



Cyber-Physical Systems Security Introductory Course for STEM Students

Prof. Sin Ming Loo, Boise State University

Sin Ming Loo is a professor at Boise State University with interests in sensor systems and cyber-physical systems security research and education. He is responsible for Hartman Systems Integration and Cyber Lab for Industrial Control Systems laboratories. He holds a joint appointment with Idaho National Lab. He is a member of IEEE/CS, ISSA, Tau Beta Pi, and amateur radio (KI4AKS).

Liljana Babinkostova

Cyber-Physical Systems Security Introductory Course for STEM Students

Abstract

We are witnessing the rapid development and adoption of Cyber-Physical Systems (CPS). CPS refers to the integration of digital and internetworked components, and physical devices in systems that affect nearly everyone in society. These devices are always connected to the internet. This connectivity gives CPS devices the capability of being in continuous monitoring mode where data and information are delivered to device owners through a proxy server. These capabilities open up all kinds of security issues for a device that has been built with such features with little regard for security considerations. At present, many Science, Technology, Engineering, and Mathematics (STEM) graduates are not fully comprehending the security impact of device connectivity. STEM students are graduating without awareness of cybersecurity or cyber-physical systems security issues/challenges and without being aware of the security issues related to algorithms or systems they are designing. This state of affairs is a consequence of the fact that security awareness is currently not part of the curriculum.

In this paper we highlight a cybersecurity program at Boise State University that includes an introductory class on CPS security. Some topics included in this course are: information technology versus operation technology, cryptography, industrial control systems, smart grid, CAN bus, risk assessment, red versus blue team, and Kali Linux. In this paper, we provide examples on how students' knowledge of CPS security changes over the course of the program, how students are supported in and out of the classroom towards advancing their knowledge in this field. We also highlight the impact that project-based and team coordinated learning can have on increasing students' understanding of the fundamentals of CPS security.

Introduction

A recent study by Cybersecurity Ventures [1], a respected publisher of cybersecurity content, predicts that 3.5 million cybersecurity jobs around the world will be unfilled by 2021. In the United States, the demand for professionals with cybersecurity expertise is outpacing all other occupations [2]. These reports, along with many others, underpin the need for increasing workforce development initiatives founded in cybersecurity principles. The workforce shortage is across all cybersecurity domains, yet our adversaries are always advancing, always probing for vulnerabilities in corporate enterprise systems, critical infrastructure systems, and vital national security systems. The cyber game is unfair, the defenders have to do everything right everyday and hackers only have to get lucky once.

To combat this persistent threat, which is a 24/7 operation, we need all hands on deck. We must work to ensure our graduates comprehend cybersecurity; we need people with different perspectives, approaches, ways of thinking, and methods to solve the cyber challenges we are facing and will face. We envision that cybersecurity education needs to take place at three different levels, not in rank of importance. These are all important. First, every graduate, no matter their major of studying, has to have cybersecurity awareness. The content related to cyber from information assurance, internet of things, cryptography, malware, ransomware, etc. are taught at a very basic level. It has been shown that even with wide ranging phishing email training, 3% still

click on phishing email that can potentially compromise information and access [3]. Awareness education can strengthen the human factor side of cyber. Second, we need to train more students to work in cyber operations. This means that they can carry out tasks either in offensive security, defensive security, and/or forensics and recovery. It is important for these students to know how to think critically and use data to solve problems. Third, we need our STEM graduates, who will design future systems, to understand cyber. It is not for them to be expert in cyber, it is for them to know enough to take cyber into consideration as part of the design/development process. It is knowing enough to call in the cybersecurity expert when needed. This is what we call cyber-informed engineering.

In this paper, we provide the details of our introductory course, Introduction to Security in Cyber-Physical Systems, as part of the STEM cyber curriculum. It is a course with lectures on related security topics, hands-on activities, and projects. The major topics of the course are presented in the following sections. These major topics were selected based on input provided by our industry partners.

Our Cybersecurity Education Approach

It is our belief that there is a need to introduce cybersecurity education into the existing curriculum. At a minimum, cybersecurity education needs to be addressed with three different levels. These levels are all important with no particular one a higher priority than the others.

