CSEC 366/466X: Critical Infrastructure and Control Systems Cybersecurity

Filipo Sharevski

Spring 2021

E-mail: fsharevs@cdm.depaul.edu
Office Hours: send me an email.
Web: www.divergentdesignlab.org
Discord: CSEC 366/466

Course Description

Course Description This course is an introduction to the cybersecurity challenges for control systems present in industry, homes and traditional businesses such as manufacturing. Topics covered include the design and setup of Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and Programmable Logic Controller (PLC) systems. As these systems are typically designed without any intrinsic security mechanism, we will study the challenges of protecting them and how to employ a defense-in-depth methodology to secure them. This class will focus on the security risks of critical infrastructure systems (such as Electrical, Pipelines, Water/Wastewater and transportation) and methods to protect them.

A Welcome Note

I am more interested in you having the right *attitude* than you coming with a *budget* for the class. "I will do this two hours on Sunday, and push comes to shove, I will email the professor, it is hard to work during pandemic." I understand that. I also understand that we live in a post-truth time. Most of you have taken a class with me or heard about me. You know I am here for every and each one of you. You'll never walk alone. Also, DePaul has ample resources for support. But you also know I will push you to do a heavy cybersecurity lifting. We have to deliver *in spite* of the pandemic. Because we are cybersecurity people. Viruses are our bread and butter. Right?

Learning Outcomes

Successful students after taking this class will be able to [1]:

- Analyze Critical Infrastructure and Control System security breaches and develop defensive measures;

- Employ best practices to create and implement policies for Critical Infrastructure and Control System protections;
- Model protection-in-depth for industrial control systems and IoT systems;
- Perform Critical Infrastructure and Control System risk assessment;
- Evaluate Critical Infrastructure and Control System breaches and defenses in the context of cyberwarfare.

Course Structure

Assignments

Week	Module	Assignment	Weight
1	Concepts and Principles	Homework 1	5%
2	Security Breaches and Defenses	Homework 2	5%
3	ICS/SCADA Security [Part 1]	Lab 1 and 2	10%
4	ICS/SCADA Security [Part 2]	Lab 3 and 4	10%
5	ICS/SCADA Security [Part 3]	Lab 5 and 6	10%
6	IoT Security	Homework 3	5%
7	Legal and Privacy Aspects	Homework 4	5%
8	Risk Assessment	Homework 5	5%
9	Cyberwarfare	Homework 6	5%
10	Presentations	Presentations	5%
11	Final Project		35%

Schedule and weekly learning goals

The schedule is tentative and subject to change. I have interesting recordings that capture an interesting combination of lecture, the context of the zeitgeist, and my personal opinions Panopto. Yes, they have another slide title on them, of course, because the any critical infrastructure and control system is essentially a cyber-physical system. Some weeks will have hands-on activities. They earn you no points, but they greatly help you to develop the necessary approach for securing critical infrastructure and control systems. Some weeks you will have to do hands-on labs using this Virtual Machine. For your final project, you will have to work on solving several, if not all, unsolved challenges in the IoT Goat project. Or perhaps do an exploration of the KITT and the HomePwn frameworks to demonstrate your *individual* pen-test skills.

Given that you have the lectures pre-recorded and available on Panopto link in D2L, we will meet only on Tuesday on Zoom to discuss any questions you have and track progress in the class. I will upload the recordings once we are done in D2L news announcement section.

In addition to the requirements and expectations described elsewhere in this syllabus, you are required to attend three on-campus sessions:

- Saturday April 17, 2021, 9:00 – 10:30 am
- Saturday May 8, 2021, 9:00 – 10:30 am
- Saturday May 22, 2021, 9:00 – 10:30 am

The exact location of these sessions will be listed in Campus Connect at the start of the Winter quarter. Attendance to these sessions counts for 10% of your final grade.

