1. EC312 Applications of Cyber Security- Systems Majors

2. 3 Credit Hours, 4 Contact Hours

3. Course coordinator: LCDR James Shey

4. Text book, title, author, and year:
    a. Principles of Electronic Communication Systems, 4th ed., Frenzel
    b. EC312 Notes, Department of Electrical and Computer Engineering, USNA
    c. VMware Workstation 12.5, or latest version
    d. Cyber2vm*.ova file, Linux-based Ubuntu OS VM, Technical Support Detachment (TSD), USNA
    e. XCTU Software

5. Specific course information
    a. The course begins with a brief review of the fundamentals of digital logic and transistors then transitions into cyber security, covering C programing though a buffer overflow. It then transitions to wireless covering communication topics such as A to D conversion, spectrum management, and communication schemes. The course ends with networking and covers basic TCP/IP connections before diving into CAN, with an in-depth look at it and vulnerabilities.
    b. Prerequisites: SI110 (Introduction to Cyber Security), ES202 (Principles of Mechatronics), and EE331 (Electrical Engineering I).
    c. Core Curriculum course, required for SCS majors.

6. Specific goals for the course
    a. (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.
    b. (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.
    c. (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.
    d. (Wireless) Express electromagnetic signals in their time and frequency domain representation, and use these concepts to analyze signal modulation and to design tuned circuits.
    e. (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.

f. (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.
g. (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.
h. (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.
i. (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.

7. Topics covered:

Part I: The Host

Transistors
Digital Logic
Number Systems
C Programs
Arrays and More C Functionality
Main Memory Mechanics
The Debugger
Intro to Pointers
User Defined Functions and Stack Mechanics
Buffer Overflow Intro
Privilege Management
A Real Buffer Overflow

Part II: Wireless

Transmission Media and RF Specturm
AM Modulation
Gain, Noise, and Filters
Tuned Circuits
Antenna Fundamentals
Antennas and Propagation
Analog to Digital and Digital to Analog
Bandwidth and Multiplexing
Digital Modulation
Electronic Warfare

- Spread Spectrum
- Error Detection/Correction
- Xbee

Part III: Intro to Networking
- The TCP/IP Model
- The Physical Layer
- Data Link Layer, LAN's and Ethernet
- The Network Layer and Internet Protocol
- CAN

Last Updated: 01 June 2018