Leveraging a cloud-based testbed and software-defined networking for cybersecurity and networking education

Mohamed Rahouti1, Kaiqi Xiong2,3, Jing Lin3

Abstract

Nowadays, real-world learning modules become vital components in computer science and engineering in general and cybersecurity in particular. However, as student enrollments have been dramatically increasing, it becomes more challenging for a university/college to keep up with the quality of education that offers hands-on experiment training for students thoroughly. These challenges include the difficulty of providing sufficient computing resources and keep them upgraded for the increasing number of students. In order for higher education institutions to conquer such challenges, some educators introduce an alternative solution. Namely, they develop and deploy virtual lab experiments on the clouds such as Amazon AWS and the Global Environment for Network Innovations (GENI), where students can remotely access virtual resources for lab experiments. Besides, Software-Defined Networks (SDN) are an emerging networking technology to enhance the security and performance of networked communications with simple management. In this article, we present our efforts to develop learning modules via an efficient deployment of SDN on GENI for computer networking and security education. Specifically, we first give our design methodology of the proposed learning modules, and then detail the implementations of the learning modules by starting from user account creation on the GENI testbed to advanced experimental GENI-enabled SDN labs. It is worth pointing out that in order to accommodate students with different backgrounds and knowledge levels, we consider the varying difficulty levels of learning modules in our design. Finally, student assessment over these pedagogical efforts is discussed to demonstrate the efficiency of the proposed learning modules.

Keywords

global environment for network innovations, security, software-defined networking, networking

1 INTRODUCTION

In the past several years, information technology (IT) advances have led to a revolutionary improvement in cybersecurity education, where information security is no longer considered an IT department’s responsibility. Thus, it becomes
very indispensable to befit a broad range of real-world learning modules and hands-on lab experiments into diverse cybersecurity curricula while fulfilling the demands of both cybersecurity academia and industry.

While the cybersecurity spending in 2020 has dramatically past 96 billion dollars based upon an estimation elaborated by Gartner Inc. (an international research and advisory firm), aligning with a significant increase in cybercrime impacting various parties (ranging from government, organizations, to individuals), more and more students nowadays seek for degrees or certificates of cybersecurity in higher education (HE). As a result, the curricula of cybersecurity learning must satisfy and fulfill the necessary technical skills and knowledge that align with various highly demanded certification exams, such as Certified Information Systems Security Professional, Security+, Information Systems Audit and Control Association, and so forth.

Although real-world/hands-on lab modules are vital and indeed essential in the cybersecurity curriculum, various key difficulties and challenges remain considerable. These challenges mainly include, but are not limited to,

- diverse student backgrounds that make teaching difficulty. Students/learners enroll in various cybersecurity concentrations, such as information assurance, cyber intelligence, and digital forensics, with diverse backgrounds.
- the unavailability of computing resources.
- insufficiency or lack of hardware and software resources. Such a resource limitation restricts the student from exploring and/or learning basic security experimentation scenarios.

Notice that the above challenges become more severe to online students because of their difficulty accessing computing resources and tutoring support.

While virtual laboratory environments offer an interactive emulation-based learning experience of real-world scenarios through a website or desktop software shown in Figure 1, the global environment for network innovations (GENI) is a well-established testbed sponsored by the United States’ National Science Foundation (NSF), and it is a federated, heterogeneous, real-world, at-scale, repeatable, and programmable testbed. GENI further provides a great opportunity for conducting experiments over a broad range of computer engineering and science areas, including, but are not limited to, computer networking, high-performance computing (HPC), and information and networking security. GENI testbed allows experimenters to run multiple experiments concurrently in isolated slices of the infrastructure as shown in Figure 2. In addition, software-defined networking (SDN) is a technology to ease network traffic management as well as cloud resource allocation through a programmable and efficient network configuration. Moreover, SDN enhances network traffic monitoring and performance through a global and logically centralized topology view.

