Virtual Laboratory: Facilitating Teaching and Learning in Cybersecurity for Students with Diverse Disciplines

Dennis Y. W. Liu
Department of Computing
The Hong Kong Polytechnic University
Hong Kong SAR
dyw.liu@polyu.edu.hk

Alven C. Y. Leung
Department of Computing
The Hong Kong Polytechnic University
Hong Kong SAR
chi-yan.al.leung@polyu.edu.hk

Man Ho Au
Department of Computing
The Hong Kong Polytechnic University
Hong Kong SAR
man-ho-allen.au@polyu.edu.hk

Xiapu Luo
Department of Computing
The Hong Kong Polytechnic University
Hong Kong SAR
csxluo@comp.polyu.edu.hk

Pit Ho Patrio Chiu
Office of Education Development and Gateway Education
City University of Hong Kong
Hong Kong SAR
patrio.chiu@cityu.edu.hk

Siu Wo Tarloff Im
Office of Education Development and Gateway Education
City University of Hong Kong
Hong Kong SAR
siuwoim3@cityu.edu.hk

Winnie W. M. Lam
Department of Mathematics and Information Technology
The Education University of Hong Kong
Hong Kong SAR
winnielam@eduhk.hk

***Abstract*—Cybersecurity education is a pressing need, when computer systems and mobile devices are ubiquitous and so are the associated threats. However, in the teaching and learning process of cybersecurity, it is challenging when the students are from diverse disciplines with various academic backgrounds. In this project, a number of virtual laboratories are developed to facilitate the teaching and learning process in a cybersecurity course. The aim of the laboratories is to strengthen students' understanding of cybersecurity topics, and to provide students hands-on experience of encountering various security threats. The results of this project indicate that virtual laboratories do facilitate the teaching and learning process in cybersecurity for diverse discipline students. Also, we observed that there is an underestimation of the difficulty of studying cybersecurity by the students due to the general image of cybersecurity in public, which had a negative impact on the student's interest in studying cybersecurity.**

Keywords—cybersecurity education, virtual laboratory, experiential learning

I. INTRODUCTION

With the growth of public awareness of cybersecurity, cultivating professionals to cope with the challenges becomes a pressing need in tertiary education these days [1, 2, 3, 4]. Nowadays, cyber threat is in a "blended" form in the sense that computers and mobile devices are susceptible to multi-pronged attacks. Also, the adoption of financial technologies in the industries increases the demand of experts in cybersecurity.

These days, lots of universities in the world offer courses/programmes in cybersecurity [5, 6, 7, 8], and there are extensive researches in this area [9, 10, 11, 12, 13, 14, 15, 16]. For example, there was a claim that the students from the undergraduate programs in computer science at U.S. universities fail to gain the concepts and awareness to implement security knowledge in coding, development, and testing [17].

There are several challenges in teaching and learning cybersecurity in tertiary education. First, cybersecurity requires a strong background in computing theories, including programming, computer architecture, network communication, and cryptography. Integrating these concepts systemically for the cybersecurity context is no easy task for students while lacking some of the concepts will make the learning curve "steeper" during the study in cybersecurity. Second, tertiary education normally puts more emphasis on theories and puts less focus on enhancing the practical skill sets of the students. Hands-on skills like web application, network and system-level programming are essential to cybersecurity professionals so that they are able to develop robust systems and have the ability to debug such systems. Third, there are always new emerging security threats, like system intrusion, malicious surveillance and ransomware attack. Both the teachers and students are required to keep abreast of the technology advancement and be familiar with the preventive mechanisms. Fourth, it is always expected that students studying cybersecurity in tertiary education should have an intermediate-to-advanced background in computing. However, due to the emerging of financial technologies like blockchain and cryptocurrency [18], students from various disciplines, e.g., finance and logistics, are required to study cybersecurity as well. Due to the variance of student background, the traditional approach of course delivery is unable to achieve the course outcome satisfactorily.

