2023 Annual Conference & Exposition
Baltimore Convention Center, MD | June 25 - 28, 2023

The Harbor of Engineering
Education for 130 Years

ASEE

Paper ID #36781

Accessible Cybersecurity Education for Engineering Students

Dr. Mai Abdelhakim, University of Pittsburgh - Main Campus

Mai Abdelhakim is an assistant professor of electrical and computer engineering at the Swanson School of Engineering at the University of Pittsburgh (Pitt). She received her PhD in electrical engineering from Michigan State University (MSU), and bachelor's and master's degrees in electronics and communications engineering from Cairo University. Her research leverages stochastic modeling, information theory and machine learning to model and design secure, reliable, and efficient Internet of Things and cyber-physical systems. Following her PhD, she was a postdoctoral research associate at MSU, where she worked on developing reliable communication networks in hostile environments. She later was a research scientist at OSRAM research center working on Internet of Things protocols, authentication mechanisms, and indoor positioning systems. Her research interests include cybersecurity, cyber-physical systems, artificial intelligence, and reliable decision-making under uncertainty.

Dr. Samuel J. Dickerson, University of Pittsburgh

Dr. Samuel Dickerson is an associate professor at the University of Pittsburgh Swanson School of Engineering. His general research interests are in the areas of electronics, circuits and embedded systems. He specializes in the deisgn of multi-physics cyber-physical systems. Dr. Dickerson has also made several contributions to engineering education research. He currently investigates the use of reflection in engineering classrooms.

2023 Annual Conference & Exposition
Baltimore Convention Center, MD | June 25 - 28, 2023

The Harbor of Engineering
Education for 130 Years

ASEE

Paper ID #36781

Accessible Cybersecurity Education for Engineering Students

Dr. Mai Abdelhakim, University of Pittsburgh

Mai Abdelhakim is an assistant professor of electrical and computer engineering at the Swanson School of Engineering at the University of Pittsburgh (Pitt). She received her PhD in electrical engineering from Michigan State University (MSU), and bachelor's and master's degrees in electronics and communications engineering from Cairo University. Her research leverages stochastic modeling, information theory and machine learning to model and design secure, reliable, and efficient Internet of Things and cyber-physical systems. Following her PhD, she was a postdoctoral research associate at MSU, where she worked on developing reliable communication networks in hostile environments. She later was a research scientist at OSRAM research center working on Internet of Things protocols, authentication mechanisms, and indoor positioning systems. Her research interests include cybersecurity, cyber-physical systems, artificial intelligence, and reliable decision-making under uncertainty.

Dr. Samuel J Dickerson, University of Pittsburgh

Dr. Samuel Dickerson is an associate professor at the University of Pittsburgh Swanson School of Engineering. His general research interests are in the areas of electronics, circuits and embedded systems. He specializes in the deisgn of multi-physics cyber-physical systems. Dr. Dickerson has also made several contributions to engineering education research. He currently investigates the use of reflection in engineering classrooms.

Accessible Cybersecurity Education for Engineering Students

Mai Abdelhakim and Samuel Dickerson
Department of Electrical and Computer Engineering
University of Pittsburgh
{ maia, dickerson }@pitt.edu

