Facilitation of Cybersecurity Learning Through Real-World Hands-On Labs

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.

Facilitation of Cybersecurity Learning Through Real-World Hands-On Labs

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

For the past several years, information technology advances have led to a significant improvement in computer science curriculums. Substantial efforts are indeed required to design various innovative teaching modules and lab experiments to facilitate learning processes in cyber security programs and fulfill industrial and technological requirements and goals with regard to cyber security paths (Bauer et al., 2018). Additionally, it could be beneficial to those who plan to work in industry if cyber security teaching could align with materials and skills needed for cyber security certification exams such as Certified Information Systems Security Professional (CISSP) and Information Systems Audit and Control Association (ISACA) exams.

However, there are key limitations and grand challenges on cyber security teaching in both online and face-to-face educational structures. The difficulties are mainly due to a broad range of student backgrounds and a lack of computing resources. In most cyber security programs, students enroll with weak or even no background in computer science and discrete mathematics. For example, based on our own experience in Applied Cryptography, an online course for a cyber security program at our university, over 75% of students do not have any or very weak computer science and discrete mathematics background. Therefore, it becomes challenging to offer labs that accommodate all students in cyber security courses such as, Applied Cryptography and Network Security.

Furthermore, a lack of computing resources such as powerful computers, network devices, and software makes it very difficult to assign many useful and important security lab assignments when those lab assignments require students to have a variety of computing resources such as multiple machines or virtual machines. Sample lab assignment topics include Man-in-the-Middle attack, Denial and Distributed Denial of Service attacks, where multiple machines or virtual machines are needed. The resource problem could be even more challenging when teaching an

online cyber security course, where students are remotely taking a course and cannot physically access computer labs on campus.

For our past teaching in different cyber security courses and workshops, we have developed a broad range of hands-on labs. Our readily-available labs are conducted in our own pre-built virtual machine image, in which we have implemented all necessary tools, software, and security and cryptographic libraries that are needed to elaborate in our developed labs and other widely considered cryptography experiments (e.g., digital certificates, symmetric and asymmetric-key cryptography, hash functions). Students only have to download our pre-built virtual machine, import it into their own computers using a virtualization platform such as VirtualBox or VMware, and then just run it on their own personal computers. As an example, Figure 1 shows a student's view of the virtual environment after a successful login.

Inspired by the SEEDLab project [4], our developed labs have been ported to the latest version of Ubuntu18.04 VM. These labs mainly focus on in the following aspects.

- Network security ranging from a variety of security attacks on TCP/IP and DNS to various network security technologies such as, Firewall, VPN, and IPSec.
- Web security that covers some of the most common vulnerabilities in web applications and attacks that target and exploit web services.
- Applied cryptography that covers three fundamental components in cryptography, including secrete-key encryption, one-way hash function, and public-key encryption and PKI, as well as mobile security that covers the most common vulnerabilities and attacks on mobile devices.