Teaching and learning cybersecurity are technology intensive in a sense that lecture/tutorial/laboratory delivery has to supplement with e-learning tools, e.g., visualization tools, network sniffers, and vulnerability programs. Also, without active participation and practices, students are unable

to grasp the ideas of cybersecurity, particularly for the concepts of intrusion attacks and cryptographic, which require substantial hands-on experiences. Furthermore, some pedagogical researches [19, 20, 21, 22] have shown that hands-on laboratories are crucial to the success of cybersecurity courses. In this case, integrating virtual laboratories in the course has high feasibility for resolving the issues in educating cybersecurity.

The objective of this project is to answer the following question:

> *"Can virtual laboratories facilitate the teaching and learning process in cybersecurity courses with students from diverse disciplines?"*

II. The Project

A. Design

In our project, three virtual laboratories, which capture the essential concepts, namely "Cryptography", "Authentication", "Access Control", "Software Vulnerability", and "Web Security", in cybersecurity are designed and integrated into a cybersecurity course. The pedagogy includes two major elements. First, the traditional lecture sessions introduce the theoretical background of the topics. For the virtual laboratories, students are given hands-on laboratory tasks, including programming and debugging, as well as utilizing common cybersecurity tools like Wireshark [23] for program and data analysis.

The followings are the background and details of the three laboratories:

- **WannaCry Ransomware Attack Lab:** WannaCry [24] is a crypto ransomware that caused a worldwide attack to millions of computers in 2017. In this lab, students are given a simplified version of WannaCry ransomware program to simulate the WannaCry ransomware attack. By understanding the vulnerability of WannaCry ransomware, students will understand more about the cryptographic algorithms adopted by WannaCry and be able to perform a reverse-engineering process and recover the encrypted files from WannaCry attack. This lab covers the topic, "Cryptography".

Fig. 1. Sample Screen of the WannaCry Ransomware Attack Lab

- **Dictionary Attack Lab:** In this lab, password security is examined thoroughly. Students are given a network sniffing tool, named Wireshark [23], to examine the detailed message flows of a web-based user authentication system. The learning objective is to help students understand the concepts of password security in online authentication process. This lab covers the topics, "Authentication" and "Web Security".

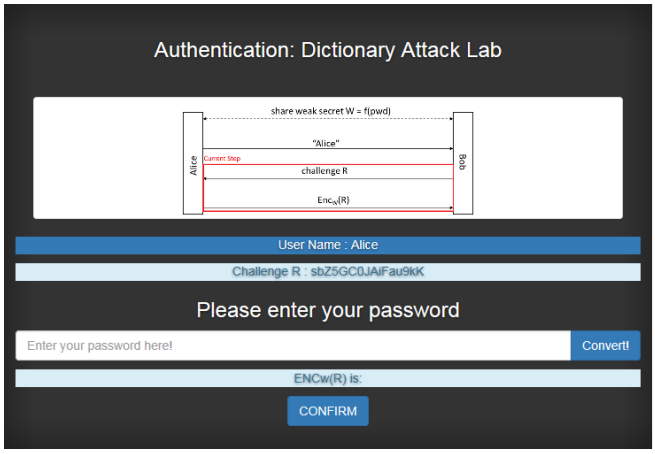

Fig. 2. Sample Screen from Authentication: Dictionary Attack Lab

- **Buffer Overflow Vulnerability Lab:** Buffer overflow is defined as the condition in which a program attempts to write data beyond the boundaries of pre-allocated fixed length buffers. This vulnerability can be utilized by a malicious user to alter the flow control of the program and execute arbitrary pieces of code. In this lab, students will be given a program with buffer overflow vulnerability, which is susceptible to program crashes and violation of access rights. With reference to a well-developed buffer overflow laboratory by [25], students are given programming tasks to perform attacks and understand the principles behind, which include computer memory organization and access control in operating systems. This lab covers the topics, "Software Vulnerability" and "Access Control".

B. Participants

The laboratories were designed for a cybersecurity course (twelve teaching weeks) in undergraduate level and have been implemented in the semesters 1 & 2 in the academic year 2018-19. TABLE I shows the outline of the course.

