A Customized Educational Booster for Online Students in Cybersecurity Education

Mohamed Rahouti[1,4][a] and Kaiqi Xiong[2,3,4][b]
[1]*Department of Electrical Engineering, University of South Florida, Tampa, FL, 33620, U.S.A.*
[2]*Cyber Florida, University of South Florida, Tampa, FL, 33620, U.S.A.*
[3]*Department of Mathematics and Statistics, University of South Florida, Tampa, FL, 33620, U.S.A.*
[4]*Intelligent Computer Networking and Security Lab, University of South Florida, Tampa, FL, 33620, U.S.A.*

Keywords: Cyber Security, Applied Cryptography, Computer Networking and Security, Virtual Environment, Online Teaching.

Abstract: Real-world lab experiments have been an integral part of computer science and engineering curriculums. However, human and computing resources as well as financial support to courses may be limited at many universities ranging from small to large universities and from liberal arts colleges to top research universities as there is a dramatic increase of student enrollments in computer science and engineering for the past ten years. Nowadays, like many other universities nation wide, University of South Florida (USF) in collaboration with the Cyber Florida center offers online cyber security degrees as well as certificates. Throughout such programs, online students are expected to acquire knowledge via an interdisciplinary set of core courses prior to taking a deep dive into one of four following concentrations: cyber intelligence, digital forensics, information assurance and computer security fundamentals. However, when it comes to training student with real-world cyber security labs, both instructors and students face various challenges with regard to resources and virtual environment for exploring and running a broad range of security experiments and tests. In order to achieve the goal of our funded NSF project, in this paper we will discuss our teaching contributions to the development of a broad range of cyber security labs, facilitation of applied cryptography learning through experimental modules, and our customized virtual machine that fits the needs of various online computer networking and security courses. Specifically, we will first present our methodology for the design of our experimental modules and then present in details our pre-built Linux-based portable virtual machine. Those learning and experimental modules have been developed at different levels to meet the need of students with different academic and industrial backgrounds.

1 INTRODUCTION

In recent years, technological advances have lead to revolutionary improvement and facilitation of e-learning through smart educational systems. Therefore, it becomes very important to befit a broad range of subjects and teaching materials into curriculums that fulfil the industrial and technological requirements and goals (Bauer et al., 2018).

Moreover, because of the dramatic increase of all technologies and practices of computer systems and electronic data, living in a world where more and more of our social lives and business are online, cyber security is an enormously growing area.

In the past, people widely considered cyber security as an IT department's responsibility. It was naively thought that as long as proper security tools and software (e.g., firewall, antivirus, encryption/decryption protocols, etc.) were put in place, people could just neglect concerns security problems and left them for IT departments to deal with.

These days, the international research and advisory firm, *GartnerInc*., estimates spending on security worldwide to pass 96.3 billion dollars by the end of 2018, which is about 8% increase within one year. In addition, for the last several years, the need for shielding and protecting information from illegitimate usage/access and malicious actors has evolved at the highest levels of institutions, business and government.

[a] https://orcid.org/0000-0001-9701-5505
[b] https://orcid.org/1111-2222-3333-4444

Rahouti, M. and Xiong, K.
A Customized Educational Booster for Online Students in Cybersecurity Education.
DOI: 10.5220/0007767205350541
In *Proceedings of the 11th International Conference on Computer Supported Education (CSEDU 2019)*, pages 535-541
ISBN: 978-989-758-367-4

Moreover, with an increasing cybercrimes that affect the government, individuals, and organizations, online cyber security certificates or degrees help remote students (could even be overseas in military duties sometimes) to pursue new opportunities that permit them to contribute in maintaining information and data secure from illegitimate usage. In the online teaching, the curricula must align with the material on cyber security certification exams such as Certified Information Systems Security Professional (CISSP), Security +, and Information Systems Audit and Control Association (ISACA) exams. Therefore, the curricula should be designed in a suitable way to befit hands-on skills and requirements of cyber security industry, whereas the university must guarantee the availability of all necessary tools and resources for students to practice and apply teaching material relevant to the workplace.

However, there exist various difficulties and key challenges with regard to the teaching of cyber security in the educational structure of online courses. These difficulties range from, but are not limited to, the broad range of student backgrounds and availability of computing resources (e.g., computers, network devices, software). Based on our past teaching experience of the Applied Cryptography, a core course in the curriculum of the online cyber security program at the University of South Florida, students enroll in the program with weak computer science and mathematics background, for example, without the completion of some basic computer science courses, such as operating system basics, computer networking fundamentals, computer programming skills, etc. According to a recent survey we conducted in our course, more than 70% of total students do not have any computer science and security background, where many students come from a completely unrelated educational background, e.g., sociology, business, music studies.

