against ret2libc-style attacks
- ASLR uses deltas generally computed at image activation (execve) time, ASR does not use deltas
  - Outliers:
    - Windows: Per-boot deltas (part of why suspend/resume on Windows dangerous)
    - FreeBSD: Partial ASR
    - OpenBSD: ASR
    - macOS: Weird mix of ASLR and ASR
- Requires address space contain zero interesting non-fixed mappings
- Position-Independent Executables (PIEs)

Address Space [Layout] Randomization

- PaX ASLR strongest form. On HardenedBSD, deltas computed at image activation:
  - PIE execution base
  - mmap(~(MAP_FIXED))
  - Stack (randomized stack top + randomized stack gap)
  - Shared page (hope to someday call this a VDSO on FreeBSD/HardenedBSD)
  - 64-bit systems: mmap(MAP_32BIT & ~(MAP_FIXED))
    - MAP_32BIT support disabled by default on HardenedBSD

Address Space [Layout] Randomization

- Propped up on pedastal
- Improper threat modeling
  - Somehow started to include browsers
- Helps frustrate remote attacks
- Weaknesses:
  - Information leak vulnerabilities
  - Certain format string vulnerabilities
  - Multi-tenancy / shared trust
- Combination of ASLR + DEP forever changed exploitation
  - Now must chain multiple vulnerabilities
  - Can fully render non-exploitable some real-world vulnerabilities

PaX SEGVGUARD

- Deterministic defense against unreliable exploitation
- Code reuse attack payload generation generally causes lots of crashes
- Track number of crashes in sliding window
- Attempt to exceed threshold result in temporary suspention of execution
- Similar to password bruteforce prevention
- Available in NetBSD and HardenedBSD
  - NetBSD: disabled by default due to memory constraint concerns
  - HardenedBSD: disabled by default due to performance concerns

Offensive Trends

- ASLR + DEP + SEGVGUARD drastically increase economic cost of successful attack
- Abusing function pointers
- Out-of-order execution (ROP and its variants)
- Data as code
- 2019 introduced multiple vulnerabilities in telnet
- Attackers paying closer attention to commit logs than defenders

Control Flow Integrity

- Multiple implementations
  - PaX Reuse Attack Protector (RAP)
  - Microsoft Control Flow Guard (CFG)
  - llvm Control Flow Integrity (CFI)
- RAP covered by multiple patents (unknown status), requires GPLv3 compiler toolchain (gcc > 4.2)
- CFG too lax
- llvm CFI incomplete, but most relevant to BSDs
  - Needs tight integration with both libc and the RTLD
  - ifunc in libc fallout
- HardenedBSD adopting llvm CFI
  - Non-Cross-DSO CFI: In use
  - Cross-DSO CFI: In development

Code Pointer Integrity - SafeStack

- Deterministic defense against arbitrary code execution
- Multiple implementations
  - PaX Reuse Attack Protector (RAP)
  - Microsoft Control Flow Guard (CFG)
  - llvm Control Flow Integrity (CFI)
- RAP covered by multiple patents (unknown status), requires GPLv3 compiler toolchain (gcc > 4.2)
- CFG too lax
- llvm CFI incomplete, but most relevant to BSDs

CHERIBSD

- Research hardware and FreeBSD derivative
- Hardware-enforced bounded capability model
  - Even pointers have capabilities
- Parts have made it into FreeBSD
  - Naturally FreeBSD-centric
- ARM picking up at least some of their work
- Problem: hardware-based solutions take multiple decades
  - Intel CET
  - SMAP
  - MPX
  - ARMv8.5

Technical security posture

- The good:
  - Collectively, the BSDs have come a long way
  - Paving the road in academia
  - Providing solutions that span decades
  - Each BSD provides different solutions to reach similar/same goals
- The not-so-good:
  - Occasionally stuck in academia
  - Lack of understanding
  - “We don’t need <X> because we have <Y>”
  - “<X> is dead!”

Political security posture

- Late or no advance notice
- Perception of violating embargoes
- Not considered large enough audience
  - Community fragmentation due to BSD fragmentation
- Lack of vendor representation

Community security posture

- Secure collaboration crucial
  - 2016: 25+ year old vulnerability in libc
  - CPU microarchitecture vulnerabilities
- Fragmentation leads to need for collaboration
- We need to build the foundation
  - Start even below the basement
- Lives are at stake
  - Remember Marta?
- HardenedBSD is building that foundation for collaboration

Call for Participation

- Increasing fragmentation of the BSDs
- Shared history, shared code
- Immediate needs:
  - Collaborate on security issues
  - Incentivize fair play
  - Centralized location for outside entities reporting issues
- Long-term needs:
  - Everything else
  - Literally
- bsdsec_collab@hardenedbsd.org
  - Invite-only for now
  - Please email shawn.webb@hardenedbsd.org or talk to me here at vBSDcon
  - 3mdeb, open source firmware vendor, first vendor on the list

Huntington Ingalls Industries

Hard Stuff Done Right ™

Technical Solutions Division

HII is NOT currently hiring:

- Arrogant Security Engineers with over-inflated egos
- Self-centered Java developers with NO interest in teambuilding
- Unethical Business Developers with dollars signs in their eyes
- "C Players" with little/no creativity or curiosity
- Complacent Systems Engineers with 8+ years of laziness under their belts
- Computer Scientists who resist change and/or accept the status quo "yawn"
- Cloud Developers who have no interest in producing highly valuable solutions

The following skills are NEVER required NOR desired:

- Consistent production of low-quality deliverables
- Excellence in blowing off deadlines and presenting excuses
- Proficiency in overlooking the needs of some, while talking down to others
- Experience sabotaging group-thinking sessions with ego-driven participation
- Effectively managing your time so that you have absolutely NOTHING to show for all your hard work
- The uncanny ability to overlook **FUN** at work

Why Choose HII Technical Solutions?

Our environment encourages employees to meet the highest standards of quality and ethical behavior, and to grow professionally. The company offers competitive wages and awards superior performance whether in skilled technical positions, technology, or professional positions.

Candidates who do NOT match the descriptions above are encouraged to apply at recruiting@g2-inc.com or visit tsd.huntingtoningalls.com