Abstract

Along with the ever-increasing adoption of connected systems in the age of the Internet of Things (IoT), there is a pressing need for preparing engineers and other technology professionals to address the growing cybersecurity challenges. Nowadays, cybersecurity education is needed not only for cybersecurity specialists but also for anyone who works with technology, especially in critical infrastructure (such as energy systems or healthcare). However, there is an evident gap in cybersecurity skills due to the dearth of accessible classes on the topic for non-specialists. This is particularly important because major attacks on critical IoT systems originate from vulnerabilities introduced by human error (via social engineering, phishing emails, etc.), committed by engineers and other professionals who are not cybersecurity experts. Hence, effective cybersecurity education aimed at a broad audience of engineering students is crucial. One way to achieve this is to offer accessible cybersecurity courses that are open to students from different backgrounds, departments, and/or majors. The challenge here is to design accessible courses while giving students the hands-on experience needed for effective learning with minimal prerequisites. In this paper, we present methods to navigate through some of the challenges resulting from removing typical prerequisites, and the trade-off between breadth and depth. Specifically, we apply this method in an undergraduate information security course in engineering that covers network security, while many students do not have computer networks background prior to taking the course. We combined two different approaches for hands-on exercises on network firewalls. The first one is a video gaming approach (CyberCIEGE), and the second one is based on setting up multiple virtual machines (SEED labs). Students are surveyed to indicate how they perceived the different hands-on methods. We analyze the results (from surveys and exam questions) to demonstrate the impact of removing typical prerequisites and the effectiveness of the hands-on methods.

Introduction

Cybersecurity education in the age of the Internet of Things (IoT) and Cyber-Physical systems (CPS) is crucial. IoT and CPS are transforming today's engineering systems that are becoming integral to different sectors and critical infrastructure, such as energy, manufacturing, transportation, and healthcare. In IoT and CPS, physical assets (machines, reactors, generators etc.) are integrated with cyber elements that can process, compute, and exchange data via a network/internet. With these disruptive technologies, engineering systems are becoming highly autonomous and interconnected. Along with the enormous benefits of IoT and CPS, there are alarming cybersecurity concerns. There are many vulnerabilities in connected engineering systems that would lead to a successful cyberattack, including network-related vulnerabilities (e.g., weaknesses in computer networks' protocols), software-related vulnerabilities (e.g. weaknesses in computer code/applications), and human-related vulnerabilities (e.g., people not trained could reveal confidential information via social engineering, such as through phishing emails).[1] In addition, due to the deep integration between physical and cyber domains in emerging engineering systems, the impacts of each cyberattack are not confined to the cyber domain but can cause devastating damage to physical assets (e.g., damage to equipment, the explosion of a reactor, blackouts in cities, etc.). That is, cybersecurity has a direct impact on public safety, health, and national security. Expanding the cybersecurity skillset among engineering graduates is crucial in mitigating the continuously evolving cyberattacks.

There is an evident shortage of skilled cybersecurity professionals and a pressing need for cybersecurity education.[2] There are existing efforts that attempt to close the cybersecurity education gap. For example, the ACM and IEEE computing curricula have included cybersecurity, and several schools now offer cybersecurity courses as a part of a degree or a certificate.[3,4,5] However, there is a shortage of accessible cybersecurity courses at the undergraduate level aimed at a broader audience of engineering students, due to prerequisites in typical cybersecurity courses that would refrain students from taking unless such courses are required for their degree. For example, an undergraduate student in electrical engineering learns about power systems, energy generation and distribution, transformers, and energy grids, but should also be able to learn basic vulnerabilities and cybersecurity challenges associated with these systems. One way to achieve this is to offer accessible cybersecurity courses that are open to students from different backgrounds, departments, and/or majors, and impose little to no prerequisites in these courses. The challenge here is to design accessible courses while giving students the hands-on experience needed for effective learning despite the minimal prerequisites. Here, we focus on the design of *accessible* cybersecurity courses.

In this paper, we access the impact of removing typical prerequisites in a cybersecurity course and the effectiveness of tools used for experiential learning. We apply this method in an information security course in the Department of Electrical and Computer Engineering (ECE). The course covers cryptography, network security, and software security. We will take the network security part as an example to study the effectiveness of the learning approach. The reason we chose the network security part is that a computer networks course is not a prerequisite; hence some students in the cybersecurity course have a background in computer networks (e.g. via a course completed or a practical work), while others do not have that background. Students in the cybersecurity course are surveyed to indicate their background level in computer networks prior to taking the class, and based on that students are divided into groups (from group 1, which means no prior background at all in computer networks, to group 5, which means a strong background in computer networks). All groups rate the impact of including network security in the course on enhancing their understanding of security problems and practices. The results show that *all* students found enhancement to their learning from adding the network security part to the course, despite the fact that more than 55% of the students did not take a prior course on computer networks.

