המרכז
לחינוך סייבר
CYBER EDUCATION CENTER

Assembly for Reverse Engineering

Introduction

Barak Gonen

Assembly Language

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Machine language: 0100 1110 1111 0001 …
- Assembly instructions are slightly more human readable: mov, add, inc, mul …
- Writing assembly code requires deep knowledge of CPU (registers, flags, memory addresses)
- Assembly preceded High Level Languages
  - C, Java, Python
  - “Hide” the CPU internals from the programmer

Why Study Assembly?

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- … Want the job? :-)

Cyber Security Researcher

- Familiarity with programming languages (e.g. C++, Java, C#, PHP, Assembly, etc.)
- Knowledge of networking and internet protocols (e.g. TCP/IP, DNS, SMTP, HTTP)
- Reverse engineering experience – a must.
- Analysis of malicious code – Major advantage

- Plus it's sooooo fun!

Course Objective

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Feel comfortable with reading assembly code
- Required for Reverse Engineering

```
call    read_hex
add     eax, eax
mov     ebx, eax
shl     eax, ?
add     ebx, eax
shl     eax, 4
add     ebx, eax
call    print_eax
```

The Amazing T-Shirt Machine

המרכז לחינוך סייבר
CYBER EDUCATION CENTER

- Let’s dive into the amazing T-Shirt machine…