CYENG 225 – SP 23: Microcontroller Essentials for Cyber Applications
Instructor: Dr. Shayan (Sean) Taheri
Gannon University (GU)

Assignment 3: Chapter 3 - Secure Processor Architectures

Total Points: 100**; and Deadline:** February/23/2023, 11:59 PM.

Note – Cheating and Plagiarism: Cheating and plagiarism are not permitted in any form and they cause certain penalties. The instructor reserves the right to fail culprits.

Deliverable: All of your responses to the questions of assignment should be included in a single compressed file to be uploaded to the Gannon University (GU) – Blackboard Learn environment.

Question. Provide short answers (i.e., no more than five lines on average with the font size of 12) for the following items. The grade for each item is **10 points**.

1. Discuss the similarities and the differences between the general-purpose processor architectures and secure processor architectures based on the privilege levels.
2. Mention multiple examples for different types of secure processor architectures.
3. Specify three assumptions as well as three limitations for secure processor architectures.
4. Discuss major real-world attacks on processor architectures.
5. Explain why and how homomorphic encryption algorithms are used to protect computing systems.

Question 2. Complete the laboratory part, titled "**EXPERIMENT #1: Introduction to Xilinx's FPGA Vivado HLx Software**" in the "**UCF-EEE3342LabManual.pdf**" file using your "**Nexys A7 FPGA Board**" to be received from the **GU – ECE Department**. The grade for this question is **50 points**. Provide a report that includes: (1) your overall understanding of the experiments; (B) the interesting points and the challenges that you faced in this laboratory; and (C) the screenshots for all of the major steps/processes in your experiments.