Journal of Cybersecurity Education, Research and Practice

Volume 2018 | Number 1 Article 6

July 2018

Experiential Learning Builds Cybersecurity Self-Efficacy in K-12 Students

Abdullah Konak
Penn State Berks, konak@psu.edu

Experiential Learning Builds Cybersecurity Self-Efficacy in K-12 Students

Abstract
In recent years, there have been increased efforts to recruit talented K-12 students into cybersecurity fields. These efforts led to many K-12 extracurricular programs organized by higher education institutions. In this paper, we first introduce a weeklong K-12 program focusing on critical thinking, problem-solving, and igniting interest in information security through hands-on activities performed in a state-of-the-art virtual computer laboratory. Then, we present an inquiry-based approach to design hands-on activities to achieve these goals. We claim that hands-on activities designed based on this inquiry-based framework improve K-12 students' self-efficacy in cybersecurity as well as their problem-solving skills. The evaluation of the program showed that the participants made significant progress towards achieving the learning outcomes of the program and developed self-efficacy in cybersecurity.

Keywords
Experiential Learning, Virtual Computing, Information Security Education, STEM Education, Cybersecurity

INTRODUCTION

Because of ever-increasing cyber threats and attacks, cybersecurity is projected to grow into a $170 billion global market in 2020 from $75 billion in 2015 (Morgan, 2015). On the opposite end of the equation, a global shortage of 1.5 million cybersecurity professionals is predicted by 2019 (Morgan, 2016). It is apparent that the demand for cybersecurity professionals is increasing far faster than the supply. In addition, government and private entities are reporting a significant lack of skills among their information security employees (Caldwell, 2013; Furnell et al. 2017).

In response to the shortages in cybersecurity workforce and talent, higher education institutions have started offering degrees related to cybersecurity in the last decade (Cabaj et al., 2018). In parallel with these efforts, many K-12 extracurricular programs such as summer camps, discovery days, and cybersecurity competitions, have been initiated to recruit and train students, especially from underrepresented and underserved populations, in the cybersecurity workforce. Overall, the primary objective of these youth programs is to increase K-12 students' interest in the cybersecurity fields (Reid & Van Niekerk, 2014; Dunn & Merkle, 2018). The *National Security Agency* (*NSA*) and the *National Science Foundation* (*NSF*) have also increased the efforts to recruit talented youth to the cybersecurity fields. For example, the *GenCyber* program (Ladabouche & LaFountain, 2016), which is a collaboration between the NSA and the NSF with the objective of introducing, intriguing, and educating K-12 students in cybersecurity, supported 130 cybersecurity summer camps, reaching out 3300 students and 800 teachers in 2017. The GenCyber requires funded camp programs to introduce the cybersecurity-first principles (Ladabouche & LaFountain, 2016) through activities that involve problem-solving, decision making, reasoning, critical thinking, and creating. GenCyber camps are responsible for developing their camp curricula and adopting instructional methods the most appropriate to their program objectives. In 2017, Penn State Berks also hosted a *GenCyber* summer program. Penn State Berks program's curriculum is unique in the way that it includes minimalist introductory lectures to familiarize students with foundational cybersecurity concepts, many hands-on activities using a remote virtual computer laboratory, and discussions with a strong emphasis on informing students of the potential career paths in information security. The students learned techniques and skills for information system protection, systems administration, cryptography, computer networking, and cyber threat identification.

There is no doubt that a K-12 cybersecurity program should provide students with valuable hands-on learning experiences. However, hands-on activities and laboratory sessions do not always achieve the expected learning outcomes. Students can complete hands-on activities on a computer by following prescriptive