We also incorporated two different approaches for hands-on activities on network security (specifically on network firewalls); one approach is based on gaming and the other is based on using a virtual machine, as will be described in the following. Then, we analyzed the learning perceived by the different groups of students from using the two different hands-on approaches. Overall, the results of this study show the feasibility and effectiveness of accessible cybersecurity education.

1 Learning by Making

It is well known that learning by making boosts the learning effectiveness. There have been a variety of tools created for cybersecurity education and provide an experiential learning experience.[6,7,8] Among the well-known tools for information assurance education is CyberCEIGE,[9] which is developed by the Naval Postgraduate School (NPS). In CyberCIEGE, a set of video gaming scenarios are created to demonstrate the different concepts in computer and network security.[7,10,11] SEED (SEcurity EDucation) virtual machine is another platform that has been designed to provide hands-on exercises/labs on a broad range of cybersecurity topics.[8] It is funded by the National Science Foundation.[12] In this study, we will use both CyberCEIGE and SEED labs and will investigate the learning experience for students, with a focus on network security using firewalls. It is worth mentioning that these are very different tools and require different skills. For example, in SEED firewall lab students need to pay attention to more networking details that are not needed in the gaming approach. Students in the different groups (based on their computer networks background) are asked to complete exercises using both tools and then rate their learning experience. The results are presented in Section 4.

2 Accessible Cybersecurity Education - Challenges and Course Design Choices

A direct approach to accessible education in academic courses is to minimize or eliminate prerequisite courses that could only be completed by a relatively small group of students. However, removing a prerequisite will have a direct impact on the content and the hands-on assignments designed for the course. In this section, we will provide an example of an accessible cybersecurity course and discuss the challenges and design choices.

We developed a new course on cybersecurity (with the title Information Security) in the Department of Electrical and Computer Engineering (ECE). Our objective in that course is to cover a wide range of possible vulnerabilities, threats, and defense/control methods. Specifically, the course is designed to include cryptography, network security, and software security. The overall structure of the course and the main topics included in each part is shown in Figure 1. The cryptography part includes symmetric and asymmetric cryptosystems. The network security part includes the internet protocol stack, transport layer, SYN flooding attack and countermeasures, firewalls, and intrusion detection systems. The software security part includes vulnerabilities in C programming language with a focus on buffer overflow attacks and countermeasures. The required background for the cryptography and software security topics in the course will be satisfied by all students as part of the core program requirements (e.g., students have a

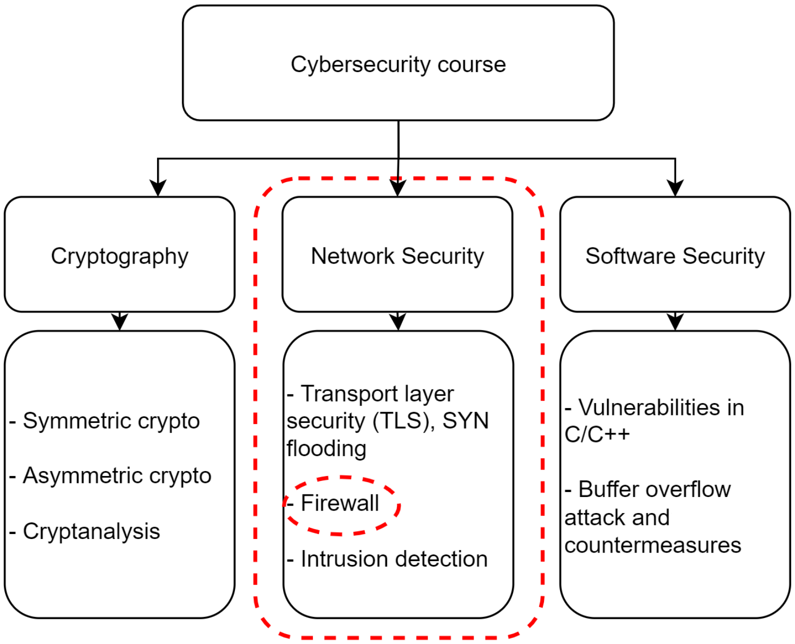

Figure 1: The overall structure of the cybersecurity course (information security). It includes cryptography, network security, and software security. The paper focuses on the feasibility of including the network security part of the course without having computer networks as a prerequisite. In the hands-on assignment, we choose the firewalls lab for assessment.

