Fostering Interest and Knowledge in the Information Security Industry for K-12 Students Using Virtual Machines

Mr. Ethan Patrick Adams, Penn State University: Berks Campus

Ethan Adams is a second-year student majoring in the Information Sciences and Technology and Security & Risk Analysis programs at Penn State Berks.

Patrick Joseph Scanlon

Patrick Scanlon is a second year year student majoring in Information Sciences and Technology and minoring in Security & Risk Analysis. He also works as a student IT consultant at Penn State Berks.

Mr. Joseph Torres, Penn State Berks GenCyber
Ms. Tricia Clark, Penn State Berks

TRICIA K. CLARK, M.S., Instructor and Program Coordinator for the Information Sciences & Technology degree program at Penn State Berks. Teaching interests include programming, information security and first-year experience. Research interests include exploring ways technology can be integrated into teaching and promoting STEM education opportunities to K-12 students.

Mr. Terence Laughlin, Blue Mountain High School
Dr. Abdullah Konak, Penn State Berks

Abdullah Konak is a Professor of Information Sciences and Technology at the Pennsylvania State University Berks. Dr. Konak received his degrees in Industrial Engineering, B.S. from Yildiz Technical University, Turkey, M.S. from Bradley University, and Ph.D. from the University of Pittsburgh. Prior to his current position, he taught at Auburn University. Dr. Konak also held visiting positions at Lehigh University and the Chinese University of Hong Kong.

Dr. Konak's current research interest is in the application of Operations Research techniques to complex problems, including such topics as network design, network reliability, facilities design, green logistics, and data mining. Dr. Konak has published papers in leading journals such as Operations Research Letters, Informs Journal on Computing, Europan Journal of Operations Research, Computers and Operations Research, IIE Transactions, IEEE Transactions on Reliability, International Journal of Production Research, and Production Economics. He has been a principal investigator in sponsored projects from the National Science Foundation, the National Security Agency, the US Department of Labor, and Venture Well.

Dr. Konak currently teaches courses on Database Management Systems, Cybersecurity, Agent Based Modelling, and Entrepreneurship. He is a member of IISE, INFORMS, and IEEE.

Fostering Interest and Knowledge in the Information Security Industry for K-12 Students Using Virtual Machines

Ethan Adams, Patrick Scanlon, Joseph Torres, Emilio Gonzales, Tricia Clark, Abdullah Konak
Penn State Berks, epa5093, pjs5482, jst5221, eag5178, tkc3, auk3@psu.edu
Terence Laughlin
Blue Mountain School District
tjlaughlin44@gmail.com

Abstract

The field of information security is growing rapidly as malicious attacks to information systems become more frequent and detrimental to individuals and organizations who have become increasingly dependent upon these systems. With such a dramatic growth in demand in a short timeframe, there exists a shortage in the supply of professionals entering the field. In order to assist in the remediation of this gap, the Penn State Berks *Information Sciences and Technology* (IST) and *Security Risk Analysis* (SRA) programs are hosting an annual NSA and NSF sponsored summer camp as part of the *GenCyber* program. This camp is focused on critical thinking, problem-solving, and igniting interest in information security and other STEM fields through the application of hands-on activities in the security of a virtual machine environment. By implementing this program, Penn State Berks aims to show students the value of information security as early as reasonably possible, share the knowledge of safe practices and principles for using the Internet safely, and instill an interest in cybersecurity, as well as the STEM field as a whole. The evaluation of the program shows that the participants make significant progress towards achieving the learning outcomes of the summer camps.

Keywords

Virtual Computing, Information Security Education, STEM Education, Cyber Security

Introduction

Because of ever-increasing cyber threats and attacks, worldwide spending on information security is up, reaching $75 billion in 2015, a projected growth towards $170 billion in 2020[1]. On the opposite end of the equation, business entities are apt to be looking for up-and-coming talent, with one million job openings reported in 2015, and a projected global shortage of 1.5 million cyber security professionals by 2019[2]. It is apparent that the demand for information security professionals is increasing far faster than the supply. The shortage of information security professionals is not the only issue plaguing the current information security climate. Additionally, business entities are reporting a significant lack of skills among their information security employees. The results of this shortage are data loss, privacy violations, service disruptions, and more. One such business, Kaspersky Lab, reported that one of their managers "typically needs to interview 40 people in order to hire one expert."[3] Additionally, a PWC survey of businesses states that 53% of respondents "were confident that they would have sufficient security skills to manage their risks in the next year."[4] In this aspect, many of those seeking work in the industry are not as

educated and specialized as they need to be in order to take on the complex information security problems facing corporations today.