Moreover, the insufficiency and or even lack of hardware resources at universities (i.e. computer labs) is another grand challenge that limits students capability to practice advanced cyber security labs. Students are not in local, so it is very inconvenient or even infeasible for students to come to the university campus to work on their assigned labs. These remote students could be overseas in military duties or work displacement, which renders it impossible for them to utilize physical labs at the Such key challenges place obstacles for implementations of suitable infrastructure of such smart teaching. Furthermore, difficulties of guaranteeing virtual resources, such as remote virtual access to computers in physical computer labs might even aggravate when labs require multiple machines for running fundamental security experiments (e.g., Client-sever communication, intrusion detection systems, Denial of Service and Distributed Denial of Service attacks, and Man-in-the-Middle attack), or even powerful computation and networking resources (e.g., hardware memory and Internet speed).

In our past teaching for different cyber security courses and workshops, we have developed a broad range of hands-on labs. Our readily-available experimental labs are conducted in our own pre-built virtual machine image as we have installed and customized all the necessary libraries, tools, and software that are needed to accomplish such a diverse range of security and cryptography labs. Students only need to be handed our virtual machine and run it on their own computers using a cross-platform virtualization application (e.g., VirtualBox and VMware) that will let them run our virtual operating system on their computers.

The rest of this paper is organized as follows. Section 2 presents an explanatory and detailed overview of some efforts that were done in the past to enhance and facilitate online cyber security learning experience. Section 3 then presents our research efforts towards the development of a broad range of cyber security labs and experimental modules, as well as our developed virtual environment for online computer networking and security courses in general and online Applied Cryptography in particular in order to achieve the goal of our funded NSF project. In Section 4 we present a taxonomic overview of students experience assessment. Finally, in Section 5 we discuss our future work. We then conclude our research study in Section 6.

2 RELATED WORK

In the past, many online educators have investigated the advantages and disadvantages of online courses (Kinnunen and Eriksson, 2018). The pros and cons strictly rely on all parties of the online instructional process, instructors, students, and the university.

In brief, Fedynich (Fedynich, 2013), Cook (Cook, 2007), and Baleni (Baleni, 2015) provided a taxonomic overview of the advantages as: (1) flexibility of where and when to study, (2) feasibility of a broad range of teaching mechanisms, and (3) efficiency in term of cost for universities. Importantly, Cook (Cook, 2007) highlighted more critical pros of the online teaching, such as (1) the freedom for study pace adjustment, (2) possibility of adopting particular teaching techniques that are impractical in traditional

(face-to-face) teaching, such as virtual platforms and virtual simulations (particular types of virtual laboratory as presented in Figure 1), and (3) easiness of delivering prompt and synchronous feedback and formative performance assessments.

On the other hand, there are numerous cons and challenges of online teaching. In summary, typical online courses (1) impose students to have computers and online access, as well as (2) might have a weak instructional design and (3) scarcity of face-to-face interactions that could lead to the poor performance of students (Fedynich, 2013), (Cook, 2007).

Additionally, teaching an online cyber security course is even more challenging. More challenges might add-up to the aforementioned list. Such courses require advanced resources, e.g., computationally powerful computers, cryptographic libraries and software, and multiple physical hosts or virtual machines for particular security experimentation scenarios. Therefore, it becomes more and more challenging to help students reach their full potential in such online cyber security core courses.

Concentrating on our online Applied Cryptography for higher education (HE) involves topics on secure software development, digital signatures, symmetric-key/asymmetric-key encryptions, and ethical hacking. Such topics must be accompanied with hands-on lab modules and exercises to better help students with understanding and practicing the course concepts and material (Topham et al., 2016). It has been used in education as well Xiong et al

Willems and Meinel (Willems and Meinel, 2012) presented a software-based solution to evaluate practical cyber security labs and experiments in an online laboratory-based on a virtual machine technology. Herein, the authors guaranteed a formal parameterization of lab scenarios and implementation of a dynamic toolkit for re-configuring virtual machines and therefore adopted the training environment with according to the defined parameters. Xiong and Pan (Xiong and Pan, 2013) presented an education approach to deploy ProtoGENI, one of GENI testbed resources, for teaching computer networking. Particularly, they have designed various capstone projects and lab modules that provide students with an opportunity to utilize a real-world testbed for different learning and research purposes.

