CS 6308 Course Syllabus

COURSE INFORMATION:

Course Title: Cyber Physical Systems and Critical Infrastructure Security for Practitioners
Section: 501
Course Term: Spring 2024

INSTRUCTOR CONTACT INFORMATION:

Name: Brian Ricks
Office: ECSS 4.701
Email Address: bwr031000@utdallas.edu
Phone: (972) 883-2674

Communication: For course related questions, please email me from your UTD account with a subject that begins with: *CS6308.501*. There is also an MS Teams channel which can be used for general course questions / discussion. I will give course announcements on eLearning.

Office Hours: Tuesday: 11:00am – 12:30pm
Wednesday: 11:00am – 12:30pm

Meetings outside of office hours can be arranged by appointment.

TA CONTACT INFORMATION:

Savyasachi Kokkirala – savyasachi.kokkirala@utdallas.edu

COURSE PREREQUISITES AND COREQUISITES:

Prerequisite: N/A
Corequisite: N/A

This course may *not* be used to satisfy the degree requirements of the MS CS or the MS SE degree plans.

COURSE DESCRIPTION:

The Stuxnet attack was a wake-up call to improve the security of our critical infrastructures, which include transportation networks, the power grid, and other cyber-physical systems, where computation, communications, and control are tightly integrated. This class covers the security of cyber-physical systems from a multi-disciplinary point of view, from computer science security research (network security and software security), to public policy (e.g., the Executive Order 13636), risk-assessment, business drivers, and control-theoretic methods to reduce the cyber-risk to cyber-physical critical infrastructures. Students are required to participate in several cyber war games.

This course may *not* be used to satisfy degree requirements for the MS CS or the MS SE degree plans. (3-0) Y

COURSE MODALITY:

This course is scheduled to be taught in the traditional (in-person) mode.

Should it become necessary to meet online, meetings will be held in MS Teams in the appropriate lecture channel. Check the course announcements on eLearning and your UTD email for updates.

Online meetings will be recorded and posted in the course MS Teams channel.

REQUIRED TEXTBOOKS AND MATERIALS:

Required textbook: *Industrial Network Security, Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Knapp / Langill (2015 – second edition)
ISBN: 978-0-12-420114-9

Optional textbooks will be used throughout the course during lecture, and may be helpful for further study:

- *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*, Ackerman (2017)
- *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, Johnson (2015)

Additional academic papers will be announced/given on eLearning.

CLASS MATERIALS:

All course materials will be posted to eLearning, including lecture slides, assignments documentation, supplementary reading materials, etc.

TENTATIVE COURSE CALENDAR:

Date	Lecture Material	Chapter
January 17	Syllabus Review	
January 22	Critical infrastructure and ICS – Introduction	Chapter 2
January 24	Critical infrastructure and ICS – History	Chapter 3
January 29	ICS Assets and Operations	Chapter 4
January 31	ICS Architectures and Design Principles	Chapters 5 – 6
February 5	ICS Architectures and Design Principles	
February 7	ICS Protocols	
February 12	ICS Protocols	
February 14	Modbus TCP / Stuxnet	
February 19	Attacks on Industrial Control Systems	Chapter 7
February 21	Attacks on Industrial Control Systems	
February 26	ICS Exploitation – Task 1 Introduction / Environment Installation	
February 28	NAT / Exam #1 Review	
March 4	**Exam #1 – In class**	
March 6	Buffer Over-read Attacks / Heartbleed	
March 11	**No class – Spring Break**	
March 13	**No class – Spring Break**	
March 18	Risk and Vulnerability Assessments	Chapter 8
March 20	Risk and Vulnerability Assessments	
March 25	Risk and Vulnerability Assessments / ICS Exploitation – Task 2 Introduction	
March 27	Risk and Vulnerability Assessments	
April 1	Network Emulation	
April 3	Network Emulation Demo / Zones and Conduits	Chapter 9
April 8	Zones and Conduits	
April 10	Implementing Security and Access Controls	Chapter 10
April 15	Implementing Security and Access Controls	
April 17	Threat Detection and Monitoring	Chapters 11 – 12
April 22	Threat Detection and Monitoring	
April 24	Standards and Regulations / Exam #2 Review	Chapter 13
April 29	Insider Threats / Ashley Madison Breach	
May 1	**Exam #2 – In class**	

This calendar is tentative and may change as the semester progresses. Please check eLearning for updates to the calendar.