In response to shortages in both information security workforce and talent, several organizations aim to increase interest in information security for those still coming up through the education system. One such program is known as *GenCyber*, which is a collaboration between the *National Security Agency* (*NSA*) and the *National Science Foundation* (*NSF*). The objective of *GenCyber* is to introduce, intrigue, and educate K-12 students in STEM fields, more specifically information and cyber security. The program is implemented in the form of summer camps hosted across the United States.

In Summer 2017, Penn State Berks hosted two *GenCyber* summer camps. The objectives of Penn State *GenCyber* program are to inform and educate K-12 students about the various career paths in cyber security related fields and to provide them with the foundational skills and understanding of cyber security. The camp's curriculum is unique in the way that it includes minimalist introductory lectures to familiarize students with foundational cyber security 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 learn techniques for information system protection, destruction, and restoration by incorporating several cybersecurity first principles. Each summer camp runs for five days, with each day focusing on a specific area of information security such as computer networking, cryptography, threats and malware, system hardening and digital forensics, and penetration testing. In this paper, we introduce how virtual computing is used to create hands-on educational experiences and the pedagogy used in the Penn State Berks *GenCyber* camps. In addition, we present the results of the camp in terms of student progress on the learning objectives of the camp.

Camp Program

To achieve the outlined goals, we designed a rigorous and technical camp curriculum. Both camps targeted students entering the 10th, 11th, and 12th grades. Twenty-four students were admitted to each camp through a competitive selection process. The camp program in each day is briefly summarized in the following.

Day 1: In the morning session, the participants were introduced to the field of cyber security using several short videos and discussions. Afterwards, the Collaborative Virtual Computer Laboratory was introduced, and the students were shown how to log onto their individual accounts and access to their Windows 7 and Backtrack virtual machines. In addition, the participants were introduced to the command prompt and basic networking commands. Netcat was used in order to communicate over the network and allowed students to create files and share them with each other through the network.

Day 2: The morning of day 2 was focused on informing the students on not only what the different protocols are, but also what their importance is and how they can be manipulated. The components of TCP/IP were discussed as well as the functions of the TCP and UDP. Packet sniffing software such as Wireshark was used to aid in student's exploration of IP network traffic. A guest speaker spoke to the students about possible career options in cybersecurity as well as how and what the

field is currently doing in a professional setting. The afternoon portion was dedicated to the various types of attacks that can occur in networks. Various types of malware, viruses, Trojans, worms, phishing attacks, and attacks that are more physical such as social engineering and shoulder surfing were introduced to the students to give them a better understanding of what is out there and how they work in order to know how properly defend against them. The students gained plenty of knowledge through hands-on activities such as IP Spoofing, Denial of Service attacks, creating a Trojan Horse, and white-hat hacking with the Armitage & Metasploit framework.

Day 3: On day 3, we reintroduced the CIA (Confidentiality, Availability, Integrity) triad to the students but reinforced it with various cryptography activities involving Caesar, Stick, Scytale, and AES Ciphers using the Cryptool 2.0 application. In the afternoon, the students completed a scavenger hunt activity that involved numerous ciphers and locations around campus that the participants had to solve to figure out the next clue.

Day 4: The morning session focused on the importance of Digital Forensics. The participants were introduced to the process of a digital investigation, explained the tools and techniques used in a digital investigation, and described the job of a forensic investigator. We described various ways to attack passwords as well as the need for longer and more complex passwords. Rainbow tables and other forms of attack such as brute force or dictionary attacks were executed by each participant. We showed how steganography could be used in a cyber-crime to hide data behind images, text files, or other documents through a hands-on lab activity. In the afternoon, the Cybersecurity First Principles were incorporated into the camp in various manners ranging from a general teaching assessment to exploring the physical security of a building, to dissecting a server.

