Instructor: Dr. Shayan (Sean) Taheri
Office: Zurn 304
Office Hours: Fridays, 10:45 AM – 12:15 AM, or by Appointment: Please email your inquiries beforehand.
Email Address: taheri001@gannon.edu
Phone Number: +1 814-871-5331
Class Location: IHK 206
Class Time: Tuesdays and Thursdays, 9:30 AM – 10:50 AM
Final Exam Date and Time: May/04/2023, 8:30 AM – 10:30 AM
University Profile: www.gannon.edu/FacultyProfiles.aspx?profile=taheri001

CYENG 225: Microcontroller Essentials for Cyber Applications
Spring 2023

Course Description:
This course is to provide a deeper understanding of secured IoT end-point architecture of microcontrollers (uC) by exploring various microprocessor (uP) and uC hardware cyber architectures, their relationship to software architectures, various IoT cyber forensics techniques and challenges, and understanding the performance metrics of uP and uC IoT devices. The various techniques used for debugging these devices during development support this exploration. This becomes the knowledge base for students to evaluate which uC to use for IoT applications.

Credit Hours: 3

Prerequisite: ECE 245.

Course Outcomes:
1. Understand principles of computer security within the context of computer architecture and secure design of microprocessors and microcontrollers.
2. Comprehend secure processor architectures and associated elements, including trusted execution environments, hardware root of trust, memory protections, protections for multiprocessor and many-core, and protections for side-channel threats.
3. Design and security analysis of secure processor architecture.

Course Outline:
The lecture plan is according to the following. The subjects of each item are presented based on time availability.

Item	Lecture Topic	Duration
1	Chapter 1: Introduction	2 Sessions
2	Chapter 2: Basic Computer Security Concepts	3 Sessions
3	Chapter 3: Secure Processor Architectures	4 Sessions
4	Chapter 4: Trusted Execution Environments	3 Sessions
5	Chapter 5: Hardware Root of Trust	3 Sessions
6	Chapter 6: Memory Protections	3 Sessions
7	Chapter 7: Multiprocessor and Many-Core Protections	3 Sessions
8	Chapter 8: Side-Channel Threats and Protections	3 Sessions
9	Chapter 9: Security Verification of Processor Architectures	3 Sessions
10	Chapter 10: Principles of Secure Processor Architecture Design	3 Sessions

Course Assessment Methods:

Assessment Methods	Outcome 1	Outcome 2	Outcome 3
Assignments	X	X	X
Examinations	X	X	X

Course Assessment Method Details:

1. Assignments: They evaluate knowledge and comprehension of lecture topics. The assignment plan is according to the following.

Item	Assignment Topic
1	Chapter 1: Introduction
2	Chapter 2: Basic Computer Security Concepts
3	Chapter 3: Secure Processor Architectures
4	Chapter 4: Trusted Execution Environments
5	Chapter 5: Hardware Root of Trust
6	Chapter 6: Memory Protections

Note: The key assignments are shown in red color.

2. Examinations: The midterm and the final exams should contain problems based on the lectures and the assignments to assess the gained knowledge and skills.

Course Textbooks:

Zferer, J., 2018. **Principles of secure processor architecture design**, ser. Synthesis Lectures on Computer Architecture. Morgan & Claypool Publishers, 9048, pp.1-175.

Course Policies:

- Integrity: Cheating in any form will not be tolerated. Willfully misrepresenting your work in this class may result in an "F" grade for the course. Please refer to the *Gannon University Code of Academic Integrity*.
- Testing: The test procedure will be announced prior to the examinations. Anyone violating the testing procedure will be dropped from class.
- Submission: Assignments should be completed and submitted by the due date. **No late homework assignments will be accepted**.
- Attendance:
- Two unexcused absences will invoke the Early Alert and Referral System (EARS).
- Two more unexcused absences from class, after an EARS will result in a grade of **F.**
- Participation: Active participation in course class sessions/meetings is expected for all students. For each submitted assignment, students should be prepared to explain their solutions to the class.
- Individual Assignments: Students are allowed to discuss course topics and assignments with each other. However, duplicate assignments are not allowed. **All submissions must represent your own work.**

Grading Policy:

Course Outcomes Assessment Criteria: The course outcomes and the corresponding student outcomes are assessed by the construction of the **EAMU** vectors - Excellent (**E**), Adequate (**A**), Minimal (**M**), and Unsatisfactory (**U**). The construction of the EAMU vectors used for course assessment applies the following scoring in all cases and based on the **Accreditation Board for Engineering and Technology, Inc.** (**ABET**) criteria for accrediting engineering programs [Ref. 1]: **Excellent** (E) is scoring 90 or better of the total points possible, **Adequate** (A) is 75 or better, **Minimal** (M) is 60 or better, and **Unsatisfactory** (U) is anything below 60.

The **PI** is an abbreviation for **Performance Indicator** and **SO** is an abbreviation for **Student Outcomes** in the following:

1. Understand principles of computer security within the context of computer architecture and secure design of microprocessors and microcontrollers.

CYENG_ABET_PI_1_2 (CYENG_ABET_SO_1): Apply discrete mathematics techniques or cryptographic technique/algorithms to problem solving when appropriate.