and step-by-step instructions without truly understanding the concepts (Abdulwahed & Nagy, 2009). In this paper, we present an inquiry-based framework to design hands-on activities for cybersecurity K-12 programs. Active learning, which is an instructional strategy to enhance learning by engaging students in the learning process (Prince, 2004), has been widely adopted in engineering and computer science classes. Hands-on activities are one of the frequently used active learning strategies in cybersecurity education. Inquiry-based learning is another active learning strategy where a problem is introduced at the beginning of a learning session to provide the context and motivation for learning (Prince & Felder, 2006). In inquiry-based learning, the problem is usually ill-formulated and open-ended. Another active learning method that we used is collaborative learning, which is defined as a set of instructional methods in which students work together in small groups toward achieving a common goal (Prince, 2004). In this paper, we argue that hands-on activities should be designed by incorporating collaborative and inquiry-based strategies to maximize their impact on student learning and engagement in K-12 cybersecurity programs. In Penn State Berks GenCyber program, all hands-on activities included a problem-solving session after an adequate skill-based scaffolding was provided to students. For example, after students were briefly introduced to traditional substitution and transposition ciphers in a hands-on activity, teams of students were asked to create a new cipher by combining traditional ciphers in CyrpTool 2 (2018). Then, students explained why their ciphers were superior to sole substitution or transposition ciphers in a short class presentation. To increase reflection and conceptualization of learning, we designed all hands-on activities as collaborative such that two or more students worked together to solve inquiry-based problems. In this paper, we present empirical evidence that the utilized inquiry-based activities improved students' self-efficacy and knowledge in cybersecurity.

Self-efficacy refers to an individual's confidence in his or her ability to perform a task according to specific performance outcomes (Bandura, 1982, 1991). Although self-efficacy is a self-reported measure, it has been shown that it affects the likelihood of whether an individual will engage in a task and the degree of the effort that an individual is willing to exert in achieving the task (Bouffard-Bouchard, 1990). Individuals with a high degree of self-efficacy in a task tend to show persistence in accomplishing the desired outcome. Therefore, building self-efficacy of K-12 students in skills and methods related to cybersecurity should be one of the objectives of extracurricular cybersecurity programs, such as the one described in this paper. This may encourage K-12 students to pursue a career in cybersecurity fields.

The research suggests that inquiry-based laboratory activities and conceptual problems are instrumental in fostering self-efficacy (Fencl & Scheel, 2005). However, these activities should include a right level of rigor and challenge to increase self-efficacy. Bandura (2000) argues that if students are faced with only easy challenges, they tend to expect quick solutions and are easily discouraged by failures. Difficult activities may also discourage students. The difficulty of an activity should be slightly above students' expected ability level to foster self-efficacy (Margolis & McCabe, 2006). Incorporating collaborative learning (Fencl & Scheel, 2005), self-reflection (Schunk & Pajares, 2002), and student input (Margolis & McCabe, 2006) into laboratory activities can positively affect self-efficacy. We used the pedagogical approaches briefly summarized above in the design of the hands-on activities of our K-12 cybersecurity program. In this paper, we provide an example of how hands-on activities should be designed for maximizing learning and self-efficacy development.

PROGRAM CURRICULUM AND USE OF VIRTUAL MACHINES

Before describing the inquiry-based framework to design hands-on activities, we briefly introduce the Penn State Berks GenCyber program in this section. A concise curriculum of the program including only hands-on activities is summarized in Table 1. The program lasted five days from 8:30 am to 4:30 pm daily. The overall theme of the program was to introduce K-12 students to different types of tasks and processes performed by cybersecurity professionals. In each day, a different topic was introduced. Overall, the curriculum was very rigorous and emphasized learning by doing. The program included many hands-on activities designed for collaborative and inquiry-based learning. In fact, the bulk of the instruction provided during a day was through these hands-on activities. The participants were K-12 students entering the 10th, 11th, and 12th grades.

Hands-on experimentations and analyses are extremely important in cybersecurity education. Cybersecurity can be a very dry topic for K-12 students unless the concepts are introduced through hands-on activities. Therefore, the program emphasized on learning by doing, and the participants performed many hands-on activities as given in Table 1. The majority of these hands-on activities, particularly the ones introducing a new topic, also included brief theoretical knowledge related to the concepts covered in the activities.

Table 1. *The summary of the daily program, learning objectives, and hands-on activities.*

