ECE4115 Course Syllabus

ECE4115

Introduction to Computer Security (3-0-3-4)

CMPE Degree
This course is Elective for the CMPE degree.

EE Degree
This course is Elective for the EE degree.

Lab Hours
0 supervised lab hours and 3 unsupervised lab hours

Prerequisites
ECE 3076 OR ECE 4110 OR ECE 3600 OR CS 3251

Corequisites
None

Catalog Description
Introductory topics in computer security are presented with an emphasis on fundamental security primitives and current security challenges facing society.

Textbook(s)
Matt Bishop, *Computer Security: Art and Science* (2nd edition), 2018. (required)

William Stallings, Lawrie Brown, *Computer Security Principle and Practice* (4th edition), Pearson, 2017. ISBN 9780134794105 (required)

Course Outcomes
Upon successful completion of this course, students should be able to:
1. Describe why system and networks are vulnerable to attacks
2. Describe various methods for defending and detecting system and network attacks
3. Describe the practical challenges with implementing and defending against system and network attacks,
4. Utilize hardware- and software-based networking and system analysis to assess the risk to systems and the benefits of specific defensive techniques

Student Outcomes
In the parentheses for each Student Outcome:
"P" for primary indicates the outcome is a major focus of the entire course.
"M" for moderate indicates the outcome is the focus of at least one component of the course, but not majority of course material.
"LN" for "little to none" indicates that the course does not contribute significantly to this outcome.
1. (M) An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics

2. (M) 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
3. (LN) An ability to communicate effectively with a range of audiences
4. (P) An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
5. (LN) An ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives
6. (LN) An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions
7. (M) An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.

Topical Outline

```
Ethical Hacking
Introduction and Overview
Fundamental Concepts
Network Security Concepts
Attacks at Multiple Layers and Countermeasures
Denial-of-Service Attacks
Firewalls
Intrusion Detection
Wireless Networking Concepts, Attacks, and Countermeasures
Network Security Concepts
Attacks at Multiple Layers and Countermeasures
Denial-of-Service Attacks
Firewalls
Intrusion Detection
Wireless Networking Concepts, Attacks, and Countermeasures
Network Security Concepts
Attacks at Multiple Layers and Countermeasures
Denial-of-Service Attacks
Firewalls
Intrusion Detection
Wireless Networking Concepts, Attacks, and Countermeasures
Operating Systems Concepts Overview
Process Security
Memory and Filesystem Security
Application Program Security
Operating Systems Concepts Overview
Process Security
Memory and Filesystem Security
Application Program Security
Insider Attacks
Computer Viruses
Malware Attacks
Privacy-Invasive Software
Countermeasures
Insider Attacks
Computer Viruses
Malware Attacks
```