In the past several years, we have taught and hosted various cybersecurity courses and workshops, respectively. We have brought GENI into the classroom and integrated SDN with GENI testbed along with a broad range of cybersecurity lab modules to meet the needs of students with diverse backgrounds. In this article, we present our efforts towards an efficient deployment of GENI testbed and SDN integration into real-world lab modules for computer networking and security education. Namely, we first present our design methodology of learning modules’ implementations, and then detail the designed GENI and SDN-based modules starting from user account creation on GENI testbed to advanced

| Laboratory | Physical Laboratory | Virtual Laboratory | Testbed-based Laboratory |
|------------|---------------------|--------------------|--------------------------|
|            | Desktop-based Virtualization | Cloud-based Laboratory | Multi-VM Laboratory |
|            | Single-VM Laboratory |                      |                          |

FIGURE 1 A hierarchy of the virtual laboratory

1
experimental GENI-enabled SDN labs, such as the management of networking traffic, intrusion detection and prevention system (IDPS), and the thwarting of common security issues. It is remarkable to note that in order for us to accommodate students with different backgrounds and knowledge levels in computer networking and security, different difficulty levels have been considered while designing these learning lab modules. Finally, student assessment and feedback over these pedagogical efforts are presented and discussed as a metric to demonstrate the efficiency of the proposed methodology.

The remaining of this article is outlined as follows. Section 2 presents an explanatory and detailed overview of some efforts that were done in the past to integrate GENI and SDN in order to facilitate and boost the cybersecurity learning experience. Section 3 then discusses our research efforts towards the integration of GENI and SDN in our teaching curriculum and the development of a broad range of cybersecurity labs and experimental modules. Section 4 gives a comprehensive summary of student feedback and assessment of our learning modules and experimental approaches. Finally, in Section 5, we present our future plans along with concluding remarks of our article.

2 | RELATED WORK

In cybersecurity for HE, curriculums encompass topics including secure software development, web security, traffic management and monitoring, and ethical hacking. Such hands-on learning units must align with the real-world lab exercise and experimentation in order to offer learners a customized and boosted opportunity for mastering and understanding in-class material and concepts. 11

Several efforts were elaborated in the past several years to support and enhance various types of laboratory environments for different cybersecurity courses. 12 Moldovan and Ghergulescu 13 classified the cybersecurity platforms to virtual labs as a service platforms, virtual machine (VM) download platforms, browser-based lab platforms, browser-based CTF platforms, hybrid platforms, and cyber ranges. Yamin et al. 14 presented a comprehensive and systematic literature review for cyber ranges and security testbeds that focus on architecture and scenarios. Among these notable efforts, Willems and Meinel 15 designed a software solution to assess online cybersecurity laboratory-based experiments based upon VM platforms. The introduced solution enables a flexible parameterization of experimental labs with an implementation of a real-time toolkit configuration of the virtual lab environment. Xiong and Pan 16 further proposed a pedagogic methodology to leverage ProtoGENI, a GENI testbed facility, alongside computer engineering education. Specifically, the authors implemented several hands-on lab units and capstone projects in order to broaden students’ conduct of various research and course projects over a real-world testbed.

Moreover, Mirkovic and Benzel 17 introduced DeterLab, an open-source platform based upon Emulab solution. The proposed facility plays a key role in an experimental environment sponsored by the United States’ NSF and Department of Homeland Security and allows online cybersecurity students to flexibly allocate and reserve computing resources (hardware and software) through a web user interface. Students here are further granted a remote access capability using their
virtual session credentials to allocated machines for only a fixed time interval in order to give up resources for other students’ experiments as the offered computing resources are limited in this facility.