TABLE I. Course Outline

Week	Lecture/Laboratory	Course Element
1	Lecture	Introduction to Computing Security
2-4	Lecture	Cryptography
5	**Laboratory**	**WannaCry Ransomware Attack Lab**
6-7	Lecture	Authentication
8	**Laboratory**	**Dictionary Attack Lab**
9-10	Lecture	Advanced Computing Security Topics
11	**Laboratory**	**Buffer Overflow Vulnerability Lab**
12	Lecture	Web Security

There are 146 students involved. All of them are undergraduate students from various disciplines. TABLE II shows their major streams and their enrolment numbers.

TABLE II. MAJOR STREAMS OF THE STUDENTS

Streams	Number of Enrolled Students
Computing	52
Enterprise Information Systems	3
Financial Technology	32
Information Security	37
Information Technology	22

While all the students are at least sophomores, they have different academic backgrounds in computing and cybersecurity. Students from the "Computing", "Information Security", and "Information Technology" streams are relatively having a solid technical background. In contrast to these three streams, the "Enterprise Information System" stream focuses more on soft skills, while at least half of the students of "Financial Technology" are having purely business background, like marketing and finance. The difficulty here is that the design of the course should be able to cater for the needs of students with different backgrounds and achieve the learning outcomes of the course.

C. Objectives

We realize "Learning by doing" or "Experiential learning" [26] is the right approach in the context of cybersecurity education. Our specially designed virtual laboratories provide hands-on experiences to the students. Through common applications and security threats that the students encounter in daily life, it serves as a good starting point for them to understand the security concepts behind the scene. The laboratories are designed to fulfill the following objectives:

- Familiarize students with the models and practical principles to protect computer systems from various attacks.
- Deepen students' understanding of the major problems in computer systems.
- Teach the students the countermeasures for mitigating the cyber-attacks.
- Enable the students' practical skills for analysing the security of computer systems by using various resources and tools.
- Educate the students to be ethical professionals in the field of cybersecurity.

D. Research Method

This project adopts both quantitative and qualitative research methods to assess its effectiveness. We collected the student expectation at the beginning of the course, as well as their feedback at the end of the course. In the first lesson, students were required to complete a pre-questionnaire. In the last lesson, a post-questionnaire was given to the students.

The pre-questionnaire is used for collecting the students' background information, such as major stream, current year of study and their impression on cybersecurity. It also includes the questions for eliciting the students' expectations of the course.

The questions in the post-questionnaire are mostly identical to those in the pre-questionnaire. In addition, it includes open-ended questions for eliciting their suggestions for course improvement.

The questions of pre- and post-questionnaire are shown in TABLE III. Q1 to Q11 are five-point Likert scale questions: 1. Strongly disagree; 2. Disagree; 3. Uncertain; 4. Agree; 5. Strongly Agree. Q1 to Q7 are used to measure their interest and level of understanding in cybersecurity and its topics, before and after the course delivery. Specifically, Q8 to Q11 appear only in the post-questionnaire and are used to assess the effectiveness of the designed virtual laboratories. Q12 and Q13 are open-ended questions. Q12 collects their expectations and feedback of the course, particularly in the view of the virtual laboratories. Q13 elicits the topics that the students are interested in most.

The collected questionnaire data were analysed using IBM SPSS software. In our project, IBM SPSS Statistics 25 is used to make independent sample *t*-test and descriptive statistics for Q1 to Q11. Also, we used IBM SPSS Modeler 18.0 to make text analytics for Q12 to Q13.

Results of both quantitative and qualitative research are used to measure the effectiveness and feasibility of our teaching and learning approach. Also, they shed some light on the limitations and weaknesses of this learning approach, which is useful for future improvement for the course.

III. OUR RESULTS

One hundred and twelve students responded to the pre-questionnaire (N = 112), and eighty-four students responded to the post-questionnaire (N = 84).

