Understanding Global Environment for Network Innovations (GENI) and Software-Defined Networking (SDN) for Computer Networking and Security Education

Mr. Mohamed Rahouti, University of South Florida

Mohamed Rahouti received an M.S. degree in Statistics in 2016 at the University of South Florida and is currently perusing a Ph.D. degree in Electrical Engineering at the University of South Florida. Mohamed holds numerous academic achievements. His current research focuses on computer networking, Software-Defined Networking (SDN), and network security with applications to smart cities.

Understanding Global Environment for Network Innovations (GENI) and Software-Defined Networking (SDN) for Computer Networking and Security Education

Mohamed Rahouti[1,4,*] **and Kaiqi Xiong**[2,3,4,+]

[1]Department of Electrical Engineering, University of South Florida, Tampa, 33620, USA
[2]Cyber Florida, University of South Florida, Tampa, 33620, USA
[3]Department of Mathematics and Statistics, University of South Florida, Tampa, 33620, USA
[4]Intelligent Computer Networking and Security Lab, University of South Florida, Tampa, 33620, USA
[*]mrahouti@mail.usf.edu
[+]xiongk@usf.edu

ABSTRACT

Hands-on modules and experiments are considered essential and fundamental components in cyber security curriculums. However, because of the significant increase in student enrollments in both online and face-to-face courses, universities face various challenges mainly related to financial support and computing resources that could be limited. To overcome such key challenges, universities have been considering alternative solutions to solve resource issues and allow students to practice real-world lab experiments through a virtual environment such as the Global Environment for Network Innovations (GENI). GENI is 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). 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. In this paper, we will demonstrate our 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 our funded NSF project. Specifically, we will first present our methodology for the design of our modules and then give the detail 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 have been developed at different levels to meet the need of different types of students. Finally, we will present our assessment and student feedback to demonstrate the efficiency of our developed GENI and SDN modules for networking and security education.

1 INTRODUCTION

In the past several years, information technology (IT) advances have led to a revolutionary improvement in cyber security education where information security is no longer considered as an IT department's responsibility. Thus, it becomes very indispensable to befit an advanced and diverse range of hands-on lab experiments and teaching materials into curriculums that meet the needs of the cyber security industry.

While the cyber security spending has past 96.3 billion dollars by the beginning of 2019 (according to the international research and advisory firm, *GartnerInc*. estimation) and cybercrimes increased to affect various parties (government, organizations, individuals, etc.), more and more students are to seek cyber security degrees or certificates. Therefore, in the cyber security teaching, the curriculum should satisfy necessary advanced skills that align with highly-demanded certification exams, e.g., Certified Information Systems Security Professional (CISSP), Information Systems Audit and Control Association (ISACA), and Security +.

It is unquestionable that hands-on experiments are indeed essential in the teaching curriculum of cyber security programs (online and face-to-face courses). However, there are various key difficulties and challenges. In brief, (1) challenges related to student backgrounds and (2) availability of experimental resources. Students enroll in cyber security programs with a very broad range of backgrounds such that many of them have a weak background in computer science and lack basics and fundamentals

of cyber security. Additionally, insufficiency of lab and hardware and software resources at universities could also be a great challenge and therefore restrict student ability of learning and exploring some basic security experimentation scenarios (e.g., Client-sever communication, intrusion detection systems, Denial of Service and Distributed Denial of Service attacks, and Man-in-the- Middle attack. Noticing that this is even more challenging when offering online cyber security courses as it most likely infeasible for remote students to benefit from local computer labs at the university campus.

While the Global Environment for Network Innovations (GENI) is 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), Software-defined networking (SDN) is a technology to ease network management as well as cloud computing through a programmable and efficient network configuration. Moreover, SDN enhances network traffic monitoring and performance through a global and logically centralized topology view [1], [2].

