Building a Cybersecurity Pipeline through Experiential Virtual Labs and Workforce Alliances

Dr. Jorge Crichigno, University of South Carolina

Jorge Crichigno received the Ph.D. degree in computer engineering from the University of New Mexico, Albuquerque (NM), USA. He is an Associate Professor in the Integrated Information Technology Department in the College of Engineering and Computing at the University of South Carolina, Columbia (SC), USA. His current research interests are in the areas of network and protocol optimization for high-throughput high-latency systems, and Internet measurements for cyber security. Dr. Crichigno has served as reviewer and TPC member of journals and conferences such as IEEE Transactions on Mobile Computing, IEEE Globecom, and as panelist for the National Science Foundation. He is a member of the IEEE Computer Society and an ABET evaluator representing the IEEE.

Dr. Sadia Ahmed, Northern New Mexico College

Assistant Professor, Chair College of Engineering and Technology Northern New Mexico College

Dr. John H. Gerdes, University of South Carolina

Dr. Gerdes is an Associate Professor in the Department of Integrated Information Technology in the College of Engineering and Computing at the University of South Carolina. Research interests include Web Data Mining, Anonymity, Cybersecurity Electronic Commerce.

Prof. Robert G. Brookshire, University of South Carolina

Dr. Robert G. Brookshire is a Professor in the Integrated Information Technology Department in the College of Engineering and Computing at the University of South Carolina, Columbia, SC. He is the director of the Master of Health Information Technology program. He holds an A.B. from the University of Georgia, an M.Ed. from Georgia State University, and a Ph.D. from Emory University. He has taught at New York University, North Texas State University, the University of Virginia, and James Madison University. He is the co-author of Using Microcomputers for Research (Sage Publications, 1985), and his articles have appeared in the Journal of Computer Information Systems, BYTE, Social Science Computer Review, Legislative Studies Quarterly, The European Journal of Operational Research, and other journals. He is past president of the Organizational Systems Research Association and editor of the Information Technology, Learning, and Performance Journal from 2001 to 2011.

Building a Cybersecurity Pipeline through Experiential Virtual Labs and Workforce Alliances

Abstract

This paper describes a project led by the University of South Carolina (USC) to address the cybersecurity workforce gap. The project creates curricular material based on virtual laboratories (vLabs). As vLabs are developed, they are adopted and tested at USC and Northern New Mexico College (NNMC), the main partnering institution in this project. These vLabs consist of virtual equipment (e.g., virtual network, virtual router, virtual firewall) emulating complete systems on-demand running in NETLAB. NETLAB is a widely used platform for training purposes across the country, with more than 1,000 institutions currently using it. USC and NNMC have also established an alliance with industry organizations and with Los Alamos National Laboratory (LANL) and Savannah River National Laboratory (SRNL) to establish internship opportunities. Currently, student interns are not only exercising technical skills but also developing soft skills such as team work and time management. Finally, in partnership with manufacturer leaders, the project permits students to earn industry certificates. These certificates are aligned with the guidelines for "Information Technology Curricula 2017 for IT programs" by the IEEE/ACM. Specifically, the guidelines indicate that IT should emphasize "learning IT core concepts combined with authentic practice" and "use of professional tools and platforms." Hands-on vLabs activities show that providing access to computing technologies (e.g., professional next-generation firewalls, routers) used in the work environment eases the transition of students from academia to the workplace.

Index Terms

Cybersecurity, information technology, hands-on learning, virtual laboratories.

1. Introduction

This paper presents the implementation of a cybersecurity project that includes hands-on, virtual-lab-based coursework in cybersecurity aligned with workforce needs, internship opportunities, and capstone experiences. The initiatives are implemented at the University of South Carolina (USC) –the leading institution– and Northern New Mexico College (NNMC). These universities are located in key strategic locations near national laboratories and private and public industries, which have pressing needs for professionals with hands-on cybersecurity skills.

The proposed coursework consists of two core courses, one internship course, and one capstone course. Core courses are enriched with many virtual laboratories (vLabs) centered around the fundamental cybersecurity principles. The universities, one of which is a designated National Security Agency (NSA) Center of Academic Excellence in Cybersecurity Defense Education (CAE-CDE), established an alliance with industry and two national laboratories to create internship opportunities in cybersecurity, with the goal of increasing the ability to produce ready-to-work graduates. The institutions are also partnering with employers in the region to strengthen the cybersecurity pipeline and increase the production of professionals to fill regional demand. As

a result, students are immediately applying IT skills in real settings, even before graduation. This activity permits them to gain marketable skills.