While Sharma and Sefchek (Sharma and Sefchek, 2007) surveyed different types of laboratories for cyber security teaching and learning, Mirkovic and Benzel (Mirkovic and Benzel, 2012) introduced *DeterLab*, an open Emulab-based technology experimental facility sponsored by the US National Science Foundation and Department of Homeland Security. This lab is hosted by USC/ISI and UC Berkeley. This experimental facility is dedicated for online cyber security teaching, where students can reserve available nodes (out of 400 computing nodes in total) through a web-based interface. However, the students are only permitted to posses the virtual sessions to these computing nodes for a very short period of time in order to grant as many users as possible access to the lab resources.

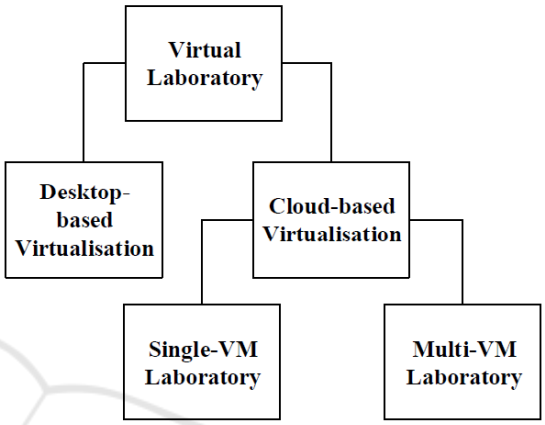

Figure 1: Virtual laboratory hierarchy.

Differently from previous teaching efforts that lack convenience and easiness for online cyber security teaching. In this paper, we discuss and detail our efficient academic guidelines in offering a readily-available virtual environment for online cyber security teaching along with a broad range of cryptography and cyber security-based labs, as well as our learning and experimental modules. In our development and implementation processes, we consider students with various academic backgrounds where many of these students might lack basic computer science fundamentals and cyber security knowledge.

3 METHODOLOGY: ADOPTING INNOVATIONS

The objectives of the education research discussed here are to enhance the efficiency of teaching online cyber security courses (even our own experience was induced from our online Applied Cryptography course at the University of South Florida). In particular, this study aims at developing convenient virtual laboratory experiments that meet the needs of cyber security students with different academic backgrounds. Moreover, in our education research we investigate how our students interact with our teaching

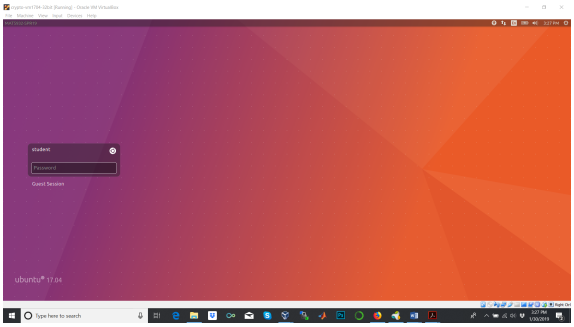

Figure 2: Our customized pre-built open-source Linux-based virtual machine.

methods and ready-to-use virtual environment for cyber security lab experiments.

3.1 Lab Development

In the past few years, we have been offering Applied Cryptography, a core course for the fully online cyber security program at the University of South Florida. This course aims at familiarizing remote students with common cryptographic building blocks, including state-of-the art techniques to encrypt data, digital signature schemes, and protocols for establishing secret keys across public networks. Students are expected to understand the strengths and limitations of common and widely used cryptographic security models, and how side-channel leakage in an unprotected implementation can subvert a theoretically strong algorithm. At the end of this course, students should know how cryptographic mechanisms secure data in today's computers and networks, and how "best practices" are applied to protect information.

Therefore, in order to fulfil such curriculum objectives, we have been dedicating great efforts to develop lab experiments that meet today's cyber security advances and needs. Given that in this program, students usually have a very broad range of academic backgrounds and many of them might even lack the fundamentals of computer systems and cyber security, and therefore, it is of a great challenge to provide labs that align with the majority of student backgrounds.

Furthermore, universities are proven cumbersome to respond to cyber security education needs. It is widely common that computer science students have to go through at least four years of the undergraduate schooling without taking any mandatory course on security (Cheung et al., 2011). Thus, such students graduate without acquiring any knowledge of cyber security. In addition, admission requirements for graduate cyber security programs enrolment at universities are not strictly imposed, and therefore students with a weak background in computer science are allowed in online graduate cyber security programs.