In the past several years, we have taught and hosted various cyber security courses and workshops, respectively. we have brought GENI into the classroom and integrated SDN with GENI testbed along with a broad range of cyber security lab modules to meet the needs of students with diverse backgrounds. In this paper, we will discuss our 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 our funded NSF project. Particularly, we will first present our methodology for the design of our modules and then give the detail 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 monitoring 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 have been developed at different levels to meet the need of different student backgrounds ranging from weak to strong computer science and cyber security backgrounds. Finally, we will present our future plans to further improve and facilitate cyber security learning.

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 integrate GENI and SDN in order to facilitate and boost cyber security learning experience. Section 3.2 then presents our research efforts towards the integration of GENI and SDN in our teaching curriculum and development of a broad range of cyber security labs and experimental modules. Finally, in Section 4 we present our future plans along with concluding remarks of our paper.

2 RELATED WORK

In cyber security for Higher Education (HE), curriculums encompass topics including secure software development, web security, traffic mangement and monitoring, and ethical hacking. Such fundamental modules should be accompanied with real-world lab experiments and exercises to provide students with a better opportunity for understanding and mastering course concepts and material [3].

As there are various types of cyber security laboratories [4], Willems and Meinel [5] introduced software to assess cyber security lab experiments through a virtual machine technology (an online-based laboratory). The solution offers an efficient parameterization of experiment scenarios as well as a dynamic toolkit implementation virtual machine configuration. Meanwhile, Xiong and Pan [6] discussed an approach to integrate ProtoGENI, a GENI testbed resource, into computer science and engineering education. Precisely, they have elaborated a variety of lab experiments and capstone projects which allow students for integrating a real-world testbed for various research and learning purposes.

Furthermore, Mirkovic and Benzel [7] presented DeterLab, a open technology based on Emulab. This technology is an experimental space/resource sponsored by the US National Science Foundation and Department of Homeland Security and this facility is dedicated for online cyber security learning. In this facility, while students can reserve entities (available nodes out of 400 computing nodes in total) via an online interface, they are allowed to keep remote access (virtual session login) to virtual nodes for a very short period of time only in order to permit other students for accessing the computing resources that are limited.

The SeedLAB project [8] provided a set of cyber security and applied cryptography lab modules for academic use. Moreover, SeedLAB provided a ready-to-use Linux-based virtual machine that comes with specific security tools and packages such as OpenSSL cryptographic library. However, using a single VM is not always practical in cyber security experiments (e.g., Man-in-the-Middle attack and Denial and Distributed Denial of Service attacks).

Different from aforementioned teaching efforts, in this paper, we discuss and detail our academic guidelines in integrating GENI testbed into cyber security 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 cyber security knowledge.

3 METHODOLOGY: ADOPTING INNOVATIONS

Our primary goal for the education research discussed here is to boost the efficiency of cyber security learning and maximize student benefits from various hands-on labs on security through GENI testbed security in SDN-enabled environments. In particular, this study aims at introducing students to GENI testbed and developing convenient lab modules in an SDN-enabled environment for cyber security students with a strong or weak background in both computer science and cyber security.

3.1 GENI Integration

As GENI can be used as a remote lab by various educators (e.g., distributed systems, networking, and cyber security) and permits them to offer real-world experiments on a large-scale network **??**, we have considered integrating it in our networking and security courses and workshops. Our reasons for this integration are the easiness of deployment, collaborative experiments, 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.