2. Project Goals and Tasks

The project has multiple goals, as presented next.

Goal 1: Establish and integrate a cybersecurity curriculum into the bachelor degrees in IT at USC and NNMC.

The programs follow the philosophy of the Wright State Model (WSM)[1] of Education. While they are technology programs, students are required to take math and science up to calculus I. The tasks supporting Goal 1 include:

Tasks for Goal 1

1.1 Create a new cybersecurity core course and implement major modifications in an existing course, which will become the second cybersecurity core course.
1.2 Enhance a pre-requisite course by infusing cybersecurity content.
1.3 Incorporate an internship experience in cybersecurity and establish capstone projects related to cybersecurity.

Execution of tasks for Goal 1: The proposed cybersecurity concentration is being implemented at NNMC (see Fig. 1). USC implements a subset of the courses:

- Introduction to Cybersecurity (3 credits, NNMC): this course is one of the two core courses. The course introduces students to applied cybersecurity.
- Information Assurance and Network Security (3 credits, NNMC): this is the second core course. The course includes intermediate and advanced material to prepare students to positions such as cyber-analysist, threat analysist, Security Operation Center (SOC) technologist, and others.
- At USC, the above two courses are combined in one course.
- Internship (400 hours, USC: mandatory; NNMC: optional): students have 400-hour internship at LANL (NNMC), SRNL (USC), or private or public companies.

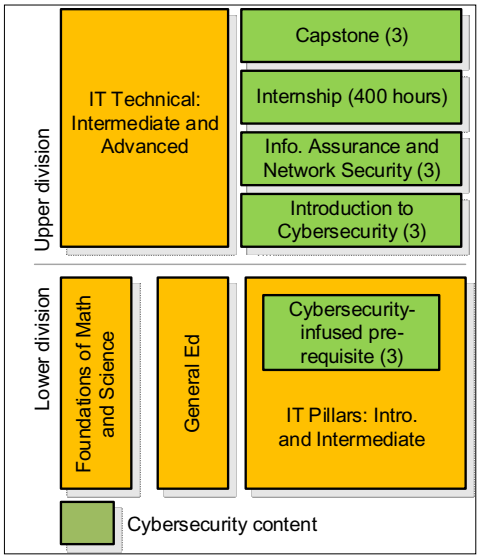

Figure 1. Articulation of the cybersecurity content implemented by NNMC and USC.

- Capstone (3 credits, mandatory at both USC and NNMC): this course culminates the cybersecurity concentration. Students work on original cybersecurity projects, or on projects related to their internships.
- Cybersecurity-infused prerequisite (3 credits): there is a 200-level pre-requisite course that is infused with cybersecurity. Topics include protocol stacks; hardening end devices, routers, and switches; access control lists; mitigation attacks in Local Area Networks (LANs).

Goal 2: Strengthen the pipeline from associate degree to bachelor degree to workforce.

IT programs at USC (bachelor degree) and NNMC (associate and bachelor degrees) have been ABET-accredited for less than 10 years. Since their initial accreditation, the programs have received very strong interest from students. In order to attain Goal 2, the project has executed the following tasks.

Tasks for Goal 2
2.1 Establish cybersecurity-related internships in conjunction with national laboratories and industry.

Execution of tasks for Goal 2: after the first year of the project, the institutions were able to recruit approximately 15 employers plus two national laboratories (LANL and SRNL) which are committed to continue providing internship opportunities. The internships consist of 400 hours, most of them carried out during the summer.

Goal 3: Increase the capacity for education of cybersecurity professionals in South Carolina and New Mexico.

Cybersecurity education is essential for the national laboratories located in South Carolina and New Mexico. To expand the education capacity, this project also organizes training sessions for faculty. The workshops focus on developing virtual labs for cybersecurity courses. Note that a key aim here is to promote the use of portable technology for experiential learning while sharing resources.

Tasks for Goal 3
3.1 Install the equipment necessary for hosting vLabs.
3.2 Offer annual workshops on "Developing Virtual Labs (vLabs)," open to all faculty.
3.3 Increase the number of faculty to produce vLabs.

