CS 4390/5390: Special Topics in CS – Network Security for Cyber-Physical Systems

Instructor: Dr. Deepak K. Tosh
Classroom: Quin 206
Class Hours: TR 3-4:20PM
Office Hours: TR 1-2PM

A. Course Description:

This course aims to offer both fundamental and in-depth knowledge on network architectures, protocols, security standpoints of emerging cyber-physical systems (CPS), with special emphasis on critical infrastructure systems. The primary concepts to be covered in this course include Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, IT/OT architectures in ICS/SCADA, industrial network protocols, risk assessment and management principles, network security case studies, and regulatory compliance standards for CPS. The goal of this course is to expose students to various fundamental security primitives pertinent to cyber-physical systems and allow them to apply learned concepts to ensure resiliency in any generic cyber-physical systems context. Hands-on experiments to implement and test different industrial communication protocols and security solutions will leverage Raspberry PIs, sensor modules, and program logic controllers.

Prerequisites: Arch-1 (C or better), and CS 4375 (okay to be taking concurrently)

B. Course Objective and Learning Outcomes

The objective of this course is to develop practical skills and understanding about generic cyber-physical system architectures and study the security landscape of IT/OT networks of CPS to enable robustness and resiliency. This course will leverage various tools and techniques used by adversaries to compromise and harden the operational technologies of ICS/SCADA environment.

At the end of this course, the students will be able to

1. Interact with cyber-physical systems components
2. Identify and classify OT components along with the cyber-risks and potential threats.
3. Work with cyber-physical systems networking protocols
4. Understand taxonomy of vulnerabilities associated to ICS/SCADA
5. Assess and potentially measure the cyber-risks associated to ICS/SCADA systems
6. Analyze network-based attacks on cyber-physical systems protocols and systems
7. Design cyber-physical systems and architectures that are resilient to attack
8. Understand the legal and ethical implications of cybersecurity as applicable to operational technology

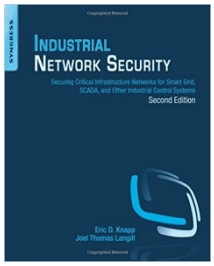
Why should you consider this course?

You may have heard of the recent infrastructure bill that promises to improve and modernize the critical national infrastructures including transportation, energy, water, manufacturing, and environment. The emergence of Internet of Things (IoT) and AI are the main driving forces behind this bill. Therefore, in the next decade or so, we are going to see drastic changes in the operational technologies behind these critical infrastructures. Through this course, you will gain the first-hand experience on how the critical infrastructure components are connected, how information flows, what protocols they leverage in communicating, how cybersecurity is crucial, what approaches can be followed to defend cyber breaches, Industry 4.0 related risks, and many more. These skills can make you very attractive to the job market. Also, there are a lot of research opportunities and national laboratories are looking for creative candidates with such skills.

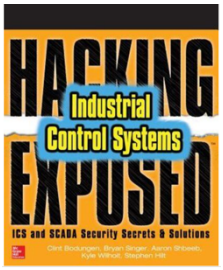
C. Course Outline (TENTATIVE):

1. Introduction to cyber physical systems
2. Review – Networking, information security, and Industry 4.0
3. Industrial Networks – architecture, standards, protocols
4. Cybersecurity in Industrial Networks – threats, history, trends
5. Overview of Industrial Control Systems and Operations
6. Industrial network design and communication protocols
7. Security principles for ICS/SCADA resiliency
8. Threats to other cyber-physical system domains
9. Policies, regulations, standardization efforts

D. Textbook and Materials:



Industrial Network Security, Second Edition: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems (2nd Edition), by Eric D. Knapp and Joel Thomas Langill



Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets and Solutions, by Kyle Wilhoit, Aaron Shbeeb, Bryan Singer, Stephen Hilt, Clint Bodungen, 2016

Note: UTEP library has access to electronic versions of the above two books.

- Other hardcopy handouts and links to reference materials will be provided as the topics get covered in class.

E. Grading (Tentative):

Your semester grade will be based on combinations of following items:

Grading Policy

- 20% - Research Paper presentations (bi-weekly)
- 35% - Semester Project (Midterm and final presentation)
- 30% - Hands-on assignments (bi-weekly)
- 15% - In-class discussions and Quiz (Weekly)

* Grading rubric for undergraduate students will be different from graduate students.

Important Note: You will have one week to appeal for your grades after the graded assignments/tests are returned. So, please keep this in mind if you think that there is a problem/issue with the grading of your work.

F. Standards of Conduct:

Students are expected to conduct themselves in a professional and courteous manner, as prescribed by the Standards of Conduct. Students may discuss work assignments and programming exercises in a general way with other students, but the solutions must be done independently. Similarly, groups may discuss group project assignments with other groups, but the solutions must be done by the group itself. Graded work should be unmistakably your own. You may not transcribe or copy a solution taken from another person, book, or other source, e.g., a web page. Professors are required to -- and will -- report academic dishonesty and any other violation of the Standards of Conduct to the Dean of Students.

G. 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.

H. Disabilities:

If you have a disability and need classroom accommodations, please contact The Center for Accommodations and Support Services (CASS) at 747-5148, or by email to **cass@utep.edu**, or visit their office located in UTEP Union East, Room 106. For additional information, please visit the CASS website at **www.sa.utep.edu/cass**.

I. Course Calendar (Tentative)

Weeks	Topic	Reading	Activities
1	Introduction of CPS w/ ICS Components	Ch 2; HE-Ch 1	
2	Networks/Security Primer	Kurose Ch-1; Hand-out provided	Assign-1 (networking practice)
3	Industrial Networks, Design, and ICS architecture	Ch 5	
4	Ladder logic, ICS operations and OT security	Ch 4; Hand-out provided	Assign-2 (ladder-logic)
5	Industrial network protocols - I	Ch 6	
6	Industrial network protocols - II	Ch 6	
7	**Midterm Presentation**		Assign-3 (Modbus)
8	Network induced risks, and ICS exploitation strategies	Ch 7, HE-Ch 4	
9	Hacking ICS	Ch 7, HE-Ch 5, 6	Assign-4 (DNP3)
10	Risk assessement	Ch 8 HE-Ch 2	
11	ICS Risk mitigation	Ch 9, 10, HE-Ch 10	Assign-5 (Risk assessment)
12	Situational awareness	Ch 11	
13	Security Standardization	Ch 13, HE-Ch 9	
14	**Final Presentation**		Project Report Due
15	**Final Presentation**		