***Key Assignment*:** Assignment 4 for "Chapter 4: Trusted Execution Environments".
Justification: Assignment 4 includes applying a cryptographic technique/algorithm, Advanced Encryption Standard (AES) to problem solving bases on provision of a Trusted Execution Environment by a Trusted Computing Base (TCB). Using AES helps in rendering of a secure processor architecture in which communicating data are protected from adversaries.

The students get hands-on experience and gain practical skills through realizing AES in a computer architecture simulator, gem5 as well as an embedded system, FPGA educational board. They also need to study the security aspects of this cryptographic system using their own attack models in their simulations. All of these items together are suitable indicators to gauge student performance for **PI_1_2**.

2. Comprehend secure processor architectures and associated elements, including trusted execution environments, hardware root of trust, memory protections, protections for multiprocessor and many-core, and protections for side-channel threats.

CYENG_ABET_PI_1_4 (CYENG_ABET_SO_1): Select and implement the desirable solution and evaluate the results.

***Key Assignment*:** Assignment 5 for "Chapter 5: Hardware Root of Trust".
Justification: Assignment 5 includes selecting and implementing physical unclonable function (PUF) defensive solutions and evaluate the results. The students are required to implement three PUF circuits using Verilog hardware description language, which they provide fingerprints that serve as unique identifiers for security operations. They also need to evaluate the hardware implementation results based on the hardware design parameters. All of these items together are suitable indicators to gauge student performance for **PI_1_4**.

3. Design and security analysis of secure processor architecture.

- **CYENG_ABET_PI_1_3 (CYENG_ABET_SO_1):** Identify security constraints on the design and develop technical specifications for acceptability of the solution.

***Key Assignment*:** Assignment 6, Steps B-E for "Chapter 6: Memory Protections".

Justification: Assignment 6, Steps B-E includes: identifying the security requirements of the memory hierarchy, especially for cache memory and main memory (i.e., random-access memory or RAM); assessing acceptability of secure hash algorithm (SHA) as a protective technology in satisfying the identified needs and being a solution for related security problems; determining the technical specifications according to your analysis and consider them in your hardware implementation of cache memory, RAM, and SHA modules; and implementing the Cache Memory, the RAM, and the SHA modules using Verilog hardware description language (HDL). All of these items together are suitable indicators to gauge student performance for **PI_1_3**.

- **CYENG_ABET_PI_2_2 (CYENG_ABET_SO_2):** Apply protective technologies and forensic techniques as part of the engineering solution.

***Key Assignment*:** Assignment 6, Steps F-H for "Chapter 6: Memory Protections".

Justification: Assignment 6, Steps F-H includes applying SHA protective technology/technique for securing the memory modules through hardware connectivity; and conducting experiments to evaluate and test their operations, and analyze their functionalities and results. All of these items together are suitable indicators to gauge student performance for **PI_2_2**.

Grading:
The following is the overall grading for the class.
- Exams: 60%
- Assignments: 40%

Letter Grade	Percentage
A+	100-97
A	96-90
A-	89-88
B+	87-85
B	84-80
B-	79-78
C+	77-75

C	74-70
C-	69-67
D	66-60
F	59 or Below

Relationship of Objective Evidence to CYENG Performance Indicator, Student Outcome, and Course Outcome:

Performance Indicator Met (Student Outcome)	**Course Outcome**	**Objective Evidence**
CYENG_ABET_PI_1_2 (CYENG_ABET_SO_1): Apply discrete mathematics techniques or cryptographic technique/algorithms to problem solving when appropriate.	1	Assignment 4
CYENG_ABET_PI_1_3 (CYENG_ABET_SO_1): Identify security constraints on the design and develop technical specifications for acceptability of the solution.	3	Assignment 6, Steps B-E
CYENG_ABET_PI_1_4 (CYENG_ABET_SO_1): Select and implement the desirable solution and evaluate the results.	2	Assignment 5
CYENG_ABET_PI_2_2 (CYENG_ABET_SO_2): Apply protective technologies and forensic techniques as part of the engineering solution.	3	Assignment 6, Steps F-H

Contribution to Professional Component:
The course contributions are: (1) getting demonstrable knowledge and skills on design and security verification of different types of processors; (2) becoming capable of identifying security vulnerabilities of microprocessors and microcontrollers; (3) acquiring experience in design, implementation, and analysis of attacks and defenses within the scopes of computer architecture and processor design; and (4) Gaining expertise in overcoming limitations and exploring opportunities in secure design of microprocessors and microcontrollers for cyber applications.

Accessibility Support Services:
The University will make reasonable accommodations for students with disabilities in compliance with Section 504 of the Rehabilitation Act and the Americans with Disabilities Act. The purpose of accommodations is to provide equal access to educational opportunities for eligible students with academic and/or physical disabilities. Gannon students who require accommodations due to a documented diagnosed physical, emotional or learning disability should contact Gannon's Office of Disability Services at extension 5522 or find more information at: https://mygannon.edu/studentresources/studentsuccesscenter/disabilitysupportservices/Page/default.aspx

Prepared by:
Dr. Shayan (Sean) Taheri, Department of Electrical and Cyber Engineering (ECE), Gannon University (GU), Erie, Pennsylvania

Date: Spring 2023