A Hands-on Modular Laboratory Environment to Foster Learning in Control System Security

Pallavi P. Deshmukh, Cameron D. Patterson, and William T. Baumann
Bradley Department of Electrical and Computer Engineering
Virginia Tech
Blacksburg, Virginia 24061
{pallavid, cdp, baumann}@vt.edu

***Abstract*—Cyber-Physical Systems (CPSes) use computers to control and monitor physical processes in domains such as aviation, industrial automation, transportation, communication, water distribution, waste treatment, and power systems. These systems are increasingly connected with both private and public networks, making them susceptible to disruption or destruction by adversaries anywhere in the world. Attacks such as the Stuxnet worm have highlighted CPS vulnerabilities and motivated the development of CPS-specific defenses. The lab modules described in this paper arose from a project initially focused on technology to counter a Stuxnet-class attack on a CPS, and the suitability of this technology's commercial off-the-shelf components for undergraduate education was later realized. CPS security is not given much attention in undergraduate programs because networks and control systems are traditionally distinct areas of study. We have developed hands-on courseware to show how an adversary can compromise a CPS in a Stuxnet-like manner by tunneling through a layered sequence of network protocol and interface weaknesses. The courseware incorporates cyber-physical security concepts into effective learning modules that highlight real-world technical issues. This modular learning approach helps students understand CPS architectures and their vulnerabilities to cyber-attacks via experiential learning, and acquire practical skills through actively participating in the hands-on exercises. This courseware uses an economical and easily replicable hardware testbed, making this experience available as an adjunct to conventional embedded system, control system design, or cybersecurity courses. To assess the impact of this courseware, an evaluation survey is developed to measure the understanding of the unique aspects of CPS security. These modules leverage existing academic subjects, help students understand the sequence of steps taken by adversaries, and serve to bridge theory and practice.**

***Index Terms*—cybersecurity; trust; embedded security; modular education; security lab; hands-on learning; embedded systems; cyber-physical systems; control systems**

I. Motivation

Cyber-Physical Systems (CPSes) have become an ubiquitous component of our everyday lives, with an immense range of applications including, but not limited to: medical devices, aviation, telecommunications, ground transportation, industrial automation, and power systems. These systems are often networked through Information Technology (IT) infrastructure to allow for a reliable exchange of information among humans and machines. However, as these applications continue to increase, so does the potential for cyber-attacks that can cause system failures and result in potentially catastrophic events.

For example, in June 2000, a disgruntled former contractor for Maroochy Water Services in Australia used radio transmitters in his car to release one million liters of untreated sewage into local waterways [1]. In June 2010, Stuxnet, a 500-kilobyte computer worm, damaged centrifuges in the Natanz uranium enrichment facility in Iran [2]. In December 2014, a malicious actor infiltrated a German steel mill facility using a phishing email to gain access to the corporate network, moved on to the plant network and caused unexpected conditions and physical damage to the plant [3]. All these attacks point out the risks and vulnerabilities of an Industrial Control System (ICS) [4], [5] and hence, it is crucial to understand the various challenges in securing a CPS.

It is widely accepted that there is a critical need today to educate students in the field of cybersecurity with respect to such critical systems. A Presidential Executive Order [6], released in 2013, discusses the need to prioritize improved security of the critical infrastructures defined in Presidential Directive 7 [7].

More specifically, there is a high demand for cybersecurity training in the context of CPSes. However, this is limited by the extremely high costs and, consequently, the lack of testbeds capable of representing actual instantiations of a CPS. In 2003, multiple national laboratories collaborated to create the National Supervisory Control and Data Acquisition (SCADA) Testbed Program funded by the Department of Energy (DOE), to leverage their integrated expertise and resources in CPS security assessment, standards, and training [8]. This program offers cybersecurity training mostly for professionals in network/control systems and operators responsible for critical infrastructure [9]. Although this program is beneficial in many ways, it is limited by various factors such as time availability, geographical locations, and high training costs. These factors create a need for local programs which aim to build awareness and relevant skills across the critical infrastructure industries.

According to the Chief Executive Officer of the National Board of Information Security Examiners (NBISE), Michael Assante, the current security strategies are too disjointed, and

there is a need to close the gaps in the software and system engineering foundations [10]. In his testimony on security issues in control systems, he criticizes the security research programs that are working on implementing yesterday's general IT security measures into today's ICSes and SCADA systems. He also argues that "these efforts were proven ineffective in general IT systems against more advanced threats." He also talks about the need for training individuals, and integrating security tools in a controls environment. The right exposure to systems with large complexity and interconnectedness will help bridge this gap.