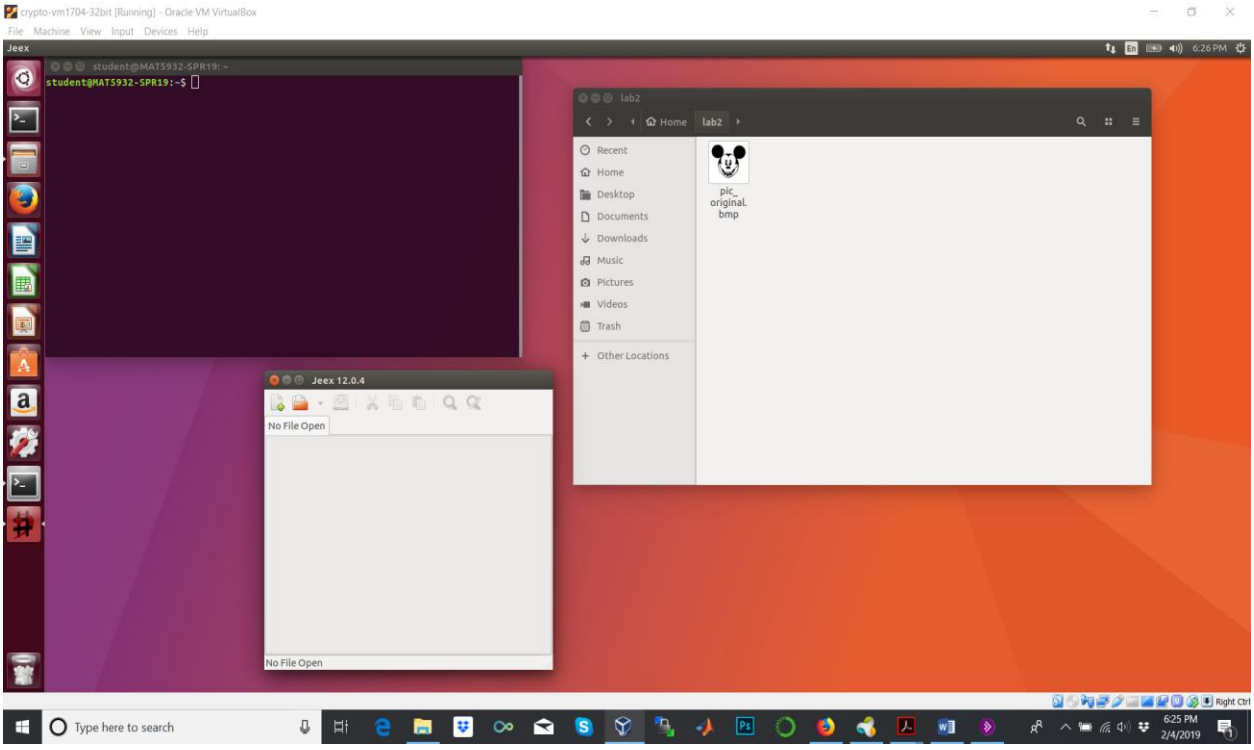

Figure 1: Our pre-built and customized virtual environment for cyber security labs. Our virtual environment consists of a set of tutorials and demos to help those students who have weak backgrounds in computer science and discrete mathematics. Instructor manuals have also been developed to assist future educators who are willing to use our cyber security and cryptography labs.

In the future work, we plan on adopting large-scale cyber security lab modules through the integration of the Global Environment for Network Innovations (GENI) and the currently developed lab modules, where GENI is a real-world, at-scale, programmable, and virtual networking-enabled laboratory for experiments in a variety of computer science and engineering areas such as cyber security and networking. GENI testbed is sponsored by the National Science Foundation (NSF) [1], [2], and [3].

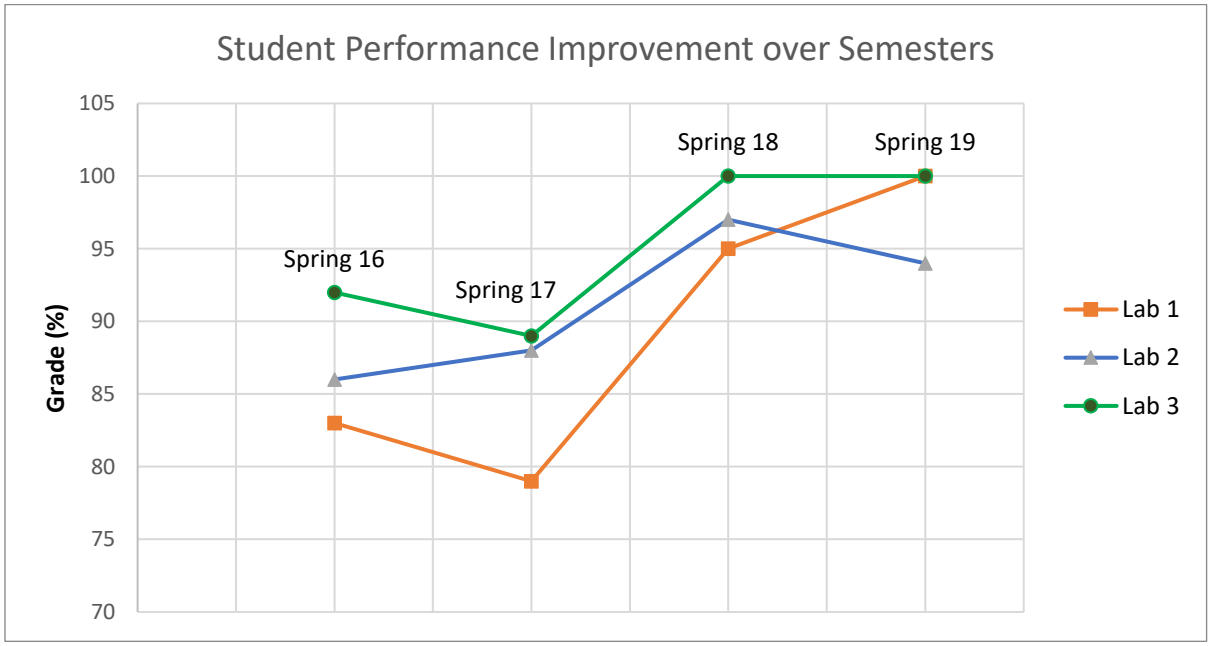

Figure 2: Our students' performance in Applied Cryptography course between Spring 2016 and Spring 2019. Before Spring 2017, we had used existing labs and virtual machine from SeedLab project [4] and starting from Spring 2017, we have introduced our pre-built virtual environment and developed lab modules. The plots demonstrate improvement in the average grade for the three required labs we assign to students in our Applied Cryptography course.

Moreover, Software-Defined Networking (SDN) is an advanced networking technology that has been widely used in cloud computing area and various cyber-physical systems. SDN enhances the network management while allowing for network programmability, monitoring, and security. Therefore, in our future work, we plan to develop a broad range of labs in SDN ranging from beginning to advanced levels in order to accomplish the needs of cyber security industry and education.

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.

References

[1] 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.

[2] Riga, N., Edwards, S., and Thomas, V. (2016). The Experimenter's View of GENI, pages 349–379. In: McGeer R., Berman M., Elliott C., Ricci R. (eds) The GENI Book. Springer, Cham.

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

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