background in Boolean algebra, discrete math, and C programming). This is not the case for the network security part since not all ECE students take a course on computer networks.

A decision to make while designing the course is whether computer networks would be required as a prerequisite for the information security course, especially since network security is an important part of the course. We decided to not add that prerequisite so as to make the course more *accessible*. It is noted that there are two programs in ECE, namely electrical engineering and computer engineering. Computer engineering students are required to take the information security course (in a recently revamped curriculum), while electrical engineering students can take it as an elective. Also, computer networks is a core course in the computer engineering program, but not in the electrical engineering program. If we had a computer networks course as a requirement for the information security course, then students majoring in electrical engineering would have to take an additional course on computer networks as an elective before taking the information security course. That hurdle would refrain many students from learning information security. Therefore, our decision was to not add computer networks as a prerequisite, which made the information security course more accessible. However, that had a big impact on the course design in terms of how to introduce the network security part effectively for the different majors and how to incorporate experiential learning.

The learning outcome of the network security part of the course is that students should be able to i) describe vulnerabilities and attacks on network protocols (specifically the internet protocol), such as SYN flooding attacks, (ii) demonstrate transport layer security (TLS) handshake and how cryptographic parameters are agreed upon in a secure connection before data exchange, (iii) differentiate between different types of firewalls, and (iv) assess intrusion detection systems performance, e.g., via Bayesian detection rate. Our first challenge was to introduce the background needed without a lot of redundancy to any group of students. For the network security part, a basic understanding of the internet protocol stack and functionality is essential. For that purpose, a lecture is dedicated to explaining the background needed on computer networks (specifically the internet) along with possible vulnerabilities and attacks. Although there has been some redundancy for those who had a prior computer networks course, the angle has been different. For example, we explained the need for port numbers (which is a topic covered in the computer networks course) but connected that to port scanning and how it could be exploited by adversaries/threat agents (which is not covered in the computer networks course). Also, while explaining a networking protocol, we emphasize the "what could go wrong" aspects (for example, connection establishment is explained and combined with Denial of Service attacks). That basic computer network background is discussed in a lecture, which was also recorded. It has been evident during the COVID-19 pandemic that the availability of recorded course material helped students' learning as it enables them to review instructor explanations anytime. Even after in-person instruction started again the recorded material would be beneficial for students, especially in parts where not all students have the background and some may need to get back to the lecture more than one time to review contents needed as the class progresses.

Our next challenge was the design of hands-on assignments. The video gaming approach, CyberCIEGE, was initially the tool of choice in the network security part of the cybersecurity course. That choice was motivated by the fact that almost anyone can play a video game. With no prerequisite on computer networks and internet protocols, video gaming seemed to be the most intuitive approach for students to apply what they learn. The SEED lab was not the choice initially for the network security part (although it has been used in the course for other parts, like cryptography). The reason is that it requires more attention to networking details (e.g., specify the port numbers and IP Addresses, instead of checking a box next to the application name as in the gaming approach). However, we decided to incorporate both the SEED labs and the gaming approach as hands-on exercises for the network security part, as we find great value in both. However, we wanted to examine the impact of removing the prerequisite on how students perceived their learning experience in the two different hands-on approaches. In the following section, we will describe the details of one assignment involving both SEED labs and CyberCEIGE then we will present how students evaluated their learning experience.

