Department of Electrical Engineering and Computing

Computing Security

CSEC 202 Reverse Engineering Fundamentals

Quiz #1

(22 Minutes)

Name:	ID

Zero-Tolerance Policy on Plagiarism

This examination is governed by a strict zero-tolerance policy towards intentional plagiarism. Any detected instance of plagiarism will result in a grade of zero for the work involved. Further, cheating and plagiarism offenses will be handled in accordance with university policies, specifically Policy 3.1.7 on Academic Responsibility.

Spring 2024
Feb 14, 2024

Section: CSEC202.601
Instructor: Emad AbuKhous

Exam Instructions:

Mark only one answer for each question

Points Equally Distributed. Questions & Options Randomized.

Complete All Questions (Total: 10 Points)

1. **Which instruction is typically used to compare two values and set the processor's flags without altering the values?**

   A) "CMP"
   B) "ADD"
   C) "SUB"
   D) "XOR"

2. **How many unique characters can standard ASCII represent?**
   A) 64
   B) 512
   C) 128
   D) 256

3. **In the Von Neumann Architecture, what role does the system bus play?**
   A) It provides a permanent storage solution.
   B) It generates graphical output for displays.
   C) It serves as a communication pathway between CPU, memory, and I/O devices.
   D) It is only used for USB communications.

4. **After executing "SUB EAX, EAX", what is the expected state of the Zero Flag (ZF)?**
   A) ZF is cleared.
   B) ZF is unchanged.
   C) ZF is set.
   D) ZF state is unpredictable.

5. **Why is reverse engineering particularly important for cybersecurity professionals?**
   A) It is practiced exclusively for hardware design and has no place in software analysis.
   B) It is solely for educational purposes to teach programming languages.
   C) It allows professionals to manually triage malware, understand attackers' methods, and devise effective defenses.
   D) Reverse engineering is only used for creating new games and entertainment software.

6. Which program combines object files and libraries into a final executable?

A) Preprocessor
B) Linker
C) Compiler
D) Assembler

7. How does the action of the CPU differ between initiating a memory read and executing a memory write?

A) For a read, the CPU sends data to memory, while for a write, it places an address on the bus.
B) For a read, the CPU updates the Program Counter, while for a write, it copies data into a register.
C) For a read, the CPU places an address on the bus, while for a write, it puts data on the bus.
D) For a read, the CPU performs an arithmetic operation, while for a write, it reads data from the bus.

10 Given the following code snippets, identify which is a RISC-style set of instructions and which is CISC-style:

Code 1:

```
ADD dword ptr [ebx], 5
```

Code 2:

```
LDR R1, [R2]
ADD R1, R1, #5
STR R1, [R2]
```

A) Code 1 is CISC; Code 2 is RISC
B) Both Code 1 and Code 2 are CISC
C) Both Code 1 and Code 2 are RISC
D) Code 1 is RISC; Code 2 is CISC

8. **What is the program counter (PC) used for?**
   A) It counts the number of programs running on the system.
   B) It controls the voltage supplied to the CPU.
   C) It stores the address of the next instruction to be executed by the CPU.
   D) It monitors the performance of the CPU.

9. **What does the "Load" operation do in CPU operations?**
   A) Saves data from a register to a disk.
   B) Loads new programs into the main memory.
   C) Transfers data from memory to a register within the CPU.
   D) Increases the CPU clock speed.

Bonus Question: [1 Point]

Note: This bonus point applies solely to this exam and cannot be transferred to other assignments or exams.

1. **Why are registers vital in the context of the Instruction Set Architecture (ISA)?**

   A) They regulate the power supply to the CP
   B) They are used for external storage devices.
   C) They serve as the primary communication method with peripheral devices.
   D) They are the fastest type of memory for immediate data retrieval and execution by the CPU.

Good Luck