The SeedLAB project\textsuperscript{18} provided a set of cybersecurity and applied cryptography lab modules for academic use. Moreover, SeedLAB provided a ready-to-use Linux-based VM with specific security tools and packages such as OpenSSL cryptographic library. However, using a single VM is not always practical in cybersecurity experiments (e.g., man-in-the-middle attack and denial and distributed denial of service attacks). Timchenko and Starobinski\textsuperscript{19} provided a simple, secure, and isolated lab environment that consists of three VMs to represent the attacker, target, and zombie machine, respectively. Nevertheless, the attacker VM has to update every few months to keep up with fast-evolving technology. That increases the staff workload. Moreover, Rahouti and Xiong\textsuperscript{20} have developed a broad range of hands-on cryptographic labs to be conducted in a readily available and customized VM (i.e., prebuilt VM image), in which all required software and library packages are implemented prior to the class start.

Different from the aforementioned teaching efforts, in this article, our learning model development includes our academic guidelines in integrating GENI testbed into cybersecurity teaching along with innovative security labs on SDN-enabled environments using GENI virtual resources. 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 cybersecurity knowledge. Finally, the work reported in this article has only been presented in a poster panel session during the 126th ASEE meeting in 2019.

3 | METHODOLOGY: ADOPTING INNOVATIONS

Given the aforementioned challenges and limitations related to higher cybersecurity education, our perceived goals presented in this work are to enhance cybersecurity education efficiency and maximize students’ benefits from various real-world lab modules through the GENI testbed. At the same time, we leverage SDN-enabled environments for advanced computer and networking security. In particular, this study aims to introduce students to the GENI testbed and develop convenient lab modules in an SDN-enabled environment for cybersecurity students with a strong or weak background in both computer science and cybersecurity (Figure 3).

3.1 | GENI integration

As mentioned earlier, GENI facilities offer a heterogeneous, real-world, at-scale, repeatable, and programmable networking-enabled testbed. It further provides an excellent opportunity for conducting experiments over a broad range of computer engineering and science areas, including, but not limited to, computer networking, HPC, and information and networking security. As GENI can be used as a remote lab and offer real-world experiments on a large-scale network, as shown in Figure 2, we have considered integrating it into our networking and security courses and workshops. Our

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{fig3.png}
\caption{Monitoring console for lab educators during a lab session\textsuperscript{10}}
\end{figure}
reasons for this integration are the easiness of deployment, collaborative experiments, and granted access to a broad range of resources, which include, but are not limited to, software and physical switches and wireless base stations that could be unavailable at some universities.

Noticing that throughout a lab session, educators can monitor the number of experimenters logged into the testbed console in real-time, all experiments currently active, experiments already submitted but await for available resources to run, and the names of experimenters.

Prior to creating slices on the GENI testbed, students need to understand resource specification (Rspec) files and learn how to establish their own based on resources needed per lab. Rspec files are XML-based documents to describe GENI resources and slice information, as shown in Figure 4. Figure 4 also depicts API calls, which use Rspec files to intercommunicate between tools and aggregate managers (AM). For instance, a student can reserve particular resources (e.g., VMs) using tool X, check their status/availability using tool Y and release them when done with experiments using tool Z.

3.2 Familiarizing students with the GENI testbed

The first step to familiarize our students with the GENI testbed is through the Lab0 and Lab1 assignments. In Lab0, students create a simple slice of two nodes. The goal of the lab is to ensure that students are capable of logging into their GENI portal accounts and comprehending the fundamentals of establishing and conducting experiments on GENI resources. A simple 2-node experiment helps students get started with GENI. Most instructors can have students do this exercise in the classroom. In Lab1, our goal is to ensure our students have a good understanding of the GENI testbed functions, the RSpec concept, and the GENI AM API. It is important to mention that through the use of the monitor feature of GENI shown in Figure 3, we can monitor the number of active students in addition to active (currently running) experiments and experiments awaiting available testbed resources to run.

3.3 Integration of SDN

SDN has become a vital network architecture for expediting management and control in networking-enabled environments. It presents a global view of network resources and logically centralized control by decoupling the control layer from the infrastructure layer. SDN eases programmability by adopting programmable interfaces to insert and push forwarding rules in SDN switches (e.g., Open vSwitch). In order for us to best leverage the SDN capabilities, the delicate holistic view of flows must be contributory to any networking-enabled application (e.g., traffic engineering, QoS-aware flow routing, and flow inspection).