3 CyberCIEGE and SEED Virtual Machine for Accessible Education

For an accessible cybersecurity course, we investigate the use of two different tools for hands-on activities, namely CyberCIEGE and SEED labs. We focus specifically on network security due to the diverse background in the course, as stated earlier. More specifically, for this study, we will use an assignment on network firewalls.

We designed the assignment such that it is composed of two parts. In the first part, students use CyberCIEGE to complete a video gaming scenario on firewalls, called "TirePly Filters Scenario". The scenario involves connecting a worker to the internet and configuring a firewall to limit traffic coming from the internet using a graphical user interface (GUI). In the second part of the assignment, we adopt parts of the SEED lab on firewalls. In particular, students have to create two virtual machines to emulate two different computers and have one start a Telnet connection with the other. Then use UFW (uncomplicated firewalls) terminal commands on the Ubuntu virtual machine to add firewall rules, and specifically block Telnet connections. It is worth mentioning that the Telnet is an insecure internet application that enables a device to remotely connect to another one. The SEED lab needs more technical skills as it delves into more details; for example, it works with IP addressing and port numbers used in the internet protocol stack, instead of a GUI that directly selects applications without specifying protocol details as in the CyberCIEGE game. After students complete the assignment, we ask them to take a survey so we learn how the different parts in the assignments contributed to their learning. The results are presented in the following section.

4 Results

In this section, we present the results of this study to assess the impact of removing the prerequisite on computer networks from a cybersecurity course that covers network security.

We surveyed students to rate their background and their learning experience in the course. The total number of students who responded to the survey is 70. In the survey, first, the students rated their background on networks before taking the cybersecurity course on a scale from 1-5, where (1) means that they have absolutely no background in computer networks, (2) means that they have a little generic background but didn't study computer networks in a course, (3) means that they have some background in computer networks (either from a course with some information on networks or from practical work), (4) means that they have a good background on computer networks (through a previous course), (5) means that they have an extensive background on computer networks (more than one course or extensive work experience). The result of the survey is summarized in Table 1 and in Fig. 2. It can be seen that more than 55.7% of the students didn't take a prior course on computer networks and only had some to no background on networks prior to joining the security course.

Table 1: Background on computer networks before joining the security course

Background level	**Count**	**Percentage**
1 - No background	15	21.43%
2 - Little background	9	12.86%
3 - Some background	15	21.43%
4 - Good background (previous course)	30	42.86%
5 - Extensive background	1	1.43%
Total	70	100.00%

Although most of the class (more than 55.7%) did not take a computer networks course prior to the cybersecurity course, the benefit of adding network security in the cybersecurity class is evident. Specifically, in the survey, we asked students to rate how much the network security part

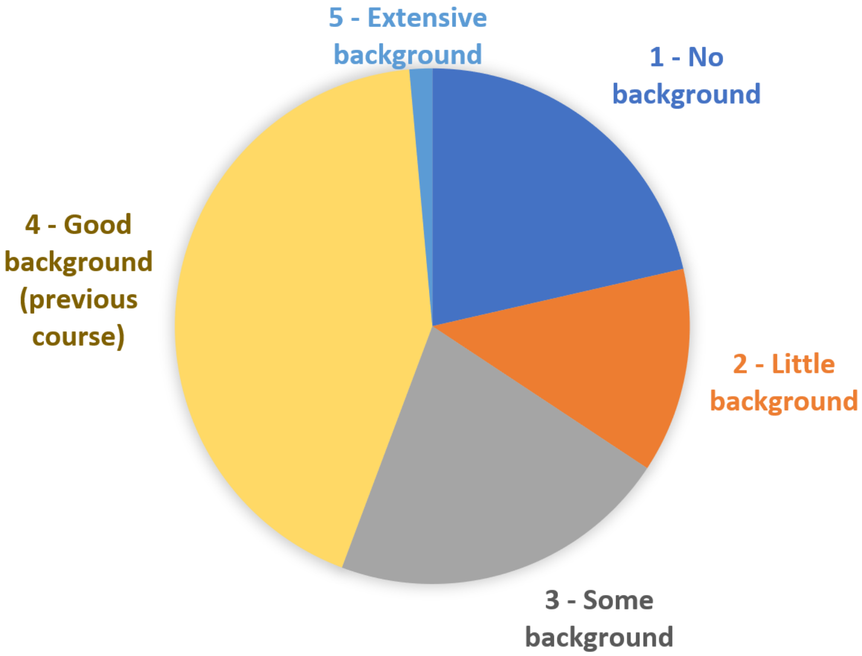

Figure 2: Students' background on networks before joining the information security class.

