Reverse Engineering Analysis of Vulnerabilities

Luis Miras

luis@ringzero.net

Agenda

[*] Types of reversing

[*] Assembly refresher

[*] Some vulnerabilities in assembly

[*] Tools and plugins

[*] Advisory to Trigger

[*] Other Topics

Types of reversing

Reverse Engineering in Security

[*] Malware analysis

[*] Exploit development

[*] Patch analysis

[*] Binary Auditing for vulnerabilities

Malware

[*] Malware goals

- Difficult to remove
- Difficult to analyze

Malware Considerations

[*] Obfuscated code

[*] Packers generally used

[*] Target RE tools

- Previous IDA problems
- OutputDebugString() format string

Vulnerability Analysis

[*] These following share similarities

- Exploit development from fuzzing, src audit, blackbox, etc.
- Patch analysis
- Binary Auditing for vulnerabilities

[*] Looking at vulnerabilities at different levels of depth

Assembly Refresher

Intel vs. ATT assembly

[*] Intel is used in

- Windows
- IDA Pro
- Ollydbg
- Windbg

[*] ATT is used in

- GCC
- GDB

Intel vs. ATT assembly

The basic difference is direction

- Intel: opcode dest, src
- mov ecx, eax
- (moves eax into ecx)

ATT: opcode src, dest

- mov %ecx, %eax
- (moves ecx into eax)

Registers

Registers are high speed memory within the processor

General:	eax, ebx, ecx, edx
Stack:	ebp, esp
Memory:	edi, esi

Mov instructions

[*] mov reg, reg

- mov eax, ecx

[*] mov reg, immediate

- mov eax, 0x10

[*] mov reg, [address]

- mov eax, [0x401010]

[*] mov reg, [reg]

- mov eax, [ebx]

[*] mov reg, [reg+offset]

- mov eax, [ebp + 8]

Comparisons

[*] Comparisons affect Eflags

- cmp reg, reg
- cmp eax, ecx
- cmp reg, immediate
- cmp eax, 1

[*] Arithmetic operations also affect Eflags

- add, reg, reg
- add eax, ebx

Branching

[*] Non-conditional

jmp offset

- jmp short loc_40102D

jmp reg

- jmp eax

call reg

- call _strcpy

[*] Condicional

jne

- jne short loc_40102D

ja

- ja short loc_40102D

Vulnerabilities

Vulnerabilities

[*] MS-Blaster (MS03-026)

[*] Trillian RSS Clientside

[*] VMware DHCP

MS DCOM RPC Overflow

[*] Microsoft Bulletin MS03-026

[*] Discovered by lsd-pl, first of many RPC vulnerabilities

[*] Remote attacker can run reliable arbitrary code as SYSTEM

\\machineName\resource

MS DCOM RPC Overflow

DEMO

Trillian RSS Clientside Overflow

[*] A vulnerability in RSS reader plugin.

[*] Client side unbound write to static buffer.

[*] Similar to MS03-026, buffer iteration bug

Credit: Matt Hargett

Trillian RSS Clientside Overflow

DEMO

Advisory to Trigger

[*] The cycle

- Advisory
- Patch Analysis
- Vulnerability identification
- Trigger vulnerability

VMware DHCP vulns

VMware Workstation DHCP Server Multiple Remote Code Execution Vulnerabilities

VMware Workstation's DHCP server is prone to multiple remote code-execution issues, including a stack-based integer-underflow issue, a stack-based buffer-overflow issue, and an unspecified vulnerability.

Credit: Neel Mehta and Ryan Smith of the IBM ISS X-Force

VMware DHCP vulns

- [*] Advisory does not reveal much information
- [*] Different research teams release more/less information
  - Eeye usually has some assembly
- [*] Need to disassemble and diff patches

VMware DHCP vulns

Bindiff demo

Plugins

Useful IDA Pro Plugins

[*] Sabre Security BinDiff

- Diff binaries

[*] Determina PDB plugin

- PDB (Symbol) loader

[*] IDA Python

- Scripting within IDA

[*] ida-x86emu

- x86 emulator

Useful IDA Pro Plugins

[*] Comment Viewer

- Recall comments and sort.
- Look for “TODO:” or “XXX:”

[*] Loop Colorizer

- Highlights loops

[*] Findcryptv2

- Finds crypto constants, sboxs, and tables

Useful Ollydbg Plugins

[*] Immunity Debugger

- Based on Ollydbg 1.10
- Includes python scripting, graphing
- Most Ollydbg plugins work

[*] OllyAdvanced

[*] Breakpoint manager

Summary

[*] Understand older vulnerabilities

[*] Use the advisory, patch, and exploit

[*] As you progress skip certain steps

History will repeat itself

Muito Obrigado!

luis@ringzero.net

http://luis.ringzero.net

Resources

OpenRCE
    http://openrce.org
IDA Pro
    http://datarescue.com/idabase/index.htm
Sabre Bindiff
    http://www.sabre-security.com/
Determina PDB plugin
    http://www.determina.com/security.research/utilities/index.html
IDA Python
    http://d-dome.net/idapython/
Comment Viewer
    http://www.openrce.org/downloads/details/237/Comment_Viewer
Loop Colorizer
    http://www.hexblog.com/

Resources

Findcrypt

- http://www.hexblog.com/

Ida-x86 emu

- http://ida-x86emu.sourceforge.net/

Immunity Debugger

- http://www.immunitysec.com/products-immdbg.shtml

Ollydbg

- http://www.ollydbg.de/

Olly Advanced

- http://www.openrce.org/downloads/details/241/Olly_Advanced

PaiMei

- http://paimei.openrce.org/

ERESI

- http://www.eresi-project.org/