Introduction to Information Security

מרצים:

Dr. Eran Tromer: tromer@cs.tau.ac.il

Prof. Avishai Wool: yash@eng.tau.ac.il

מתרגלים:

Itamar Gilad (itamargi@post.tau.ac.il)

Nir Krakowski (nirkrako@post.tau.ac.il)

Course Guidlines

- The course exercises aren't easy!
  - You will have to learn and do a lot.
  - Google is your friend, but so are we!
- Best 75% of exercises will be used to calculate the average exercise grade.
- Exercises are to be submitted the week after the recitation
- Ask questions!!!
- Download exercises from website https://course.cs.tau.ac.il/infosec14/exercises
- **Fill out the course questionnaire!**

Instructors

- Nir and I will be instructing the course together
- **We've added an extra recitation: 17:00-18:00**
- Reception hour:
  - Right after the final recitation (18:00-19:00) if possible
  - Best: Schedule an appointment by email

- General note: Please keep in mind that the lectures and recitations will often not match. This is by design, not a mistake.

Recitation #0

- Subjects:
  - X86 Assembly
  - Course IT Framework

X86 assembly

- Instruction – A sentence (verb + noun / nouns)

- Opcode – what you want to do - verb
- Operand – what do you want to operate on (source) or with (dest) – nouns

Opcode Types

- Data operations (i.e.: MOV, XOR, ADD, SUB, INC, DEC, SHL, SHR, **TEST, CMP**)
- Unconditional control flow (branching) operations (i.e.: JMP, CALL, RET)
- Flag based conditional control flow operations (i.e.: JZ, JNE, JNZ, JBE, JG)
- Stack operations (i.e.: POP, PUSH, PUSHA, POPA)

- And many (many…) more!

Operand Types

- Registers
- Constants
- Memory addresses
- Pointers
- Flags

Command structure

- Command structure (no operand):
  - Opcode
  - Example: NOP
  - Example: RET
- Command structure (single operand):
  - Opcode operand
  - Example: INT 0x3
  - Example: JMP [memory address]
  - Example: POP [register]

Command structure

- Command structure (dual operand):
  - Opcode dest-operand source-operand
  - Example: MOV EAX, 0
  - Example: SAR EBX, 2
  - Example: MOV ECX, [EBX]
  - Note: there are limitations (i.e.: cannot use two memory based operands)

- Cheat Sheet: https://www.ssucet.org/mod/resource/view.php?id=886
- Google: x86 assembly cheat sheet

Extra - Common Register Uses

- EAX, EBX, ECX, EDX… - Generic registers
- EIP – Instruction pointer (next instruction to be executed)
- ESP – Stack pointer
- EBP – Frame pointer
- ESI – Source index
- EDI – Destination index
- EAX – function return value
- ECX – this pointer (in C++)

Course IT Framework

- VirtualBox VM file, with Ubuntu 12.04.2 LTS
  - Username: 'student'
  - Password: 'do or do not there is no try'
  - Change the password with the command: passwd
- Wine: IDA, Hexworkshop
- Python
- vi, gedit, ghex, hexedit
- To get more tools:
  - **sudo apt-get install [toolname]**
  - sudo pip install [pythonmodulename]
  - Google for more tools
- All exercises will be provided to work within the VM Framework.
- Most exercises **will not work** on a standard machine.

VM Demo

This week's exercise

- VM setup
- (Very) simple x86 Assembly exercises
- It isn't hard – but please start early and contact us if you have any trouble with the setup

- **Make sure to follow the exercise submission guidelines!**