Lecture Topics	Sample Learning Objectives	Hands-on Activities
Day 1: Data Encoding and Decoding Introduction to TCP/IP	-Describe TCP/IP addressing & port numbers -Use basic networking commands in Windows -Describe port numbers -Explain client/server paradigm -Create backdoors to exploit network applications	-Number systems -Data encoding and decoding -CVCLAB Login Tutorial -Introduction to Networking with Windows 7 (TCP/IP Lab) -Netstat & File Sharing -Netcat
Day 2: TCP/IP Protocol Malware, Trojans, Viruses, Social Engineering Attacks Introduction to Linux Kali Network Attacks	-Describe the functions of the TCP/IP protocol layers -Use a packet analyzer to analyze network traffic -Classify various types of malware -Use standard techniques to identify malicious activity on a computer -Explain how social engineering can be used to gain access to systems -Define the threats posed to networks -Discuss methods to defense against network attacks	-Analyzing IP packets in Wireshark -Creating a Trojan Horse -Keylogger -Phishing IQ Test -Linux networking tools -IP Spoofing -Denial of Service Attacks -Hacking Using Armitage & the Metasploit Framework
Day 3: Data Confidentially Traditional Ciphers Attacks on traditional ciphers Symmetric Algorithms Key exchange	-Describe data confidentiality -Describe the process of encryption/decryption -Explain cipher operators -Conceptualize the strength of a cipher -Describe the strength of an encryption algorithm (diffusion versus confusion) -Describe components of block ciphers -Apply symmetric algorithms for confidentiality -Test cryptographic strength of ciphers -Describe key exchange	-Stick Cipher, Caesar Cipher & Scytale Cipher in Cryptool -Brute force attacks -Frequency analysis - Mini project: design your traditional cipher -Data encoding/decoding in Cryptool -Using Symmetric Algorithms (AES) -Comparing RC4 and AES - Impossible: Mission Game
Day 4: Data Integrity Password Attacks Steganography Digital Forensics	-Apply data integrity methods to verify files and messages -Describe various methods to attack passwords -Explain the need for strong passwords -Describe the process of a digital investigation -Explain the tools and techniques used in a digital investigation -Use file carving techniques to recover digital evidence	-Hash functions -Password cracking -Using jphide and jpseek -Rhino Digital Forensic Case
Day 5: System Hardening Penetration Testing	-Explain the roles of policies -Apply policies to secure computer systems -Describe the penetration testing process -Apply penetration testing tools to scan networks and hosts -Use penetration testing tools appropriate to the task	-Firewalls -Local Security Policies -Group Policy -Target discovery -Target enumeration -Vulnerability assessment

Providing students with exciting hands-on experiences in cybersecurity topics is challenging for many reasons. A major problem is the University information technology (IT) policies that restrict students' privileges on laboratory computers. Such IT policies severely limit the types of hands-on activities that can be performed in traditional computer laboratories. Therefore, the Collaborative Virtual Computer Laboratory (CVCLAB) at Penn State Berks was used to provide participants a safe learning environment without the threat of harming real computers on the network or violating the University IT policies. The CVCLAB is based on virtual machine technology which is a software implementation of an OS that runs exactly like a real computer. The CVCLAB was designed and implemented based on VMware's vSphere technology. Using a virtualization technology, a server can host multiple virtual machines with isolated operating systems that share the resources of the server. Users can access and use virtual machines remotely through a client. Interested readers can refer to the previous papers (Konak et al., 2012; Konak & Bartolacci, 2012; Richards et al. 2015; Konak & Bartolacci, 2016) for more information about the infrastructure and capabilities of the CVCLAB. Alongside the use of virtual machines, a wide variety of applications were presented to and used by the participants to enhance their understanding of how cyber-attacks may occur and how to defend against them.

INQUIRY-BASED FRAMEWORK TO DESIGN HANDS-ON ACTIVITIES

Including hands-on activities in a youth program do not ensure that students will have a good learning experience. In many cases, students go through hands-on activities by following step-by-step instructions without understanding the concepts behind them (Abdulwahed & Nagy, 2009). In particular, K-12 students can feel overwhelmed as they follow voluminous instructions that guide them through activity steps over an extended period. Therefore, the design of hands-on activities is critical to ensure student engagement and learning in youth programs. As mentioned earlier, collaborative and inquiry-based learning approaches were utilized in the design of hands-on activities and the delivery of the camp program. Collaborative learning is a particularly useful strategy to support novice technology users who have difficulty in navigating remote virtual computer laboratories (Konak et al., 2016; Wagner et al., 2013). Collaborative learning not only makes learning more engaging but also initiates peer-to-peer learning by encouraging advanced students to help other students who lack the necessary computer skills. Thereby, collaborative learning can alleviate some of the problems caused by the different backgrounds and experiences of program participants (Konak & Bartolacci, 2016).

