Integrating Cyber Physical System Security Concepts in Computer System Security Curriculum

Heena Rathore
Department of Computer Science
Texas State University
San Marcos, Texas
heena.rathore@ieee.org

2023 IEEE Integrated STEM Education Conference (ISEC) | 979-8-3503-0001-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISEC57711.2023.10402293

***Abstract*—Cyber physical systems (CPS) are becoming increasingly prevalent in our daily lives, from connected vehicles and medical devices to critical infrastructure systems. As there is growing emphasis both in industry and academia on the security aspects of CPS, students should have sufficient foundational knowledge about these topics as they transition into their professional careers. This manuscript describes the integration of modern CPS security concepts into the traditional required Computer System Security undergraduate course at Texas State University. Content is introduced through a group course project, where students reviewed and replicated results from a recent relevant CPS security paper. Papers were self-selected by groups based upon ten recommendations covering content from emerging CPS security topics, such as connected vehicle security and industrial IoT. Based upon the success of this initial implementation, future efforts to expand the scope of CPS coverage in future course iterations are proposed.**

***Index Terms*—computer system security, cyber physical systems, undergraduate curriculum, group projects**

I. Introduction

Cyber Physical System (CPS) security refers to the protection of physical and cyber systems, along with networks, and data from unauthorized access, manipulation, and disruption [1], [2]. These systems are important because they play a crucial role in various areas of society, and includes critical systems such as industrial control systems, medical devices, connected vehicles and internet of things (IoT) devices. Security in CPS is essential to ensure the safety, reliability, and functionality of these systems, along with preventing disruptions to critical infrastructure and system operations [3].

To meet future workforce demands in CPS security, there is a pressing need to increase the number of trained professionals in this area. This will require a combination of new workforce programming, dedicated new academic offerings at the undergraduate (UG) and graduate level, along with the broad integration of these concepts into existing academic offerings. Several initiatives to meet this demand have been recently described in the literature. For example, Boise State University has proposed a three-level program intended to introduce CPS security concepts on a broad scale using various approaches, including the development of a new Introductory Cybersecurity course designed for both engineering and math majors [4]. While introducing dedicated new courses and programs is beneficial, the potential scale of impact using this approach is limited versus the integration of CPS security concepts within required courses in relevant degree programs.

When considering potential required pathways in which to integrate CPS security concepts, UG computer science programs are a natural first choice due to the prevalence of security-oriented courses within the degree plan [5]. An UG course in computer security typically includes topics such as network security, operating system security, cryptography, software security [6]. There are several efforts ongoing to integrate CPS security concepts into UG CS programs. For example, Arizona State University is employing a two-factor approach for selecting courses for potential integration, which considers not only the course material, but also potential scale of students impacted [7].

This paper describes recent efforts to integrate CPS security within the Computer System Security course (CS4371/5378) at Texas State University during the Fall 2022 semester. CS4371 course is required for all UG CS majors, and is also taken by a significant number of graduate students under a cross-listed course (CS5378). A group-based active learning experience was utilized, where students selected and replicated a research paper in CPS security. Details regarding the logistics of the project implementations and lessons learned for future implementations are described herein.

II. Methods

A. Project Logistics

Due to the placement of the course within the UG degree sequence, along with the integrated graduate cross-listed section, the curricular modifications were formulated using a research experience pedagogy. Namely, groups of students were required to review a state-of-the-art paper in CPS security and conduct a basic implementation project (i.e.: replication of simulations used within the paper, demonstration of an alternative solution, etc.). In addition to exposing students to cutting-edge concepts within the field, this experience was also intended to encourage the exploration of CPS security concepts during graduate studies. To help prepare students for this project, 2 weeks of CPS security concepts were added to the course lectures. At the end of the semester, each group had 15 minutes to present their project. Students were also required to submit their code to github at the conclusion of the project.

Seventy total students (both UG and graduate) were enrolled in the course during the fall semester. A total of 15 groups were formed with group size ranging between 3-5 members. Ten representative papers were provided to students as potential review options. Students were also open to select other research papers that were related to the topics covered in the class. There were a total of 4 groups who selected other papers which were not in the pool of representative papers. Student groups were required to provide a brief project proposal based upon their initial review for the paper.

B. CPS Security Topics

The representative papers mentioned above were chosen to align with the most relevant emerging application domains of CPS security. These domains included - 1) connected vehicles, 2) industrial IoT, 3) IoT and cloud storage, 4) Byzantine Fault Tolerance (BFT), and 5) Standard Cryptographic Algorithms. A brief description of the relevance of each of these topics to modern CPS security, along with the representative papers chosen for each category, are described below:

- *Connected vehicles security*: As more vehicles are equipped with embedded sensors, it is critical to ensure their security to prevent security vulnerabilities and privacy risks. Distributed ledger techniques are one way of enhancing the security of CV and one representative paper was covered and discussed in the class [8]. Six groups selected distributed ledger techniques as their group project. Among these, one group used the learnings to build a secure voting system to validate the votes.
- *Industrial IoT*: Industrial IoT security is important because it helps to ensure the reliability and safety of industrial systems that use connected devices. One group learned the security challenges posed by the use of connected devices in industrial systems, and developed the technologies, practices and frameworks that apply to industrial IoT security [9].
- *IoT and cloud storage*: One of the groups developed a secure constructed deduplication supporting authorized duplicate check in hybrid cloud architecture. Duplicate-check tokens of files were generated by the private cloud server with private keys to eliminate duplicate copies of repeating data [10].
- *Byzantine Fault Tolerance (BFT)*: BFT is a technique used to ensure the reliability and security of CPS even in the presence of failures or malicious behavior by some of its components. This is accomplished by replicating data and ensuring that multiple copies of the same data are available to the system. Three groups worked in this area to show the different types of BFT algorithms and the criteria used to evaluate their performance, such as fault tolerance, performance, and scalability in CPS systems.
- *Standard Cryptographic Algorithms*: Some groups selected encryption and decryption algorithms, along with cryptographic protocols, and their applications in securing CPS systems. One group created a modified and enhanced form of Caesar cipher [12], a traditional substitution cipher technique. They also converted the encoded message to a binary Fibonacci sequence based on the numeric values of each character.
- *Student Selected Papers*: Two groups of graduate students selected their own papers based upon machine learning content presented within the course. The first paper discussed machine learning algorithms for malware detection, while the second discussed number plate detection for unauthorized access to attackers for smart CPS systems [13].

Table I summarizes the details of the group project selection process. It details the number of papers given in a specific category, along with the number of groups who selected those papers. The table also denotes whether or not the paper was selected from the set of papers originally presented to the class.

TABLE I
DETAILS OF GROUP PROJECT PAPERS BY CATEGORY

Topics	# of papers given	# of groups chose	Selected from given	Independent
1. Connected Vehicles	1	6	✓	-
2. Industrial IoT	3	1	✓	-
3. IoT and Cloud	3	1	-	✓
4. BFT	2	4	✓	-
5. Cryptographic based	1	3	✓	✓

C. Student Performance and Feedback

Student performance on the project was strong. All group presentations showed evidence of comprehension of the underlying paper, along with its relevance to broader issues in CPS security. In addition, beyond performing basic replications of the algorithms discussed within the assigned papers, students also showed evidence of considerable creativity, either extending the application scope of the paper algorithm or proposing extensions.

Feedback on the project was also provided through the open-ended written questions integrated within the standard course evaluation. Students generally indicated that they enjoyed the opportunity to apply the concepts and techniques that were covered in class to a real-world CPS security problem. Some even suggested to expand the coverage of CPS security concepts within the curriculum. One suggested activity was holding a CPS security capture the flag (CTF) competition as part of future course offerings.

III. CONCLUSIONS AND FUTURE WORK

UG computer security courses have historically focused on network-based cryptography approaches. As CPS emerges, broader exposure to relevant cybersecurity concepts within the UG curriculum is required. While some initiatives have delivered this content through newly developed elective courses,

integrating CPS content into required classes ensures maximum impact. This manuscript described the integration of CPS content into a required UG Computer System Security course. CPS content was integrated through a group project assignment, where students reviewed and replicated content from a recent relevant publication.

Based upon student feedback, future modifications will focus on expanding the coverage of CPS security content into the course beyond the group project and supporting lectures. Some additional activities to be integrated include a CPS-based CTF competition to further expose students to market-relevant skills. In addition, the number of lectures covering CPS-related security content will also be increased due to the expanding relevance of these topics within the modern economy.

REFERENCES

[1] US Department of Homeland Security, "Cyber Physical System Security", https://www.dhs.gov/science-and-technology/cpssec, [accessed on Feb 5, 2023]

[2] H. Rathore, A. Mohamed, and M. Guizani, "A survey of blockchain enabled cyber-physical systems", *Sensors*, vol. 20, no. 1, p.282, 2020.

[3] J.P.A Yaacoub et al., "Cyber-physical systems security: Limitations, issues and future trends". *Microprocessors and microsystems*, 77, p.103-201, 2020.

[4] S.M. Loo, & L. Babinkostova, "Cyber-physical Systems Security Introductory Course for STEM Students", *ASEE Virtual Annual Conference Content Access, Virtual On line.* 10.18260/1-2–34366, 2020.

[5] M.N. Islam, J. Abel and Q. Gao, "Computer Security in Undergraduate Curriculum". In *ASEE Zone I Conference & Workshop*, 2019.

[6] E. Crowley, "Information system security curricula development". In Proc. *4th conference on Information technology curriculum*. pp. 249-255, 2003.

[7] U. Kannan, and R. Swamidurai, "Integrating Cybersecurity Concepts Across Undergraduate Computer Science and Information Systems Curriculum Paper", *ASEE Virtual Annual Conference Content Access, Virtual Conference*, https://peer.asee.org/37357, 2021.

[8] H. Rathore, A. Samant, and M. Jadliwala, "TangleCV: A distributed ledger technique for secure message sharing in connected vehicles". *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 1, pp.1-25.

[9] S. Latif et al., "A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things". *Journal of Industrial Information Integration*, no. 21, p.100-190, 2021.

[10] J. Li et al., "A hybrid cloud approach for secure authorized deduplication". *IEEE transactions on parallel and distributed systems*, vol. 26, no. 5, pp.1206-1216, 2021.

[11] F. Muratov et al., "YAC: BFT consensus algorithm for blockchain". *arXiv preprint arXiv:1809.00554*, 2018.

[12] K. Goyal, and S. Kinger, "Modified caesar cipher for better security enhancement". *International Journal of Computer Applications*, vol. 73, no. 3, pp.0975-8887, 2013.

[13] C. Mujeeb Ahmed, "Machine learning for CPS security: applications, challenges and recommendations". *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*, pp.397-421, 2021.