Nowadays, cybersecurity in both industry and academia is faced with a dramatically growing set of impedance factors (e.g., threat actors). Threat actors are becoming more capable of exploiting sophisticated tactics and methodologies by leveraging sophisticated software and security tools, which are applied within multiphased campaigns to achieve the
desired attacks or goals. Therefore, it is of a great necessity to educate STEM students about cybersecurity according to the up-to-date technological advances in both networking and security. As significant challenges always remain in how threat actors/adversaries are approaching the response to sophisticated security breaches and vulnerabilities, we focus on SDN as an emerging networking technology and infrastructure to provide our students with significant gains over existing approaches.

Therefore, the necessity of SDN integration into applied cybersecurity teaching for STEM education curricula is of great interest as students can profit from SDN-enabling security to elaborate opportunities for an intelligent and thorough response to threats on a granular basis by resolving illegitimate traffic without sacrificing the benign flows. Moreover, students can learn and experience opportunities of security implementation in SDN (e.g., Rest API applications) to thwart networking anomalies by diverting designated network traffic to selective enforcement and policy check points (e.g., firewalls and IDPS).

3.4 | Lab development

In order to meet the needs of the networking and cybersecurity industry and advance the academic curriculum, we have made a great effort to develop lab modules that focus on computer security in general and SDN. Noticing that in cybersecurity programs, it is not unusual that students lack the necessary background in computer science and security since the programs attract many students with diverse backgrounds. Therefore, it is highly challenging to assign labs, which align with most students in a class. Thus, while developing lab modules, we considered this challenge by designing labs with an increasing difficulty level. Moreover, for each designed lab, we have created step-by-step tutorials and demos for students without a minimal background to place them on the track. Besides, we have created instructor manuals for each lab module to better help future educators apply such labs in their own teaching or workshops.

In Table 1, we present the comprehensive and diverse set of lab modules we have developed to introduce students to GENI and get familiar with the testbed components and features, starting from the very beginning where students learn how to create and set their GENI accounts (including PEM certificate, private key, and public key). In addition, we have designed a comprehensive set of lab modules for SDN environments ranging from creating and configuring an OpenFlow environment to conducting advanced experiments over an SDN-enabled environment, such as traffic management and writing new modules in an open-source SDN controller. The developed introductory labs in Table 1 are aimed to enable a

| Labs | Objectives | Time (h) |
|------|------------|----------|
| Getting started on GENI-Part 1 | (1) Introduction to GENI. (2) GENI account setup. (3) Getting familiar with GENI testbed | 2 |
| Getting started on GENI-Part 2—Hello GENI | (1) Reserve resources/slice. (2) configure and ssh to nodes (Figure 6) | 2 |
| Web server application | Elaborate client-server based communication with multiple VMs | 1.5 |
| Mac-using SFTP to transfer files | Using SFTP for Mac OS to exchange files with GENI resources | 1 |
| Using WinSCP with GENI nodes | Using WinSCP for Windows OS to exchange files with GENI resources | 1 |
| Introduction to OpenFlow | (1) Introduction to OpenFlow. (2) Learn about OpenFlow-enabled environment | 2 |
| Your first experiment using SDN (Floodlight controller) | Creating an OpenFlow topology. (2) Deploying an SDN controller (Figure 5) | 2 |
| Advanced SDN/OpenFlow lab configurations | Establish a completely functional SDN environment | 3 |
| Introduction to Rest API of Floodlight | Explore RestAPI features and main functions | 2 |
| Write your first module in Floodlight | Creating a first module in Floodlight | 4 |
| Statistics collection and manipulation in Floodlight SDN | Advanced lab on OpenFlow and requires advanced programming skills | 2 |
| OpenFlow based load balancing router | Learn about flow balancing in Floodlight controller | 2 |

Abbreviations: GENI, global environment for network innovations; SDN, software-defined networks; VM, virtual machine.
FIGURE 5  An SDN-based lab topology using GENI testbed. The topology shown herein is an example of a completely configured and functional GENI slice where OVS 1.5\textsuperscript{21} and Floodlight are deployed as OpenFlow and SDN controller\textsuperscript{22}, respectively. The experiment shown relates to traffic management lab in SDN Floodlight controller software. GENI, global environment for network innovations; SDN, software-defined networks.