The hands-on activities given in Table 1 are designed based on the inquiry-based framework outlined in (Konak et al., 2013, 2014). This inquiry-based framework is inspired by Kolb's Experiential Learning Model (Kolb, 1984). In essence, each hands-on activity includes four components: concrete experience, reflective observation, abstract conceptualization, and active experimentation. We describe the function of each component below. Figure 1 illustrates how an encryption activity can be structured based on the inquiry-based framework. In this activity, two students use an asymmetric cipher to send secret messages to one another. In the following, the four components of the inquiry-based framework are explained using this activity based on (Konak et al., 2013, 2014).

Concrete Experience: This component of a hands-on activity includes the step-by-step instructions for the tasks involved in the activity. Therefore, the concrete experience is not very different from hands-on activities that can be found in many cybersecurity laboratory manuals. Since students may not be familiar with the concepts introduced and the software packages used in a hands-on activity, step-by-step instructions should aim to familiarize students with the software packages and demonstrate the different ways of using it. Step-by-step instructions should also use visual aids until a satisfactory level of familiarity is achieved. In the first part of the asymmetric cipher example, the two students follow the step-by-step instructions to create a public and private key pair using the CrypTool 2 software.

Reflective Observation: Reflective observation includes activities such as discussions and reflective questions that require students to reflect on their hands-on experience. A hands-on activity is typically organized into several sections, and reflective activities are performed after each section. This strategy also helps the instructor phase the activity across multiple groups. In the illustrative example in Figure 1, after the students create a public and private key pair by following the step-by-step instructions, they are asked to analyze the components of their public keys and discuss questions such as why they must secure their private keys. Reflective observation activities also encourage student-to-student interactions in order to achieve a higher level of reflection. Reflective observation components of an activity usually incorporate group work to achieve a more meaningful reflection.

Abstract Conceptualization: Through the abstract conceptualization components of a hands-on activity, students are expected to create generalized knowledge of what is performed in the activity. In other words, students are expected to connect the hands-on learning experience to the overall theoretical knowledge. Without achieving the connection between the theory and practice, a complete learning cannot take place. The instructor plays an essential role in the process of abstract conceptualization. A class discussion led by the instructor may help students solidify the mental picture of the concepts learned. Another useful strategy is using generalization questions. In the illustrative example, the students

are asked to list the pros and cons of asymmetric ciphers after the activity is completed. Generalization questions can also be combined with the next stage of active experimentation to construct new knowledge.

Active Experimentation: This component of the hands-on activity mainly constitutes inquiry-based learning. At this stage, students are ready to plan and try out another hands-on experience. Active experimentation can be of two levels. In the first level, students complete a new task similar to what they performed by following the step-by-step guidance, but this time without providing specific instructions. For instance, students are asked to send messages to other students in the illustrative example. If the step-by-step instructions have provided the adequate level of scaffolding, students should be able to achieve this new task without detailed instructions.

In the second level, active experimentation requires the integration of several skills and topics to achieve a new task. For example, students can be challenged to devise a process to verify the integrity and source of a message using an asymmetric algorithm. This type of active experimentation requires the integration of several concepts introduced in the hands-on activity.