Execution of tasks for Goal 3: The course material (vLabs and associated manuals) are key for the curriculum implementation. They are portable, ready to use and deployable without the need for configuration or package installation using NETLAB^2. The only file that is required into the virtual environment is a standard Open Virtual Appliance Format (OVA) file containing the necessary virtual machine and hardware orchestration. While the physical devices used to deploy the virtual laboratory are located at USC, the virtual laboratory is available at both institutions and accessible via the Internet. Each lab experiment uses a pod of equipment, e.g., virtual desktops, virtual servers, virtual firewalls, etc. Pods are available 24/7, so that students can access these equipment pods to conduct laboratory experiments. All access is controlled by reservation via a scheduler. The annual workshops are organized twice per year: one in the summer and another in the winter. The workshops are typically 2-day long and covers the full cycle of how to develop virtual labs.

3. First-year Results

After the first year of this three-year project, USC and NNMC have executed most tasks related to Goals 1-3. These tasks and corresponding outcomes are described next.

3.1 Goal 1: Curriculum

A concentration in cybersecurity has been established in NNMC. The same content has also been implemented at USC. The two core courses (Introduction to Cybersecurity and Information Assurance and Network Security) provide students with not only fundamental background but also practical hands-on skills. Virtual laboratories (described in more detail in Section 3.3) were developed to reinforce each major topic, as shown in Table 1. Additionally, the pre-requisite for the two core cybersecurity courses, namely Introduction to Networks, was infused with cybersecurity content.

Table 1. Virtual laboratories implemented for the two core courses of the cybersecurity concentration.

Introduction to Cybersecurity		
Major Modules	**vLab experiments**	**Tools used in vLabs**
Introduction to cybersecurity, malware, applications, and network-based attacks	• Emulating a malware attack and performing reverse shell in Linux and Windows systems • Best practices on protecting against LAN attacks using file system's encryption, port security and role-based authentication.	• Virtual network with end devices running netcad, psexec (tools that allow the user execute commands on a remote machine) • Modern switches capable of implementing port security
Cryptography, symmetric and public-key algorithms, hash functions, digital signatures	• Sending confidential messages using symmetric-key algorithms (AES, DES) • Generating and importing a public key • Sending confidential messages using a public-key algorithm (RSA) • Using digital signatures • Using digital envelops	• Virtual network with end devices running GPG software and a key management server (SKS, an OpenPGP key-server)
Information Assurance and Network Security		
Major Modules	**vLab experiments**	**Tools used in vLabs**
Operational security, next-generation firewalls	• Mitigating attacks by classifying applications (application identification) • Mitigating attacks by inspecting content (content identification) • Blocking malicious URLs • Skills-based assessment: developing zone-based security policies with URL filtering, content identification, and application identification	• Virtual network with end devices and Internet connectivity • Next-generation firewall with state-of-the-art features protecting the virtual network from the Internet
Cyber operations	• Analyzing logs and packet captures to identify injection attacks (e.g., MySQL) • Identifying and extracting malware using packet capture files • Exploit a vulnerable server using known exploits, and review the logs to determine the compromised hosts and file.	• Virtual network with end devices • Kali and Security Onion VMs
Introduction to Networks (pre-requesite)		
Topics	**vLab experiments**	**Tools used in vLabs**
Hardening devices, access control lists and best practices for network management	• Encrypting configuration files • Using hash function to store credentials • Applying access control lists (ACLs) • Sniffing a Telnet sessions for passwords	• Virtual local area networks • Modern routers and switches with management capability

	• Using Secure Shell Protocol (SSH) as a replacement of Telnet for managing devices • Secure local area networks (LANs) by blocking unknown devices based on MAC addresses	

3.2 Goal 2: Internships

USC and NNMC partnered with LANL[3] and SRNL[4]. Both laboratories have large cybersecurity employee needs. LANL provided several internships during year 1. SRNL will offer internships starting year 2. To promote internships, the team organizes workshops on how to apply to them (see Fig. 2). There are two workshops per year: one in the Spring semester and one in the Fall semester.

Additionally, the project team recruited 14 companies looking for interns, summarized in Table 2. Every student completed at least 400 hours of work, and some of them continued as student employees after the summer.

"How to Apply to LANL Internships."

Table 2. Companies and agencies that provided internship positions related to cybersecurity.