Day 5: The last day of the camp was more focused on the building blocks of cybersecurity, including the information security policies and how to harden systems against attacks. The penetration testing process was covered through instruction and the application of penetration testing tools, particularly nmap, to scan networks and hosts. The afternoon was a wrap up of the camp. Collectively, the participants mapped the camp activities to cybersecurity first principles before the camp graduation ceremony.

Use of the Virtual Machines

There is no doubt that learning experiences that involve hands-on experimentations and analyses are extremely important in cyber security education. Cyber security can be a very dry topic for K-12 students if the concepts are not introduced through hands-on activities. However, providing students with exciting hands-on experiences in cyber security topics is also 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 on traditional computer laboratories. Therefore, the Collaborative Virtual Computer Laboratory (CVCLAB) was used to provide participants a safe learning environment without the threat of harming real computers on the network or breaking the University IT policies. The CVCLAB is based on virtual machine technology which is a software implementation of a computer that runs exactly like a real computer. The CVCLAB was designed and implemented based on VMware's vSphere technology. Using this technology, a server can host multiple virtual machines with isolated operating systems that share the resources of the

server. Users are able to access to and use virtual machines remotely through a client. Interested readers can refer to our earlier papers[5-7] 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. All of the software presented in Table 2 was available in the CVCLAB for use throughout the week and had a specific activity tailored to each of them.

Table 2: The list of the software packages used in the camp program.

Software/Tool	Description	Camp Use
Netcat	Back-end networking utility	Port-scanning and creating a backdoor for use in a Trojan virus
Wireshark	Packet sniffer/analyzer	Packet capture and analysis for various activities
EliteWrap	Application wrapper	Created Trojan virus using netcat and minesweeper
All In One Keylogger	Subtle keylogger application	Lessons in the function of keyloggers and hiding folders
Low Orbit Ion Cannon	Basic DDoS tool	DDoSing an IP within the virtual network
nmap/Zenmap	A port scanner	Target enumeration, port scanning, and vulnerability detection
smurf6	DDoS attack that utilizes spoofed ping messages	Exercise in Linux-based DDoS attacks
hping3	Packet generator and analyzer for the TCP/IP	IP Spoofing and DDoS attacks
fping / genlist	Tool for sending ping requests to multiple hosts	Target discovery
netdiscover	Active/passive address reconnaissance tool	Discovering live hosts on a network
nbtscan	Tool for finding NetBIOS name information	Finding OS and MAC address information on a given host
xprobe2	OS Fingerprinting Tool	Determining a target's OS
Armitage	Cyber-attack management tool	To take students through the entire process of vulnerability assessment, penetration testing, and hacking.
CrypTool 2.0	E-learning software for cryptography and cryptanalysis	Exercises in different forms of ciphers (both traditional and modern), encoding, encryption, and cryptanalysis
Ophcrack/Cain&Abel	Password cracking tools	Illustrating different forms of password cracking, including brute force and rainbow table attacks
Pwdump7	Outputs password hashes of local users	Used in conjunction with Ophcrack to provide the list of passwords to crack
Jphs05 / Camouflage	Steganography tool	Exercises for hiding data and images within other images
WinMD5	Tool for calculating MD5 hashes	Finding the hash value of files to verify integrity
Hex Workshop 6	Hex Editor	Comparing unmodified images with images embedded with data
Autopsy	Open source cyber forensics tool	Exercise in cyber forensics with data carving, and data hiding
Microsoft Baseline Security Analyzer	Checks for missing security updates and insecure settings on a Windows machine	Assess the vulnerability of a windows machine within the virtual network

