Course Policy Statement
USNA Department of Electrical & Computer Engineering

EC 312: Applications of Cyber Engineering for Systems Majors (2-2-3)
Spring AY 2017

Coordinator: LCDR James Shey (shey@usna.edu) Maury Rm. 354, Ext 3-6154

Website: http://www.usna.edu/EE/ec312 (The website provides the syllabus and other course resources, and will also be used for coursewide announcements.)

Course Survival Guides (Textbooks):
Course notes (posted for each lesson as hyperlinks off the course website)

Prerequisites: SI110 (Introduction to Cyber Security), ES202 (Principles of Mechatronics), and EE331 (Electrical Engineering I).

Course Purpose: EC312 is the second in a two-part series of cyber security courses, provided by the Electrical and Computer Engineering Department to give midshipmen the technical background necessary to understand the security ramifications of operating communications and networking equipment that they will encounter as commissioned officers. This version of Cyber 2 is specifically tailored for Systems Engineering Majors and the curriculum has been designed in conjunction with the Weapons and Systems Department, therefore it should be considered a majors course just as much as a core course.

**DISCLAIMER**: As a student in this class, you will be taught concepts and gain experience with tools that could be put to unethical uses. DON'T!!

This course is challenging but worthwhile. Getting behind is costly and should be avoided. Seek help from your instructor early if you are struggling!

Laptops: Your issued laptop is required for each class. You are encouraged to bring a mouse if it enhances your computing experience. The laptops should be used only for coursework, and when your instructor tells you to “close lids” or “stop using your laptops” you are expected to do so and provide your full attention.

Calculators: You should bring your calculator to class every day; only calculators approved for the Fundamentals of Engineering Exam (FE) may be used. (You should already have an FE-approved calculator from EE331; acceptable calculators are listed at: http://ncees.org/exams/calculator-policy/.) In the event of a calculator failure, manual calculation will be required.

Classroom Decorum: Students may drink beverages in the classroom provided that they are in closeable containers and are not taken to the lab benches. No food is allowed in the classroom. Sleeping is not allowed in class; stand up if you find yourself drifting off.

Homework: Homework is essential to your comprehension of the course material. A Problem Set (PS) will be assigned for each lesson and failure to complete all homework assignments to the satisfaction of your instructor may be grounds for course failure. Late work will be accepted at the discretion of your instructor.
Labs: Security Exercises (SXs) (i.e. labs) are designed to be completed in class and will primarily be performed on student laptop computers and at the lab stations. Reading SXs prior to class is required and will greatly increase your understanding of the learning objectives covered and minimize errors during execution. SXs may be worked individually or in groups at the instructor’s discretion. Each SX will be posted on the course website and your instructor will promulgate a due date.

Exams and quizzes: Two midterm exams and a final exam will be given. The midterm exams will be administered during the 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-sided, handwritten 8 ½” by 11” note sheets may be used for the exams as follows: one sheet for the first midterm, two sheets for the second midterm, and three sheets for the final exam. These note sheets will be collected by your instructor and returned after the exam. 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, having multiple exams scheduled at the same time, etc.). Arrangements for an alternative testing time must be made in advance and will not be entertained after the fact. Quizzes will be administered at the discretion of individual instructors. They may be closed or open-book, announced or unannounced.

Honor: Your individual instructor, in their course policy supplement, will discuss the policy on homework collaboration that will apply for your section. You should not under any circumstances turn in someone else’s work (homework or security exercise) as your own. In particular, since security exercises are designed to provide hands-on experience to augment and reinforce theoretical knowledge, each student should perform all required steps in the assignment statement (e.g. compiling code, taking voltage measurements, etc.) and should not just copy results from another student. To avoid even the appearance of plagiarism, you should always give credit where credit is due. If a student is uncertain with regards to the application of this policy in a particular circumstance, the student should seek clarification from the instructor.

All quizzes and examinations are to be completed individually, and all work turned in must represent only your own individual effort. To receive or give help on a quiz or an exam (from a student or any other unauthorized source) is a violation of the Honor Concept. When taking examinations, you are not permitted to use a calculator that has been programmed with any equations, notes, problem solutions or any other course information. Sharing of calculators is not permitted during exams.

Section Leader: The Section Leader will be appointed by the instructor and will be responsible for taking attendance during each class, in addition to any other duties assigned by the instructor. The Section Leader will call the section to attention and report by name the individuals that are absent at the beginning of each class, as well as calling the class to attention for dismissal at the end of the period. In the event the instructor is late for class (in excess of 10 minutes); the Section Leader will contact the ECE Dept. Office (x3-6150). Pending the arrival of someone to take charge of the class, the Section Leader will supervise the class in a study period, collect any assignments due for that period and deliver them to the ECE Dept. Office at the end of the period. Under no circumstances is the Section Leader to secure the class.
**Calculation of course grade.** Grades will be calculated as follows:

<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>Homework/Quizzes/Participation*</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
</tr>
<tr>
<td>Security Exercises</td>
<td>15%</td>
<td>15%</td>
<td>15%</td>
</tr>
<tr>
<td>Midterm 1 (the 6-week exam)</td>
<td>65%</td>
<td>30%</td>
<td>20%</td>
</tr>
<tr>
<td>Midterm 2 (the 11-week exam)</td>
<td>35%</td>
<td>35%</td>
<td>20%</td>
</tr>
<tr>
<td>Final Exam</td>
<td></td>
<td></td>
<td>25%</td>
</tr>
</tbody>
</table>

*Individual instructors will promulgate the breakdown for this category.

**Course Outcomes:** Upon completing this course, you should be able to:

1. (Host) Describe the basic operating characteristics of transistors and logic gates, and explain how they are used as the basis for digital computing and Cyber-Physical Systems.
2. (Host) Analyze basic software programs in C and assembly language, tracing the control flow and how data is manipulated and stored in main memory. Apply the principles of function calls to create a memory schematic depicting the development of the stack.
3. (Host) Identify the vulnerabilities in computer programming that give rise to buffer overflow attacks, design an attack to compromise data integrity, and describe techniques used for more sophisticated attacks. Describe methods for preventing buffer overflow attacks.
4. (Wireless) Express electromagnetic signals in their time and frequency domain representation, and use these concepts to analyze signal modulation and to design tuned circuits.
5. (Wireless) List antenna design parameters and use them to characterize different antenna types. Use the Friis Free Space equation and an understanding of environmental effects to predict the signal power at a given range in a wireless communication system.
6. (Wireless) Demonstrate the process of analog-to-digital conversion, and describe different techniques used in digital communication systems, to include multiplexing, digital modulation, and error correction. Apply this understanding of digital communications to determine bandwidth and transmission rates for various digital modulation schemes.
7. (Wireless) Identify the vulnerabilities in wireless communication systems, and describe how they can be exploited in electronic warfare. Describe methods for securing wireless communications by means of spread spectrum techniques.
8. (Network) Describe the fundamental concepts of networking, to include layer structure, encapsulation, and protocols. For the TCP/IP protocol, describe the structure of an IP address and trace the process for routing packets.
9. (Network) Describe the physical and data link attributes of the Controller Area Network (CAN) protocol. Utilize the CANopen application layer to implement a closed loop Cyber-Physical System. Identify and demonstrate vulnerabilities at each network layer.