Thus, it is quite apparent that there is a need for remotely accessible, open-source programs that build awareness and relevant skills in the field of CPS security. Also, there is a strong demand for a hands-on modular educational approach that uses an economical mock testbed to delve more deeply into a wide range of topics in this area.

Our aim is to build a foundational framework that is well-suited to advance a cybersecurity emphasis in CPSes and encourage students to learn about the unique aspects of CPS security. Thus, the challenge is to develop hands-on learning modules from the perspective of maintaining reliable process control, including known exploits as well as attacks, to reinforce security concepts. Cyber-physical security education and training in control systems and other related programs is an excellent method of building awareness in students.

The remainder of the paper is organized as follows: Section II discusses the previous educational work in the area of CPS security. Section III provides the relevant background to establish the research goals of this work. Section IV discusses the learning goals and provides a roadmap of incremental modules to penetrate into the lowest layer that interacts with physical processes. Sections V to VII discuss the different modules in the network, regulatory and reconfiguration layers, respectively. Section VIII evaluates the effectiveness of these modules by highlighting students' feedback. Section IX concludes with what was achieved through this research and discusses the future work of integrating these labs with a course.

II. Previous Educational Work

As security has become a critical issue that affects our everyday life, there has been a consistent effort to develop courses that involve security training. Rowe et al. discuss the role of cybersecurity in IT education [11]. Although modules have been a common pedagogical platform for cybersecurity [11]–[15], these do not highlight the real-world security issues in CPSes.

Navarro et al. discuss the use of cybersecurity in smart grid systems as an education tool in which they use a simulated environment to understand the penetration process that can compromise a SCADA system [16]. Yardley et al. propose a pedagogical framework to promote a modular learning platform in smart grid security [17]. It is clear, however, that these approaches do not focus on hands-on learning experiences.

In the past few years, there have been efforts to implement a SCADA security course in the academic curriculum [18]. This course focuses on understanding SCADA security concepts, and the need for SCADA system security in academia and its role in Australia's critical infrastructure. Although a good example of curriculum for CPS education, this is a specialist engineering course targeting a graduate program.

There are a limited number of institutions that offer limited training programs for CPS security. InfoSec Institute offers a 5-day course in SCADA security architecture [19]. SANS Institute also has a five-day training course called ICS410 ICS/SCADA Security Essentials [20].

III. Background

A CPS can be described as an integration of computation, networking, and physical processes [21]. Typically, a CPS is a complex and interconnected system, organized into multi-layer hierarchies that contain numerous embedded control nodes with different functionalities. A CPS has three layers of control and computation (see Figure 1):

- The lowermost level in the hierarchy is the *infrastructure layer* that contains sensors, actuators, and the physical process.
- The *regulatory layer* includes a Programmable Logic Controller (PLC) and a Remote Terminal Unit (RTU) that govern the physical process through interaction with the supervisory and plant layers.
- The *supervisory layer* consists of a SCADA or a Human-Machine Interface (HMI) that monitors as well as controls the system via the regulatory controllers.

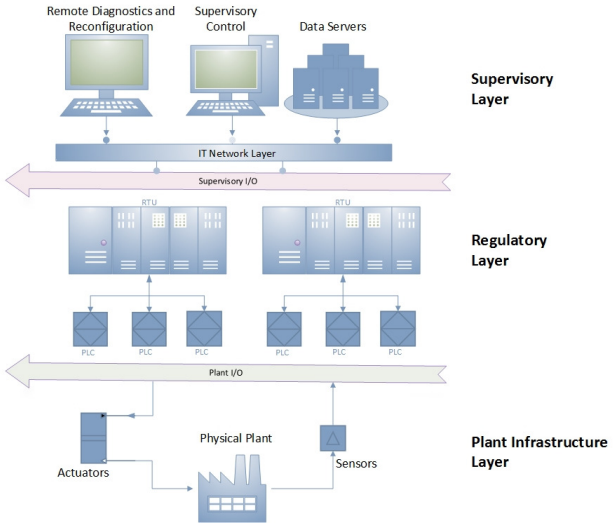

Figure 1. Hierarchical topology of a CPS

The RTU and PLC components in the regulatory layer are custom embedded controllers that interact with the supervisor through the IT network telemetry. A similar network channel exists for reconfiguration and remote diagnostics used for firmware updates and troubleshooting issues. The IT network layer connects to the regulatory layer making the embedded controllers susceptible to malicious reconfiguration that not only violates the network integrity of the channel, but also threatens the integrity of the physical process since the regulatory layer interacts directly with the components of the plant infrastructure.

These multi-layered hierarchical systems are responsible for timely information exchange, computation, and process control. CPS leaf nodes are interfaced through RTUs for interaction with the IT infrastructure. Conforming to the conventional cyber-physical control, our testbed implements regulatory controllers interfaced with the cyber network and a Rotary Inverted Pendulum (RIP) application as the physical process shown in Figure 2.