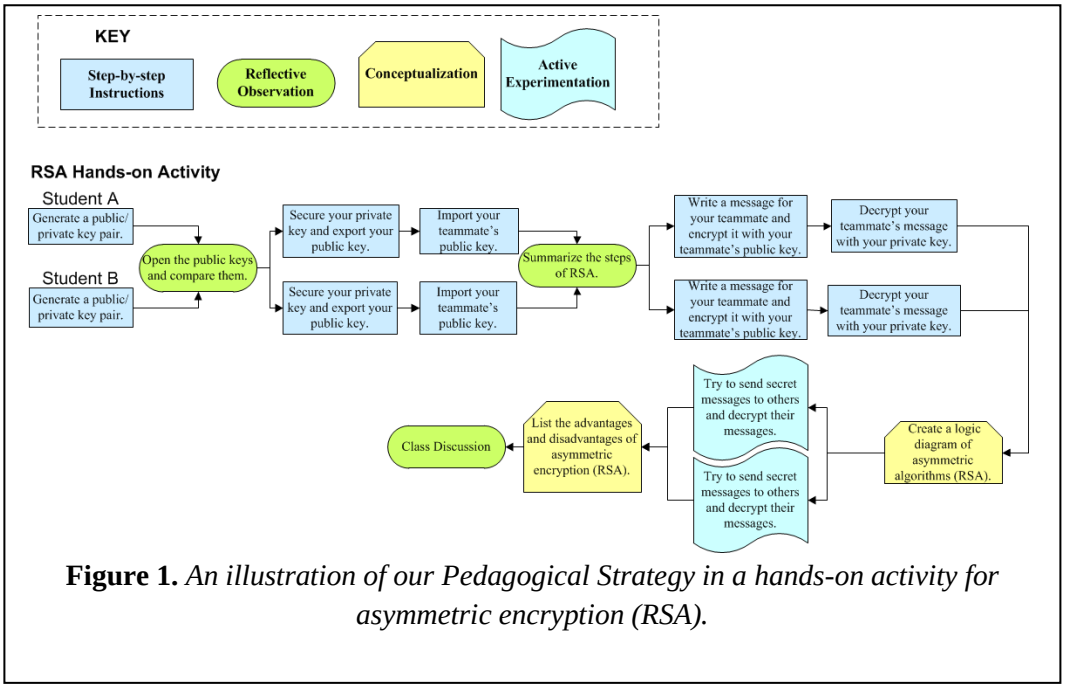

Figure 1. *An illustration of our Pedagogical Strategy in a hands-on activity for asymmetric encryption (RSA).*

EMPIRICAL RESULTS

In this section, we present the outcomes of the program in terms of increasing participants' self-efficacy and knowledge of cybersecurity. We used pre- and post-program questionnaires and tests to measure the participants' self-efficacy in cybersecurity-related skills before and after the camp. The camp program included the hands-on activities in the following four skill-based learning outcome areas:

- **System Administration**: Secure operating systems using various controls and policies.
- **Computer Networking:** Apply fundamental networking tools to set up and diagnose computer networks.
- **Cyber Threat Identification:** Identify and describe common cybersecurity threats.
- **Cryptography:** Describe how cryptographic techniques are used to ensure data confidentiality/integrity as well as authentication.

The self-efficacy of these four learning outcome areas was measured by a questionnaire based on the Cybersecurity Engagement and Self-Efficacy Scale (Amo et al., 2005). The Cyber Engagement and Self-Efficacy Scale does not include items related to cryptography, which was an important part of the program. Therefore, we designed new questions for this learning outcome area. All questions were operationalized using 4- level Likert scale from 1-Strongly Disagree to 4-Strongly Agree. The self-efficacy score of a learning outcome area was computed by averaging the ratings of all questions related to that learning outcome area. The Cronbach's α values, which indicate the internal reliability of the measures, are provided in Table 2.

Before the start of the program and directly after, the participants completed the questionnaire. The participants' prior knowledge of the learning outcome areas was also assessed using a multiple-choice test which was administered at the beginning of the program. The same test was also administered at the end of the program to measure any knowledge gained. For each participant (N=41), the difference between the post-program and pre-program questionnaire scores were computed, and a paired t-test was used to test whether the average increase from the pre-program to post-program scores differed from zero. Table 2 presents the means, standard deviations, and 95% confidence intervals of the paired differences as well as the statistics of the t-test. In addition, the average percent improvement (100×(Post-score – Pre-score)/Pre-score) of each variable is given in the table.

As seen Table 2, significant improvements were observed in the participants' self-efficacy in all learning outcome areas. The most significant improvement was observed in the learning outcome area of Networking. On the average, the participants rated their self-efficacy in the area of Networking 63% higher at the

end of the program compared to the beginning. The second most significant improvement was observed in the learning outcome area of Cryptography with a 59% average increase. The smallest improvement was in Systems Administration with a 42% increase. The differences between post-program and pre-program mean scores of the variables were statistically significant at $p < 0.001$ for all variables. The lower bound of the 95% confidence interval was quite far away from zero for each variable as well.

Figure 2 illustrates the individual improvement of the participants in the skilled-based learning outcome areas. In Figure 2, the improvement is expressed as the ratio of the increase in self-efficacy scores (Post-score – Pre-score) to the maximum possible increase (4 – Pre-score) for each participant. It is clear that the program was able to improve self-efficacy of the participants significantly. Only a few participants reported no increase in their self-efficacy. An overwhelming majority reported more than 60% improvement as seen in the figure. These results strongly support that the hands-on activities based on the inquiry-based framework were effective in fostering the participants' self-efficacy in the learning outcome areas.

