Course Coordinator:

LCDR Matthew Rehberg, Maury Hall Room 247, rehberg@usna.edu, 3-6170.

Prerequisites:

SY110, Cyber Security I and either SP212 (General Physics II) or SP222 (Electricity and Magnetism I).

Course Objective:

The objective of EC310 is to continue educating each midshipman about cyber infrastructure and systems, inherent cyber vulnerabilities and threats, and appropriate defensive security procedures, thereby enabling them to make principled decisions regarding the potential benefits, consequences, and risks from a proposed use of an information system in today’s cyber warfare environment.

Textbooks:

EC310 Course Notes, version 2020.1. Readings, lectures, example problems, lab exercises and homework problems will be assigned from this text. This text is REQUIRED in class!!!

Course Website:  https://www.usna.edu/ECE/ec310/index.php.

Check the course website regularly for course updates. Your instructor may also use Blackboard and email to communicate information regarding the course.

Laptop and Calculator:

**Your issued laptop and issued calculator are REQUIRED for each class!** In the event of a calculator failure, manual calculation will be required. Sharing of calculators will not be permitted during examinations. Laptops will be used for coursework as directed by your instructor. When your instructor tells you to “stop using your laptops” you are expected to do so and give him/her your full attention.

Extra Instruction (EI) and Make-up:

MGSP is available and highly encouraged. The schedule will be announce via email and your instructor. If necessary, arrange additional EI directly with your instructor or Lab Tech.

Since this course continually builds upon material previously presented, it is crucial that you seek EI early and often, particularly if you have difficulty understanding the material.
Homework:

Homework is designed to reinforce your understanding of the concepts presented in lecture. Homework are assigned for each lesson and located at the end of each chapter. Some instructors may choose to assign homework via Blackboard. The best way to thoroughly learn the material is by doing all homework assignments. Due dates and acceptance of late work is at the discretion of your instructor.

Quiz Information:

Quizzes will be administered at the discretion of individual instructors. They may be closed or open-book, announced or unannounced. It is ECE Department policy that at least one quiz must be administered during the first and second marking periods.

Security Exercises:

Each chapter includes a security exercise (i.e., a lab session) where students will apply the principles and theories discussed during lecture. Security exercises may be worked individually or in small groups at the instructor’s discretion. Due dates for each exercise is at your instructors discretion.

Exam Information:

Two midterm exams and a final exam will be given. The midterm exams will be administered during the assigned AcReserve Week 50-minute X-period. The final exam is a 180-minute comprehensive exam. All exams will be closed book/closed notes. A calculator may be used for each exam. Additionally, one single-sided, handwritten 8 ½” by 11” note sheet may be used for the first midterm, two-sided for the second midterm, and three (sides) handwritten 8 ½” by 11” note sheets may be used for the final exam. These note sheets will be collected by your instructor and returned after the exams, except the final.

Discussion of the contents of the exam with other students prior to the solution posting on the course website is strictly forbidden and constitutes a violation of the Honor Concept.

You must inform your instructor in advance if you will miss an exam (e.g., due to movement orders, simultaneous exams scheduled, etc.). Arrangements for an alternative testing time must be made in advance and will not be entertained after the fact.

Example midterms are posted on the EC310 Course Website > Old Exams with the expectation that students practice taking the exams BEFORE reviewing the solutions. Solutions will be posted approximately one week prior to the exam. Example finals exams are NOT posted but additional practice problems are provided.

Grades:

<table>
<thead>
<tr>
<th></th>
<th>6-Week Grade</th>
<th>12-Week Grade</th>
<th>Final Course Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>SX/HW/Quizzes/Participation (*)</td>
<td>40%</td>
<td>35%</td>
<td>30%</td>
</tr>
<tr>
<td>Midterm 1 (the 6-week exam)</td>
<td>60%</td>
<td>30%</td>
<td>20%</td>
</tr>
<tr>
<td>Midterm 2 (the 11-week exam)</td>
<td></td>
<td>35%</td>
<td>20%</td>
</tr>
<tr>
<td>Final Exam</td>
<td></td>
<td></td>
<td>30%</td>
</tr>
</tbody>
</table>

* Note: Consult your individual instructor's course policy addendum to see how this 30% is distributed for your particular section.
Mandatory Cyber Lectures:

Two lectures will be scheduled during the semester organized by the Center for Cyber Security Studies. These lectures are intended to complement your learning experience by exposing you to real-world events, and have mandatory attendance. Schedules will be announced during the semester as they are subject to change.

Additionally, one Classified Cyber Operations Brief may be scheduled during your normal classroom time. More information will be provided as the event is finalized. Unfortunately, international students are not permitted to attend.

Section Leaders:

A section leader and an assistant section leader will be appointed by the instructor and will be responsible for taking attendance. At the start of class, the section leader will call the section to attention and report absentees. Calling "attention on deck" at the end of class or lab will be at the instructor's discretion. In the event that an instructor is more than ten minutes late for class, the section leader is to contact the ECE Main Office (3-6150) to report the absence. The section leader will then instruct the class to quietly study for the duration of the period and will deliver any assignments due for that period to the ECE Main Office (Maury Room 327).

Absences:

If you know you will miss a class, notify your instructor ahead of time. Being absent does not absolve you of your responsibility to complete all assigned work. Arranging for make-ups of exams, quizzes or security exercises is the responsibility of the student. All midshipmen are required to take the exams at the times prescribed by the Academic Dean.

This course is offered all six periods, Monday through Friday. If you miss, or expect to miss, a lecture or lab, consider attending an alternate class according to either the BLUE (MTWF) or GOLD (MWRF) schedules, available on the EC310 homepage.

Classroom Decorum:

Your individual instructor may allow you to drink beverages in the classroom provided that they are in closeable containers; however, no drinks are allowed in the lab benches area. No food or open-container drinks are allowed in the classroom – remember you are in an electrical laboratory. Sleeping is not allowed in class and it is disrespectful to the instructor - stand up if you find yourself drifting off.

Honor:

Honor is at the core of the Naval Academy. Your individual instructor, in their course policy supplement, will discuss the policy on collaboration that will apply for your section. You should not, under any circumstance, turn in someone else's work as your own. To avoid even the appearance of plagiarism, you should always give credit where credit is due.

All quizzes and examinations are to be done individually, and all work turned in must represent only your own individual effort. To receive or give help on a quiz or an exam is sufficient to earn a grade of F in the course, and will be handled as a violation of the Honor Concept.
Course Objectives:

The course objectives appear on pages iii of your text, and are repeated below.

Upon completing this course, you should be able to:

1. Describe in depth the principles, mechanisms, and technologies of information systems’ hardware and software in both computers and communications domains, and describe the development of typical exploits used against vulnerabilities in information systems.

2. Identify action that can be taken to protect information systems’ hardware and software in both computers and communications domains against potential exploits.

3. Trace the lifecycle of a program through development, compilation, and execution to explain the methodology and ramifications of exploiting a process.

4. Discuss steps that should be taken to prevent a process from being exploited.

5. Describe the fundamental networking technologies and design principles behind internetworking and how these can be exploited by malicious actors.

6. Discuss steps that should be taken to prevent networks from being exploited and identify who or what is responsible for performing these preventative actions and where or when they should be applied.

7. Describe, qualitatively and quantitatively, how underlying electromagnetic spectrum technology is implemented in wireless communication and electronic warfare systems.

8. Evaluate the security and robustness of communications systems by determining which characteristics allow a system to transmit sensitive information to an intended receiver across a noisy or vulnerable channel.

M. M. Rehberg
LCDR, USN