The Chapter column refers to relevant chapters in the primary textbook for the lecture topics. Additional relevant reading materials (optional textbook chapters, academic papers, etc) will be announced / posted on eLearning.

INSTRUCTOR POLICIES:

Grading Policy:
Your course average will be calculated as follows:

Exam #1 – 20%
Exam #2 – 25%
Assignments – 25%
ICS Exploitation – 30%

Exams:
Course exams will be administered in class and be given in an essay / short answer format.

Make-up exams will be administered *only for well-documented emergencies*, and you must make every attempt possible, via email, MS Teams private message, or phone, to notify the instructor *prior* to the scheduled date and time or *immediately thereafter*. If notification is not received in a timely manner, no make-up exam will be given.

ICS Exploitation:
These are two hands-on tasks involving real exploitation of an industrial control system. Students will work individually to exploit an ICS in a virtual environment to induce events that will ultimately blow up a boiler in a factory. Students will be required to install the ICS virtual environment on their laptops to complete these tasks. One day of class will be dedicated to installation of this environment.

Each task will require a write-up (or post-mortem) explaining the steps required to complete the task, and possible mitigation strategies.

MORE FROM UTD:

Class Materials

The instructor may provide class materials that will be made available to all students registered for this class as they are intended to supplement the classroom experience. These materials may be downloaded during the course, however, these materials are for registered students' use only. Classroom materials may not be reproduced or shared with those not in class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Classroom Conduct Requirements Related to Public Health Measures

UT Dallas will follow the public health and safety guidelines put forth by the Centers for Disease Control and Prevention (CDC), the Texas Department of State Health Services (DSHS), and local public health agencies that are in effect at that time during the Fall 2021 semester.

Class Attendance

The University's attendance policy requirement is that individual faculty set their course attendance requirements. Regular and punctual class attendance is expected. Students who fail to attend class regularly are inviting scholastic difficulty. In some courses, instructors may have special attendance requirements; these should be made known to students during the first week of classes.

Class Participation

Regular class participation is expected. Students who fail to participate in class regularly are inviting scholastic difficulty. A portion of the grade for this course is directly tied to your participation in this class. It also includes engaging in group or other activities during class that solicit your feedback on homework assignments, readings, or materials covered in the lectures (and/or labs). Class participation is documented by faculty. Successful participation is defined as consistently adhering to University requirements, as presented in this syllabus. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Class Recordings

Students are expected to follow appropriate University policies and maintain the security of passwords used to access recorded lectures. Unless the Office of Student AccessAbility has approved the student to record the instruction, students are expressly prohibited from recording any part of this course. Recordings may not be published, reproduced, or shared with those not in the class, or uploaded to other online environments except to implement an approved Office of Student AccessAbility accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

The instructor may record meetings of this course. These recordings will be made available to all students registered for this class if the intent is to supplement the classroom experience. If the instructor or a UTD school/department/office plans any other uses for the recordings, consent of the students identifiable in the recordings is required prior to such use unless an exception is allowed by law.

Comet Creed

This creed was voted on by the UT Dallas student body in 2014. It is a standard that Comets choose to live by and encourage others to do the same:

"As a Comet, I pledge honesty, integrity, and service in all that I do."

Academic Support Resources

The information contained in the following link lists the University's academic support resources for all students.

Please see http://go.utdallas.edu/academic-support-resources.

UT Dallas Syllabus Policies and Procedures

The information contained in the following link constitutes the University's policies and procedures segment of the course syllabus. Please review the catalog sections regarding the credit/no credit or pass/fail grading option and withdrawal from class.

Please go to http://go.utdallas.edu/syllabus-policies for these policies.

The descriptions and timelines contained in this syllabus are subject to change at the discretion of the Professor.