In addition to the four skilled-based learning outcome areas, the program included activities focusing on online safe behaviors, and the active experimentation components of the hands-on activities involved the application of problem-solving skills. Therefore, we also measured the self-efficacy of the participants in Online Safe Behavior and Problem Solving. The participants' self-efficacy of Online Safe Behavior and Problem Solving were measured by questions operationalized using a five-level Likert scale from Strongly Disagree (1) to Strongly Agree (5). The Cronbach's α values of these measures are also given in Table 2.

It is notable that the program was able to improve the participants' self-efficacy in problem-solving (6% on the average). We attribute this result to the active experimentation components of the hands-on activities. As described before, the hands-on activities were designed differently from a cookbook approach in which students follow step-by-step directions without considering what they are learning. The active reflection and abstract conceptualization components of the activities encouraged the participants to construct knowledge rather than to memorize it. In the active experimentation parts of the activities, the participants solved problems by applying their newly gained knowledge and skills. During our classroom observations, we experienced that the participants engaged in the active experimentation components of the activities the most. In the active experimentation stage, many participants became aware of the gaps in their learning and actively sought help from their peers and the instructors although they were able to complete the step-by-step concrete experience component of the activity successfully. Therefore, we recommend incorporating inquiry-based challenges in

youth programs. As seen in Table 2, the program was also able to improve the participant's self-efficacy of Online Safe Behavior although the participants had a very high self-efficacy at the beginning of the program.

Table 2. *The comparison of the pre-program and post-program questionnaire ratings. (All mean differences were significant at p < 0.001).*

		Difference (Post – Pre)		95% Confidence Interval of the Difference		
Variable (Cronbach's α values)	**Percent Increase**	**Mean**	**Std. Dev.**	**Lower Bound**	**Upper Bound**	***t***
Systems Administration Self-Efficacy (0.962)	42%	0.89	0.57	0.71	1.07	9.95
Networking Self-Efficacy (0.957)	63%	1.13	0.65	0.93	1.34	11.11
Cyber Threat Identification Self-Efficacy (0.977)	49%	1.11	0.63	0.92	1.31	11.36
Cryptography Self-Efficacy (0.966)	59%	0.94	0.65	0.73	1.14	9.18
Problem Solving (0.748)	6%	0.23	0.41	0.10	0.36	3.63
Online Safe Behavior (0.870)	25%	0.63	0.75	0.39	0.86	5.32

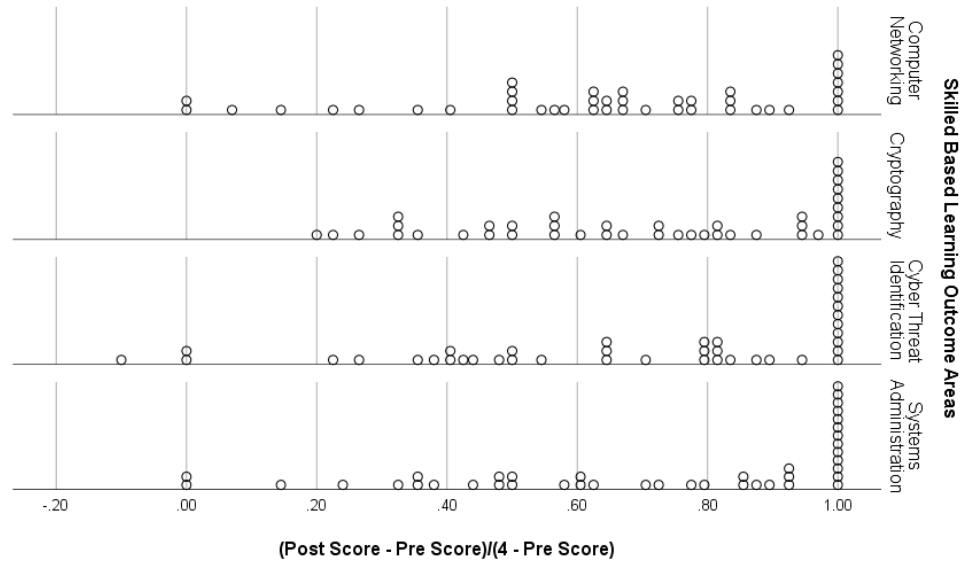

Figure 2. *The distribution of the normalized increase in self-efficacy of the skill-based learning outcome areas.*