Level 1: Cybersecurity for All

A set of courses that provides cyber security background for everyone. The objective is to raise the cybersecurity awareness across the campus.

Level 2: Cyber Operations

A set of courses that provide cyber operations cybersecurity skill sets. The objective is to train students and to provide industry certification opportunities for those interested in this as a career.

Level 3: Cyber-Informed Engineering Curriculum

A set of courses that provide cyber-informed engineering skill sets for STEM students. The objective is to train the future engineers and scientists to incorporate cyber (as a requirement) into the design process for systems more resilient against the security threat.

This paper is on the introductory course in Level 3. The curriculum that Boise State University put together started with an introductory course (this paper) that introduces students to security topics. This curriculum is available to engineering and math majors. This course is offered during Fall semester only. The students enrolled in the past two offerings of the course were students from Computer Science, Electrical Engineering, and Mechanical Engineering while the program is also open to students from Civil Engineering and Mathematics. The curriculum was structured where all credit hours earned contribute to their graduation requirements. The introductory course is an elective course. The objective is not for students to be security experts, rather it is about knowing enough to understand cyber threat impacts to the system design process, understand how to protect against such threats, and be able to know when to call the cybersecurity experts. Although there are many degree programs in cybersecurity as a major and research in cyber physical system

related to smart infrastructure & connected communities, and securing cyber-physical systems [4, 5], we are not aware that currently exist an educational model that integrates cyber security as part of STEM curriculum. The program’s goal is to broaden knowledge of our STEM graduates to be aware of cyber issues as engineers. The curriculum is shown in Figure 1, where 4 tracks are available for the student’s interest and major of study. The courses within each track are existing courses with security content added to them.

