Department of Electrical Engineering and Computing

Computing Security

CSEC 202 Reverse Engineering Fundamentals

Quiz #1

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

Sections: CSEC202.601
Instructor: Emad AbuKhousa

Exam Instructions:

Complete All Questions (Total: 10 Points)

Points Equally Distributed. Questions & Options Randomized.

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

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

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

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

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

5. **Which program combines object files and libraries into a final executable?**
   A) Preprocessor
   B) Compiler
   C) Assembler
   D) Linker

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

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

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

9. **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 places an address on the bus, while for a write, it puts data on the bus.
   C) For a read, the CPU updates the Program Counter, while for a write, it copies data into a register.
   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) Code 1 is RISC; Code 2 is CISC
C) Both Code 1 and Code 2 are CISC
D) Both Code 1 and Code 2 are RISC

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

Good Luck