To consider such weaknesses in student backgrounds and to overcome the previously discussed key challenges, inspired by existing advanced cyber security labs such as SEEDLab projects (Du, 2011), we develop our own labs with detailed step-by-step instructions. These labs are shown in Table 1 and mainly focus on applied cryptography, which covers three essential mechanisms in cryptography, including secrete-key encryption, one-way hash function, public-key encryption and Public Key Infrastructure (PKI). Besides, we also cover vulnerabilities of common cryptographic algorithms. Prior to assigning these labs to students, we require them to finish an introductory lab. This lab is about downloading our virtual machine (it will be described in Subsection 3.2) and importing it into their own computers after installing an open-source virtualization platform (e.g., VMware and VirtualBox).

Moreover, we develop detailed Instructor Manuals. For the majority of our developed labs, we create corresponding manuals, which are only for instructors use. These manuals basically come from reports of graduate teaching assistants and graduate research associates. These detailed reports describe how tasks of each lab modules can be accomplished. These manuals are for the sake of assisting educators with the preparation for their labs.

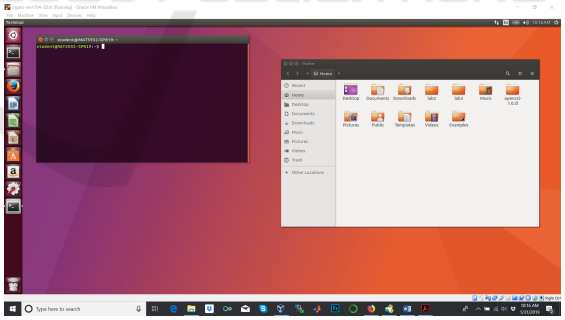

Figure 3: Our customized pre-built open-source Linux-based virtual machine is equipped and pre-configured in a convenient way to help students with a weak background to get started on course labs. It also comes with all necessary implementations of libraries and tools.

3.2 Virtual Environment Implementation

In order to address the key challenges discussed in Section 1, we have built a Linux-based virtual machine environment for students use in their lab experiments by using Ubuntu with a variety of latest ver-

Table 1: A sample of our developed labs for Applied Cryptography course at the University of South Florida.

Lab	Objectives	Duration (Hrs)
Getting started	Virtual environment set up	5
Secret Key cryptography	(1) Getting familiar with symmetric-key encryption (2)writing programs to encrypt and decrypt different messages (3) Encryption modes (4) Encryption padding (5) Initial vectors (IV)	15
Hash functions and MAC	Getting familiar with (1) hash functions and Message Authentication Code (MAC) (2) exploring strengths and weaknesses of common hash functions properties	8
Digital certificates and CA creation	Getting familiar with (1) digital certificates (2) create own certificate authority (CA) (3) signing and validation of digital certificates	8

sions for different semesters. For your information, the virtual environments depicted in Figures 2 and 3 are screen-shots taken before and after students log into the virtual machine, respectively. Based on different levels of students, we have provided the virtual machines with different levels of configurations. That is, students with better backgrounds receive less configured virtual machines. Generally speaking, the virtual machine environments are customized and adjusted to fit our online teaching goals. They are preconfigured in a convenient way to fit students with different background needs and shortages in hands-on and computer science skills. Particularly, we implement all necessary libraries, packages, and software that students need to work on our applied cyber security labs. Moreover, our virtual machine is delivered to students via the university course web page. All what students need to do is downloading the virtual machine and importing it into their own computers without the need of changing any settings or parameterization. Such a ready-to-use virtual machine provides a portable environment for our remote students such that they do not need to struggle with affording computationally powerful computers and cyber security software. Furthermore, this virtual environment is equipped with all necessary material for labs accomplishment starting from labs manuals to directory hierarchy for each corresponding lab and experimentation modules.

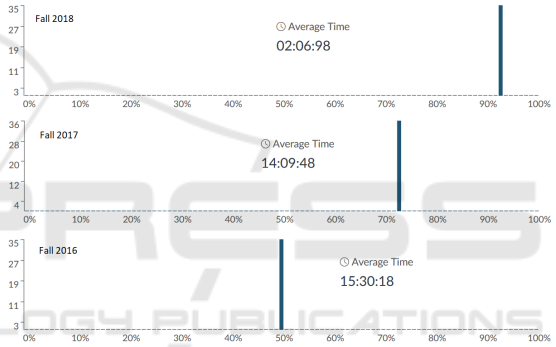

Figure 4: Students performance before and after the development of our own virtual environment and new lab modules (i.e., before and after Fall 2018, respectively).