Company	Location	Number of internship positions
Los Alamos National Laboratory	Los Alamos, NM	8
Capgemini	Columbia, SC	1
IT Services USC	Columbia, SC	2
SC Department of Education	Columbia, SC	1
USC	Columbia, SC	1
Global Pundits	Lexington, SC	1
Savannah River National Lab	Savannah River Site, SC	1
SC Government	Columbia, SC	1
IBM	Columbia, SC	1
SC Cyber	Columbia, SC	3
U.S. Air Force	Charleston, SC	1
Blue Cross Blue Shield	Columbia, SC	2
SC Election Commission	Columbia, SC	1
Sealed Air	Simpsonville, SC	1
Spirit Communications	Columbia, SC	1
Charles Schwab	Phoenix, AZ	1
TOTAL		**27**

3.3 Goal 3: Capacity of Cybersecurity Education

During the first year, the project team deployed the virtual environment required to host vLabs. Each pod consists of virtual appliances, e.g., virtual desktops, virtual servers, virtual networks, virtual firewall, etc. Virtual appliances have the same capability as physical appliances, as they implement the same software packages.

All pods and associated management equipment are hosted at USC. Pods are managed by an orchestration server (see Fig. 3) which interfaces with remote users (students). To access pods, remote users only use a web browser to connect and login into the system. Within a pod, students can access virtual devices (e.g., virtual switch, virtual IPS, virtual router, etc.) by simply clicking on the lab diagrams. The orchestration server also provides scheduled access to virtual machines and lab equipment. By using a calendar interface, students can view available pods and available timeslots to schedule lab time at their convenience.

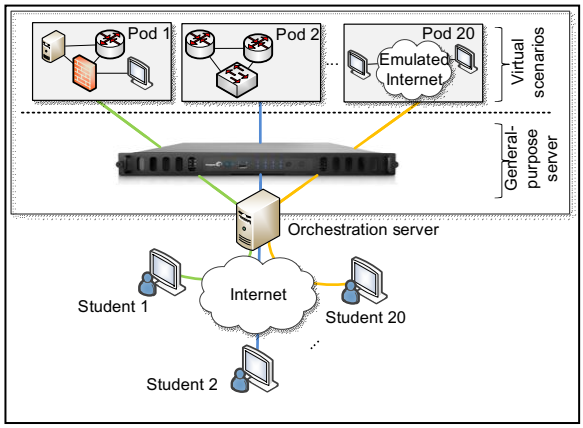

Figure 3. Virtual lab platform.

During year 1, the project team developed two custom pods and 15 vLabs. Additionally, by partnering with Palo Alto Networks[5] and Cisco Systems[6], 15 additional vLabs using state-of-the-art appliances from these companies were incorporated. Fig. 4 illustrates the custom pod used for the cryptography module. The pod consists of four Linux machines (Alice, Bob, Eve, and Key server) and a virtual network. Exercises include topics on public-key and symmetric-key systems, digital signatures, digital envelopes, hash algorithms, web of trust, and others. Note that all vLabs are interactive and provide a real context to students (e.g., transmitting an encrypted message through the virtual network using GPG[8] from Bob and Alice while Eve attempts to intercept the message. GPG is an open source implementation of Pretty Good Privacy[9]).

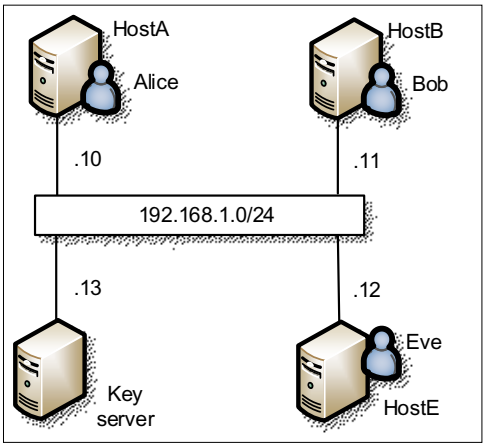

Figure 4. Pod used for cryptographic vLabs.

The second custom pod is a modification of a pod developed by Palo Alto Networks[5], shown in Fig. 5. The pod presents a realistic enterprise setting where security zones are divided according to the levels of trust (e.g., private, demilitarized (DMZ), and public zones). The pod consists of a client, a DMZ server, a next-generation firewall (donated by Palo Alto Networks), and a virtual router connected to the Internet. This pod permits students to experience with features such as application and content identification using real (production) traffic, as Internet connectivity is enabled via the campus network (external network). This pod is used to develop vLabs related to operational security and next-generation firewalls (see Table 1).