The ZedBoard implements a PLC leaf node with supervisory and reconfiguration channels interfaced through an RTU. This PLC node contains the control loops that govern the physical process, the RIP system in our testbed. As shown in Figure 2, a Raspberry Pi serves as the RTU, mediating communication between the ZedBoard and IT network. The first author's thesis elaborates on the implementation of these components and their functions in different layers of the system, and also describes the Trustworthy Autonomic Interface Guardian Architecture (TAIGA) technology countermeasures developed for Stuxnet-like threats to CPSes [22]. A lab guide is being derived from the thesis and will be publicly available. The generic lab modules apply to any standard CPS setup although the details may vary, and illustrate CPS vulnerabilities by performing different tasks to penetrate into the leaf-node controllers. This work helps students understand the basic steps required of the designer to improve security.

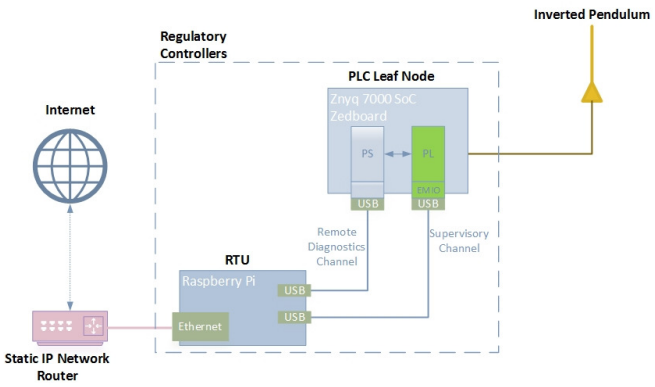

Figure 2. Testbed with a CPS topology

IV. Overview of the Modules

A. Learning Aspects

All computing and technology programs should ensure a thorough and pervasive security curriculum within their courses. Not only would the lack of a strong security curriculum disadvantage students, but it would also be detrimental to have students trained with advanced technical skills but lacking in security awareness. Such an exclusion would almost certainly result in the systems designed by these graduates containing potential security vulnerabilities.

It is widely accepted that learning-by-doing is one of the most effective ways to learn [23], [24]. Ma et al. studied different methods of laboratory instruction and concluded that hands-on and remote labs help to build design skills and conceptual understanding in students [25]. The labs we describe here allow students to select tools and methodologies to come up with open-ended solutions to better understand the importance of cybersecurity in real CPSes. As emphasized by Rowe [11], these labs should not be exclusively connected to a particular technology, but rather should focus on concepts, methodologies, and skills. Extending this premise, the CPS security labs focus on using many different modules to understand a CPS environment and its vulnerabilities.

Reflective Practice: The main idea is to implement a reflective practice approach that can refocus students' skills and knowledge to these hands-on security modules. Reflective learning involves using practical experiences and developing skills that are essential for problem solving and decision making [26]. Using a reflective approach, students can establish a theoretical knowledge base reinforced with practical hands-on modules. The modules can be aligned with Hinett's four-step [27] reflective approach that enables students to:

1) *understand what they already know,*
   The modules introduce the CPSes and leverage the students' understanding of different network protocols and tools.
2) *identify what they need to know in order to advance understanding of the subject,*
   The modules establish a roadmap to introduce the CPS system architecture and present the various components.
3) *make sense of new information and feedback in the context of their own experience,*
   The modules actively engage the students in a series of incremental tasks and collect reflective feedback on this newly gained knowledge.
4) *guide choices for further learning.*
   These modules can help encourage students to relate this experience to industry practice and open new cybersecurity outlooks.

B. Organization of the Modules

The modules are organized in an incremental fashion to understand the vulnerabilities in each control system layer penetrated to gain access to the leaf-node controllers. Each module includes the following components: Learning Objectives, Tools, Assumptions, and Hands-on Exercises.

The Stuxnet worm was designed to sabotage industrial processes controlled by Siemens SIMATIC WinCC and PCS 7 control systems. It exploited at least four zero-day vulnerabilities to install, infect and propagate itself and was covert enough to evade state-of-the-art security technologies and procedures [2]. One of the key takeaways from this example is how complex and interconnected a typical control system is. We know that potential pathways exist from the outside world, through the enterprise IT network and down to the process controllers. As illustrated in Figure 3, Eric Byres et al. summarize various pathways in an attack graph that Stuxnet used to reach its target processes [28]. To secure critical infrastructure, it is important to understand the complexity of these systems that are now the target of Stuxnet-like attacks. In particular, security programs need to:

1) Consider all possible infection pathways and develop strategies for mitigating those pathways.
2) Recognize no protective security measure is perfect, and take steps to understand the vulnerabilities in each of the CPS layers to limit the consequences of a compromise.
3) Look beyond the traditional network layer security and towards securing the local communication between a PLC and RTU.

