Mach-O Fun

Michael Feiri

The world before main()

fork() into existence

- Klassischer unixoider Programmstart
  - fork()
  - execve()
  - crt0/crt1
  - loader/linker
  - _start()/main()

influential environment

- Beeinflussungsmöglichkeiten im frühen Programmstart
  - OS compatibility
  - dynamic linking
  - UPX
  - path/env magic

dyld

- executable_path, loader_path, rpath
  - useful to stuff libraries in .app packages
  - reuse libraries from macports
    - install_name_tool
- DYLD_*

Demo?

- DYLD_PRINT_OPTS=1
  DYLD_PRINT_LIBRARIES=1
  DYLD_PRINT_STATISTICS=1
  DYLD_PRINT_INITIALIZERS=1
  DYLD_PRINT_BINDINGS=1
  DYLD_PRINT_SEGMENTS=1 clang -v
- DYLD_IMAGE_SUFFIX=_debug
- DYLD_INSERT_LIBRARES=/usr/lib/libgmalloc.dylib

TN2124: Mac OS X Debuggng Magic

early memory layout

- DYLD_PRINT_SEGMENTS=1 clang -v
  - __PAGEZERO
  - __TEXT
  - ...
- COMMPAGE

crt1

- clang -m32 -Os tiny.c -v
- „/opt/local/bin/../libexec/gcc/i686-apple-darwin10/4.2.1/ld“ -dynamic -arch i386 -macosx_version_min 10.6.0 -o a.out -lcrt1.10.6.o ....
- Opensource Projekt „Csu“

Extreme Minimization

a minimal c app

- int main() { return 42; }
- clang -m32 -Os tiny.c
  - 8608 bytes
- strip a.out
  - 8472 bytes
- ./a.out ; echo $?

a minimal assembly app

- looks pretty big in otool -tv
- clang -m32 -Os tiny_asm.s -nostartfiles
  - 4220
- strip
  - 4204

a minimal handcrafted assembly app

- still pretty big in otool -lv
- yasm -f bin tiny_singh.asm
    - 242 bytes
- yasm -f bin tiny_mfeiri.asm
    - 164 bytes

a minimal ... with a twist

- afsctool -cvv -9 tiny_singh
- File size (compressed data fork): 110 bytes
- afsctool -cvv -9 tiny_mfeiri
- File size (compressed data fork): 89 bytes
- ditto --hfsCompression <src> <dst>

Mach-O Infection

Mac OS X is not special

- weitgehend unixoid
- diverse blackhat paper
  - Infecting the Mach-o Object Format - Nemo
  - Let your Mach-O fly - Iozzo
  - ...

ASLR, Codesigning

- address space layout randomization bisher nur für Bibliotheken
- bestimme API calls können schon heute signierten code erfordern, z.B. task_for_pid, siehe auch lldb
- Jordan Hubbard at LISA 2008