Week 01: Concepts and Principles

- **Overview:** Concepts and principles of Critical Infrastructure and and Control Systems Security: confidentiality, integrity, availability, non-reputation, veracity, and plausibility. Impacts of cyber-physical attacks. Comparison between ICT and CPS with respect to requirements for performance, reliability and risk management; system operation;
- **Hands-on Activity:** Choose one of the options in the first Hands-on Activity; Download the Excel Spreadsheet; Complete it by yourself; submit it in the homework 1 Folder.
- **Homework:** Read and review the following article [2]. That means that you have to read and write about your take, opinions, critiques, or grievances instead of summarizing your reading notes with the lazy "The authors said...." How to access the article? DePaul has a full article access to the ScienceDirect library.

Week 02: Security Breaches and Defenses

- **Overview:** Known security incidents in cyber physical systems: smart grids, ICS/SCADA systems, IoT Systems. Defenses for breaches and incidents in Cyber Physical Systems
- **Hands-on Activity:** Choose one of the hacks in the second Hands-on Activity; Download the Excel Spreadsheet; Complete it by yourself; submit it in the homework 1 Folder.
- **Homework:** Read and review the following article [3]. That means that you have to read and write about your take, opinions, critiques, or grievances instead of summarizing your reading notes with the lazy "The authors said...." How to access the article? DePaul has a full article access to the ACM Digital library.

Week 03: ICS/SCADA Security [Part 1]

- **Overview:** SCADA Control System and SCADA networking
- **Lab Manuals:** Lab 1 and Lab 2
- **Homework:** Submit a report where you briefly describe your progress in the lab and what you have learned. The labs manuals are written in a way that you need to work yourself to complete the lab report.

Week 04: ICS/SCADA Security [Part 2]

- **Overview:** DoS Attacks and Network Packet Alternation
- **Lab Manuals:** Lab 3 and Lab 4
- **Homework:** Submit a report where you briefly describe your progress in the lab and what you have learned. The labs manuals are written in a way that you need to work yourself to complete the lab report.

Week 05: ICS/SCADA Security [Part 3]

- **Overview:** SCADA Snort IDS and SCADA encryption authentication
- **Lab Manuals:** Lab 5 and Lab 6
- **Homework:** Submit a report where you briefly describe your progress in the lab and what you have learned. The labs manuals are written in a way that you need to work yourself to complete the lab report.

Week 06: IoT Security

- **Overview:** Computing, physical, and networking components' in IoT: Sensors and actuators, LoPAN and WiFi communication; Vulnerabilities in IoT systems; Penetration testing, security assessment, and protection configuration for IoT deployments.
- **Homework:** Now is the time to set up the IoT Goat environment, emulate the firmwhare and all that. I specifically encourage you to share ideas, solutions, tips, and tricks on Discord. Submit a report of the installation with steps you took, screenshots, and try to solve one of the challenges, say the No 1: Hardcoded user credentials compiled into firmware.

Week 07: Legal and Privacy Aspects

- **Overview:** Privacy laws for cyber-physical systems, Regulation: FTC and FCC protections for unfair and deceptive security practices for cyber -physical systems.
- **Hands-on Activity:** Choose one of the three IoT hacks and analyze them using the legal/privacy approach from class Hands-on Activity; Download the Excel Spreadsheet; Complete it by yourself; submit it in the homework 7 Folder.
- **Homework:** Proceed with the second challenge, you got the mojo going by now, and it's getting interesting to find insecure network services. Submit a report of solution with screenshots and all experiment you did on your own, if you let your curiosity run unbound.

Week 08: Risk Assessment

- **Overview:** Application of NIST Cybersecurity Framework for Critical Infrastructure and Cyber Physical Systems
- **Hands-on Activity:** Choose one of the critical infrastructure and control system incidents and analyze them using the NIST Cybersecurity Framework: Hands-on Activity; Download the Excel Spreadsheet; Complete it by yourself; submit it in the homework 8 Folder.
- **Homework:** Select and report what you want to do for your final project. Start the configuration of the particular framework (IoT Goat, KITT, or HomePwn) and report on what, after an initial assessment, what you will focus on in your exploration/solving challenges. Remember, you have to abide to the ethical standards and tailor your exploration only to demonstration and education, not sending links with tools like SayCheese to actual people. That will get you zero points and a troublesome hearing with the academic integrity committee. Maybe you can even find another IoT/Control System framework to explore. That will work too.