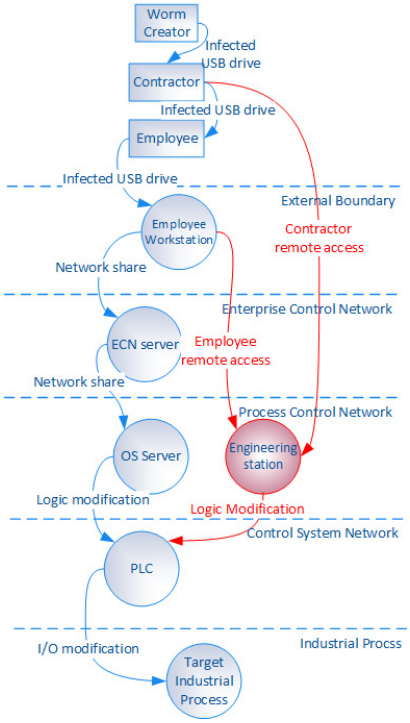

Figure 3. Stuxnet attack graph

4) Include security assessments and testing as part of system development. Perimeter security should be augmented with an independent last line of defense.
5) Work to improve the awareness in security of critical infrastructure and enable students to build relevant skills across industries.

Table I
OVERVIEW OF THE HANDS-ON MODULES

Module Name	SHODAN	SSH MITM attack	Replay attacks	Reconfiguration attacks
Learning Objectives	Search engine exploitation, vulnerability assessment	SSH1 vs SSH2, ARP poisoning	Packet capturing, video streaming	Memory corruption, exploiting the boot image
Tools Used	SHODAN, google hacking	PuTTY, Python, Cain and Abel, processing	MJPG streamer, Wireshark, Ettercap	Linux terminal
Tasks	• Using SHODAN search engine to find systems connected to the Internet. • Accessing the security vulnerabilities in the spotted unsecured devices. • Learning the importance of vulnerability assessment and creating awareness about CPS security.	• To use Address Resolution Protocol (ARP) poisoning to intercept packets transferred and execute Man-in-the-Middle (MITM) attacks. • To use network security testing software such as Cain and Abel to intercept Secure Shell (SSH) login credentials. • Understand the different versions of SSH and how SSH-2 is much more secure than SSH-1.	• To understand the basics of packet capture and finding the data inside them. • Using Python libraries (such as Socket) to write scripts to help execute the replay attack. • To perform a replay attack on a Raspberry Pi Camera Module by exploiting the video streaming service in Linux.	• To modify the reconfiguration channel to modify the boot image and gain system information using the memory debug channel.
Assessment	Demonstration of the solution and feedback from the hands-on exercises			

This work mainly focuses on demonstrating the vulnerabilities of CPSes to cyber attacks with the goal of making CPS designers aware of security issues. All the modules are developed to have a generic nature that can be applied to different CPS settings. These modules focus on understanding and exploiting the vulnerabilities that affect these systems. Students are exposed to exploitation techniques and tools that may be used against these systems. Similar to the Stuxnet attack flow, the modules incrementally gain access to the controller regulating a physical process.

Our intent is to augment an existing course with hands-on experience in critical infrastructure and control systems security. Perhaps the greatest value of this modular approach lies in the potential to adopt modules as supplements to other courses on cyber security, embedded systems, or control systems. The key to advancement in this field lies in the recognition of the multi-disciplinary nature of CPS security. Table I provides a brief overview of the modules.

V. Network Layer Modules

In a CPS, embedded controllers govern a physical process based on operator commands. Increasingly, the need for remote monitoring and control entails a networked CPS environment. A networked interface for the supervisory layer in a CPS is a means for effective and timely flow of information between plant supervisors and processes. Supervisory interaction with the RTU accessible via the Internet introduces a set of diverse security issues. Network integrity attacks exploit the IT network vulnerabilities that can lead to an adversary communicating with the Process Control System (PCS). We summarize the network integrity attacks as:

1) Man-in-the-Middle (MITM) attacks: In a MITM attack, the adversary can use known methods like ARP poisoning and intercepting network packets to view or modify sensitive data sent by the operator to the CPS component. Sending false messages may cause the operator to believe that the plant is functioning correctly in spite of an active attack.
2) Eavesdropping attacks: Eavesdropping refers to an attack where an adversary can intercept one or more communication channels in a CPS. Although a passive attack, CPS can be particularly susceptible to eavesdropping through network traffic analysis such as intercepting the data transferred by HMIs and commands sent by operators.
3) Denial of Service (DoS) attacks: In a DoS attack, the adversary can prevent legitimate requests for network resources from being processed by the system. DoS is a type of network attack that prevents the system from functioning normally [29]. These attacks initially target the communication interfaces to deactivate supervisory monitoring and interaction with the PCSes. Once the adversary penetrates the CPS, the adversary can tamper with various aspects of the system, such as:
   - Overloading the controller by sending a large number of commands.
   - Sending false sensor data, which may cause abnormal process behavior.
   - Block access to networked resources that can result in loss of access by the supervisor.

