Instructor: Dr. Shayan (Sean) Taheri
Office: Zurn 304
Office Hours: Fridays, 9:00 AM – 10:30 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: Mondays and Wednesdays, 1:25 PM – 2:45 PM
Final Exam Date and Time: May/01/2023, 4:00 PM – 6:00 PM
University Profile: www.gannon.edu/FacultyProfiles.aspx?profile=taheri001

CYENG 351 (GECE 594): Embedded Secure Networking
Spring 2023

Course Description:
This course is a hands-on approach to implement various embedded systems communication techniques. The student will have a hands-on approach of understanding basic communication used by embedded systems supported by limited real-time operating systems. Discussions and applications on limitations, constraints, and how to secure applied network strategies.

Credit Hours: 3

Prerequisite: CYENG 312.

Course Outcomes:
1. Understand principles of computer security within the context of embedded networks.
2. Comprehend network communications protocols, built-in security, security protocols and algorithms, secure sockets layer, wireless system, application-layer and client/server protocols.
3. Security analysis and enhancement of embedded networks at software- and hardware-level.

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: Computer Security Introduction and Review	3 Sessions
2	Chapter 2: Network Communications Protocols and Built-in Security	3 Sessions
3	Chapter 3: Security Protocols and Algorithms	3 Sessions
4	Chapter 4: The Secure Sockets Layer	3 Sessions
5	Chapter 5: Embedded Security	5 Sessions
6	Chapter 6: Wireless	2 Sessions
7	Chapter 7: Application-Layer and Client/Server Protocols	4 Sessions
8	Chapter 8: Choosing and Optimizing Cryptographic Algorithms for Resource-Constrained Systems	3 Sessions
9	Chapter 9: Hardware-Based Security	2 Sessions
10	Chapter 10: Conclusion—Miscellaneous Security Issues and the Future of Embedded Applications Security	2 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: Computer Security Introduction and Review
2	Chapter 2: Network Communications Protocols and Built-in Security
3	Chapter 3: Security Protocols and Algorithms
4	Chapter 4: The Secure Sockets Layer
5	Chapter 5: Embedded Security
6	Chapter 6: Wireless

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:

Stapko, T., 2011. **Practical embedded security: building secure resource-constrained systems**. Elsevier.

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: **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 embedded networks.

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

***Key Assignment*:** Assignment 4 for "Chapter 4: The Secure Sockets Layer".
Justification: Assignment 4 includes selection and implementation of the operations of the Domain Name System (DNS) security solution and evaluation of their results. The students learn the hierarchical and distributed naming system of the DNS for computers, services, and other resources in the Internet or other Internet Protocol (IP) networks. They also understand the translation process of hostnames to IP addresses by this security solution for embedded secure networking.

The students employ "nslookup" operation that allows the host running this operation to invoke the underlying DNS services to implement its functionality and query any specified DNS server for a DNS record. They also need to investigate the content of the DNS resolver cache along with analyzing and tracing the DNS messages. All of these items together are suitable indicators to gauge student performance for **PI_1_4**.

2. Comprehend network communications protocols, built-in security, security protocols and algorithms, secure sockets layer, wireless system, application-layer and client/server protocols.

CYENG_ABET_PI_1_1 (CYENG_ABET_SO_1): Apply probability and statistics to problem solving in Cyber Engineering.

***Key Assignment*:** Assignment 5 for "Chapter 5: Embedded Security".
Justification: Assignment 5 includes applying statistics to problem solving in Embedded Network Security according to which the students are required to perform certain statistical analyses on the input data and the output data of their hardware-software implementation (i.e., in Verilog HDL and C++ language respectively) of the Advanced Encryption Standard (AES) algorithm to analyze its security strength and encryption performance. They are guided to execute their statistical analyses in either MATLAB or Python scripting languages. All of these items together are suitable indicators to gauge student performance for **PI_1_1**.

3. Security analysis and enhancement of embedded networks at software- and hardware-level.

CYENG_ABET_PI_6_2 (CYENG_ABET_SO_6): Conduct experiments, detect faults, troubleshoot, and perform measurements for analysis.

***Key Assignment*:** Assignment 6 for "Chapter 6: Wireless".
Justification: Assignment 6 includes implementing universal asynchronous receiver-transmitter (UART) and serial peripheral interface (SPI) networking modules, conducting experiments to evaluate and test their hardware operations, and analyzing their functionalities and results. All of these items together are suitable indicators to gauge student performance for **PI_6_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_1 (CYENG_ABET_SO_1): Apply probability and statistics to problem solving in Cyber Engineering.	2	Assignment 5
CYENG_ABET_PI_1_4 (CYENG_ABET_SO_1): Select and implement the desirable solution and evaluate the results.	1	Assignment 4
CYENG_ABET_PI_6_2 (CYENG_ABET_SO_6): Conduct experiments, detect faults, troubleshoot, and perform measurements for analysis.	3	Assignment 6

Contribution to Professional Component:
The course contributions are: (1) getting demonstrable knowledge and skills on design, testing, and security verification of different types of embedded networks; (2) becoming capable of identifying external and internal security vulnerabilities of embedded systems and their associated networks; (3) acquiring experience in design, implementation, and analysis of attacks and defenses for different networking architectures; and (4) Gaining expertise in overcoming limitations and exploring opportunities in security aspects of embedded networks.

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