Usage of vLabs

Prior to this project, cybersecurity courses were based on traditional lectures, without hands-on activites. During the first year of the project, vLabs were developed and adopted, and incorporated

into one of the two core courses of the cybersecurity concentration (see Fig. 1). The total usage at NNMC was 473 lab reservations. The number of users at NNMC was 20 students/users. Students enrolled in the course used the platform for a total of 625.22 hours (see Fig. 6). Thus, on average each student spent 1.95 hours per week (the course that adopted vLabs was offered on a 16-week schedule).

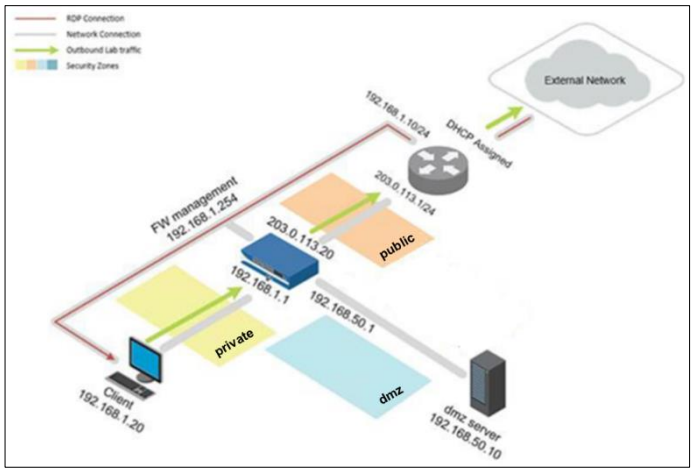

Figure 5. Pod used for operational security and next generation firewalls vLabs.

Similarly, the total usage at USC was 982 lab reservations and 892 labs attended. The number of students/users at USC was 40. Students enrolled in the course used the platform for a total of 1541.28 hours (see Fig. 7). Thus, on average each student spent 2.4 hours per week (the course that adopted vLabs was offered already twice, on a 16-week schedule).

Admin > Usage > Community Usage > List

Community Usage

Search

ID	Name	Reservations Made	Labs Attended	Hours Reserved	Hours Attended
1	default	473	473	2012.76	625.22
	Page Total:	473	473	2012.76	625.22
	Table Total:	473	473	2012.76	625.22

Showing 1 to 1 of 1 items

Figure 6. Usage of virtual laboratories at NNMC.

Admin > Usage > Community Usage > List

Community Usage

Search

ID	Name	Reservations Made	Labs Attended	Hours Reserved	Hours Attended
1	default	982	892	2462.03	1541.28
	Page Total:	982	892	2462.03	1541.28
	Table Total:	982	892	2462.03	1541.28

Showing 1 to 1 of 1 items

Figure 7. Usage of virtual laboratories at USC.

Additional benefits of partnering with the industry

Some vLabs use security appliances provided by Palo Alto Networks and Cisco Systems at no cost. The partnership allows students to access state-of-the-art technology from these two companies. Moreover, students can opt to earn stackable certificates. Note that the joint

IEEE/ACM task group for IT programs released guidelines for IT degrees[10] in December of 2017. According to this document, IT should emphasize "learning IT core concepts combined with authentic practice" and "use of professional tools and platforms." The guidelines also indicate that "educators can ease the transition from academia to the workplace by getting access to computing technologies in the work environment." The IEEE/ACM joint committee also found that "benefits of certified IT employees include better job performance than non-IT certified staff, longer retention, and higher likelihood of receiving promotion." Thus, this project is well aligned with such guidelines.

4. Qualitative Results

While the project team did not collect numerical quantitative results yet, the benefits of using vLabs were capture by an external evaluator who conducted focus group interviews with students.

This section summarizes information during the focus group with eight students, enrolled at NNMC. Participants were interviewed by the project evaluator using a focus group strategy. After a brief summary of the purpose of the focus group, participants introduced themselves and provided their year in college. Six students were seniors, one student was a fifth year senior, and one student was a junior. The group included seven males and one female. The evaluator used the course syllabus to guide the discussion related to course content. Students agreed the course content was relevant to their needs, met or exceeded their expectations, and incorporated a variety of strategies to maximize learning.