The network layer consists of the operator units that connect to the regulatory layer containing the PLCs. In this section, we discuss two attack modules that describe methods to penetrate the network layer to gain access to RTU.

A. SHODAN Search Engine Lab

This module describes the SHODAN search engine that can be used to discover devices connected to the Internet. SHODAN can be used to find PCSes and SCADA systems and their open services. This information can be used to access the underlying systems by exploiting protocol vulnerabilities and inadequate security policies. This lab module consists of the following key components:

1) SHODAN search engine: Understanding basic operations of the SHODAN search engine and using the SHODAN website to find PLCs, routers, web cameras, and open services like telnet.
2) SHODAN Command-line Interface (CLI): Using the SHODAN CLI enabled in Python to get an overview of SHODAN commands to perform advanced search queries.

At the end of this lab, the students will learn:

1) How we can find many traffic lights, security cameras, home automation devices, and heating systems connected to the Internet with very few or no security safeguards.
2) The importance of having proper security in place to design a system with the least number of vulnerabilities.
3) How these tools can be used to avoid cyberattacks by finding these unsecured, connected devices and services using SHODAN, and alerting owners and operators about the vulnerabilities.

B. Man-in-the-Middle Attack Lab

This module uses a SSH downgrade connection to perform a MITM attack to sniff SSH credentials. This attack can be accomplished by downgrading the connection from a more secure protocol (SSH-2) to a less secure protocol (SSH-1) by deceiving the parties into thinking that one or more clients can only support the less secure protocol. This lab module consists of the following key components:

1) SSH protocol: Understanding the difference between SSH-1 and SSH-2.
2) ARP poisoning: Using ARP poisoning to create a MITM scenario and exploit the weak password authentication method in SSH-1.

At the end of this lab, the students will learn:

1) How ARP poisoning can be used to intercept packets transferred and execute a MITM attack.
2) How to use network security testing software such as Cain and Abel to intercept SSH login credentials.
3) The different versions of SSH and how SSH-2 is much more secure than SSH-1.

VI. Regulatory Layer Modules

In this section, we discuss the supervisory components of a CPS and their security vulnerabilities. A supervisory system consists of a HMI system with read-only or supervisory access control. A supervisory workstation collects information from process sensors connected via a supervisory channel and presents that information through Internet-facing web portals. HMIs allow operators to start and stop process cycles, adjust set-points, and perform other functions required to adjust and interact with control processes.

Although securing the channel is one of the important aspects of ensuring resilience, attackers can disrupt the physical process by exploiting this channel using valid set-points but issued in a manner that can damage the physical process. An active adversary may attempt to manipulate message routing and network coordination by injecting messages, recording and replaying old ones, or exploiting protocol interactions. A combination of these attacks can be used as a platform for a more stealthy attack if the adversary gains access to reconfiguration resources. In this section, we discuss various attacks that can disrupt the functioning of the system by manipulating the processes managed by the RTU:

A. Replay Attack on Processing GUI Lab

This attack targets the client HMI interface, namely the Processing Graphical User Interface (GUI), that receives real-time process information and displays it on all the clients. This lab module consists of the following key components:

1) RTU webserver manipulation: Using the RTU access (achieved as a part of the MITM lab) to capture and modify data sent to the Processing GUI.
2) Scripting the replay attack: Use tools such as Wireshark [30] for packet capturing and Python Socket library to replay the modified packets.

At the end of this lab, the students will learn:

1) The basics of packet capture and extracting the data inside them.
2) Using Python libraries (such as Socket) to write scripts to help execute a replay attack.

B. Replay Attack on the Web Camera Lab

This attack targets the remote surveillance component of the system provided by the web camera. In this attack, the adversary attempts to transmit an old camera feed to the client. This lab consists of the following key components:

1) Capturing images of the working system using access to the RTU.
2) RTU video-streamer modification: Modifying the streamer application on the RTU to stream new images to perform a replay attack.

At the end of this lab, the students will learn:

1) Using Wireshark to sniff packets of web camera live data.
2) Using MJPG-Streamer to modify the video streaming software to execute the replay attack on the web camera.

