Tutorial 02

Security

Contents

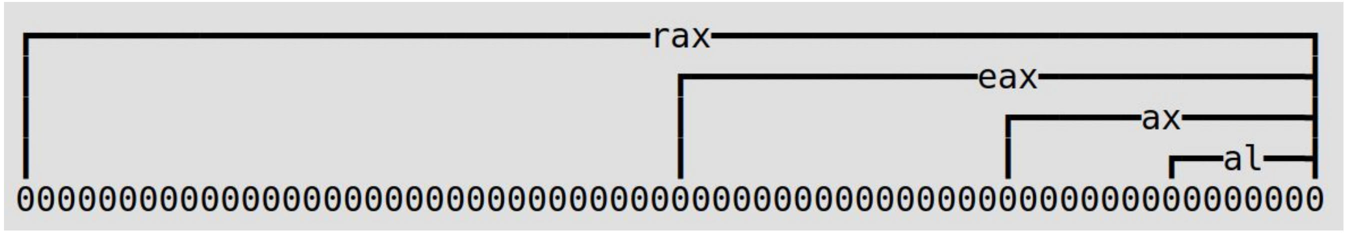
Frequent Mistakes in Exercise Sheet 1

- E 1.1 (b)
  - We need to consider compromise of keys.
- E 1.1 (d)
  - Collision resistance is stronger notion than second preimage resistance
  - Easy to find arbitrary collision than for fixed input
- E 1.2
  - B was offline
  - Reflection attack works

Questions from Exercise Sheet 2?

General Purpose Registers [Recap]

- rax
- rbx
- rcx
- rdx
- rsi
- rdi
- rbp
- rsp
- r8 - r15



and remember **rip** and **flags**

Intel Assembly Syntax [Recap]

- <Opcode> <destination operand>, <source operand>
- mov rax, rbx;

- I am using pwndbg
- Free to use pwndbg, gef, ...

Assembling .asm files

- sudo apt install nasm

- vim demo1.asm
- nasm -f elf64 -o demo1.o demo1.asm
- ld -o demo1 demo1.o

- ./demo1

Assembling .asm files

- vim demo2.asm
- nasm -f elf64 -o demo2.o demo2.asm
- ld -o demo2 demo2.o

- ./demo2
- echo $?

Variables: What about them?

- vim demo3.asm

- ./demo3
- echo $?

- objdump -s demo3 | less
- objdump -d demo3 -M intel | less

gdb quick notes

- break _start
- b _start
- b *<address>
- run | r
- continue | c
- si
- ni
- set $eax = 0xff
- info registers
- info functions
- disassemble main

Basic Instructions

- Quick walkthrough basic assembly instructions.

- Use demo4

Quick Reminder

- Install pwndbg before starting.
    - Or any tool of you choice.

Todo Task 1

- Try writing a simple assembly program to print strings using write syscall
- Similar to **demo2.asm**
- Template code is given
- Useful: https://chromium.googlesource.com/chromiumos/docs/+/HEAD/constants/syscalls.md#x86-32_bit

Todo Task 2

- What will be the value of eax just before line x? Annotated with “-->”. Parts:
    - 2a
    - 2b
    - 2c
- First try to do it on paper
- Then verify by running with gdb

Todo Task 3

- Source code for program is given in **todo3.c**
- There is no way to reach function **fun()**
- Can you still force it to run **fun()** while using gdb?

Todo Task 4

- Source code for program is given in **todo4.c**
- Can you find the correct key?

Time for Clarifications/Mistakes in Marking

- Any gripes?

Feedback Form

- Would like to see anything different?
- Liked it, hated it, something can be improved?

- Link: https://docs.google.com/forms/d/e/1FAIpQLSfVW3Uh73PKfrAIjcsTzTtZVV_2bWobt-E9VRvXc1J3erHpVg/viewform