Week 09: Cyberwarfare

- **Overview:** Cyberwarfare laws and international conventions, use of force and retaliation relative to cyber-physical systems.
- **Hands-on Activity:** Choose one of the critical infrastructure and control system incidents and analyze them using the cyberwarfare reasoning from class: Hands-on Activity; Download the Excel Spreadsheet; Complete it by yourself; submit it in the homework 8 Folder.
- **Homework:** Report on your project progress AKA progress update.

Week 10: Presentations

- We will do this on final Zoom meeting. Rules: You have 120 seconds to present. No PowerPoint or any slides. Verbal presentation only. I will share my screen where I will run a stopwatch. The moment the time is up, you are muted and we move to the next presenter. I determine the presentation order by a local random generator. No one will get a preferential treatment.
- In the presentation folder, you have to generate and submit couple of tweets. The The first tweet has to summarize your project findings. Yes, tell us what you have done in 280 words. You can attach an image with the some data if you like, but don't do the boring trick of attaching an image with extra text in it (the goldfish is rigged not to give extra 10,00 wishes anyhow). The second tweet has to give your honest feeling about the class. The first one is challenging because you have to cram or pick what to say from so much data or papers or exploits you use. This one is challenging to express yourself in a self-reflective manner. Two tweets, 120 seconds of talk.

Week 11: Final Paper

- No meetings. Incorporate your feedback. Submit your final project report.

Project

- For your final project, you will have to work on solving several, if not all, unsolved challenges in the IoT Goat project. Or perhaps do an exploration of the KITT and the HomePwn frameworks to demonstrate your *individual* pen-test skills. A nice summary report must be submitted where I can follow the steps and commands and get to the same results as you. You have to make sure the commands work and the objectives are achieved to receive all the points.
- You mist include a section "What I have learned" at the end of the report where you reflect on your learning experience. This is a student-centered class so you have to independently and individually push and work on achieving as much as you think could be achieved.

Course Policies

During Class

Netiquette: Help each other on Discord and talk constructive research stuff. Do not use the discussion board on D2L or the D2L built-in email. We will talk on Discord or Zoom. Do no harm, you are almost a Master of Science. In cybersecurity, no less.

Attendance: I expect you will be *proactive* in this class. At least make sure to watch the lectures and be honest to yourself to plan early on your work. Don't bite more than you can chew.

Class Cancellation: Unless DePaul closes because of weather, we will have class. Unless Zoom explodes, the internet is gone, and COVID-19 takes the better of the humanity, we will have class.

Changes to Syllabus: I reserve the right to change the syllabus and you will be timely informed of such changes. I don't expect significant deviations of the course agenda.

Academic Policies

Academic Policies: Keep an eye of DePaul's Academic Policies. They change frequently as the COVID-19 progresses.

Academic Integrity I expect that you have read and understood DePaul's Academic Integrity policy. This is crucial when working on deliverable that produce new cybersecurity knowledge.

Students with disabilities: Contact the Center for Students with Disabilities (CSD) prior to the class start.

Preferred Name & Gender Pronouns: I will gladly honor your request to address you by an alternate name or gender pronoun.

References

[1] Lorin W Anderson and Lauren A Sosniak. *Bloom's taxonomy*. Univ. Chicago Press Chicago, IL, 1994.

[2] Tejasvi Alladi, Vinay Chamola, and Sherali Zeadally. Industrial control systems: Cyberattack trends and countermeasures. *Computer Communications*, 155:1–8, 2020.

[3] Jakapan Suaboot, Adil Fahad, Zahir Tari, John Grundy, Abdun Naser Mahmood, Abdulmohsen Almalawi, Albert Y. Zomaya, and Khalil Drira. A taxonomy of supervised learning for idss in scada environments. 53(2), April 2020.