C. Supervisory Set-point Violation Attack Lab

This attack exploits the physical process by using a combination of legitimate set-points through the supervisory channel, but executed in a custom manner. In order to disrupt the pendulum process using valid set-points, the process should be monitored to gain an understanding of the operational guards and set-point commands. This lab consists of the following key components:

1) Physical plant process: Understanding the physical process and supervisory commands used to control the process.
2) Python script: Using Python to develop a script to issue set-point commands to sabotage the physical process.

At the end of this lab, the students will learn:

1) How to exploit the supervisory channel to disrupt the physical process.
2) Using Python libraries (such as Socket) to write scripts to help execute the set-point violation attack.

VII. Reconfiguration Layer Modules

In the previous section, different attack modules were discussed that explored the weaknesses in a RTU and attacks that exploit the supervisory system. These attacks can be combined with reconfiguration attacks on the controller that are more stealthy in nature. At times, exploitation of CPSes requires adaptive behaviour in the presence of faults [31]. Reconfiguration attacks can be executed by reading values of variables, executing functions and procedures, and performing input/output. All of these operations are performed in modern microcontrollers by reading/writing specific memory addresses. For example, remote diagnostic ports can be exploited allowing adversaries to access the same debugging tools as the system developers. An adversary can then read symbol tables, read/write memory, and cause the processor to start execution from a certain address. Most modern CPSes provide a remote diagnostics channel that

is responsible for controller debug and update. After getting access to this channel, an adversary can execute many attacks while maintaining a certain level of stealthiness, for example by executing a remote memory dump or reading/writing critical variables.

This section presents two modules that exploit the reconfiguration/remote diagnostics channel:

A. Memory Debug Channel Lab

An adversary can exploit the memory debug channel realized through the remote diagnostics channel to understand the controller algorithm and system organization. This lab consists of the following key components:

1) Memory read/write: Understanding read/write access to On-Chip Memory (OCM) of the processor system.
2) Channel access: Sending the memory read/write commands through the memory debug channel.

At the end of this lab, the students will learn about:

1) Exploiting the remote diagnostics channel to access the memory debug channel.
2) Reading and writing controller memory to gain system knowledge.

B. Boot Image Update Lab

An adversary can modify the boot image used by the system. This lab consists of the following key components:

1) Boot process: Understanding the boot process in the PLC.
2) Boot image: Understanding the contents of the boot image BOOT.BIN.
3) Image transfer: Using the remote update channel to modify the boot image in the Secure Digital (SD) card.

At the end of this lab, the students will learn about:

1) Exploiting the reconfiguration channel to corrupt the memory boot image.
2) Modifying and sending the boot image through a Universal Asynchronous Receive Transmit (UART) channel and replacing the file on the SD card.

VIII. Evaluation and Discussion

The experience gained from these hands-on modules can be categorized as follows:

- **Benefits:** This project creates a mock CPS testbed by repurposing existing undergraduate control system instruments connected to low cost commercial-off-the-shelf boards, and avoids any large up-front investment compared to more expensive and proprietary SCADA hardware testbeds. These modules provide a comprehensive view of CPS complexity and heterogeneity, and an interactive approach to understanding security vulnerabilities.
- **Limitations:** In the current implementation, students need access to the internal private static router to successfully complete all the modules.
- **Assessment:** Undergraduate computer engineering students were actively involved in developing these modules in order to collect feedback and implement changes to better suit the students targeted by this work.

An evaluative survey was developed to gauge students' understanding in the subject of critical infrastructure cybersecurity. The idea is to understand student perceptions by administering a survey before and after module presentations. The survey was completed by participating students. Here is a representative response obtained from one of the students:

Sample Student Response

1) For a critical infrastructure under operation, what is more important: network security or process reliability?
   Student response: ***4, process reliability***
   A process with good error handling and correction can overcome a network compromise, while a good network but unreliable process will usually yield unsatisfactory results.
2) How effectively can IT security measures protect a CPS?
   Student response: ***3, somewhat effectively***
   Network security is so easy to compromise nowadays, it almost seems like a non-issue for hackers.
3) How vulnerable are Internet-connected systems, and how easily can such systems be detected?
   Student response: ***5, highly vulnerable***
   If a device is open to the Internet, it gives a hacker a 24/7 window to remotely attempt any hacking technique.
4) How secure are network protocols to protect from attacks like man-in-the-middle?
   Student response: ***3, somewhat secure***
   Depending on the attack and the protocol, man-in-the-middle attacks may be completely blocked, or completely overlooked.
5) Is the software update process used by computers in a CPS a good solution or a major issue in process reliability?
   Student response: ***1, good solution***
   When tested, updates can effectively patch known exploits.
6) What is your understanding of CPS hardware, software, communication, and control of physical processes?
   Student response: ***3, some understanding***
   I have limited experience outside of working with

TAIGA over this past summer.