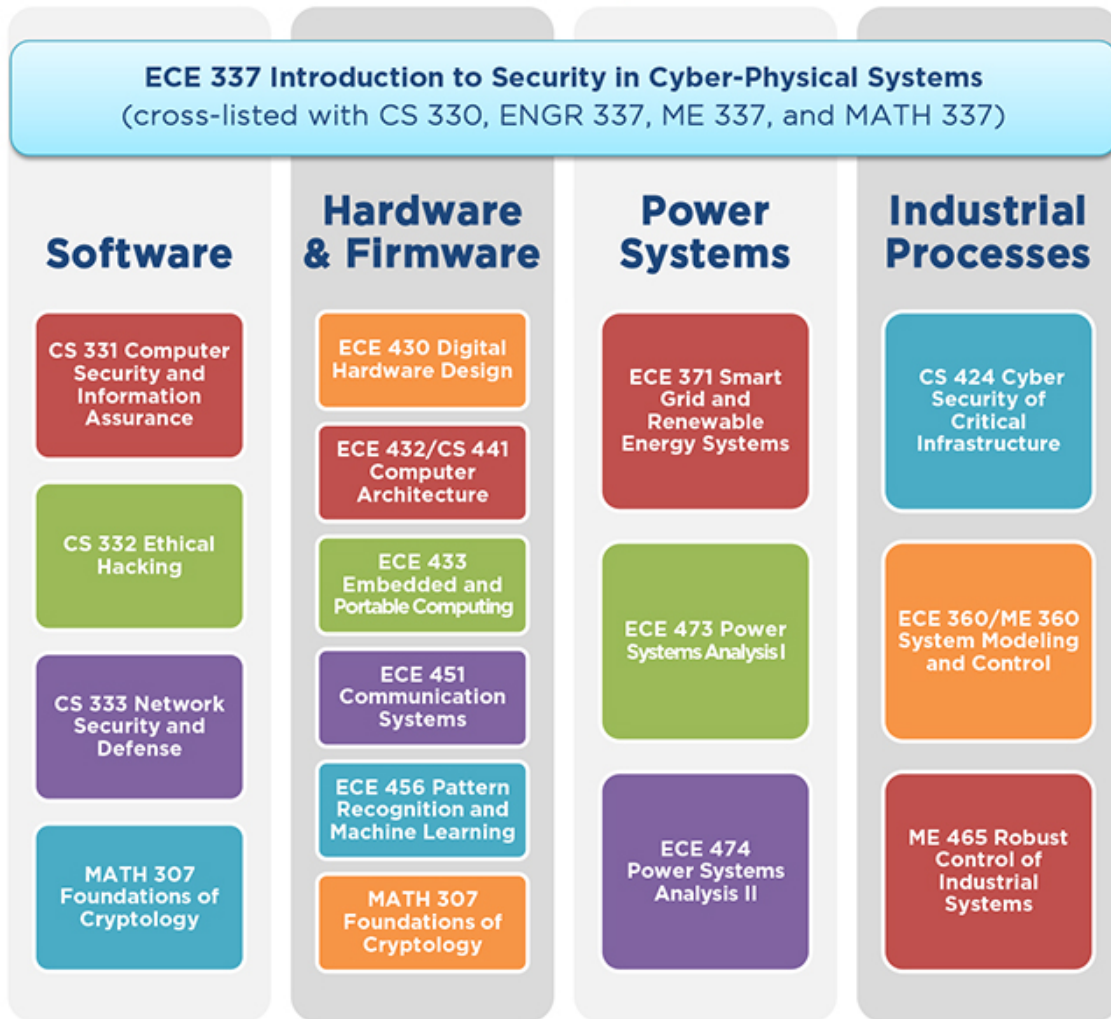


Figure 1: Cyber-informed engineering curriculum for STEM majors. Each track gives the students an opportunity to earn a security certificate as part of their undergraduate degree. The color of boxes has no special meaning.

The introductory course (top light blue box, an elective course) was the only new course added to the existing curriculum. For existing engineering courses, security content was added. This decision was made to emphasize that cybersecurity should be considered as complementary to existing design criteria. For example, the ECE 433 Embedded and Portable Computing course is a traditional embedded systems course which introduces students to embedded system design after the junior microprocessor course. As part of the cyber-informed engineering curriculum,

techniques for secure systems coding, bootloaders and system lock bits, and data encryption are incorporated into the course.

As for the Power related courses, the emphasis is on SCADA, CIP-014, and CIP-002. The topics include the use of SCADA, cyber security, physical security, and how to classify, protect, and operate CIP equipment. For the Communication course, the physical layer of security is discussed.

In the Computer Architecture course, Meltdown and Spectre vulnerabilities are discussed and how these arose from pipeline and cache designs. Virtual memory is also introduced, and how it can be used to keep processes separated.

Major Topics of the Introductory Course

The course has been designed with the following grading breakdown: in-class weekly quizzes (40%), participation and discussion (10%), hands-on assignment (20%), and project (30%). The following are the major topics presented. This is an introductory course with the objectives of introducing related topics without in-depth coverage. After taking this course, the students should be able to:

- Identify the importance of cyber-physical system security
- Understand cryptography and the importance of cryptography in modern society
- Develop proficiency using Kali Linux
- Learn/demonstrate a PLC ladder logic program
- Identify the similarities and differences between IT and OT networks
- Understand industrial control system, Shodan, and smart grid
- Identify the working of CAN bus
- Discuss the ethics of cybersecurity and problems of many hands
- Learn/demonstrate penetration test (WiFi, network scan, Nessus, Metasploit, etc)
- Understand Risk Assessment and threat modeling
- Learn/demonstrate basics of forensics

Introduction and Legal Ramifications

The introductory lecture of the course includes definitions of Confidentiality, Integrity, and Availability (CIA), the triad of information assurance. The lecture also contains cyber intrusion examples that will resonate the most with these students. The cases highlighted include Stuxnet, Jeep intrusion, Ukraine power grid, and trusting sensors. These were used as reading assignments [6-10]. As part of the class, students also have to sign an agreement on what to do and what not to do. This was put together with help from the university's legal office.

IT Versus OT Network

This topic of the course introduces the differences between Information Technology (IT) network and Operational Technology (OT) network. IT is a network where confidentiality and integrity are more important than availability. However, for OT network, availability is the most important as production has to continue in all conditions. No production means no revenue. There are many IT practices that won't work well in an OT network. For example, scanning in IT network is a normal

practice. However, scanning OT network can potentially cause unresponsiveness of a PLC, which will disrupt production.

