Improving student learning performance in a virtual hands-on lab system in cybersecurity education

Zhen Zeng
School of Computing, Informatics, and Decision Systems
Arizona State University
Tempe, Arizona, USA
zzeng22@asu.edu

Yuli Deng
School of Computing, Informatics, and Decision Systems
Arizona State University
Tempe, Arizona, USA
ydeng19@asu.edu

IHan Hsiao
School of Computing, Informatics, and Decision Systems
Arizona State University
Tempe, Arizona, USA
sharon.hsiao@asu.edu

Dijiang Huang
School of Computing, Informatics, and Decision Systems
Arizona State University
Tempe, Arizona, USA
dijiang.huang@asu.edu

Chun-Jen Chung
School of Computing, Informatics, and Decision Systems
Arizona State University
Tempe, Arizona, USA
cchung20@asu.edu

***Abstract*—This Research Work in Progress paper presents a study on improving student learning performance in a virtual hands-on lab system in cybersecurity education. As the demand for cybersecurity-trained professionals rapidly increasing, virtual hands-on lab systems have been introduced into cybersecurity education as a tool to enhance students' learning. To improve learning in a virtual hands-on lab system, instructors need to understand: what learning activities are associated with students' learning performance in this system? What relationship exists between different learning activities? What instructors can do to improve learning outcomes in this system? However, few of these questions has been studied for using virtual hands-on lab in cybersecurity education. In this research, we present our recent findings by identifying that two learning activities are positively associated with students' learning performance. Notably, the learning activity of *reading lab materials* ($p < 0.01$) plays a more significant role in hands-on learning than the learning activity of *working on lab tasks* ($p < 0.05$) in cybersecurity education. In addition, a student, who spends longer time on reading lab materials, may work longer time on lab tasks ($p < 0.01$).**

***Index Terms*—cybersecurity education, virtual hands-on lab system, learning performance, learning activity**

I. Introduction

As the demand for cybersecurity-trained professionals rapidly increasing, virtual hands-on lab systems are introduced into cybersecurity class recently as a tool to enhance student learning. The virtual hands-on lab system is a unique learning environment. It integrates lectures and lab environments to support students' "learning by doing [1]". In a virtual hands-on lab, students learn concepts through hands-on practices [2]. Hands-on learning is especially crucial for cybersecurity courses that involve complex concepts and skills (e.g., configuring multiple network servers to simulate information sharing, validation, or cyber-attacks). Moreover, through a virtual hands-on lab platform, instructors are able to reach a large number of students across the virtual space to extend their learning outside the classroom.

This research is to present our study on improving student learning performance in a virtual hands-on lab system for cybersecurity education. This project is to fill the gap of current research on how to improve a student's learning performance in a virtual hands-on lab system in cybersecurity education. In this study, we explore the research questions, such as, what learning activities are associated with student learning performance in this system, what relationship exists between different learning activities, and what instructors can do to better impact learning in this system. In our recent work, we collect learning activities data in a virtual hands-on lab system from a computer network security course. The learning activities of *reading lab materials* and *working on lab tasks* are identified, which are positively associated with student learning performance. This study provides more insights of learning in a virtual hands-on lab system. It helps instructors to understand how these two learning activities might affect each other or hands-on learning outcome. These findings can support instructors to improve teaching by preparing virtual hands-on labs for cybersecurity education.

II. Background

A. Hands-on learning in Computer Science

Hands-on learning is essential in Computer Science education, especially for cybersecurity education [3]. In a hands-

978-1-5386-1174-6/18/$31.00 ©2018 IEEE

on lab, students are "learning by doing [1]" or "learning through practice [4]". Students' learning gains are grounded in their experiences in learning activities in a lab session [2]. Comparing to other research topics in Computer Science education, little research work focuses on hands-on learning in Computer Science education [4]. Moreover, under the content of cybersecurity, fewer studies have been conducted. The published work on studies in cybersecurity education mainly focus on designing a hands-on lab system. For example, there are investigations on a controlled lab environment, where users can safely test security threats and defenses [5], such as an internetwork laboratory for teaching theoretical network security class [6], and a cloud-based virtual hands-on lab system [7]. Among these studies, little work had been focus on how to improve students' learning performance in a virtual hands-on cybersecurity lab.

