Full Name: ___________________________ Gannon Identification Number: __________________________

CYENG 225: Microcontroller Essentials for Cyber Applications
Spring 2023, Final/Third Examination
Gannon University (GU)
May 04, 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 **10:30 AM**.
- There are **30 points** total, distributed **evenly** among **3** questions.

Question	Maximum	Earned
1	10	
2	10	
3	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 **the Principles, Security Verification Approaches, Secure Processor Architectures,** and **Protecting Software within Trusted Execution Environments**.

A. Specify a set of five principles that can be followed to achieve a secure design. Explain one of these principles.
B. Explain the general procedure for security verification. Describe one of the steps in this procedure that includes theorem provers or model checking.
C. Mention different options for implementation of hardware TCB.
D. Describe an alternative that does not necessarily use the linearly ordered set of privilege levels at all.
E. Determine the purpose of adding new privilege levels to a computing system and discuss them using a figure.

Full Name: ___________________________ Gannon Identification Number: __________________________

Question 1. (Cont.)

Full Name: ___________________________ Gannon Identification Number: __________________________

Question 2. (10 points) Complete the following items on **Multiprocessor Security**, and **Many-Core Processors and Multi-Processor System-on-a-Chip**.

A. Discuss the similarities, the differences, and the tradeoffs of the SMP and the DSM.
B. Specify the threat models for the SMP and the DSM using figures.
C. Briefly explain the factors of "Confidentiality and Integrity of Communication", "Confidentiality and Integrity of Memory", "Memory Access Pattern Protection", and "Key Management" for the DSM.
D. Describe what NoC is and determine its threat models using a figure.
E. Explain defense techniques for securing NoC communications.

Full Name: ___________________________ Gannon Identification Number: __________________________

Question 2. (Cont.)

Full Name: __________________________ Gannon Identification Number: _________________________

Question 3. (10 points) Complete the following items on **Side and Covert Channels**, and **Processor Features and Information Leaks**.

A. Discuss the similarities and the differences between side channels and covert channels using figures.
B. Explain how side and covert channels are for processors and specify their classifications.
C. Determine and explain characteristics of modern processors and their design which lead to microarchitectural-based information leaks that can form a basis for a side or covert channel using a figure.
D. Mention how functional units can be exploited by adversaries to cause leakage of side/covert channel information.
E. Discuss the vulnerabilities of the memory-related elements (such as controllers and interconnects) for successfully launching side-channel attacks.

Full Name: ___________________________ Gannon Identification Number: __________________________

Question 3. (Cont.)