Table 3 presents the mean differences between the post and pre-test results for the four learning outcome areas as well as the overall test score. A paired *t*-test was used to compare the pre-program and post-program test scores. The *t*-values and 95% confidence intervals for the mean differences are also provided in the table. All mean differences were significant at $p < 0.001$. The percent increases in the table represent the increase in the mean values (100×(*mean*(Post-score) – *mean*(Pre-score))/*mean*(Pre-score)). Overall, the average test score increased from 41 to 80 (out of 100 maximum available points), representing a 94% increase. Similar to the improvement in the self-efficacy scores, the largest improvement was observed for the Networking learning outcome area with a 200% increase, and the second largest improvement was in the Cryptography learning outcome area with a 141% increase.

Table 3. *The comparison of the pre-program and post-program test results. (All mean differences were significant at p < 0.001).*

		Difference (Post – Pre)		**95% Confidence Interval of the Difference**		
Learning Outcome Area	**Percent Increase in Means**	**Mean**	**Std. Dev.**	**Lower Bound**	**Upper Bound**	***t***
Systems Administration	43%	38	31	29	48	8.02
Networking	200%	54	28	45	63	12.15
Cyber Threat Identification	26%	22	28	13	31	5.04
Cryptography	141%	45	31	35	54	9.23
Test Overall	94%	38	19	32	44	12.91

Next, we compared the relative increase observed in the average scores of female (N=9) and male (N=32) participants using MANOVA. Table 4 presents the average and standard deviations of the relative increase ((Post-score – Pre-score)/Pre-score) for each variable across the gender and the F and p statistics of MANOVA. Although the sample size is small for a reliable comparison, it is notable that female participants demonstrated much higher improvement in all variables compared to male participants. For example, female participants improved their Networking Self-Efficacy by 87% compared to 56% for male participants (F=3.04, p=0.09). Most remarkably, the average test score increased 236% for females whereas 127% for males (F=4.20, p=0.05). In other two variables, although the improvements of females were higher than those of males, the differences were not statistically significant.

Table 4. *The comparison of the normalized improvement ((Post-score – Pre-score)/Pre-score) across the gender using Multivariate Analysis of Variance.*

	Female Mean	**Female Std. Dev**	**Male Mean**	**Male Std Dev**	***F***	***p***
Systems Administration Self-Efficacy	0.53	0.37	0.37	0.42	0.97	0.33
Networking Self-Efficacy	0.87	0.57	0.56	0.45	3.04	0.09
Cyber Threat Identification Self-Efficacy	0.64	0.54	0.43	0.50	1.17	0.29
Cryptography Self-Efficacy	0.56	0.40	0.55	0.56	0.00	0.96
Test Score	2.36	1.70	1.30	1.27	4.20	0.05
Problem Solving	0.07	0.10	0.06	0.11	0.02	0.89
Online Safe Behavior	0.39	0.33	0.20	0.31	2.59	0.12

CONCLUSION

In this paper, we introduce the curriculum and the pedagogical approach of a weeklong program to expose K-12 students to cybersecurity concepts and skills. A unique aspect of the program is the use of the Collaborative Virtual Computer Laboratory (CVCLAB) to engage K-12 students in experiential learning through exciting hands-on activities that are designed based on pedagogical approaches such as collaborative learning and inquiry-based learning. The evaluation of the program showed that the program was able to foster self-efficacy of the participants to a great degree. We firmly believe that these significant results are due to rigorous hands-on learning experiences in a virtual environment (CVCLAB) and the inquiry-based framework that we used in the design of hands-on activities.

REFERENCES

Abdulwahed, M., & Nagy, Z. K. (2009). Applying Kolb's experiential learning cycle for laboratory education. *Journal of Engineering Education*, 98(3), 283-294.

CrypTool 2 (2018, April 16). URL https://www.cryptool.org/en/cryptool2

Amo, L. C., Zhuo, M., Wilde, S., Murray, D., Cleary, K., Amo, C., . . . Rao, H. R. (2005). *Cybersecurity Engagement and Self-Efficacy Scale*.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist, 37*(2), 122-147.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational behavior and human decision processes, 50*(2), 248-287.