Cryptography

This module focuses on the fundamentals of cryptography such as block ciphers, stream ciphers and digital signatures. Cryptographic schemes are used to secure passwords and other sensitive information, in addition to playing a key role in device communication and authentication. The RC4 encryption scheme is used to demonstrate how cryptographic schemes are used in CPS security. The RC4 algorithm is illustrated in detail and with visualization to demonstrate the work of RC4 algorithm and make it more understandable. RC4 has subtle security flaws, and these are pointed out so that students also grasp that every component of the system has to be taken into account, not only the physical aspects.

Pentesting - Kali Linux

For this module, penetration testing is introduced using Kali Linux. Students struggle through a guided process of installing Kali Linux or boot to memory using a USB drive. Not all built-in WiFi transceivers will accommodate Kali Linux as it is not able to be set to monitoring mode. As part of this module, students are also introduced to the use of Aircrack-ng/Fern, John the Ripper, and Wireshark.

Smartgrid

This module gives an overview of a smart grid, its architecture and its properties such as digitalization (digital platform which makes the system fast and reliable), intelligence (inherits an intelligent technology), resilience (not affected by any attacks), customization (client tailored), and flexibility (compatible, expandable, and adaptable). Several security challenges regarding smart grid are discussed such as availability, confidentiality and integrity.

Industrial Control System

This module gives an overview of Programmable Logic Controller and Supervisory Control and Data Acquisition (SCADA). SCADA is system gathering and processing data and applying operational controls over long distances. The use of SCADA systems in distribution systems is discussed including those such as water distribution and wastewater collection systems, oil and gas pipelines, electrical utility transmission and distribution systems, and rail and other public transportation systems.

CAN Bus

Controller Area Network (CAN) is a vehicle bus network designed to allow microcontrollers and devices to communicate without a host device. We used a background introduction video by [11].

Risk Assessment

Exposure to some widely accepted risk management standards and guidelines for risk management activities such as the NIST framework and IEC 62351. Main threats and vulnerabilities of CPS systems and security countermeasures to mitigate the risk are discussed.

Threat Modeling

The main differences between CPS security analyses and conventional network security analyses are discussed. This module features threat models such as attacks on availability, integrity and privacy. Availability represents the accessibility of every component of the system as well as of the information transmitted and collected when needed. Attacks compromising availability are known as denial-of-service (DoS) attacks. Integrity refers to the credibility of the data collected and transferred over the CPS. Attacks targeting integrity through what is known as deception attacks of the transferred data can have major effects on the system. Privacy refers to the private data that users transmit as part of cyber-physical interactive systems such as in the smart grid.

Metasploit Framework

Metasploit Framework is a software platform for exploit development, testing, and execution. It has exploit modules for exploiting system weakness. It is a powerful tool for penetration testing. It is a tool that one needs to use wisely as it has the ability to generate a payload for attachment to email or setup for downloading to a website. This gives ability to easily create a reverse shell from the victim's system to the intruder's system.

Forensics

Forensics was introduced as a hands-on exercise module. Prior to assigning the forensics module, students had an introductory lecture on the usage of command lines. We found that this is needed as students' command line skills were lacking.

Hands-On Activities

Ladder Logic

The ladder logic hands-on assignment is to give student a feel of what's PLC ladder logic, the critical part of industry control systems. This one-week hands-on ladder logic programming uses Automation Direct's CLICK PLC software and PLC (C0-00DD2-D). Students were grouped in teams of 2 or 3. They were given a one-page instruction sheet to install the CLICK PLC ladder logic software, work through Automation Direct's ladder logic tutorial, and complete an assignment using buttons and LEDs. All teams completed the assignment. No students had prior ladder logic programming experience.

Hands-on Practice Network Scanning and Password Cracking

This hands-on activity is to close the loop on the pen-testing module. A WiFi learning network (air gap, no connection to the internet or campus network) has been set up for students to learn penetration testing. The learning network consists of a WiFi access point, an android cell phone, a Raspberry Pi, and Windows computers. As part of the activity, a student uses tools in Kali Linux to crack the WiFi password, get into the network, scan the network, leave a mark on Raspberry Pi, and crack the password hash on the Raspberry Pi. All teams completed most of the assignment. Some teams didn't crack all the password hashes.

Forensics

This hands-on activity is to give students an introduction to forensics. We utilized a Webserver Forensic Analysis module developed by ENISA [12]. The idea is to provide students a hands-on experience of mounting a virtual image as readable only, and using Linux command lines to search for intrusion traces. This is an individual assignment. Over 90% of the class completed this forensics activity.