FIGURE 6  A student view over multiple ssh sessions to their reserved virtual machines once the slice is active and running.
virtual experimental environment for our teaching in cybersecurity, information security, IT, and computer networking and security. These labs deliver step-by-step tutorials with corresponding networking and computation knowledge and resources that introduce students to the latest real-world tools and technologies.

3.5 Advanced labs: Exercises to challenge students’ assumptions about computer networks

As one of our project goals is to broaden and extend the path to the STEM profession through cybersecurity learning, we extended our efforts to develop advanced GENI, cryptography, and SDN learning labs and experimental modules in order to achieve the goal of our funded NSF project. The challenging labs require students to have an advanced background in both networking and computer programming. The key learning modules are as follows.

- Rest API implementation
- Writing an SDN software module
- Statistics customization and collection
- Load balancing
- Dynamic flow pushers

3.6 Design considerations and workflow

Our principal objective in this pedagogical project is to train students mainly on computer networking and security rather than testbeds. Students often do not have solid experimental skills, so we opt to reduce the number of the testbed-nominated skill sets needed to complete our elaborated lab modules. Instead, our students are expected to deploy their intellectual efforts and knowledge rectifying and strengthening their computer networking and cybersecurity skill set along with critical-thinking skills.

The common process for every learning lab module listed in Table 2 consists of the following steps as depicted in Figure 7.

| Labs | Objectives | Time (h) |
|------|------------|----------|
| Network traffic and denial-of-service (DoS) | Detection and analysis of DoS traffic | 2 |
| Certificate authority (CA) | Establish and configure your own CA | 2 |
| Correlation and mitigation using SDN | Learn about threat mitigation techniques through SDN | 2 |
| Intrusion detection and prevention system (IDPS)—Snort | Installation and configuration of Snort IDPS rules | 3 |
| Ransomware in SDN | Learn about ransomwares in SDN | 2 |
| Covert storage channel | Learn and explore covert storage channel attack in SDN | 1.5 |
| Man-in-the-middle (MITM) attack | Experimenting MITM attack in SDN | 2 |
| CTF password | Learn about CTF passwords in an OpenFlow environment | 2 |
| Introduction to steganography | Getting familiar with steganography using GENI testbed resources | 2 |
| Access control list (ACL) in SDN | (1) introduction to ACL (2) configuring ACL rules in Floodlight SDN | |
| Privilege escalation | Learning about privilege escalation in SDN Floodlight controller | 2.5 |
| Sniffing and spoofing in SDN environment | Getting a dip dive into sniffing and spoofing through Wireshark | 3 |
| Firewall configuration in SDN controller | Firewall configuration in Floodlight SDN controller | 2.5 |
| Web tracking | Tracking and monitoring web services | 3 |

Abbreviations: GENI, global environment for network innovations; SDN, software-defined networks.
4.1 Learning assessment

In the past couple of years, we considered collecting feedback from our students in the graduate level cybersecurity core course (Applied Cryptography) and students in the precollege STEM summer program. Demonstrator’s performance scores are calculated from the weighted average of responses on a 5-point Likert scale from “Very Satisfied” (5) to “Very Unsatisfied” (1) as shown in Table 3.