Students were asked to describe their experience with vLabs assignments and to share their most significant learning. All of the respondents described the vLabs as a positive new experience rich with learning opportunities. They especially noted the hands-on experiences with the programs and the step-by-step approach accompanied by feedback, including the effects of each action taken. Students also mentioned their "hacking" experiences. One said, "Yeah, that was cool. I like doing that. It was definitely cool to learn and see it actually works. And, to see how someone would do it if they were actually attacking." Students found that the hands-on learning experiences significantly boosted their understanding of the content because the virtual labs provided "real time" knowledge about the consequences of their actions. The instructor acted as a coach in the student-centered labs rather than a didactic instructor where students were allowed to make mistakes but were supported in finding their errors and guided to an adequate solution. Students expressed strong sentiment that they never felt abandoned by the instructor even though he allowed them to sort it out themselves when possible. This repositioning of mistakes lifted pressure and created an enjoyable atmosphere for students to practice and students expressed a good amount of enthusiasm: "Oh that was fun!" Students did offer several recommendations that would provide more scaffolded instruction over a period of time. Few students recommended also conducting some vLabs in class because "they weren't that time consuming" and their questions could be addressed in a timely manner. Frustration was felt by some; however, research supports and shows that when students make mistakes while learning content, that new synaptic connections are made

when they think about why something is wrong, although this can be frustrating[7]. Students' feedback will be incorporated during the second year of the project.

5. Dissemination

The proposed education model relies on virtual labs. As an affordable model (no need for additional technicians and equipment, other than few servers to host vLabs), the project team is committed to make vLabs available to other institutions and to disseminate best practices by organizing workshops on "Developing Virtual Labs." During the first year of the project, two workshops were organized. The first workshop was on January 10-12, 2018 at NNMC. The attendance to this event was 20 instructors (30 instructors registered to the workshop). The second workshop was on July 30-31, 2018 at USC. The attendance was 61 instructors (91 instructors registered to the workshop) from 25 states. The workshop covered the following topics:

- Review of virtual platform infrastructure
- Creating virtual machines
- Design of virtual laboratories
- Design of equipment pods supporting virtual laboratories
- Deploying equipment pods supporting virtual laboratories
- Available resources

Workshops were evaluated using a survey with the following questions:

- Q1: How would you rate the workshop you attended?
- Q2: How would you rate the instructor?
- Q3: How would you rate the presentation materials?
- Q4: How likely are you to attend another workshop?
- Q5: How likely are you to attend an online webinar?

The scores for each question were:

- 5: Extremely satisfied
- 4: Very satisfied
- 3: Moderately satisfied
- 2: Slightly satisfied
- 1: Poor / not at all satisfied

Fig. 8 shows the survey results (averages). Results were very satisfactory and far beyond initial expectations (Q1). Attendees praised the quality of the material (Q3) and the ability and skills of the instructor (Q2). Q4 indicates the desire of instructors to learn about this technology and attend more workshops. Now, as the attendance increased in workshop 2, the quality (see Q5, score of 4.1) was lower. With a high online attendance in workshop 2 (~30 online attendees), the time

allocated for questions from online attendees decreased. Nevertheless, note that the average, even for this large number of participants, was 4.1. We will continue developing virtual labs on a regular basis, as more instructors are now familiar with vLabs.

