CS4390/5390: Cyber-Security for Critical Operational Technology
Spring 2014 Syllabus

Instructor: Dr. Irbis Gallegos
Office: Burges Hall 303
Phone: 747-7629
email: irbisg@utep.edu
Office Hours: W 11:00-1:00 pm or by appt.

Class Time: MW 4:30-5:50 pm in PSIC 314
TA: TBA

Prerequisites: CS 2302 with a grade of C or better.

Text Book:
Tyson Macaulay and Bryan Singer, "Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI and SIS", CRC Press, 1st Ed. 2012.

Course Description:
This course focuses on the methodology to conduct cyber-security risk assessments for critical cyber and cyber-physical systems. Students will learn risk assessment methodology techniques to: identify, classify, and analyze cyber threats and vulnerabilities in cyber and cyber-physical systems, conduct criticality and impact analysis, and create risk mitigation plans. Also, students will learn how to design cyber-infrastructures to securely capture, process, and manage cyber-security data obtained from embedded systems deployed in industrial infrastructures, SCADA networks, and control systems.

Course Learning Outcomes:

Level 1: Knowledge and Comprehension
Level 1 outcomes are those in which the student has been exposed to the terms and concepts at a basic level and can supply basic definitions. The material has been presented only at a superficial level.

Upon successful completion of this course, students will be able to:
1a. Define operational technology (OT) components in the context of cyber-security.
1b. Identify and classify OT components such as Supervisory Control and Data Acquisition (SCADA), Remote Terminal Unit (RTU), Distributed Control System (DCS), Programmable Logic Controller (PLC), Human-Machine Interface (HMI), Telecommunications networks.
1c. Identify the main differences between OT and IT components and risk factors.
1d. List and describe cyber-security standards used by government agencies, critical sectors, and industry.
1e. Define concepts such as: impact, vulnerability, threats, and risk, in the context of cyber-security and operational technology.
1f. Describe the process to conduct collection and analysis of cyber-security data associated with operational technology.
1g. Understand the legal and ethical implications of cyber-security as applicable to operational technology.

Level 2: Application and Analysis

Level 2 outcomes are those in which the student can apply the material in familiar situations, e.g., can work a problem of familiar structure with minor changes in the details.

Upon successful completion of this course, students will be able to:

2a. Select a cyber-security standard and determine if a critical infrastructure is compliant with such standard.
2b. Quantify and categorize impact factors associated with operational technology assets.
2c. Identify and categorize cyber vulnerabilities in an operational technology asset.
2d. Understand the various types of vulnerabilities (Vulnerability Taxonomy), their underlying causes, and the ways in which they are exploited.
2e. Use industry standard tools to analyze software for security vulnerabilities.
2f. Use testing methodologies to build test cases that demonstrate the existence of vulnerabilities.
2g. Implement exploits for discovered vulnerabilities.
2h. Identify and categorize cyber threat sources associated with operational technology assets.
2i. Calculate the cyber threat likelihood associated with specific operational technology asset.
2j. Calculate the cyber risk associated with a specific operational technology asset.
2k. Collect cyber-security data from data repositories for operational technology assets.
2l. Conduct cyber-security vulnerability assessments on operational technology infrastructures.
2m. Conduct analytics on cyber-security data.
2n. Create risk mitigation plans applicable to specific vulnerability and threat profiles.

Level 3: Synthesis and Evaluation

Level 3 outcomes are those in which the students can apply the material in new situations. This is the highest level of mastery.

Upon successful completion of this course, students will be able to:

3a. Create vulnerability assessment reports for OT infrastructure.
3b. Design a data-intensive, cyber-security cyber-infrastructure to secure and monitor critical assets in an OT infrastructure.

Teams: I believe that the ability to work with other software developers is essential. Therefore, students will be required to work effectively in teams throughout the semester.

Examinations: Examinations are assumed to be closed book, close notes, in class, unless otherwise specified. Make-up examinations are not given. If you miss an examination for a legitimate reason (such as illness, death in the family, participation in a college sponsored activity), then the remaining examinations and homeworks will be counted extra to compensate for the missed work. If you miss an examination without a legitimate reason, a grade of 0 will be recorded for that examination. If you know you will be missing an exam date due to a college sponsored activity, you may arrange to take the exam in advance.

Grading Summary: Final grades in this course will be determined by the following sequence:

1. Reading Quizzes and Homework: 25%
2. Projects: 50%
3. Final Report: 20%

4. Final Presentation: 5%

The final grade in the course will nominally be assigned according to the scale A: 90-100 B: 80-89 C: 70-79 D: 60-69 F: 59 and below.

General policies:

Use of electronics in class: UTEP supports the use of technology for learning.

Laptops can be an asset to some students and help them in their note-taking and learning. Students will be allowed to use laptops in this class provided they follow the rules described below. Failure to follow these guidelines will result in suspension of laptop privileges in class.

- Charge your laptop batteries fully before coming to class.
- Set your laptop volume control to mute or off before coming to class.
- Keep your laptop closed during presentations and other specific in-class activities.
- Do not engage in unauthorized communication or entertainment (web surfing, instant messaging, chat room chatting, DVD viewing, music playing, game playing, etc.) during class unless it is part of the lesson.

