Gannon University (GU) Course Syllabus **Department of Electrical and Cyber Engineering (ECE)**

Instructor: Dr. Shayan (Sean) Taheri
Office: Zurn 304
Office Hours: Thursdays, 2:00 PM – 3:00 PM, or by Appointment: Please email your inquiries beforehand.
Email Address: taheri001@gannon.edu
Phone Number: +1 814-871-5331
Class Location: IHK 206
Time: Tuesdays and Thursdays, 9:30 AM – 10:50 AM
University Profile: www.gannon.edu/FacultyProfiles.aspx?profile=taheri001

CYENG 312: Trusted Operating System (OS)
Fall 2022

Course Description:
This course covers basic understanding and configuration for hardening and securing an embedded Linux operating system. Topics include boot-time configurations and forensics, user and directory hardening, application vulnerability minimization, and minimizing memory attacks. The course will focus on a common Linux distribution architecture, security modules, cryptography tools, and how the system works. The student will experience securing the system, applying tools and secured applications as a user and administrator.

Credit Hours: 3
Pre-requisite: CIS 219 (Linux Programming) or Approval of the ECE Chair.

Course Outcomes:
1. Comprehend the fundamental concepts of security and trustworthiness of operating systems.
2. Comprehend the essential theories of SELinux and AppArmor.
3. Comprehend the theoretical and the practical aspects of cryptographic algorithms.
4. Comprehend principles of computer forensic within the context of operating system.

Course Outline:

Item	Topic	Duration
1	Introduction to Basic OS functions • Boot • Task/Application Management • File Management • User Management	3 weeks
2	Secure OS Introduction • Introduction and motivation • SELinux and AppArmor • Securing User Accounts • Encrypting and SSH Hardening	3 weeks
3	Access Control • Discretionary • Control Lists & Directory Managment • Mandatory Access SELinux / AppArmor	4 weeks
4	Forensics • Auditing • Scanning • Detecting • Hardening • Intro to Bootloaders, BIOS, and UEFI	4 weeks

Course Assessment Methods:

Assessment Methods	Outcome 1	Outcome 2	Outcome 3	Outcome 4
Assignments	X		X	
Examinations	X	X	X	X

Course Assessment Method Details:

1. Assignment: Assignment problems shall be designed to test knowledge and comprehension of a secured Linux OS. The expected experiments are according to the following:

- Assignment 1: Fundamentals of Operating Systems and Cybersecurity.
- Assignment 2: Analysis of Management and Security Computations in Operating Systems.

2. Examination: The exam shall contain problems designed to test knowledge and comprehension, the Linux user-level architecture, commands, and IPC.

- Midterm Exam: (a) Introduction to Operating Systems Cybersecurity, and Law Enforcement; (b) Booting and Management Systems; (c) SELinux and AppArmor; and (d) Cryptography.
- Final Exam: (a) User Authentication (Securing User Accounts); (b) Cryptography; and (c) Computer Forensics.

Course Textbooks:

Mastering Linux Security and Hardening, Donald Tevault, Packt, ISBN 978-1-78862-030-7.

Supporting Materials and Tools:

1. *SELinux by Example,* by Frank Mayer, Prentice Hall, ISBN 0-13-196369-4.
2. Centos & RHEL Linux SELinux online material.

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: Homework assignments are due before the class time of the due date. **Late homework assignments are penalized 20% plus 5% for each day late.**
- Attendance:
- Two unexcused absences or late homework assignments 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 meetings is expected of all students. With each submitted assignment, students should be prepared to explain their solutions to the class.
- Individual Assignments: Students are encouraged to discuss course topics and homework 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. Comprehend the fundamental concepts of security and trustworthiness of operating systems.

CYENG_ABET_SO_2: An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.

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

Key Assignment**:** Assignment 2.
Justification: Assignment 2 includes: (1) guiding them on proper understanding and applying of a computing process scheduling/handling algorithm, a common attack on operating systems, and two security algorithms to protect OSes; and (2) strengthening their practical and programming skills through implementation and analysis of the mentioned cases in (1). All of these items together satisfy the requirements of **CYENG_ ABET_SO_2**.

2. Comprehend the essential theories of SELinux and AppArmor.

CYENG_ABET_SO_2: An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.

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

Key Assignment**:** Midterm Exam – Question 3.
Justification: Midterm Exam – Question 3 includes evaluating the theoretical and the analytical understanding of the students on securing Unix-based operating systems using two major Linux Security Modules. The item satisfies the requirements of **CYENG_ ABET_SO_2**.

3. Comprehend the theoretical and the practical aspects of cryptographic algorithms.

CYENG_ABET_SO_1: An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science and mathematics.

- **CYENG_ABET_PI_1_2:** Apply discrete mathematics techniques or cryptographic technique/algorithms to problem solving when appropriate.

Key Assignment**:** Assignment 1.
Justification: Assignment 1 includes: (1) enhancing their knowledge on the emerging topics on security and trustworthiness of operating systems; (2) helping them to well understand computations and applications of a resource allocation and deadlock avoidance algorithm, a synchronization algorithm, a file allocation algorithm, a scheduling algorithm, a resource allocation algorithm for thread computing, and three cryptographic algorithms; and (3) improving their practical and programming skills through implementation of the resource allocation and deadlock avoidance algorithm and an advanced cryptographic algorithm. All of these items together satisfy the requirements of **CYENG_ ABET_SO_1**.

4. Comprehend principles of computer forensic within the context of operating system.

CYENG_ABET_SO_2: An ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors.

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

Key Assignment**:** Final Exam – Question 3.
Justification: Final Exam – Question 3 includes evaluating the theoretical and the analytical understanding of the students on the processes in computer forensic based on a systematic format. The item satisfies the requirements of **CYENG_ ABET_SO_2**.

Grading:

The following is the overall grading for the class.

- Exams: 70%
- Assignments: 30%

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: Apply discrete mathematics techniques or cryptographic technique/algorithms to problem solving when appropriate (**CYENG_ ABET_SO_1**).	3	Assignment 1
CYENG_ABET_PI_2_2: Apply protective technologies and forensic techniques as part of the engineering solution (**CYENG_ ABET_SO_2**).	1, 2, 4	Assignment 2, Midterm Exam – Q. 3, Final Exam – Q. 3

Contribution to Professional Component:

Securing operating systems, specifically the ones used in embedded systems is like managing shifting sands. Understanding the basic approaches/techniques to Detect, Protect, and React in the OS around the Linux Kernel is key to a business and product. New versions of the open-source operating systems like Linux are a challenge to a product and to still maintain the time domain of the applications, this course can only introduce the security constraints to a system, the rest is left to design out, limit or control the access points.

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: Fall 2022