Full Name: _____ Gannon Identification Number: _____

CYENG 225: Microcontroller Essentials for Cyber Applications
Spring 2023, First Examination
Gannon University (GU)
February 23, 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 **2:10 PM**.
- There are **30 points** total, distributed **evenly** among **3** questions.

Question	Maximum	Earned
1	10	
2	10	
3	10	

Advice:

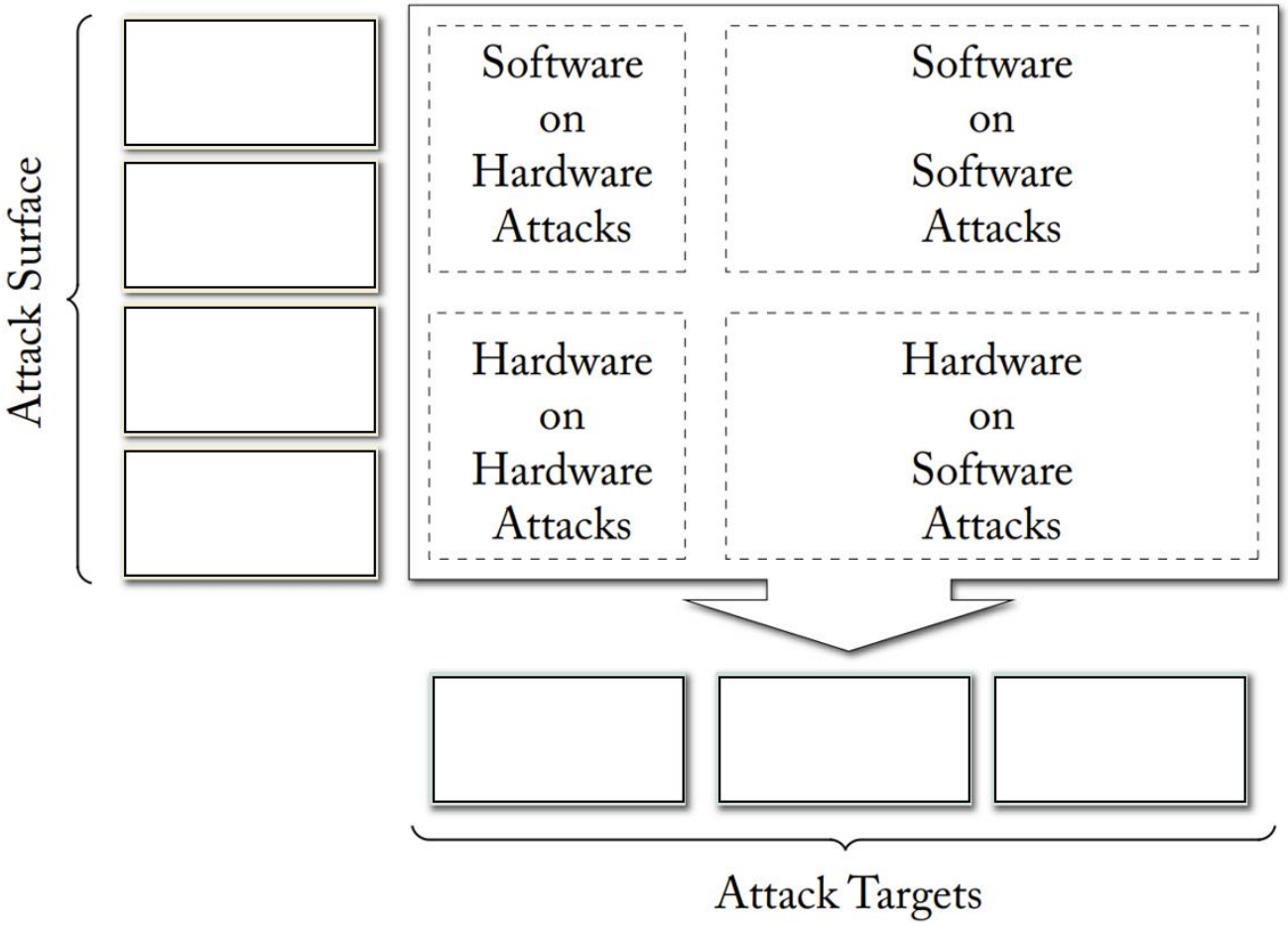
- Read questions carefully. Understand a question before you start writing your answer.
- Write down thoughts and intermediate steps so you can get partial credit. Clearly circle your final answer.
- The questions are not necessarily in order of difficulty. **Skip around.** Make sure you get to all the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

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

Full Name: _____ Gannon Identification Number: _____

Question 1. (10 points) Complete the following items.

A. Explain the terms, "**Attack Surface**" and "**Attack Targets**" according to the terminology of Computer Security.
B. Specify the relationship between the Attack Surface and the Attack Targets.
C. Fill out the empty boxes in the following figure.
D. Discuss how **information flows** can cause security threats.
E. Mention the threats to hardware after the design phase.



