Full Name: _____ Gannon Identification Number: _____

CYENG 225: Microcontroller Essentials for Cyber Applications
Spring 2023, Second Examination
Gannon University (GU)
April 13, 2023

Please do not turn the page until you are informed.

Rules:

- The exam is closed-book, closed-note, closed shared calculator, and closed electronics.
- Please stop promptly at **10:00 AM**.
- There are **20 points** total, distributed **evenly** among **2** questions.

Question	Maximum	Earned
1	10	
2	10	

Advice:

- Read questions carefully. Understand a question before you start writing your answer.
- Write down thoughts and intermediate steps so you can get partial credit. Clearly circle your final answer.
- The questions are not necessarily in order of difficulty. **Skip around.** Make sure you get to all the problems.

Wishing you the best of luck,
Dr. Shayan (Sean) Taheri

Full Name: _____ Gannon Identification Number: _____

Question 1. (10 points) Complete the following items on **Secure Processor** and **TEE**.

A. Name and describe **the new privilege levels** that can be added to general-purpose processor architectures to provide Trusted Execution Environments (TEEs) and facilitate protection of software (software modules, applications, or even VMs).
B. With **"N" privilege levels**, determine the number of possible combinations of security architectures based on different assumptions according to which whether each level is trusted or not.
C. Specify what **three-dimensional integration** is and what advantages and disadvantages it has based on Cybersecurity perspective.
D. Determine the relationships between **TCB** and **TEE**.

Full Name: _____ Gannon Identification Number: _____

Question 1. (Cont.)

Full Name: _____ Gannon Identification Number: _____

Question 2. (10 points) Complete the following items on **Root of Trust** and **Memory Protection**.

A. Provide a single and brief overview of the **chain of trust**, the **security measurements**, and the **root of trust** using a figure.
B. Explain why and how the security measurements are **validated**. Specify whether this process can be done **remotely** and if yes, then how.
C. Determine the major techniques that can provide **memory protection**.
D. Explain the functionality and the operations of **ORAM** using a figure.

Full Name: _____ Gannon Identification Number: _____

Question 2. (Cont.)