7) How likely are you to pursue a career that involves security of critical infrastructure?
Student response: ***4, likely***
The demand for jobs in embedded systems seems to be heading in the direction of security. With a large number of positions available, I'm sure that I will consider security in systems that I work with in almost all of my career positions.

Comments: *My experience over this past summer working with TAIGA was very informative. It taught me a lot about working in an environment that was unfamiliar. My first week or so of working with TAIGA was spent getting up to speed on the project they were working on. Once I had a grasp of the project, I was given the job of finding ways to break the system. It was a very open-ended job and allowed for a lot of creativity on my part. I learned much more than I would have in a classroom setting, as security and practicality of my solutions, and of TAIGA in general, were high priorities.*

The survey helped us understand the students' assessment of the material. A lab setting with open-ended tasks helped the students learn on their own and evaluate the feasibility of their solutions. It helped us understand the basic awareness amongst the students about cyber threats to critical infrastructure, their interests in the field of security, and ideas about design of embedded systems. Also, it served as an aid in evaluating student understanding of a CPS system, differences between IT and CPS security, and the importance of process reliability in CPSes.

IX. Conclusions

This work explored conventional CPS topologies to understand cyber attack vectors, and defined various modules to illustrate a possible attack pathway to compromise a process controller. A modular approach provides a open-source, hands-on experience that emphasizes the unique aspects of a CPS and raises students' awareness and skills in this field.

The effectiveness of the SHODAN search engine shows how various home automation systems, traffic lights, security cameras, and SCADA systems are connected to the Internet with very few or no security safeguards in place. While this search engines exposes the lack of security measures in Internet-connected devices, these vulnerabilities can be exploited to perform protocol downgrade attacks by using ARP poisoning. The regulatory layer provides the supervisory control and monitor functionalities. Protecting this layer is imperative since the overall security of a control system network could be weakened if the supervisory system becomes an open attack vector to the CPS. These modules discuss how an adversary can manipulate message routing and network coordination to perform replay and set-point violation attacks. A combination of these attacks can enable more stealthy damage if the adversary also gains reconfiguration resources. The memory debug channel can be exploited to gain system information, whereas the system boot image can be corrupted by maliciously accessing the update channel. These modules show how an adversary can ultimately gain access to the process controller.

Motivated by the Stuxnet worm's demonstration of CPS vulnerabilities, these modules highlight potential ways to remotely compromise a physical process. A mock testbed is created with commercial-off-the-shelf hardware, which makes it economical and easy to replicate. This courseware exposes students to a wide range of network tools and software, specific knowledge of device architectures, and low-level programming techniques for representative CPS hardware and software. This work emphasizes thorough understanding of threats and their impacts, and bridges the IT and CPS domains just as real attacker would. Cyber defense involves preventative measures to protect systems. We highlight the defense strategies by presenting appropriate network- and system-level topics.

In future, this courseware will be evaluated for pedagogical effectiveness. A comprehensive framework is being developed which can be integrated in a curriculum for critical infrastructure security. Future work will include setting up a virtual machine environment to allow experimentation to take place without physical access and introducing forensic data analysis and risk management.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant Number CNS-1222656. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. We are grateful for ZedBoard and tool donations from Xilinx, Inc.

References

[1] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," *Critical Infrastructure Protection*, vol. 253, pp. 73–82, 2007.

[2] D. Kushner, "The real story of Stuxnet," *Spectrum, IEEE*, vol. 50, no. 3, pp. 48–53, March 2013.

[3] R. M. Lee, M. J. Assante, and T. Conway, "ICS CP/PE Cyber-to-Physical or Process Effects Case Study German Steel Mill Cyber Attack," https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf, Sans ICS, Dec 2014.

[4] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response," in *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*. ACM, 2011, pp. 355–366.

[5] E. Luiijf, "Understanding cyber threats and vulnerabilities," in *Critical Infrastructure Protection*. Springer, 2012, pp. 52–67.

[6] The White House, "Executive Order: Improving Critical Infrastructure Cybersecurity," https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity, Feb 2013.