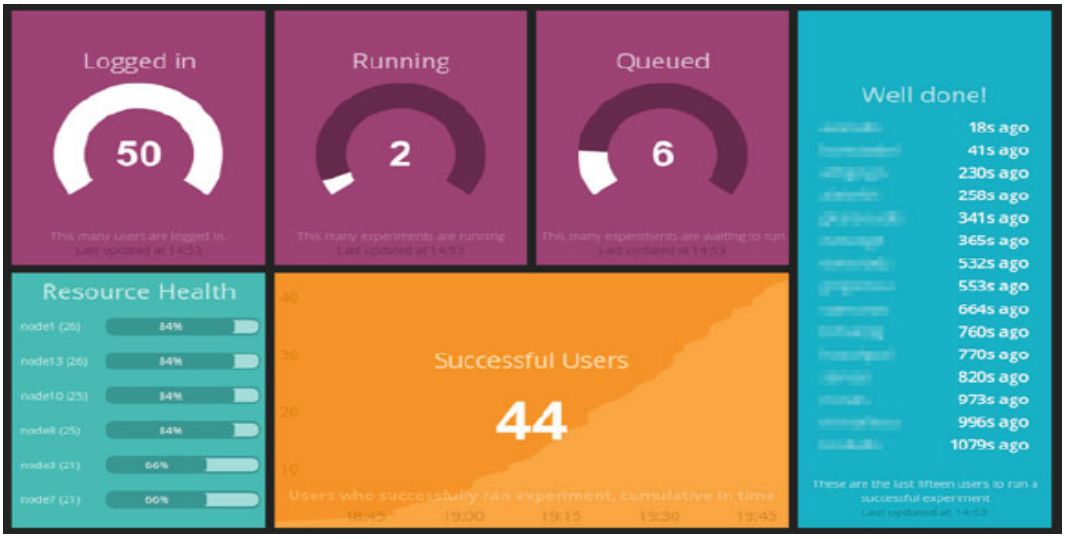

Figure 1. Monitoring console for lab educators during a lab session [9]

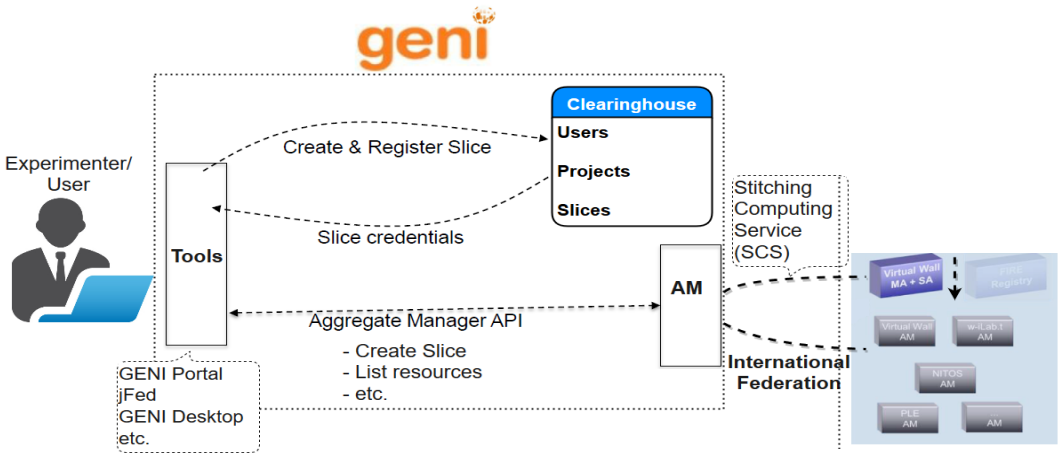

Figure 2. Interaction layers between experimenters and GENI resources

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

Prior to creating slices on 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

Table 1. Samples of our developed computer networking labs using GENI testbed.

Lab	Objectives	Time (Hrs)
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	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	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

slice information as shown in Figure 2. Figure 2 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 Lab Development

In order to meet the networking and cyber security industry needs and advances and academic curriculum, we have dedicated a great effort to develop lab modules that focuses in computer security in general and SDN. Noticing that in cyber security programs, most likely students lack the necessary background in computer science and security, and therefore, it is very challenging to assign labs, which align with most student in a class [10]. Thus, while developing lab modules, we considered this challenge by designing labs with an increasing difficulty level. Moreover, for each designed lab, we made a step-by-step tutorials and demos for students without a minimal background to place them on the track. In addition, 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). Additionally, we have designed a comprehensive set of lab modules for SDN environment ranging from creating and configuring an OpenFlow environment to