4 EVALUATION

Figures 4 and 5 depict students assessment in our online Applied Cryptography course for three semesters in the last three years in a row, starting from Fall 2016 through Fall 2018. Stating that before 2018, we have used existing SEEdLab (Du, 2011) machine along with existing laboratories developed by the SEEDLab project. Figure 4 shows that our students performance has been enhanced since we offer them a convenient and efficient virtual environment along with newly developed labs that meet the necessities and considerations of weaknesses in student backgrounds. The overall grades were significantly improved whereas the time spent on labs dramatically decreased.

Moreover, Figure 5 shows students assessment of difficulty level of our labs for the same three semesters between 2016 and 2018. The figure demon-

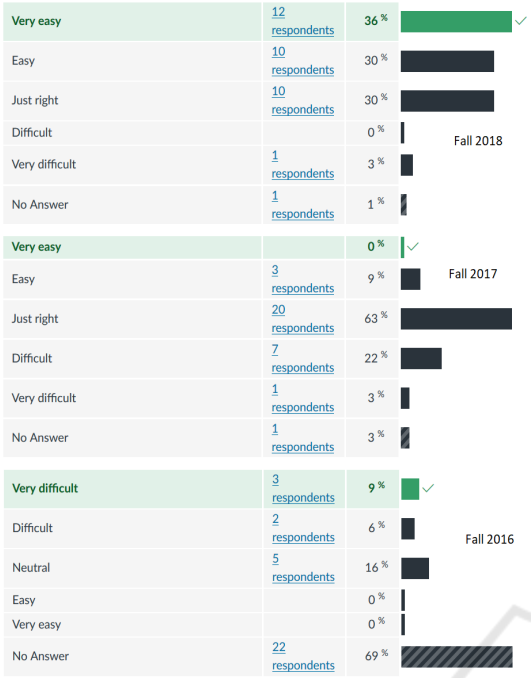

Figure 5: The feedback of our students in Applied Cryptography course regarding the difficulty level of labs before and after developing/implementing our new lab modules.

strates the satisfaction of our online cyber security students with our newly developed lab modules. It is obviously demonstrated that based on our student assessments the difficulty level of these cyber security labs has been significantly reduced. Noting that throughout these successive semesters, our labs cover the same tasks and experimentation scenarios. The reason our newly introduced labs are less difficult than previously used ones from the SEEDLab project (Du, 2011) is that our virtual machine provides students with necessary demos, training exercises, tutorials, and step-by-step manuals to understand labs content, goals, and findings. These integrated demos and manuals in our virtual machine are intended to help students who need additional tutorials and guidance to catch up on basic fundamentals, such as Linux operating system, shell scripting, OpenSSL library, etc.

5 DISCUSSIONS AND FUTURE WORK

Hands-on lab experiments have been an integral part of computer science and engineering curriculums. However, human and computing resources as well as financial support to courses may be limited at many universities ranging from small to large universities and from liberal arts colleges to top research universities as there is a dramatic increase of student enrollments in computer science and engineering for the past ten years.

As future work for facilitating and improving large-scale cyber security experimentation, we plan to adopt the Global Environment for Network Innovations (GENI), a real-world, repeatable, programmable, at-scale, virtual infrastructure for experiments in a variety of computer science areas such as networking, security, and distributed computing sponsored by National Science Foundation (NSF) (Berman et al., 2014), (Thomas et al., 2016), (Riga et al., 2016), (Chin et al., 2018).

Furthermore, Software-Defined Networking (SDN) has been a core technology in cloud computing and other cyber-physical systems where SDN facilitates network management and enables network programmability and efficient network configuration to improve network performance, monitoring, and security (Chin et al., 2017). In our future work, we will dedicate great efforts in the development of GENI and SDN learning and experimental modules for computer networking and security courses in order to achieve the goal of today's advanced cyber security needs. Specifically, we will introduce our methodology for the design of our modules and then provide the details of GENI and SDN modules including GENI account setup and resource reservation, measurement tool labs, as well as SDN labs for network traffic management and the detection and mitigation of several well-known security attacks, such as Denial of Service Attacks (DoS), Distributed Denial of Service Attacks (DDoS), phishing attacks, and Domain Generation Algorithm (DGA) malware detection. Those learning and experimental modules will be developed at different levels to meet the need of students with different academic backgrounds.