[7] Department of Homeland Security, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," http://www.dhs.gov/homeland-security-presidential-directive-7, Dec. 2003.
[8] "National SCADA Test Bed," http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf, 2003.
[9] Daniel Noyes , "Cyber Security Testing and Training Programs for Industrial Control Systems ," https://inldigitallibrary.inl.gov/sti/5411182.pdf, Mar. 2012.
[10] Michael J. Assante, "Testimony on Securing Critical Infrastructure in the Age of Stuxnet," http://www.hsgac.senate.gov/hearings/securing-critical-infrastructure-in-the-age-of-stuxnet, Nov. 2010.
[11] D. C. Rowe, B. M. Lunt, and J. J. Ekstrom, "The role of cyber-security in information technology education," in *Proceedings of the 2011 Conference on Information Technology Education*, ser. SIGITE '11. New York, NY, USA: ACM, 2011, pp. 113–122. [Online]. Available: http://doi.acm.org/10.1145/2047594.2047628
[12] R. K. Raj, S. Mishra, C. J. Romanowski, and T. M. Howles, "Cybersecurity as General Education," http://cisse.info/resources/archives/category/16-papers?download=187:16-2011.
[13] T. Howles, C. Romanowski, S. Mishra, and R. K. Raj, "A holistic, modular approach to infuse cybersecurity into undergraduate computing degree programs," in *Annual Symposium On Information Assurance (ASIA), Albany, NY*, 2011, pp. 7–8.
[14] J. E. Huss, "Laboratory projects for promoting hands-on learning in a computer security course," *SIGCSE Bull.*, vol. 27, no. 2, pp. 2–6, Jun. 1995. [Online]. Available: http://doi.acm.org/10.1145/201998.202000
[15] V. J. H. Powell, C. T. Davis, R. S. Johnson, P. Y. Wu, J. C. Turchek, and I. W. Parker, "Vlabnet: The integrated design of hands-on learning in information security and networking," in *Proceedings of the 4th Annual Conference on Information Security Curriculum Development*, ser. InfoSecCD '07. New York, NY, USA: ACM, 2007, pp. 9:1–9:7. [Online]. Available: http://doi.acm.org/10.1145/1409908.1409918
[16] D. Navarro, J. C. Mendez, K. Berrios, E. Ortiz-Rivera, and E. Arzuaga, "Using cybersecurity as an engineering education approach on computer engineering to learn about smart grid technologies and the next generation of electric power systems," in *Frontiers in Education Conference (FIE), 2014 IEEE*. IEEE, 2014, pp. 1–8.
[17] T. Yardley, S. Uludag, K. Nahrstedt, and P. Sauer, "Developing a smart grid cybersecurity education platform and a preliminary assessment of its first application," in *Frontiers in Education Conference (FIE), 2014 IEEE*, Oct 2014, pp. 1–9.
[18] J. Slay and E. Sitnikova, "Developing SCADA Systems Security Course within a Systems Engineering Program," in *12th Colloquium for Information Systems Security Education*, Nov 2011.
[19] InfoSec Institute, "SCADA Security Course," http://www.infosecinstitute.com/courses/scada_security_training.html#learn/.
[20] Eric Cole and Eric Cornelius and Justin Searle, "ICS/SCADA Security Essentials," https://www.sans.org/course/ics-scada-cyber-security-essentials.
[21] F. Hu, *Cyber-Physical Systems: Integrated Computing and Engineering Design*. CRC Press, 2013. [Online]. Available: https://books.google.com/books?id=PGPSBQAAQBAJ
[22] P. Deshmukh, "A hands-on modular laboratory environment to foster learning in control system security," Master's thesis, Virginia Tech, Blacksburg, VA, Feb. 2016.
[23] M. M. Lombardi, "Authentic learning for the 21st century: An overview," *Educause learning initiative*, vol. 1, no. 2007, pp. 1–12, 2007.
[24] P. M. Stohr-Hunt, "An analysis of frequency of hands-on experience and science achievement," *Journal of research in Science Teaching*, vol. 33, no. 1, pp. 101–109, 1996.
[25] J. Ma and J. V. Nickerson, "Hands-on, simulated, and remote laboratories: A comparative literature review," *ACM Computing Surveys (CSUR)*, vol. 38, no. 3, p. 7, 2006.
[26] J. Mezirow *et al.*, "How critical reflection triggers transformative learning," *Fostering critical reflection in adulthood*, pp. 1–20, 1990.
[27] K. Hinett and T. Varnava, *Developing reflective practice in legal education*. Citeseer, 2002.
[28] "How Stuxnet Spreads: A Study of Infection Paths in Best Practice Systems," White Paper, Toinfo Security, Feb. 2011.
[29] T. H. Morris and W. Gao, "Industrial control system cyber attacks," in *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research 2013*. BCS, 2013, pp. 22–29.
[30] Ulf Lamping and Richard Sharpe and Ed Warnicke, "Wireshark 2.0," Available at https://www.wireshark.org/.
[31] R. C. Pinto and J. Rufino, "Exploiting non-intrusive monitoring in real-time embedded operating systems." in *EWiLi*, 2014.