B. The learning activities of hands-on learning in Computer Science

To the best of our knowledge, the only previous work studying students' learning performance in a hands-on lab in Computer Science education is a theoretical work [4], in which it is a qualitative study to model student's learning activities based on skills, such as *read*, *write*, and *test and debug*. For example, the learning activity of reading code and understanding how to execute code is associated with the skill of *read*; the learning activity of designing and implementing code is associated with the skill of *write*; and the learning activity of reading and understanding error message and correcting error is associated with the skill of *test and debug*.

C. The relationship between learning activities and learning performance

Different learning activities are associated with different knowledge-change processes, and finally lead to different learning outcomes [8]. When reading lab materials, a student is in the knowledge-change process of *storing information*; and when copying some of the problem solution steps or choosing a justification from a menu of options, a student is in the knowledge-change process of *integrating information* [8]. These two knowledge-change processes are not isolated. The learning activities in the process of *storing information* might lead to the learning activities in the process of *integrating information* [8]. A student who integrates information might have better learning outcome than who only stores information [8].

III. Research Hypothesis

Using a cybersecurity hands-on lab, a student usually reads lab material first, and then practices in a hands-on lab environment by implementing, testing and debugging comments. The learning activities of *reading* and *working* are associated with the knowledge-change processes of *storing information* and *integrating information*, respectively. More specifically, in a virtual hands-on lab system, the learning activity of *reading lab materials* (e.g., open a lab instructional webpage, read and understand how to execute comments) is associated with *storing information*. The learning activity of *working on lab tasks* (e.g., implementing, testing and debugging comments) is associated with *integrating information*. Thus, we propose that a student will obtain better learning performance by reading more or working more. Because *storing information* might lead to *integrating information*, we propose that a student who reads more might work more.

In summary, we proposed three hypotheses in this study.

- H1: Student who spends longer time to read lab materials will spend more time on working on lab tasks.
- H2: Student's working time on lab tasks is positively related to learning outcome.
- H3: Student's reading time on lab instructional materials is positively associated with learning outcome.

IV. Research Methods

To examine these three hypotheses, this study analyzes students' data in a computer network security course in the Fall 2016 semester at Arizona State University in the United States. Data was collected from 109 undergraduates and graduate students from a cybersecurity course titled "Computer Network Security". We tracked students' learning activities by logging their actions in a virtual hands-on lab system.

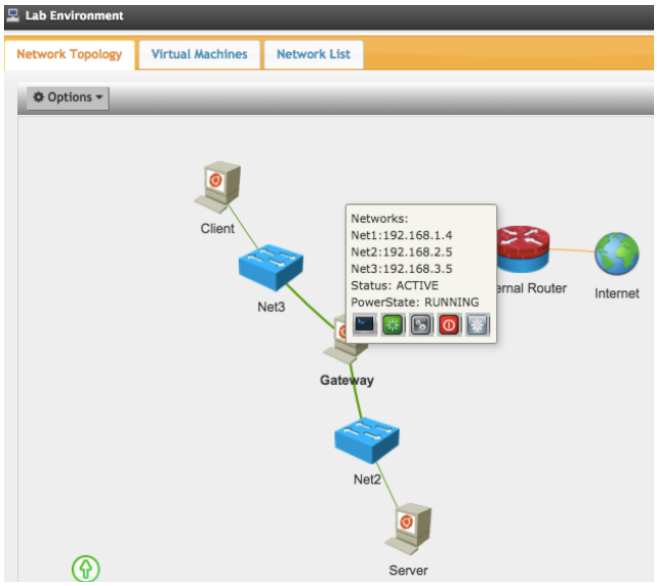

Fig. 1. The example of the firewall lab environment in a virtual hands-on lab system.