6 CONCLUSIONS

In computer science and engineering curriculums, hands-on lab experiments have been an integral part, especially in cyber security paths. However, the key challenges always relate to human and computing resources as well as financial support to such online courses. These resources could be limited at many higher education institutions ranging from small to large colleges as there is a dramatic increase of student enrollments in online cyber security programs ranging from degrees to certificates.

In collaboration with the Cyber Florida center,

University of South Florida offers accredited online cyber security programs. Throughout such online programs, remote students have the opportunity to gain knowledge through an interdisciplinary set of core courses and then take a deep dive into the field of cyber security.

Therefore, in order to fulfil the industrial needs of cyber security and while considering the aforementioned challenges, in this paper, we have presented our great efforts in facilitating the learning process of the online cyber security learning. Specifically, we have presented our methodology for the design of our modules and then given the detail of our pre-built Linux-based portable virtual environment. Those learning and experimental modules have been developed at different levels to meet the need of students with different academic and industrial backgrounds. Moreover, we provided an evaluation of our teaching experience as well as students performance in Applied Cryptography, the online cyber security course we have been teaching for the last few years. Finally, in our future work, we will bring the Global Environment for Network Innovations (GENI) testbed in classroom and integrate it with this teaching design and even conduct advanced computer networking and security laboratories.

ACKNOWLEDGEMENTS

We would like to acknowledge the National Science Foundation (NSF) who partially sponsored the work under grants #1620868, #1620871, #1620862, #1651280, and BBN/GPO project #1936 through NSF/CNS grant. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied of NSF.

REFERENCES

Baleni, Z. G. (2015). Online formative assessment in higher education: Its pros and cons. *Electronic Journal of e-Learning*, 13(4):228–236.

Bauer, M., Bräuer, C., Schuldt, J., and Krömker, H. (2018). Adaptive e-learning technologies for sustained learning motivation in engineering science. In *Proceedings of the 10th International Conference on Computer Supported Education*, volume 1. CSEDU 2018.

Berman, M., Chase, J. S., Landweber, L., Nakao, A., Ott, M., Raychaudhuri, D., Ricci, R., and Seskar, I. (2014). Geni: A federated testbed for innovative network experiments. *Computer Networks*, 61:5–23.

Cheung, R. S., Cohen, J. P., Lo, H. Z., and Elia, F. (2011). Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer ....

Chin, T., Rahouti, M., and Xiong, K. (2018). Applying software-defined networking to minimize the end-to-end delay of network services. *ACM SIGAPP Applied Computing Review*, 18(1):30–40.

Chin, T., Xiong, K., and Rahouti, M. (2017). Sdn-based kernel modular countermeasure for intrusion detection. In *International Conference on Security and Privacy in Communication Systems*, pages 270–290. Springer.

Cook, D. A. (2007). Web-based learning: pros, cons and controversies. *Clinical Medicine*, 7(1):37–42.

Du, W. (2011). Seed: hands-on lab exercises for computer security education. *IEEE Security & Privacy*, 9(5):70–73.

Fedynich, L. V. (2013). Teaching beyond the classroom walls: The pros and cons of cyber learning. *Journal of Instructional Pedagogies*, 13.

Kinnunen, P. and Eriksson, T. (2018). Teachers' viewpoint on online courses. In *Proceedings of the 10th International Conference on Computer Supported Education*, volume 1. CSEDU 2018.

Mirkovic, J. and Benzel, T. (2012). Teaching cybersecurity with deterlab. *IEEE Security & Privacy*, 10(1):73–76.

Riga, N., Edwards, S., and Thomas, V. (2016). *The Experimenter's View of GENI*, pages 349–379. Springer International Publishing, Cham.

Sharma, S. K. and Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. *Computers & Security*, 26(4):290–299.

Thomas, V., Riga, N., Edwards, S., Fund, F., and Korakis, T. (2016). Geni in the classroom. In *The GENI Book*, pages 433–449. Springer.

Topham, L., Kifayat, K., Younis, Y. A., Shi, Q., and Askwith, B. (2016). Cyber security teaching and learning laboratories: A survey. *Information & Security*, 35(1):51.

Willems, C. and Meinel, C. (2012). Online assessment for hands-on cyber security training in a virtual lab. In *Global Engineering Education Conference (EDUCON), 2012 IEEE*, pages 1–10. IEEE.

Xiong, K. and Pan, Y. (2013). Understanding protogeni in networking courses for research and education. In *Research and Educational Experiment Workshop (GREE), 2013 Second GENI*, pages 119–123. IEEE.