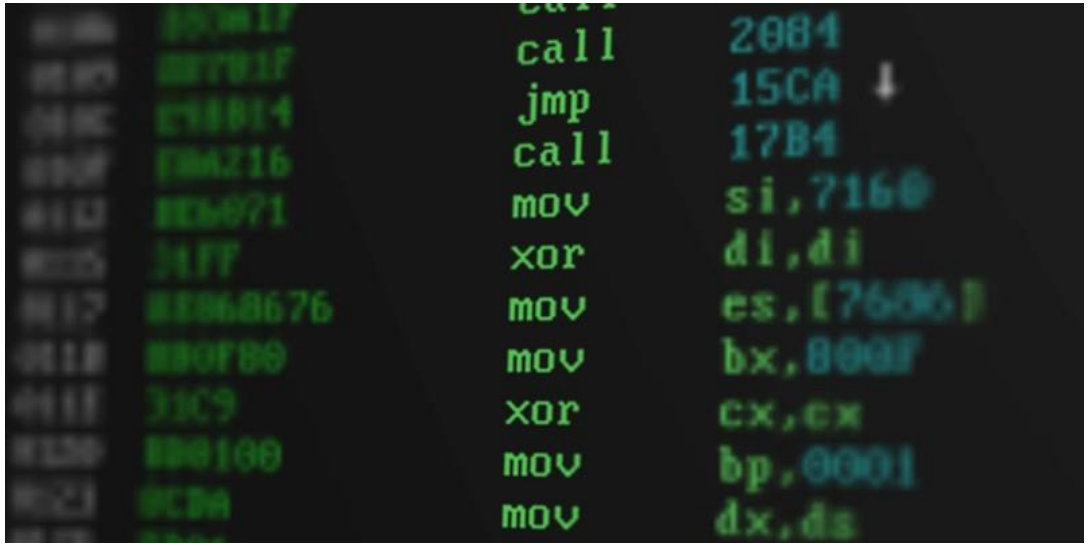
המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

Reverse Engineering Course

x64



Barak Gonen

Differences Between x32 – x64

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- 64 bit registers
- 64 bit data & address busses
- New registers
- New calling convention
- Stack alignment
- RIP Relative Addressing Mode

64 Bit Registers

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

All registers are extended to 64bit, notation “R”

RAX, RBX, RCX…

RBP, RSP…

RIP

RAX	EAX	AX	AH | AL

Effects of 64 Bit busses

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

1. More data is copied in memory access
2. 2^64 address space *

* Assume no limitations by OS or CPU

64 Bit Address Canonical Form

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

The “Unusable” address space saves chip complexity and cost

2^64-1 … 2^64 – 2^47	0xFFFFFFFFFFFFFFFF … 0xFFFF800000000000
Unusable	Unusable
2^47-1 … 0	0x00000FFFFFFFFFFF … 0

New Registers

המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

R7, R8, … R15

D - last double word bits (32). Example: R7D

W – last word bits (16). Example: R7W

B – last byte. Example: R7B

X64 Calling Convention

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

Let’s study hands on ☺

https://godbolt.org/

Try using char, short, int, long long

```
#include <iostream>
long long sum(long long a, long long b, long long c, long long d);

int main(){
    long long result = sum(1, 2, 3, 4);
    printf("%lld", result);
    return 0;
}

long long sum(long long a, long long b, long long c, long long d){
    return a+b+c+d;
}
```

X64 Calling Convention – cont.

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

Linux \ GNU version:

RDI

RSI

RDX

RCX

R8

R9

Other params- pushed to stack

Microsoft version:

RCX

RDX

R8

R9

Other params – pushed to stack

X64 Calling Convention – cont.

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

Stack must be aligned to 16 bytes before any call instruction

Aids performance of Intel’s extended vector instruction set (SSE)

x32 Address Relocation Issue

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

Problem: The address of a JMP changes

```
my_func:
    xor     eax, eax
my_label:
    ; do something
    jmp my_label
    ret
```

Process	JMP to (example) Address
Original function	00000001
After linking with another function	00000205
Loader assigned different address	00402245

Relocation tables are required

In x64, MOV EAX, [RIP] is possible – Relative addressing mode

Class Work

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

https:\\data.cyber.org.il\reversing\reg64.exe

- איך מועברים הפרמטרים לפונקציה?
- הגיעו אל מסר ההצלחה *בלי לפצ'פץ'*

Home Work

המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

https:\\data.cyber.org.il\reversing\Crackme64.exe