A. The virtual hands-on lab system

The virtual hands-on lab used in this study is a web-based, virtualized platform for cybersecurity education [3]. It has positive effect on promoting hands-on practice, reducing training time, and leading to a higher completion rate in Computer Science education [3]. This virtual hands-on lab system can adopt personalized learning capabilities to provide an active personalized learning [9]. All students' activities are tracked for data analysis [10]. Figure 1 shows the firewall lab

environment in this study. In this firewall lab environment, there is a Server and a Client connect to Internet through the Gateway. Three virtual machines are used to construct Server, Client, and Gateway, respectively. Because this virtual hands-on lab system provides a web-based access to each virtual machine in a student's hands-on lab, the student can easily work on the hands-on lab by visiting website from anywhere with Internet access. Moreover, there is no need on student-side installation.

B. An example of a hands-on lab in cybersecurity education

This study collects data from a cybersecurity course titled as "Computer Network Security" at Arizona State University in the United States. This course focuses on introducing practical network security techniques. Students gain hands-on experience on network security techniques by using network analytic and diagnostic tools to complete lab tasks in a virtual hands-on lab system. This course is typically offered to over 200 undergraduates and graduate students on Fall and Spring semester each year. Most students in this course are senior, who are trained on the foundations of Computer Science, such as, programming, operating system, and data structure.

This course includes a lecture session and a lab session. In the lecture session, an instructor elaborates concepts or cases in class by following power point notes. In the lab session, students need to complete lab assignments in this course. All required lab environments have been set up by an instructor. Three key learning objectives covered in this course are:

- *Network basics*: including network service setup and scanning and sniffing. Students gain the fundamental knowledge of computer network system.
- *Network security issue*: including TCP/IP attack, Heartbleed attack, and DNS attack. Students have an inside view of threats that defenders are facing, such as, what are weak points in the current network, and what are attack approaches adversaries use.
- *Network defense*: including the firewalls and intrusion detection systems. Students have opportunities to propose and deploy defense mechanisms.

To better understand learning activities in a cybersecurity hands-on lab, we collect data from the firewall lab assignment. This lab assignment is to practice the usage and functionality of IPTABLES in the firewall. Students learn how to configure IPTABLES for packet filtering. Figure 2 shows the screenshot of a student's work in the firewalls lab, where the student is configuring the system. In this study, all submitted lab assignments are graded based on the number of the completed lab tasks. This firewall lab assignment contains eight lab tasks as follows:

- Use IPTABLES NAT to make the Client virtual machine (VM) and Server VM access to the internet.
- Use NAT to hide Server VM from Client VM.
- Set and check Client. It should be able to Ping Gateway, but cannot Ping Server.
- Set and check Gateway. It should be able to Ping Server. Set Server. It should be able to Ping Gateway.
- Set and check Server. It should be able to initiate an SSH connection to Gateway.
- Set and check Client. It should be able to initiate an SSH connection to Server, using Gateway as NAT.
- Client can access Website hosted on Server, using Gateway as NAT.
- All other traffic should be dropped.

To understand the learning activities in this hands-on lab, we follow the learning model of a previous work on hands-on learning [4] to identify a student's learning activity that associated with the skill of *read* (e.g., open a lab instructional webpage, read and understand how to execute comments) as *reading lab materials*, and the learning activity that associated with the skill of *write* and *test and debug* (e.g., implementing, testing and debugging comments) as *working on lab tasks*. More specifically, the learning activity of *reading lab materials* is measured as the total time that a student is active on the webpage of lab materials. The learning activity of *working on lab tasks* is measured as the total time that a student is active in his/her lab assignment workspace in the virtual hands-on lab system. In this study, we use the time intervals between a student's actions on opening/closing a webpage of lab materials or workspace to calculate the total active time.