Table 3 and Figure 8 present students’ feedback and performance measures provided by our STEM students and workshop attendees, respectively. Table 3 represents the survey results for 10 participants among all workshop attendees, while Figure 8 represents assessment results for 29 among 35 students in total from the Applied Cryptography course.
Table 3 depicts individual feedback/assessment provided by the attendees of a summer cybersecurity workshop we hosted at our university cybersecurity center. The participants consisted of undergraduate students, graduate students (with different backgrounds ranging from mathematics/statistics, business and communication systems, computer science and engineering, IT, and so forth), and faculty members. The attendees were asked to take an anonymous satisfaction and experience survey. According to the collected survey responses, the majority of our attendees confirmed their complete satisfaction and usefulness of our pedagogical approach of adopting an advanced federated testbed, GENI, and SDN as experimental modules into our teaching of cybersecurity concepts and topics.

Moreover, we attempted to understand the performance of our students in applied cryptographic labs using a traditional VM we have prebuilt in the past few years and a GENI testbed. In this evaluation scenario, different students in the same course and with similar computer science and engineering background were assigned cryptographic labs, namely, symmetric encryption lab, asymmetric encryption lab, and hash functions and Public-Key Infrastructure (PKI). Next, the time each student spent on each was recorded and collected. We then calculated the average time students spent on the three labs on both the GENI testbed and the VM. The goal behind this evaluation is to assess the process of systematically examining and refining the fit between the course content and the sophisticated labs we have developed over the GENI testbed and what learners (e.g., students) should know after finishing all lab modules. As shown in Figure 8, the average time spent working on these labs using the GENI testbed is significantly smaller than the time spent on the VM.

Typically, objectives behind this pedagogical approach can be summarized as follows.

- Overcome the financial challenges and computation resources accessibility that many universities and colleges have encountered due to a rapid change of hardware and software
- Provide convenient and flexible access to experimental modules and resources for those students who need to conduct experiments remotely or face-to-face
- Help learners in applying security principles/concepts related to real-world computing networking and communication systems
- Provide learners with the technological capabilities and skills (software and hardware) needed to analyze and evaluate existing security threats and solutions with regard to a given end-to-end communication scenario in a real-world federated networking environment

Finally, our presented teaching approach offers efficient learning modules while considering existing constraints of computing resources and the demand for computer networking and the security industry.
### 4.2 Discussions

Hands-on lab experiments have been an integral part of computer science and engineering curricula. 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 in student enrollments in computer science and engineering for the past 10 years. The proposed learning modules can be feasibly replicated by other educators in the cybersecurity field. Moreover, instructor manuals are developed for each lab module to help other instructors from different engineering schools and universities adopt these learning modules in their cybersecurity curricula.

However, the deployment of learning modules and hands-on labs presented in this article has the following limitations and challenges:

- The testbed facilities may need to be updated and upgraded periodically.
- Some students may require additional training on how to use and manipulate testbed resources efficiently.
- Some students may require additional tutorials and/or training on the Linux systems to efficiently deploy the GENI VMs that are mostly built on Linux images.
- The number of surveyed workshop participants may be small to draw general conclusions, and thus a part of the presented assessment analysis may appear insufficient to the readers. However, this analysis can be repeated with a larger number of participants at future workshops.

### 5 Conclusion and Future Work

Real-world experiments and hands-on lab units are essential components of cybersecurity curriculums. However, as the students' enrollment in hybrid, online, and face-to-face courses has been dramatically increasing, it becomes more challenging for universities to keep up with the students' experiment quality. Furthermore, the lack of hardware and software resources at most universities and the incapability of online students to have physical access to computing resources laboratories render various cybersecurity courses challenging to teach. To resolve such limitations, we presented dedicated efforts to enhance experimental student learning outcomes in this article. In particular, we integrated and deployed virtual lab experiments based on GENI, a well-established testbed sponsored by the US NSF, a federated, heterogeneous, real-world, at-scale, repeatable, and programmable testbed facility. GENI allows experiments in a variety of computer science areas such as networking, security, and distributed computing sponsored by NSF. Besides, as SDN is a core technology for networking, cloud computing, and various cyber-physical systems, we went beyond the scope of cybersecurity teaching in traditional networking. We developed a broad range of security labs in SDN-enabled environments.