Projects

As the semester progressed, student teams had to submit a short project idea write-up for approval. Teams also provide 2-minute project updates throughout the semester. Projects include monitoring camera hacking, CAN bus hacking, smart lock, garage door opener, car remote entry system, return oriented programming, RF jamming, binary manipulation of STM F4 board, keylogger, security orion, and evil twin WiFi attack. At the end of the semester, each team has 10 minutes to present their project and a report is submitted a few days later. 80% of the projects were successfully completed. 20% of the projects aren't completed or they didn't try hard enough.

Lessons Learned

After offering this course twice in the last two years (30 students Fall 2018, 35 students Fall 2019), there are a wide range of students' motivation and skill sets. A large portion of the students performed well.

However the lack of self-regulation, interpersonal skills and constrained mindset was evident. We describe this evidence through the following example: As part of the penetration testing hands-on activity, we had an air-gap learning network for students to practice WiFi penetration using Aircrack-ng/Fern, network scanning using Nmap/Zenmap, and password cracking using John the Ripper. This learning network consists of a wireless access point, Raspberry Pi, cellphone, and some Windows computers. Students are to leave a mark on the Raspberry Pi by using the default userid and password (representing a badly configured machine) and access the shadow password file. Leaving this network running for days allowed students to apply what they learned. However, someone change the default user password and root password of the Raspberry Pi keeping other students from finishing the exercise. We learned how to configure a better learning network.

Although students' prior knowledge and experiences were taken into account, the lack of conceptual understanding of Linux sometimes made the instructions challenging. How to provide the right amount of challenge and support on relevant learning tasks requires further investigation.

Summary

The introduction of security content into our STEM curriculum has begun. It is rewarding and challenging. We have offered this course twice with 30 students in Fall 2018 and 35 students in Fall 2019. Teaching this course is a challenge as it covered a wide range of topics. We are continuously improving the process. We have learned that basic networking is another topic that we need to cover.

References

- [1] Morgan, Steve. (2019, October 24). Cybersecurity Talent Crunch To Create 3.5 Million Unfilled Jobs Globally By 2021. Retrieved from <https://cybersecurityventures.com/jobs/>, Vi
- [2] nist_gov. (2018, November 7). New Data Show Demand for Cybersecurity Professionals Accelerating. Retrieved from <https://www.nist.gov/news-events/news/2018/11/new-data-show-demand-cybersecurity-professionals-accelerating>
- [3] Verizon. (2019, May 21). 2019 Data Breach Investigations Report. Retrieved from <https://enterprise.verizon.com/resources/reports/dbir/>
- [4] USC. (2016, October). USC Viterbi Establishes Center for Cyber-Physical Systems and the Internet of Things (CCI). Retrieved from <https://minghsiehece.usc.edu/2016/10/usc-viterbi-establishes-center-for-cyber-physical-systems-and-the-internet-of-things-cci/>
- [5] Cybersecurity Degrees. (2020). The 50 Best Universities for Cyber Security and Information Assurance. Retrieved from <https://www.cybersecuritydegrees.com/rankings/the-best-universities-for-cyber-security-and-information-assurance/>
- [6] Greenberg, Andy. (2019, September 12). New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction. Retrieved from <https://www.wired.com/story/russian-hackers-attack-ukraine/>
- [7] Greenberg, Andy. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway—With Me in It. Retrieved from <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- [8] Zetter, Kim. (2014, November 3). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. Retrieved from <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>
- [9] Kushner, David. (2013, February 26). The Real Story of Stuxnet How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program. Retrieved from <https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>
- [10] Fu, Kevin. Xu Wenyuan. (2018, February). Risks of Trusting the Physics of Sensors. Retrieved from <https://cacm.acm.org/magazines/2018/2/224627-risks-of-trusting-the-physics-of-sensors/fulltext>
- [11] CSS Electronics. (2020). CAN Bus Explained - A Simple Intro (2020). Retrieved from <https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en>
- [12] European Union Agency for Cybersecurity. (2020). Retrieved from https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational#Forensic_analysis_Webservice_analysis