TABLE III. QUESTIONS OF PRE- AND POST-QUESTIONNAIRE

	Questions
Q1.	I am interested in topics of cybersecurity.
Q2.	Before studying the course, I understand what "Cryptography" is.
Q3.	Before studying the course, I understand what "Authentication" is.
Q4.	Before studying the course, I understand what "Access Control" is.
Q5.	Before studying the course, I understand what "Software Vulnerability" is.
Q6.	Before studying the course, I understand what "Web Security" is.
Q7.	I think studying cybersecurity is difficult.
*Q8.	The "WannaCry Ransomware Attack Laboratory" was helpful in strengthening my understanding of the topics covered in the lecture.
*Q9.	The "Authentication: Dictionary Attack Laboratory" was helpful in strengthening my understanding of the topics covered in the lecture.
*Q10.	The "Software Vulnerability Laboratory" was helpful in strengthening my understanding of the topics covered in the lecture.
*Q11.	I think computer-aided tools are important to facilitate the study of cybersecurity.
Q12.	Do you have any suggestion/expectation for the laboratory session? If yes, please provide details.
Q13.	Name one topic of cyber security that you are particularly interested in.

*Q8 to Q11 only appear in post-questionnaire

A. *Effectiveness*

The results of the questionnaires are summarized in TABLE IV and TABLE V.

TABLE IV. RESULTS OF Q1 TO Q7 (DESCRIPTIVE STATISTICS)

Questions	Pre/Post	Mean	SD
Q1.	Pre	4.00	0.81
	Post	3.79	0.79
Q2.	Pre	3.21	1.22
	Post	4.12	0.61
Q3.	Pre	3.51	1.12
	Post	4.13	0.64
Q4.	Pre	3.54	1.01
	Post	3.93	0.70
Q5.	Pre	3.00	1.12
	Post	3.77	0.72
Q6.	Pre	3.31	0.93
	Post	4.10	0.63
Q7.	Pre	3.53	0.86
	Post	3.83	0.86

*Five-point Likert Scale: 1 (Strongly Disagree) to 5 (Strongly agree)

TABLE V. RESULTS OF Q1 TO Q7 (INDEPENDENT SAMPLES T-TEST)

Questiona	Levene's Test for Equality of Variances		t-test for Equality of Means		
	F	*Sig.*	*t*	*df*	*Sig. (2-tailed)*
Q1.	2.147	0.145	-1.856	194	0.065
Q2.	50.203	0.000	6.881	171.939	0.000
Q3.	30.045	0.000	4.906	181.763	0.000
Q4.	19.186	0.000	3.153	192.405	0.002
Q5.	17.375	0.000	5.869	189.579	0.000
Q6.	20.342	0.000	7.003	192.318	0.000
Q7.	0.969	0.326	2.469	194	0.014

The mean value of Q2 improves 0.91 point (from 3.21 to 4.12), and the significant value from *t*-test is 0.000, which indicates that the students have more understanding about "Cryptography" after taking the course. We believe that the WannaCry Ransomware Attack Lab plays a crucial role in which a practical example is provided to them to study and get familiar with the concepts in "Cryptography".

For Q3, the mean value improves 0.62 point (from 3.51 to 4.13), and the significant value from *t*-test is 0.000. Also, Q6 mean value has improved 0.79 points (from 3.31 to 4.20), and the significant value from *t*-test is 0.000. These two results indicate that the students have more understanding about "Authentication" and "Web Security". Again, these significant improvements can be linked to the effectiveness of the "Dictionary Attack Lab".

The mean value of Q4 improves 0.39 point (from 3.54 to 3.93), and the significant value from *t*-test is 0.002. Furthermore, Q5 mean value has improved 0.77 point (from 3.00 to 3.77), and the significant value from *t*-test is 0.000. Results of Q4 and Q5 indicate that the students have more understanding about "Access Control" and "Software Vulnerability". In other words, We realize that "Buffer Overflow Vulnerability Lab" is able to strengthen students' concepts in these topics.

