Session 9

Defense Mechanisms

Security Summer School

ACS/Ixia/Hexcellents

Contents

- Executable Space Protection
- Address Space Layout Randomization
- Bypass NX
- Bypass ASLR

Executable Space Protection

- principle of least privilege
- 3 permissions: read, write, execute
- writable regions cannot also be executable
- most importantly: the stack

Different OSes

- NX (Linux)
    - alternative implementation in Linux: PaX (grsecurity)
- Data Execution Prevention (Windows)
- Exec Shield (Red Hat)
- W xor X (OpenBSD)

Implementations

- NX bit
  - hardware support
  - requires 64-bit processor
  - large enough Page Table Entry for this extra bit
- Physical Address Extension (PAE)
  - main purpose: access more than 4GB of memory in 32-bit CPUs
  - also added support for the NX bit
- Emulation
  - older 32-bit systems
  - "overloads" the Supervisor bit
  - PaX: PAGEEXEC, SEGMEXEC

Just-in-Time (JIT) compilation

- NX cannot be active in JIT pages
- JIT has to write AND execute
- attack: JIT spray
    - Dion Blazakis @ Black Hat & DEF CON 2010

Syscalls

- `mmap()`
- `mprotect()`
- flags: `PROT_READ`, `PROT_WRITE`, `PROT_EXEC`

Mechanism

- ELF segments specify required permissions
- loader maps segments in memory pages
- permissions can later be changed using mprotect()

Address Space Layout Randomization (ASLR)

- maps regions and random addresses
- stack, data (heap), shared libraries, VDSO page
- entropy is important
  - 32-bit vs. 64-bit processors

Address Space Layout Randomization (ASLR)

- successful buffer overflow
- but no static address to jump to available

PLT and GOT

- Global Offset Table (GOT)
    - symbols from shared libraries
    - addresses filled in by loader just before runtime
- Procedure Linkage Table (PLT)
    - functions from shared libraries
    - addresses filled in by loader stub at runtime
    - lazy binding
- sections: `.got` (variables), `.got.plt` (function pointers), `.plt` (stubs)

Bypass NX

- ret-to-plt
- ret-to-libc
- mprotect()
- Return Oriented Programming (ROP)

Bypass ASLR

- bruteforce
- NOP sled
- jmp esp
- restrict entropy
- information leak

Resources

- http://en.wikipedia.org/wiki/PaX#PAGEEXEC
- http://en.wikipedia.org/wiki/PaX#SEGMEXEC
- http://www.semantiscope.com/research/BHDC2010/BHDC-2010-Slides-v2.pdf
- http://www.semantiscope.com/research/BHDC2010/BHDC-2010-Paper.pdf
- https://grsecurity.net/
- https://pax.grsecurity.net/docs/mprotect.txt