Cell Phones are nearly universal in our modern culture. Under normal circumstances, however, you are expected to refrain from using cell phones during class time. Your cell phone should be set to silent mode or turned off before class. Under no circumstance will you be allowed to use text messaging (sending or receiving) or web browsing features of your phone while you are in class. In an emergency, there may be a genuine, rare need for you to use a cell phone during class time. In this case, you will excuse yourself from class and leave the classroom to answer an incoming call. You will not be permitted back into the classroom for the remainder of class. It is never permissable to place an outgoing call while you are in class.

Other Wireless Communications Devices are not allowed in class.

Grading errors: I am only human. I can and will make mistakes. You have one week after graded material is returned to the class to rectify any grading errors or to argue for additional credit. After the week has passed, no changes in grades will be made.

*Class Attendance and Participation***:** As a college student, you have the freedom to choose whether or not to attend class. However, in this course I am committed to cooperative techniques, which can only work if students attend regularly and on-time. Part of what we are encouraging in this course is the establishment of professional behavior. Therefore, we will take attendance. Your final grade will be lowered by one point for each unexcused absence above three. For the purposes of this class, you will be counted as absent if you are not present when we take attendance. If you feel that you must interact with people using cell phones, PDAs, Blackberries, email, twitter, chat, or any other electronic means, you are free to do so outside of class. If we find you doing these things in the classroom, we will ask you to leave, and to avoid disturbing the rest of your classmates, you should not return until the start of the next class.

Office hours: I expect you to meet with me outside of class time whenever you feel you need to further discuss the course material . You may contact me by office phone, in person, or email to arrange a suitable time to meet.

Let me make one more point here: I am available to *assist* you in solving problems, not to *think or do* work for you. Office meetings are for helping you by clarifying material and for assisting you with problems you are encountering. It is not for repeating things you missed when you skipped class. You should come to office appointments prepared. The harder you work at it, the harder I will work to help you.

Incomplete: Students receive a grade of Incomplete only under extraordinary circumstances: when they have substantially completed the course work with a passing grade, but cannot finish the course for a legitimate reason. Legitimate reasons include severe illnesses and debilitating accidents. Class or workloads that are too demanding are NOT legitimate reasons.

Lecture material: You are expected to preview lecture material BEFORE coming to class, including reading the assigned material from the text book. Some material may not be in the text: references will be provided, but you are responsible for the content.

Academic dishonesty: Cheating is defined as submitting work under your name that was not done entirely by you for individual assignments or by your team for team assignments. (This includes taking programs from the web or cutting text from web pages and pasting them into documents, even if the source is cited). Cheating will not be tolerated--those caught cheating will be reported to the Dean of Students. You should be aware of the Standards of Conduct posted at http://www.utep.edu/vpfa/student_affairs/student/studindex/htm.

Disabilities: If you have or suspect a disability and need accommodations, you should contact The Student Disabled Services Office (DSSO) at 747-5148. You can also email the office at dss@utep.edu or go by the Union Building East, Room 106. For additional information, visit the DSSO website at www.utep.edu/dsso/.

HELP: Please confer with me if you experience difficulty with any aspect of the course – I am here to help you to learn. If you request help via email, make sure to write HELP in the subject line. Call me. Send me mail. Ask me questions.

Important Dates

January 20:	Martin Luther King, Jr. day (university closed)
January 21:	Class begins
February 5:	Census day
March 10-14:	Spring break (no classes)
March 31:	Cesar Chavez day (no classes)
April 4:	Course drop deadline
May 9:	Dead day
May 12:	Final on Monday at 4:00 pm–6:45 pm

CS 4390/5390 Cybersecurity for Operational Technology Schedule (Spring 2014)

The following table shows a planned schedule for the course.

Dates		Topics	Readings	Project
Week 1	Jan. 22	- Intro to CS 4390/5390		
Week 2	Jan. 27, 29	- Software Engineering Code of Ethics - Industrial Control Systems Overview	ACM Code of Ethics Executive Order 13636 Chapter 1	Industry Description
Week 3	Feb. 3,5	- Industrial Control Systems Cybersecurity Requirements - Criticality Factor Analysis	To Kill a Centrifuge Handout	Impact Analysis
Week 4	Feb. 10, 12	- Impact Analysis - Vulnerability Taxonomy		
Week 5	Feb. 17, 19	- Vulnerability Assessment - Vulnerability Analysis	Chapter 3	Vulnerability Analyisis
Week 6	Feb. 24, 26	- Secure Software Development		PA1: ICS Simulation
Week 7	Mar. 3,5	- Threat Analysis	Chapter 2	
Week 8	Mar. 10, 12	Spring Break		
Week 9	Mar. 17, 19	- Risk Analysis	Chapter 4	Threat Analysis
Week 10	Mar. 24, 26	- Risk Standards	NIST 800-53 NIST 800-82 NIST Cyber Security Framework NERC- CIP	
Week 11	Mar. 31, Apr. 2	- Criticality/Vulnerability data analytics methodologies		Risk Analysis
Week 12	Apr. 7,9	- Threat/ Risk data analytics methodologies		
Week 13	Apr. 14, 16	- Cyber-security data analytics tools		PA2: Cyber-Security Analytics
Week 14	Apr. 21, 23	- Risk Mitigation		
Week 15	April 28,30	- Secure Cyberinfrastructure Design		
Week 16	May 5, 7	- Project Work		Presentation
Week 17	May 12	**Final** at 4:00 pm–6:45 pm		Report