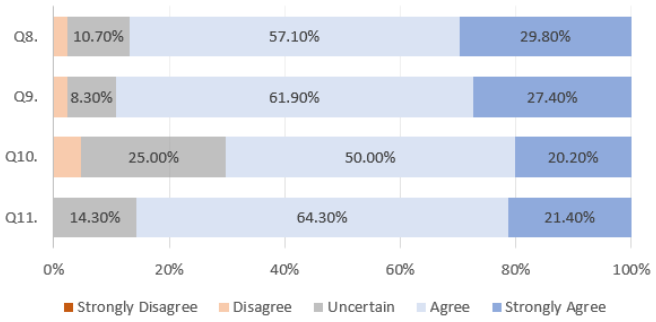

Fig. 3. Results of Q8 to Q10

The effectiveness of the three laboratories can be confirmed by the results of Q8, Q9 and Q10. There are 86.9%, 89.3% and 70.2% of respondents agree that "WannaCry Ransomware Attack Lab", "Dictionary Attack Laboratory" and "Software Vulnerability Laboratory" were helpful respectively.

For Q11, none of the respondents disagree the fact that computer-aided tools are essential to facilitate the study of cybersecurity, even though 14.5% of the students are still uncertain of their effectiveness. Therefore, it implies that computer-aided tools, if properly designed, can facilitate the learning process in cybersecurity.

B. *Suggestions/Feedback from Participants*

Q12 and Q13 are used to seek for the suggestions/feedback from the students on the course and their interested cybersecurity topic(s). These suggestions/feedback can help the teaching team improve the course in the future. All the answers from Q12 and Q13 are passed to IBM SPSS Modeler 18.0 for text analytics. The result is shown in TABLE VII.

TABLE VII. RESULTS OF Q12 TO Q13 (TEXT ANALYTICS)

Questions	Concepts	Frequency Count (Percentage)
Q12.	Lab	10 (13%)
	Example	2 (3%)
	Lecture	2 (3%)
Q13.	Cryptography	27 (18%)
	Web Security	20 (13%)
	Blockchain	15 (10%)

*Only the top three interested concepts are shown.

In total, there are 77 responses for Q12 and 150 responses for Q13 in the pre- and post-questionnaire. The most mentioned concept for Q12 is "Lab". The followings are some of the responses from Q12:

"I think more labs would be better"

"More lab, More interesting topic"

"Increase the number of laboratory lessons"

"More lab instead of lecture will raise up the interest of the lesson"

"The lab is very useful to us"

The responses from Q12 show that the participants have positive emotion about the use of virtual laboratories for cybersecurity education.

For Q13, the top 3 ranked topics of interest are “Cryptography”, “Web Security”, and “Blockchain”. It is not out of our expectation that students are interested to topics in cybersecurity which are related to the state-of-the-art technologies and frequently encountered in real-life applications.

IV. Discussion

In this project, we designed three virtual laboratories for improving the effectiveness of teaching cybersecurity to undergraduate students with diverse disciplines. After all, the research results show that our approach is effective. Responses from the participants showed their positive emotion about the virtual laboratories. Also, it shows that virtual laboratories are able to strengthen the students' understanding of various topics in cybersecurity, namely Cryptography, Authentication, Web Security, Software Vulnerability and Access Control. Our approach allows students to first have an understanding of common applications and their security requirements. The applications for the laboratories were built in a way that the students were able to understand and experience the roles of various cybersecurity mechanisms. It is particularly effective for students having less technical background, like the students of the “Enterprise Information Systems” and “Financial Technology” programme.

But still, the teaching team realizes that teaching students with diverse disciplines in the same course is challenging due to a wide spectrum of knowledge level in computing. The students who have a solid background in computing can quickly accomplish most of the tasks, while some of the students need to put a lot of effort on understanding the lab requirement and the knowledge required to complete the tasks. In this case, the teaching team had to provide more support and guidance to them. Although they need to spend more time studying and completing the tasks, we realize there is a significant improvement on the understanding of the course materials after completing the laboratory tasks. Besides, the laboratory tasks were designed with various difficulty levels, e.g., basic, intermediate and advanced levels, so that students were able to achieve the learning outcomes progressively.