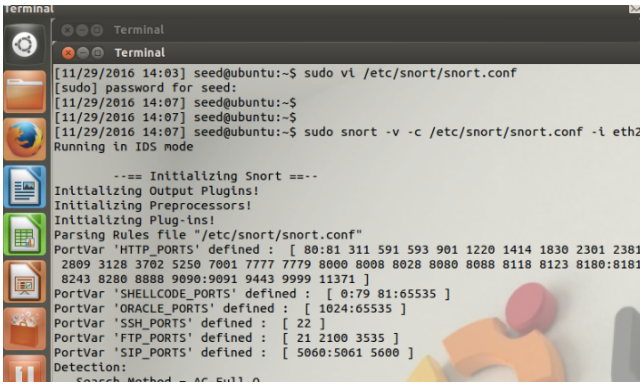

Fig. 2. The example of a student's work in the firewall lab.

TABLE I
STUDENTS' LEARNING ACTIVITIES IN THE FIREWALL LAB

Learning activities	Descriptive statistic summary[a]			
	Mean	*Standard deviation*	*Min*	*Max*
Reading lab materials	26	28	0	82
Working on lab tasks	121	56	42	270

[a]Unit: mins.

Two types of data are extracted from the log data of the virtual hands-on lab system: the amount of time (i.e, minutes) that a student spends on reading lab materials; the duration that a student works on lab tasks. In our data collection period in the 2016 Fall semester, students have nine days to complete eight lab tasks in the firewall lab. Our data are from 104 students who submitted their works for grading. Among them, sixteen students whose grade is zero, eight of them spend 0 minute on reading lab materials. Table I show that, on average,

students spend 26 mins on reading lab material, and spend 121 mins on working on lab tasks. Figure 3 shows the scatter plot of students' time on reading and working. From the visual observation of this scatter plot, there is no prominent outliers.

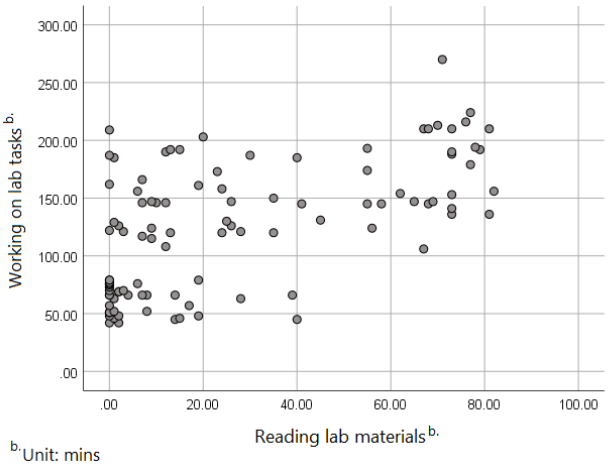

Fig. 3. The scatter plot of students' time on reading lab materials and working on lab tasks in the firewall lab.

C. Spearman's Correlation Coefficient

These three hypotheses examine the monotonic relationship between variables, so the Spearman's correlation coefficient analysis is performed (see Table II). Students' grades of this firewall lab are used as hands-on lab work learning outcomes. After running the Spearman's correlation coefficient analysis in SPSS, the result of H1 indicates that a student's reading time on lab materials significantly affects the working time on lab tasks ($p < 0.01$).

TABLE II
SPEARMAN'S CORRELATION COEFFICIENT

Hypotheses	**Correlation coefficient**	Significant[c]
H1	0.576	0.000**
H2	0.204	0.038*
H3	0.295	0.002**

[c] $^{*}p < 0.05$, $^{**}p < 0.01$.

To examine H2, the result reveals that a student's working time positively affected learning outcome ($p < 0.05$). Notably, the correlation of H3 is strongly significant. In a cybersecurity hands-on lab, the longer time a student reads lab materials, the better learning performance the student might hold ($p < 0.01$).

V. Discussion

This study shows two learning activities in a virtual hands-on lab system are associated with learning performance in cybersecurity education. These two learning activities are *reading lab materials* ($p < 0.01$) and *working on lab tasks* ($p < 0.05$). From the data analysis results in Table II, some findings are revealed. First, when learning in a virtual hands-on lab system, the longer time a student spends on reading lab materials, the more likely s/he works longer time on lab tasks. Such results indicate that when a student spends time on reading, s/he is not just superficially skimming, but is storing knowledge for hands-on practices [11]. Second, we found that in a cybersecurity hands-on lab, working longer does not always lead to better learning outcome; only if the student also engages in reading lab materials, s/he would improve the learning.