As future work for facilitating and improving large-scale cybersecurity experimentation, we plan on deploying the GENI testbed in other cybersecurity courses such as blockchain technology and network intrusion detection. At the moment, our students utilize a VM we have built for the different cybersecurity courses. In this virtual environment, all course tools and libraries are implemented and customized. However, students find it challenging when lacking powerful personal computers. Therefore, migrating to the GENI testbed will be a great addition to such courses.

Moreover, we plan to adopt ExoGENI and Fed4Fire testbeds in our cybersecurity training workshops at our university. Fed4FIRE+ is a European Union testbed, which offers the largest federation worldwide of Next Generation Internet testbeds, whereas ExoGENI is a new GENI testbed linking GENI testbed to two advances in virtual infrastructure services outside of GENI: open cloud computing (OpenStack) and dynamic circuit fabrics.

### Acknowledgments

We would like to acknowledge the National Science Foundation (NSF) that 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.

### Peer Review Information

*Engineering Reports* thanks the anonymous reviewers for their contribution to the peer review of this work.
PEER REVIEW
The peer review history for this article is available at https://publons.com/publon/10.1002/eng2.12395.

DATA AVAILABILITY STATEMENT
Research data are not shared.

CONFLICT OF INTEREST
Authors have no conflict of interest relevant to this article.

ETHICS STATEMENT
Participation in this study was completely voluntary. Students and workshop attendees have chosen to participate and voluntarily took the survey. Participants were informed that they may stop participating at any time and may decide not to answer any specific question.