There is an interesting observation that although the learning approach improved the effectiveness of teaching cybersecurity, it decreased the students’ interest in cybersecurity. It can be realized by the result of Q1. The mean value decreases by 0.21 point (from 4.00 to 3.79), and the significant value from *t*-test is 0.065. We believe that it is due to the fact that the students underestimated the difficulty in learning cybersecurity. From Q7, the mean value decreases by 0.30 points (from 3.53 to 3.83), and the significant value from *t*-test is 0.014. Due to the underestimation, the students lose interest in studying cybersecurity. The underestimation may be due to a false expectation by students, because of the “fancy” image of cybersecurity, generated by various sources of the media, like news and movies. Before studying the course, what the students can normally see about cybersecurity is the “heroic” side of security professionals, while misunderstanding the difficulty of being a well-qualified one. Also, some students may have insufficient background to understand various concepts of cybersecurity. Due to the steep learning curve, some students gradually lose interest in studying cybersecurity.

To solve the above-mentioned problem, we suggest that virtual laboratories should be designed using a top-down approach. Cybersecurity educators may first figure out the hot security issues/threats that are attractive to the students. Then, extract the necessary cybersecurity concepts behind these issues/threats. Finally, design the virtual laboratory so that they can have hands-on practices in which those addressed issues/threats can be encountered. For example, in our research, we realize that WannaCry is a good and well-known practical example for demonstrating the ideas of cryptographic algorithms. By building up a simplified version of WannaCry and develop a set of relevant tasks/exercises in the virtual laboratory, students show more interest and are able to grasp the concepts easier. Besides, at the end of our research, it is discovered that the students are interested in the security in “Blockchain”. In the future, a virtual laboratory can be developed for the students to understand the security requirements and mechanisms of blockchain-based system.

V. Conclusion and Future Work

Cybersecurity education is no easy task. It is even more challenging when the students are from diverse disciplines with various academic backgrounds. In our project, a number of virtual laboratories are developed to facilitate the teaching and learning process in a cybersecurity course. The aim of the laboratory is to strengthen students' understanding of cybersecurity topics, and to provide students hands-on experience of encountering various security threats.

The results of this project indicate that virtual laboratories do facilitate the teaching and learning process in cybersecurity for diverse discipline students and fulfilled the learning objectives of the course.

However, we realize a decrease of the students’ interest in cybersecurity in general. To alleviate the situation, educators should strive to understand the hot topics that the students are particularly interested in, and then design and develop relevant teaching materials and virtual laboratory exercises. Also, students’ misconceptions about cybersecurity lead to an underestimation of the complexity and subtlety of the topics. It is recommended that educators should seek ways to help student recognize the right image of cybersecurity.

Acknowledgment

This project is supported by the Teaching Development Grant (TDG) 2016-19, The Hong Kong Polytechnic University.

References

[1] O. Margalit, "Using Computer Programming Competition for Cyber Education," in *2016 IEEE International Conference on Software Science, Technology and Engineering*, Beer-Sheva, Israel, 2016.

[2] H. Aldawood and G. Skinner, "Educating and Raising Awareness on Cyber Security Social Engineering: A

Literature Review," in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering*, Wollongong, NSW, Australia, 2018.

[3] J. Addae, M. Radenkovic, X. Sun and D. Towey, "An extended perspective on cybersecurity education," in *IEEE International Conference on Teaching, Assessment, and Learning for Engineering*, Bangkok, Thailand, 2017.

[4] J. LeClair, K. M. Hollis and D. M. Pheils, "Cybersecurity education and training and its Reliance on STEAM," in *2014 IEEE Integrated STEM Education Conference*, Princeton, NJ, USA, 2014.

[5] W. Du, "SEED: Hands-On Lab Exercises for Computer Security Education," *IEEE Security & Privacy*, vol. 9, no. 5, pp. 70-73, 2011.

[6] J. T. Terry, H. Yu, K. Williams and X. Yuan, "A Visualization based Simulator for SYN Flood Attacks," in *the International Conference on Imaging Theory and Applications and International Conference on Information Visualization Theory and Applications*, Vilamoura, Algarve, Portugal, 2011.

