CSE 316/426 - Cyber Physical Systems Security Syllabus

Online Only. Covid-19 University Directive.
Instructor: Filipo Sharevski fsharevs@cdm.depaul.edu
Office Hours: email me or drop a message in the discord server: https://discord.gg/mtQyq6s

Course Description

Cyber Physical Systems Security (CPSS) breaches and defense, standardization, best practices, policies, protection-in-depth modeling, vulnerability and risk assessment for CPSS, CPSS and cyberwarfare, industrial control systems, Internet-of-Things (IoT).

Textbook

No text book is required. All the articles are posted in D2L for the respective week.

Agenda

W	Topic	Homework/Assignment
1	CPSS: Concepts and Principles	*Monitoring Security of Networked Control Systems - It's the Physics*
2	Security Breaches and Defenses in CPS	*Robust Cyber–Physical Systems: Concept, models, and implementation*
3	ICS/SCADA Security [Part 1]	*Lab 1 and Lab 2*
4	ICS/SCADA Security [Part 2]	*Lab 3 and Lab 4*
5	ICS/SCADA Security [Part 3]	*Lab 5 and Lab 6*
6	IoT Security	Research on IoT Hacks
7	CPSS: Legal and Privacy Aspects	*Designing Ethical Cyber-Physical Industrial Systems*
8	CPSS and Risk Assessment	*Safety and Security in Cyber–Physical Systems and Internet-of-Things Systems*
9	CPSS and Cyberwarfare	*Draft Paper / Presentation*
10	Paper/Presentation [PowerPoint 5 slides; Zoom Recording (or any type of recording, YouTube, voice over PowerPoint…), link submitted into the D2L folder]	

Topics

CPSS: Concepts and Principles

Concepts and principles of Cyber-Physical Systems Security (CPSS): 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;

Security Breaches and Defenses in CPS

Known security incidents in cyber physical systems: smart grids, ICS/SCADA systems, IoT Systems. Defenses for breaches and incidents in Cyber Physical Systems

Industrial Control Systems (ICS)/ SCADA Security

Computing, physical, and networking components' in ICS/SCADA: PLCs (Lager Logic), HMI, Modbus/Profibus TCP; Vulnerabilities in ICS/SCADA systems; Penetration testing, security assessment, and protection configuration for ICS/SCADA

IoT Security

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

CPSS: Legal and Privacy Aspects

Privacy laws for cyber-physical systems, Regulation: FTC and FCC protections for unfair and deceptive security practices for cyber -physical systems.

CPSS and Risk Assessment

Application of NIST Cybersecurity Framework for Critical Infrastructure and Cyber Physical Systems

CPSS and Cyberwarfare

Cyberwarfare laws and international conventions, use of force and retaliation relative to cyber-physical systems.

Assignments and Grading

Homeworks/Assignments are due a week 11:59 PM after each one is assigned. No late assignments will be accepted. Absolutely NO grade bargaining will be allowed.

Assignment	Weight in final grade
Homework	20%
Labs	30%
Project / Paper	50%
Presentation	10%

Grading is based on a percentage basis, which is then convert to a letter as:

Percentage Grade	Letter Grade	Manner of fulfillment
92-100	A	Excellent
90-91	A-	
88-89	B+	
82-87	B	Very Good
80-81	B-	
78-79	C+	
72-77	C	Satisfactory
70-71	C-	
68-69	D+	
62-67	D	Poor
60-61	D-	
0-59	F	

Homework

On weeks where there are articles assigned, you need to critically review them. What's an article? A journal/conference paper. What's critical review? It's not summarizing the article as in "Authors said…". DO NOT focus what the authors have said. I have assigned this reading to you so I already know what they have said. Instead, you need to analyze the content of the article in the context of the lectures and provide your constructive opinion on the implications steaming from the problem/solution at stake.

Labs

All labs will be conducted using a virtual machine. You can download it:
https://drive.google.com/file/d/1XIg9yNGRdopRPIz6IzJqapJ5byraZ0vH/view?ts=5cb8d244
The Lab manuals are included in the respective submission folders.

Project

Any security assessment of a cyber-physical system will do. Constructive, practical, applied, and critical approaches are encouraged and expected. I would strongly encourage you to try to do the challenges in the IoTGoat project as your final project: https://github.com/scriptingxss/IoTGoat. So, an individual hands-on project. This is an advanced class and your project/paper needs to demonstrate you have successfully achieved the learning objectives in this class. Reading online articles and copy/paste simple text is not one of them. You have access to unlimited throve of academic articles, books, and proceedings through DePaul's Library. Use it.

Presentation

You will do a PowerPoint presentation. Record your voice. Submit it into the respective folder (or a link to it). Or do a Zoom recording, YouTube, or whatever is available to you. No more than 5 slides. The gist of your paper. Extra content or extra slides will be

penalized. Its more simple than you think it is. I need to hear your contribution in the project. Briefly and precisely to the point.

Learning Outcomes

At the end of the course the students will be able to:

1. Analyze CPSS breaches and develop defensive measures;
2. Employ CPSS best practices to create and implement policies for CPSS protections
3. Model CPSS protection-in-depth for industrial control system and IoT systems.
4. Perform CPSS risk assessment
5. Evaluate CPSS breaches and defenses in the context of cyberwarfare

Other Important Information

1. Attendance: I expect you will attend every class [or watch the lecture].
2. Class Cancelation: Unless DePaul closes because of weather, we will have class.
3. Academic Integrity: I expect that you have read and understood DePaul's Academic Integrity policy: https://offices.depaul.edu/academic-affairs/faculty-resources/academic-integrity/Pages/default.aspx
4. Changes to Syllabus: I reserve the right to change the syllabus and you will be timely informed of such changes.
5. Academic Policies: https://www.cdm.depaul.edu/Student-Resources/Pages/PoliciesandProcedures.aspx
6. Students with disabilities: Contact the instructor or the Center for Students with Disabilities (CSD) at: csd@depaul.edu prior to the class start.
7. Online Teaching Evaluation: Please evaluate the course in CampusConnect when you receive a notification towards the end of the quarter.
8. Preferred Name & Gender Pronouns: I will gladly honor your request to address you by an alternate name or gender pronoun: https://policies.depaul.edu/login.aspx?ReturnUrl=/policy/policy.aspx?pid=332