Full Name: _____ Gannon Identification Number: _____

CYENG 351: Embedded Secure Networking
Spring 2023, Final/Third Examination
Gannon University (GU)
May 01, 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 **6:00 PM**.
- 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 **Dealing with Attacks** and **High Performance in Silicon**.

A. Fill out the empty spaces in the following statement: *Any system connected to ____ (e.g., the Internet or proprietary) will be subject to attacks - both ____ (i.e., malicious hackers) and ____ (i.e., heavy network traffic leading to Denial of Service)*.
B. Specify the first line of defense in Embedded Applications Security.
C. Discuss the advantages and the disadvantages of the FPGA systems for hardware-based security solutions.
D – *Option 1*. Explain how to recover after multiple existing defense mechanisms failed and an attack was launched successfully on a computing system.
D. – *Option 2*. Describe multiple methods with examples that auxiliary hardware can assist processor in security applications.

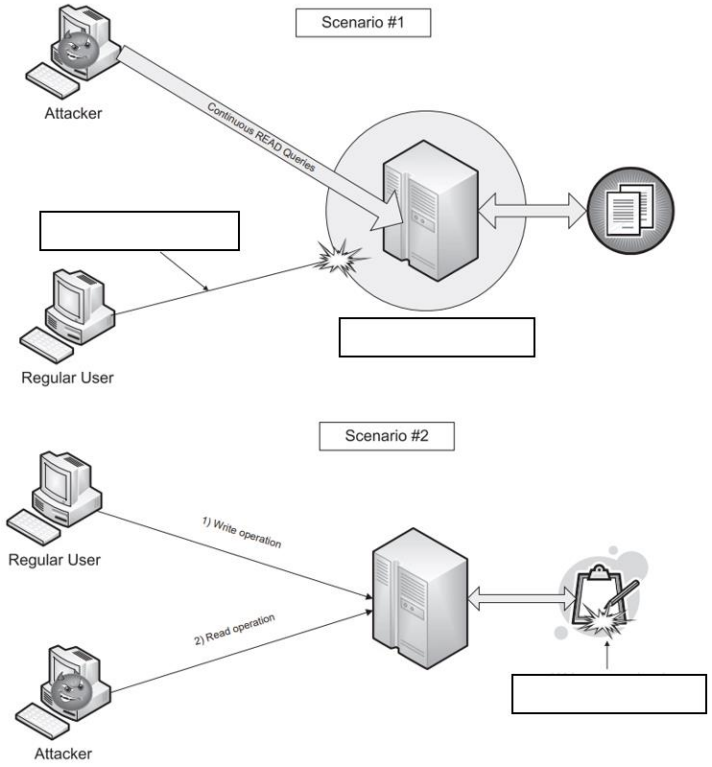
Full Name: _____ Gannon Identification Number: _____

Question 1. (Cont.)

Full Name: _____ Gannon Identification Number: _____

Question 2. (10 points) Complete the following items on **Hashing - Low Security**, **High Performance**, **To Optimize or Not to Optimize**, and **the KISS Principle**.

A. Mention the useful properties and consequences of using different classes of security algorithms.
B. Briefly explain the rules for optimization of security algorithms with provision of implementation/coding examples.
C. Explain the KISS principle with provision of a "computing" example.
D. The following figure shows "Inadvertent Read Behavior that Prevents a Write from Happening". Fill out the empty boxes.



Full Name: _____ Gannon Identification Number: _____

Question 2. (Cont.)

Full Name: _____ Gannon Identification Number: _____

Question 3. (10 points) Complete the following items on **Standardized Security in Practice, SSL Under the Hood,** and **Web-Based Interfaces**.

A. Discuss the basic protocol that the Web is built upon and the language it uses.
B. Explain the man-in-the-middle attack using a figure for the communication between a server and an embedded system.
C. Describe simultaneous generation of keys on client and server using a figure.
D – *Option 1*. Show the SSL record and explain the SSL handshake processes using figures.
D – *Option 2*. Briefly describe the computations of DES, RC4, AES, and RSA algorithms.

Full Name: _____ Gannon Identification Number: _____

Question 3. (Cont.)