VI. Conclusion

This study provides more insights of learning in a virtual hands-on lab system in cybersecurity education from two important points. First, we identify two key learning activities that associated with learning performance. These two learning activities are *reading lab materials* and *working on lab tasks*. These two learning activities are associated with the key skills of hands-on learning, which are *read*, *write* and *test and debug*. Second, there is an association between these two learning activities. A student, who spends longer time on reading lab instructional material, may work longer time on lab tasks. These findings help instructors to understand how a student learns in a virtual hands-on lab system, and how learning activities affect learning performance. To better impact learning in virtual hands-on lab systems, instructor can focus on monitoring learning progress on these two key learning activities.

In addition, our current findings show that the longer time that a student works, does not mean that the student works more and learns more. Even though the hands-on learning is learning by doing, the learning activity of *reading lab materials* plays a more significant role on learning in a cybersecurity hands-on lab. A student unblocks misconceptions or develops new knowledge by reading [11]. Thus, if instructors can provide more personalized lab materials, students might gain more in their hands-on lab learning.

VII. Future Work

In future, we plan to extend our work to explore more methods on improving student hands-on learning in cybersecurity education by effective reading. For example, what factors affect reading time in a hands-on lab in cybersecurity education, and how we can improve students reading gains to better support their hands-on learning.

Acknowledgment

This study is based upon work supported by the National Science Foundation under Grant No. DGE-1723440.

References

[1] L. E. Carlson and J. F. Sullivan, "Hands-on engineering: learning by doing in the integrated teaching and learning program," International Journal of Engineering Education, vol. 15, pp. 20-31, 1999.
[2] W. Du, "SEED: hands-on lab exercises for computer security education," IEEE Security & Privacy, vol. 9, pp. 70-73, 2011.
[3] L. Xu, D. Huang, and W.-T. Tsai, "Cloud-based virtual laboratory for network security education," IEEE Transactions on Education, vol. 57, pp. 145-150, 2014.

[4] A. Eckerdal, "Relating theory and practice in laboratory work: A variation theoretical study," Studies in Higher Education, vol. 40, pp. 867-880, 2015.
[5] J. Mirkovic and T. Benzel, "Teaching cybersecurity with DeterLab," IEEE Security & Privacy, vol. 10, pp. 73-76, 2012.
[6] R. T. Abler, D. Contis, J. B. Grizzard, and H. L. Owen, "Georgia tech information security center hands-on network security laboratory," IEEE Transactions on Education, vol. 49, pp. 82-87, 2006.
[7] L. Xu, D. Huang, and W.-T. Tsai, "V-lab: a cloud-based virtual laboratory platform for hands-on networking courses," in Proceedings of the 17th ACM annual conference on Innovation and technology in computer science education, 2012, pp. 256-261.
[8] M. T. Chi and R. Wylie, "The ICAP framework: Linking cognitive engagement to active learning outcomes," Educational Psychologist, vol. 49, pp. 219-243, 2014.
[9] Y. Deng, D. Huang, and C.-J. Chung, "ThoTh Lab: A Personalized Learning Framework for CS Hands-on Projects," in Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education, 2017, pp. 706-706.
[10] Z. Zeng, Y. Deng, S. Hsiao, D. Huang, and C.-J. Chung, "Conceptualizing Student Engagement in Virtual Hands-on Lab: Preliminary Findings from a Computer Network Security Course," in Proceedings of the 49th ACM Technical Symposium on Computer Science Education, 2018, pp. 1073-1073.
[11] W. Campbell and E. Bolker, "Teaching programming by immersion, reading and writing," in Frontiers in Education, 2002. FIE 2002. 32nd Annual, 2002, pp. T4G-T4G.