ORCID
Mohamed Rahouti https://orcid.org/0000-0001-9701-5505

REFERENCES
1. Rahouti M, Xiong K. A Customized Educational Booster for Online Students in Cybersecurity Education. In: Proceedings of the 11th International Conference on Computer Supported Education (CSEDU). SciTePress, Setubal, Portugal. 2019;535-541.
2. Riga N, Edwards S, Thomas V. The Experimenter’s View of GENI. Cham, Switzerland: Springer International Publishing; 2016:349-379.
3. Baleni ZG. Online formative assessment in higher education: its pros and cons. Electron J e-Learn. 2015;13(4):228-236.
4. Palvia S, Aeron P, Gupta P, et al. Online Education: Worldwide Status, Challenges, Trends, and Implications. Taylor & Francis; 2018.
5. Fedynich LV. Teaching beyond the classroom walls: the pros and cons of cyber learning. Journal of Instructional Pedagogies, ERIC. 2013;13.
6. Chin T, Xiong K, Rahouti M. SDN-based kernel modular countermeasure for intrusion detection. Paper presented at: Proceedings of the 13th EAI International Conference on Security and Privacy in Communication Networks. Niagara Falls, Canada; 2017:270-290.
7. Chin T, Rahouti M, Xiong K. Applying software-defined networking to minimize the end-to-end delay of network services. ACM SIGAPP Appl Comput Rev. 2018;18(1):30-40.
8. Rahouti M, Xiong K, Ghani N, Shaikh F. SYNGuard: dynamic threshold-based SYN flood attack detection and mitigation in software-defined networks. IET Netw. 2021.
9. Rahouti M, Xiong K, Xin Y. Secure software-defined networking communication systems for smart cities: current status, challenges, and trends. IEEE Access. 2020;9:12083-12113.
10. Thomas V, Riga N, Edwards S, Fund F, Korakis T. GENI in the Classroom. New York, NY: Springer; 2016:433-449.
11. Topham L, Kifayat K, Younis YA, Shi Q, Askwith B. Cyber security teaching and learning laboratories: a survey. Inf Secur. 2016;35(1):51.
12. Rao AR, Dave R. Developing hands-on laboratory exercises for teaching STEM students the internet-of-things, cloud computing and blockchain applications. Paper presented at: Proceedings of the IEEE Integrated STEM Education Conference. Princeton, NJ; 2019:191-198; IEEE.
13. Moldovan AN, Ghergulescu I. Leveraging virtual labs for personalised group-based assessment in a postgraduate network security and penetration testing module. Paper presented at: Proceedings of the 15th International Workshop on Semantic and Social Media Adaptation and Personalization. Zakynthos, Greece; 2020:1-6.
14. Yamin MM, Katt B, Gkioulos V. Cyber ranges and security testbeds: scenarios, functions, tools and architecture. Comput Secur. 2020;88:101636.
15. Willems C, Meinel C. Online assessment for hands-on cyber security training in a virtual lab. Paper presented at: Proceedings of the IEEE Global Engineering Education Conference. Marrakech, Morocco; 2012:1-10.
16. Xiong K, Pan Y. Understanding protogeni in networking courses for research and education. Paper presented at: Proceedings of the 2nd GENI Research and Educational Experiment Workshop. Salt Lake, UT; 2013:119-123.
17. Mirkovic J, Benzel T. Teaching cybersecurity with DeterLab. IEEE Secur Priv. 2012;10(1):73-76.
18. Du W. SEED: hands-on lab exercises for computer security education. IEEE Secur Priv. 2011;9(5):70-73.
19. Timchenko M, Starobinski D. A simple laboratory environment for real-world offensive security education. Paper presented at: Proceedings of the 46th ACM Technical Symposium on Computer Science Education. Kansas City, MO; 2015.
20. Rahouti M, Xiong K. Board 129: facilitation of cybersecurity learning through real-world hands-on labs. Paper presented at: Proceedings of the ASEEE Conferences. Tampa, FL; 2019. https://peer.asee.org/32228.
21. Pfaff B, Pettit J, Koponen T, et al. The design and implementation of open vs switch. Paper presented at: Proceedings of the 12th USENIX Symposium on Networked Systems Design and Implementation. Oakland, CA; 2015:117-130.
22. Floodlight OpenFlow Controller. Project Floodlight. http://www.projectfloodlight.org/floodlight/.
23. McKeown N, Anderson T, Balakrishnan H, et al. OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Comput Commun Rev. 2008;38(2):69-74.
24. Rahouti M, Xiong K, Chin T, Hu P. SDN-ERS: a timely software defined networking framework for emergency response systems. Paper presented at: Proceedings of the IEEE International Science of Smart City Operations and Platforms Engineering in Partnership with Global City Teams Challenge. Porto, Portugal; 2018:18-23.

25. Ni H, Rahouti M, Chakrabortty A, Xiong K, Xin Y. A distributed cloud-based wide-area controller with SDN-enabled delay optimization. Paper presented at: Proceedings of the IEEE Power & Energy Society General Meeting (PESGM). Portland, OR; 2018:1-5.

26. Chin T, Xiong K, Rahouti M. Kernel-space intrusion detection using software-defined networking. *EAI Endors Trans Secur Safety*. 2018;5(15).

27. Cheung RS, Cohen JP, Lo HZ, Elia F. Challenge based learning in cybersecurity education. Paper presented at: Proceedings of the Steering Committee of the World Congress in Computer Science, Computer Engineering, and Applied Computing. Las Vegas, NV; 2011:1.

28. Baldin I, Chase J, Xin Y, et al. Exogeni: a multi-domain infrastructure-as-a-service testbed. *The GENI Book*. New York, NY: Springer; 2016:279-315.

29. Vermeulen B, Meersche V, Walcarius T. jFed toolkit, fed4fire, federation. Paper presented at: Proceedings of the GENI Engineering Conference. Bloomington, IN; Vol. 19; 2014.

How to cite this article: Rahouti M, Xiong K, Lin J. Leveraging a cloud-based testbed and software-defined networking for cybersecurity and networking education. *Engineering Reports*. 2021;3:e12395. https://doi.org/10.1002/eng2.12395