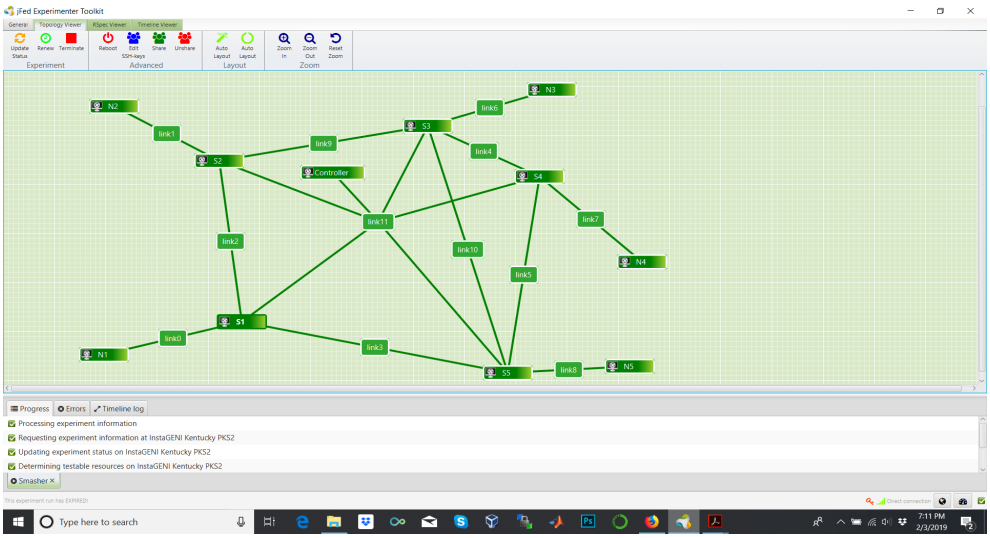

Figure 3. An SDN-based lab topology using GENI testbed. The topology shown herein is an example of a completely configured and functional GENI slice where OVS 1.5 and Floodlight are deployed as OpenFlow and SDN controller, respectively. The experiment shown relates to traffic management lab in an SDN Floodlight controller.

conducting advanced experiments over an SDN-enabled environment, such as traffic management and writing new modules in an open-source SDN controller.

4 CONCLUSIONS AND FUTURE WORK

Hands-on modules and lab experiments are indeed fundamental parts of cyber security curriculums. However, there are various key challenges related to cyber security paths in higher education due to the significant increase in student enrollments in cyber security programs, lack of hardware and software resources at universities, and most of online students cannot physically access computer labs. To address such grand obstacles, in this paper we presented our efforts and contributions to improve cyber security teaching and facilitate students learning. Specifically, we aimed at integrating and deploying 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 NSF. Furthermore, as SDN is a core technology for networking, cloud computing and various cyber-physical systems, we went beyond the scope of cyber security teaching in traditional networking such that, we developed a broad range of security labs in SDN-enabled environments.

As future work for facilitating and improving large-scale cyber security experimentation, we plan on deploying GENI testbed in our online Applied Cryptography course. At the moment, our students utilize a virtual machine we have built for the course. 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 GENI testbed will be a great addition to such a course.

Moreover, we plan to adopt ExoGENI [11] and Fed4Fire [12] testbeds in our cyber security training workshops at our university. Fed4FIRE+ is a European Union testbed, which offers the largest federation worldwide of Next Generation Internet (NGI) testbeds, while 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.

ACKNOWLEDGEMENTS

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.