Bandura, A. (2000). Cultivate self-efficacy for personal and organizational effectiveness. *Handbook of principles of organizational behavior, 2*, 0011-0021.

Bouffard-Bouchard, T. (1990). Influence of self-efficacy on performance in a cognitive task. *The Journal of Social Psychology, 130*(3), 353-363.

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security, 75*, 24-35.

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security, 2013*(7), 5-10.

Dunn, M. H., & Merkle, L. D. (2018, February). Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests. *In Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 62-67.

Fencl, H., & Scheel, K. (2005). Engaging students. *Journal of College Science Teaching, 35*(1), 20.

Furnell, S., Fischer, P., & Finch, A. (2017). Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security, 2017*(2), 5-10.

Kolb, D. A. (1984). *Experimental learning: experience as the source of learning and development*. Englewood Cliffs, NJ: Prentice Hall.

Konak, A., Bartolacci, M., & Huff, H. (2012, July 29). *An Exploratory Factor Analysis of Student Learning in a Collaborative Virtual Computer Laboratory.* Paper presented at the Proceedings of AMCIS 2012 Seattle, WA.

Konak, A., & Bartolacci, M. R. (2012, October 11-14). *Broadening E-Commerce Information Security Education Using Virtual Computing Technologies.* Paper presented at the 2012 Networking and Electronic Commerce Research Conference, Riva Del Garda, Italy.

Konak, A., & Bartolacci, M. R. (2016). Using a virtual computing laboratory to foster collaborative learning for information security and information technology education. *Journal of Cybersecurity Education, Research and Practice, 2016*(1 (Article 2)), 1-27.

Konak, A., Bartolacci, M. R., Kulturel-Konak, S., & Nasereddin, M. (2016, 12-15 Oct. 2016). *Impact of collaborative learning on student perception of virtual computer laboratories.* Paper presented at the 2016 IEEE Frontiers in Education Conference (FIE), 1-4. DOI: 10.1109/FIE.2016.7757640.

Konak, A., Clark, T., & Nasereddin, M. (2013, March 9). *Best Practices to Design Hands-on Activities for Virtual Computer Laboratories.* Paper presented at The Third Integrated STEM Education (ISEC)-IEEE, Princeton, NJ, 1-7.

Konak, A., Clark, T., & Nasereddin, M. (2014). Using Kolb's Experiential Learning Cycle to Improve Student Learning in Virtual Computer Laboratories. *Computers & Education, 72*, 11-22.

Ladabouche, T., & LaFountain, S. (2016). GenCyber: Inspiring the Next Generation of Cyber Stars. *IEEE Security & Privacy*, 14(5), 84-86.

Margolis, H., & McCabe, P. P. (2006). Improving self-efficacy and motivation: What to do, what to say. *Intervention in school and clinic, 41*(4), 218-227.

Morgan, S. (2015). Cybersecurity market reaches $75 billion in 2015; expected to reach $170 billion by 2020. *Forbes, December, 20*.

Morgan, S. (2016). One million cybersecurity job openings in 2016. *Forbes. com*.

Schunk, D. & Pajares, F (2002). The development of academic self-efficacy. *In Educational Psychology*, edited by Allan Wigfield and Jacquelynne S. Eccles, Academic Press, San Diego, 2002, 15-31.

Prince, M. (2004). Does active learning work? A review of the research. *Journal of engineering education*, 93(3), 223-231.

Prince, M. J., & Felder, R. M. (2006). Inductive teaching and learning methods: Definitions, comparisons, and research bases. *Journal of Engineering Education*, 95(2), 123-138.

Richards, R., Konak, A., Bartolacci, M. R., & Nasereddin, M. (2015, April 10-11). *Collaborative Learning in Virtual Computer Laboratory Exercises.* Paper presented at the Spring 2015 Mid-Atlantic ASEE Conference, 2015 Villanova University, 1-13.

Reid, R., & Van Niekerk, J. (2014). Snakes and ladders for digital natives: information security education for the youth. *Information Management & Computer Security*, 22(2), 179-190.

Wagner, K. G., Myers, M. C., & Konak, A. (2013). *Fostering Student Learning in Information Security Fields through Collaborative Learning in Virtual Computer Laboratories.* Paper presented at The Third Integrated STEM Education (ISEC), 1-7.