Full Name: _____ Gannon Identification Number: _____

Question 1. (Cont.)

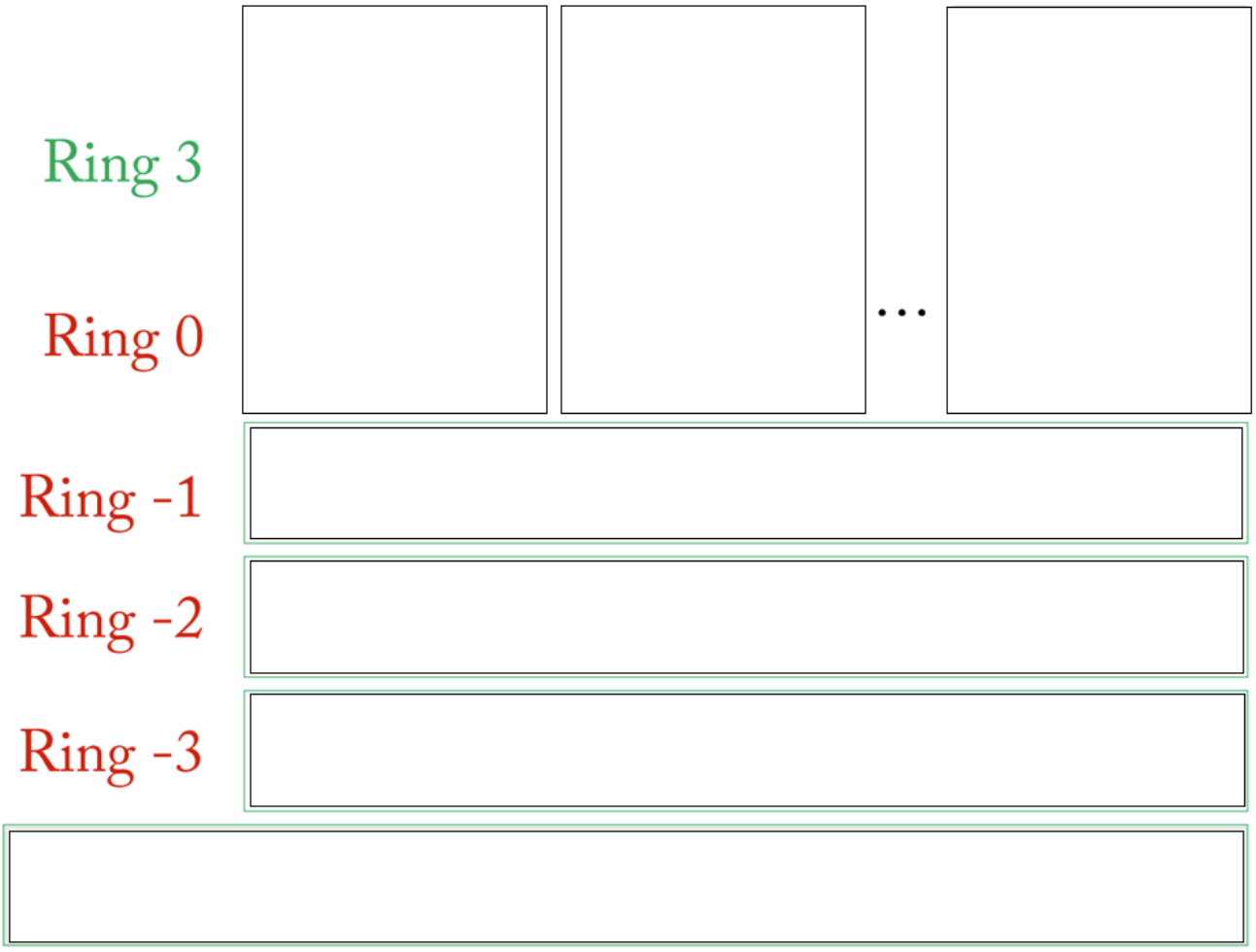
Full Name: _____ Gannon Identification Number: _____

Question 2. (10 points) Explain the computations and the applications/usages of **Secure Hashes**. Mention their main properties. Draw a hash tree and specify its usage.

Full Name: _____ Gannon Identification Number: _____

Question 3. (10 points) Complete the following items.

A. Mention **four real world attacks** on modern processors and explain their computations.
B. Explain whether there is (are) any relationship(s) between the **hardware design parameters** with provision of examples.
C. Discuss the meaning and the usage of the term, "**Ring**" in computer security. Fill out the empty boxes in the following figure. Add one component on top of the "Ring 3" and one component below the "Ring -3" (before the larger box) with their descriptions. Explain how the ring index for one component can be changed to a higher or a lower value.



Full Name: _____ Gannon Identification Number: _____

Question 3. (Cont.)