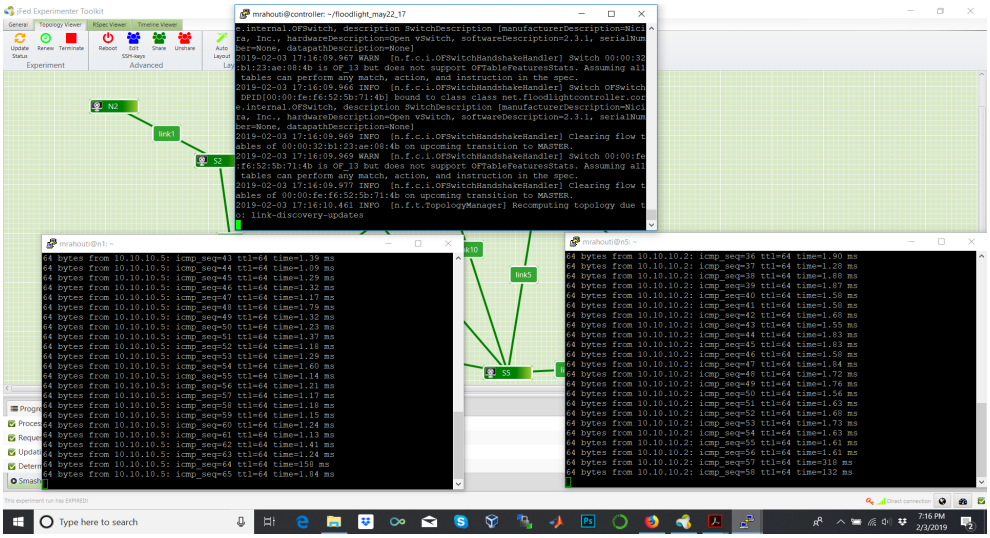

Figure 4. A student view over multiple ssh sessions to their reserved VMs once the slice is active and running

References

1. Chin, T., Xiong, K. & Rahouti, M. Sdn-based kernel modular countermeasure for intrusion detection. In *International Conference on Security and Privacy in Communication Systems*, 270–290 (Springer, 2017).
2. Chin, T., Rahouti, M. & Xiong, K. Applying software-defined networking to minimize the end-to-end delay of network services. *ACM SIGAPP Applied Computing Review* **18**, 30–40 (2018).
3. Topham, L., Kifayat, K., Younis, Y. A., Shi, Q. & Askwith, B. Cyber security teaching and learning laboratories: A survey. *Information & Security* **35**, 51 (2016).
4. Sharma, S. K. & Sefchek, J. Teaching information systems security courses: A hands-on approach. *Computers & Security* **26**, 290–299 (2007).
5. Willems, C. & Meinel, C. Online assessment for hands-on cyber security training in a virtual lab. In *Global Engineering Education Conference (EDUCON), 2012 IEEE*, 1–10 (IEEE, 2012).
6. Xiong, K. & Pan, Y. Understanding protogeni in networking courses for research and education. In *Research and Educational Experiment Workshop (GREE), 2013 Second GENI*, 119–123 (IEEE, 2013).
7. Mirkovic, J. & Benzel, T. Teaching cybersecurity with deterlab. *IEEE Security & Privacy* **10**, 73–76 (2012).
8. Du, W. Seed: hands-on lab exercises for computer security education. *IEEE Security & Privacy* **9**, 70–73 (2011).
9. Thomas, V., Riga, N., Edwards, S., Fund, F. & Korakis, T. Geni in the classroom. In *The GENI Book*, 433–449 (Springer, 2016).
10. Cheung, R. S., Cohen, J. P., Lo, H. Z. & Elia, F. Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)*, 1 (The Steering Committee of The World Congress in Computer Science, Computer . . . , 2011).
11. Baldin, I. *et al.* Exogeni: A multi-domain infrastructure-as-a-service testbed. In *The GENI Book*, 279–315 (Springer, 2016).
12. Vermeulen, B., Van de Meerssche, W. & Walcarius, T. jfed toolkit, fed4fire, federation. In *GENI Engineering Conference*, vol. 19 (2014).

Table 2. Samples of our developed cybersecurity labs using GENI testbed.

Lab	Objectives	Time (Hrs)
Network Traffic and Denial of Service	Detection and analysis of denial of service traffic	2
Certificate Authority	Establish and configure your own CA	2
Correlation and Mitigation using SDN	Learn about threat mitigation techniques through SDN	2
Intrusion Detection Systems - 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	3
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