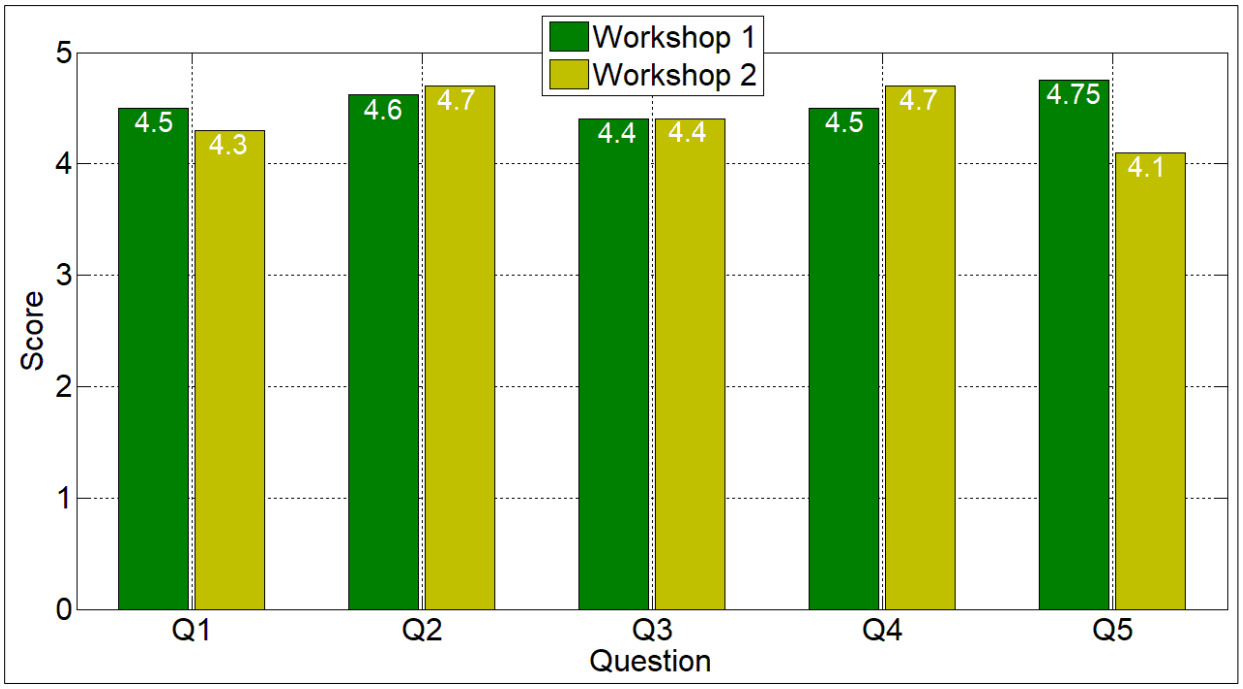

Figure 8. Survey results for the workshops "Developing Virtual Labs." Q1-Q5 refer to the following questions: Q1: How would you rate the workshop you attended? Q2: How would you rate the instructor? Q3: How would you rate the presentation materials? Q4: How likely are you to attend another workshop? Q5: How likely are you to attend an online webinar?

6. Conclusion

This paper presents a hands-on model for cybersecurity education using vLabs. The curriculum is being implemented as part of ABET-accredited programs at the University of South Carolina and Northern New Mexico College. The vLabs permit students to learn core cybersecurity concepts combined with authentic practice and use of professional tools and platforms. The latter is achieved by partnering with leading technology companies, namely Palo Alto Networks and Cisco Systems, that provide virtual appliances used in vLabs. In addition to reinforcing theoretical concepts, vLabs ease the transition of students from academia to the workplace by enabling them apply cybersecurity concepts with state-of-the-art tools.

The proposed model also includes partnerships with national laboratories and industry to create internship opportunities in cybersecurity. After the first year of the project, almost 30 students from USC and NNMC have experienced meaningful 400-hour internship experiences that not only fostered their hard skills (cybersecurity) but also enhanced the efforts to bolster national security and to mitigate the shortage of cybersecurity professionals.

The project team has also organized two 2-day workshops on "Developing Virtual Labs" to disseminate best practices on this technology. Results indicate a very strong interest in the adoption of vLabs, as reflected by the attendance to the workshops (an aggregate of over 100 instructors from more than 70 institutions, 25 states). Future work includes expanding the number of vLabs, increasing the number of internship opportunities, disseminating vLabs, and numerically quantifying the impact of the enhanced cybersecurity model.

Acknowledgement and Disclaimer

Support for this project has been received from the National Science Foundation (NSF) Grant 1822567. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of NSF.

References

1. N. Klingbeil, K. Rattan, M. Raymer, D. Reynolds, R. Mercer, The Wright State Model for Engineering Mathematics Education: A Nationwide Adoption, Assessment and Evaluation, ASEE Annual Conference and Exposition, Austin, TX, June, 2009.
2. NETLAB. Available online: https://www.netdevgroup.com/products/
3. Los Alamos National Laboratory. Available online: https://www.lanl.gov/
4. Savannah River National Laboratory. Available online: https://srnl.doe.gov/
5. Palo Alto Networks. Available online: https://www.paloaltonetworks.com/
6. Cisco Systems. Available online: https://www.cisco.com/
7. D. Kolb, Experiential Learning: Experience as the Source of Learning and Development, Prentice Hall, 1984.
8. GNU Privacy Guard (GPG). Available online: https://www.gnupg.org/
9. J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer, OpenPGP Message Format, Request for Comments 4880. Available online: https://www.ietf.org/rfc/rfc4880.txt
10. Information Technology Curricula Guideline 2017 (IT2017), report by the ACM / IEEE Task Force on Information Technology Curricula, Dec. 2017. Available online: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/it2017.pdf