[7] J. Tao, J. Ma, M. S. Keranen and J. Mayo, "RSAvisual: A visualization tool for the RSA cipher," in *the 45th ACM technical symposium on Computer science education*, Atlanta, Georgia, USA, 2014.

[8] L.-C. Chen, L. Tao, X. Li and C. Lin, "A Tool for Teaching Web Application Security," in *the 14th Colloquium for Information Systems Security Education*, Baltimore, Maryland, 2010.

[9] H. Yu, X. Yuan, J. H. Kim, J. Xu and T. Kim, "Using Cybersecurity Education Tool Assessment Method to Measure the Effective of Different Teaching Methods," in *the World Congress on Engineering 2016*, London, U.K., 2016.

[10] A. Abuzaid, H. Yu, X. Yuan and B. Chu, "The Design and Implementation of a Cryptographic Education Tool," in *the 3rd International Conference on Computer Supported Education*, Noordwijkerhout, Netherlands, 2011.

[11] C. Willems and C. Meinel, "Online assessment for hands-on cyber security training in a virtual lab," in *IEEE Global Engineering Education Conference*, Marrakesh, Morocco, 2012.

[12] R. Matusa, L. Butkus, T. Krilavičius, K. L. Man and H.-N. Liang, "Improving the teaching of Computer Networks through the incorporation of industry based training courses," in *2013 IEEE International Conference on Teaching, Assessment and Learning for Engineering*, Bali, Indonesia, 2013.

[13] T. Kakeshita, K. Matsunaga and K. Sado, "A Comparison Analysis between Achievement and Requirements for Computing Education," in *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering*, Wollongong, NSW, Australia, 2018.

[14] D. Towey, "Lessons from a failed flipped classroom: The hacked computer science teacher," in *2015 IEEE International Conference on Teaching, Assessment, and Learning for Engineering*, Zhuhai, China, 2015.

[15] S. Pancho-Festin and M. J.-a. Mendoza, "Integrating computer security into the undergraduate software engineering classes: Lessons learned," in *2014 IEEE International Conference on Teaching, Assessment and Learning for Engineering*, Wellington, New Zealand, 2014.

[16] R. Y.-Y. Chan, K. M. Ho, S. Jia, Y. Wang, X. Yan and X. Yu, "Facebook and information security education: What can we know from social network analyses on Hong Kong engineering students?," in *2016 IEEE International Conference on Teaching, Assessment, and Learning for Engineering*, Bangkok, Thailand, 2016.

[17] "CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education," CloudPassage, [Online]. Available: https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/.

[18] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf.

[19] J. Hill, C. Carver, J. Humphires and U. Pooch, "Using an Isolated Laboratory to Teach Advanced Networks and Security," *SIGCSE Bulletin: Proc. 32nd Technical Symposium on Computer Science Education,* vol. 33, pp. 36-40, March.

[20] P. Mateti, "A Laboratory-Based Course on Internet Security," *SIGCSE Bulletin: Proc. 34th Technical Symposium on Computer Science Education,* vol. 35, pp. 252-256, March 2003.

[21] M. Micco and H. Rossman, "Building a Cyberwar Lab: Lessons Learned," *SIGCSE Bulletin: Proc. 33rd Technical Symposium on Computer Science Education,* vol. 34, pp. 23-27, March 2002.

[22] X. Yuan, J. Hernandez, I. Waddell, B. Chu and H. Yu, "Hands-on Laboratory Exercises for Teaching Software Security," in *the 16th Colloquium for Information Systems Security Education*, Lake Buena Vista, Florida, 2012.

[23] "Wireshark," [Online]. Available: https://www.wireshark.org/.

[24] S. Askarifar, N. A. A. Rahman and H. Osman, "A Review Of Latest Wannacry Ransomware: Actions And Preventions," *Journal of Engineering Science and Technology*, pp. 24 - 33, 2018.

[25] W. Du, "SEED Project," Syracuse University, 2006-2019. [Online]. Available: https://seedsecuritylabs.org/.

[26] D. A. Kolb, Experiential learning: experience as the source of learning and development, Englewood Cliffs: Prentice-Hall, 1984.