Pedagogical Approach

Collaborative learning through hands-on, inquiry-based activities is very important for K-12 students. In the delivery of the camp program, we used collaborative learning and inquiry-based strategies. These strategies made not only hands-on activities more engaging but also initiated peer-to-peer learning by encouraging skilled students to help their teammates who were not as skilled as themselves. Hands-on activities were designed based on an inquiry-based framework defined in our earlier work[8-10]. This framework is inspired by Kolb's Experiential Learning Model. In addition to step-by-step instructions, each of the camp hands-on activities has three components to enhance student learning- Reflective Observation, Abstract Conceptualization, Active Experimentation. The reflective observation part of a hands-on activity includes learning

components such as discussion and reflective questions that require students to reflect on their hands-on experiences. Through abstract conceptualization, students are expected to create generalized knowledge of what is performed in the activity. Class or peer-to-peer discussions are helpful to connect the hands-on learning experience to the overall theory. At this stage, instructor intervention is important. A class discussion led by the instructor may help students solidify a mental picture of the concepts learned. In Active experimentation, students are asked to complete a new task, which combines a few related topics covered in the same hands-on activity, without detailed step-by-step instructions.

Evaluation of the Student Learning

One of the main objectives of the camp program is to increase student knowledge, skills, and abilities in cyber security. In order to evaluate the attainment of this objective, we used pre- and post-camp questionnaires and tests. The questionnaires aimed to measure participants' self-efficacy in common cyber security concepts before and after the camp. Although self-efficacy is a self-reported subjective measure, the research supports that it is one of the important variables determining how successful one will be in a domain. In addition to the self-efficacy measures, we used the pre- and post-camp tests to assess the level of knowledge gained by the participants. The progress of participants was measured with respect to the following learning outcome areas:

- **Online Safe & Ethical Behavior**
- **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 cyber security threats.
- **Cryptography:** Describe how cryptographic techniques are used to ensure data confidentiality/integrity as well as authentication.

The participants' self-efficacy of Online Safe & Ethical Behavior was measured by five questions operationalized using a five-level Likert scale from 1-Strongly Disagree to 5-Strongly Agree. The self-efficacy of the participants in the other four learning outcome areas was measured by a questionnaire based on the Cybersecurity Engagement and Self-Efficacy Scale[11]. This instrument distinguishes between the self-efficacy of understanding and the self-efficacy of performing tasks related to cyber security. The Cyber Engagement and Self-Efficacy Scale does not include items related to cryptography, which was a significant part of the camp program. Therefore, we designed new questions for this learning outcome. All questions are operationalized using 4- level Likert scale from 1-Strongly Disagree to 4-Strongly Agree. Directly prior to the start of the camp activities, as well as directly after, the participants were asked to complete the questionnaire. The participants' prior knowledge in the learning outcome areas of System Administration, Computer Networking, Cyber Threat Identification, and Cryptography was assessed using a pre-camp test which was administered at the beginning of the camp. The same test was also administered at the end of the camp to measure any knowledge gained.

Table 3 summarizes the results of the pre- and post-camp questionnaire and tests. In the table, the mean score of a learning outcome area indicates the average ratings of all questions related to the learning outcome area. The pre-camp and post-camp results were compared by ANOVA to test the hypothesis that the pre- and post-camp mean scores were different. The *F* statistics of the

ANOVA are also given in the table. As seen Table 3, the participants made tremendous progress towards mastering the learning objectives. The participants' progress is evident from both the subjective measures (the pre- and post-camp questionnaire) and the objective measures (the pre- and post-camp tests). The post-camp mean scores of all measured constructs were significantly higher than the pre-camp scores (p <0.001 for all measures).

Table 3: The comparison of the pre-camp and post-camp questionnaire and test results. (All pre- and post-camp means were significant at $p < 0.001$).

Learning Objectives	**Pre-Camp Mean (*N*=44)**	**Pre-Camp Std. Dev.**	**Post-Camp Mean (*N*=41)**	**Post-Camp Std. Dev.**	**Increase (100x (Post-Pre)/Pre)**	***F* Value**
Online Safe & Ethical Behavior	3.40	0.672	4.08	0.39	19%	31.5
Systems Administration Understanding	2.69	0.75	3.63	0.45	35%	48.0
Systems Administration Self-Efficacy	2.54	0.69	3.45	0.49	36%	48.5
Networking Understanding	2.30	0.74	3.45	0.49	50%	71.3
Networking Self-Efficacy	2.22	0.71	3.35	0.51	51%	69.6
Cyber Threat Identification Understanding	2.70	0.81	3.62	0.45	34%	41.3
Cyber Threat Identification Self-Efficacy	2.45	0.80	3.44	0.52	40%	45.0
Cryptography Understanding	2.49	0.73	3.56	0.45	43%	65.1
Cryptography Self-Efficacy	2.21	0.59	3.44	0.46	56%	113.9
System Administration Test	35.23	23.08	73.78	24.97	109%	54.7
Networking Test	23.30	28.22	77.44	17.50	232%	111.0
Cryptography Test	31.25	30.08	76.83	23.31	146%	60.3
Cyber Threat Identification Test	64.55	28.24	88.29	14.12	37%	23.5

We observed the most significant improvements in the learning outcome areas of Cryptography and Computer Networking, in which the participants had the lowest levels of pre-camp self-efficacy. In Cryptography, the mean understanding and self-efficacy scores increased 43% and 56%, respectively. The participants also scored 146% higher in the post camp cryptography test than the pre camp test. Similarly, the participants score 232% higher in the post-camp computer networking test compared to the pre-camp one. In this area, their self-efficacy scores increased about 50% during the camp. In all other learning outcome areas, the progress was quite significant.

Conclusion

In this paper, we introduce the curriculum and the pedagogical approach of the GenCyber summer camps organized by Penn State Berks. A unique aspect of the summer programs 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 Kolb's experiential learning. The results presented above strongly support that both summer camp programs were able to achieve the goals of the program exceedingly. We firmly believe that these results are due to our capability to deliver rigorous hands-on learning experiences through the CVCLAB in addition to the inquiry-based framework that we used in the design of these hands-on activities.

References

1 Morgan, S. (2015, December 21). Cybersecurity Market Reaches $75 Billion In 2015; Expected To Reach $170 Billion By 2020. Retrieved August 31, 2017, from https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#71dbf07b30d6

2 Morgan, S. (2016, January 04). One Million Cybersecurity Job Openings In 2016. Retrieved August 31, 2017, from https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#aaba8a427ea2

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

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

5 Konak, A. and Bartolacci, M.R (2012). Broadening E-Commerce Information Security Education Using Virtual Computing Technologies," The 2012 Networking and Electronic Commerce Research Conference, Riva Del Garda, Italy, October 11-14.

6 Richards, R., Konak, A., Bartolacci, M. R. and Nasereddin, M. (2015). Collaborative Learning in Virtual Computer Laboratory Exercises. Spring 2015 Mid-Atlantic ASEE Conference, 2015 Villanova University,1-13.

7 Konak, A. and 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, Vol. 2016: No. 1, Article 2, 1-25.

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

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

10 Konak, A., Kulturel-Konak, S., Nasereddin, M. and Bartolacci, M. R. (2017). Impact of Collaborative Work on Technology Acceptance: A Case Study from Virtual Computing. Journal of Information Technology Education: Research ,16, 15-29.

11 Amo, L.C., Zhuo, M., Wilde, S., Murray, D., Cleary, K., Amo, C., Upadhyaya, S., Rao, H.R. (2015). Cybersecurity Engagement and Self-Efficacy Scale. Unpublished instrument.

Ethan Adams is a second-year student majoring in the Information Sciences & Technology and Security & Risk Analysis programs at Penn State Berks, Reading, PA.

Patrick Scanlon is a second-year student majoring in Information Sciences & Technology and minoring in Security & Risk Analysis programs at Penn State Berks, Reading, PA.

Joseph Torres is a fourth-year student majoring in the Information Sciences & Technology and Security Risk Analysis programs at Penn State Berks, Reading, PA

Emilio Gonzales is a recent graduate of the Information Sciences & Technology program at Penn State Berks, Reading, PA.

Tricia Clark is an instructor and program coordinator of Information Sciences & Technology and Security & Risk Analysis at Penn State Berks, Reading, PA

Terence Laughlin is a chemistry teacher in Blue Mountain School District, PA.

Abdullah Konak is a professor of Information Sciences & Technology at Penn State Berks, Reading, PA