of the course enhanced their understanding of information security problems and practices. The rating was on a scale from 1-5, where (1) means no enhancement, (2) means little enhancement, (3) means a moderate amount of enhancement, (4) means a lot of enhancement, and (5) means a great deal of enhancement. The results are summarized in Table 2. As observed none of the students chose level 0 (no enhancement), and 58.57% of all students indicated that the network security part has contributed to enhancing their understanding "a lot" or by "a great deal". The table shows the results for the two groups of students, i.e., the group of students who took a prior course on computer networks and those who did not take such a course. The results show that more than 64% of students who did not take a prior course on computer networks find that including network security has enhanced their understanding of information security problems and practices by "a lot " or "a great deal", and 51.6% of those who completed a computer networks course had those ratings ("a lot" or "a great deal"). This interesting observation shows the importance of not refraining from adding network security topics in a course that does not have a computer networks prerequisite.

One main objective of this study is to examine the choice of tools to use for the hands-on activities in an accessible cybersecurity course, as described in the previous section. Recall that here we designed a hands-on assignment on network firewalls to be composed of two parts: (Part 1) video game - CyberCIEGE, and (Part 2) SEED virtual machine (VM) firewall exercise, as stated in Section 3. We asked the students to rate how much the second part (SEED VM) enhanced their understanding of network firewalls. Students rate their learning from 1 to 4, where (1) means that Part 1 (video game) is sufficient and Part 2 (VM) did not contribute to the understanding of firewalls, (2) means that Part 2 contribution to the understanding is minimal; (3) means that Part 2 complements Part 1 and improved their understanding of firewalls; (4) means that Part 2 is essential in the hands-on assignment, as it clarified aspects that were unclear or not observed in

Table 2: Rating of how much the network security part of the course enhanced the understanding of information security problems and practices. The table shows the results for two groups of students: students who took or did not take a computer networks (net.) course before taking the cybersecurity course.

Enhanced understanding of Info. Sec	**Count, w prior net. class**	**Count, w/o prior net. class**
1- Not at all	0 (0%)	0 (0%)
2- A little	5 ($\simeq$ 16.1%)	3 ($\simeq$ 7.7%)
3- Moderate amount	10 ($\simeq$ 32.2%)	11 ($\simeq$ 28.2%)
4- A lot	11 ($\simeq$ 35.5%)	17 ($\simeq$ 43.6%)
5- A great deal	5 ($\simeq$ 16.1%)	8 ($\simeq$ 20.5%)
Total	31	39

Part 1 (and Part 1 only was not sufficient). The total number of students who responded to this question is 69, out of which 69.56% indicated that the SEED VM is essential in the hands-on exercise or complements the CyberCIEGE gaming part. The results are shown in Table 3 and Figure 3. We also found that out of the 24 students who have little to no background in networks prior to the information security class (Table 1), 15 students (i.e., 62.5%) found that the SEED VM complements the video gaming exercise or is essential to their understanding.

In addition to survey results, we assessed students learning of firewalls using four exam questions. We found that out of 24 students with little to no background on networks, there are 16 students (that is 66.67%) who answered three or four questions correctly in the exam. This shows that a prerequisite of a computer networks course is not essential for students to learn network security in an information security course.

Table 3: Rating of the extent by which part 2 (VM) of the lab was important for the experiential learning

Video game vs VM	**Count**	**Percentage**
1- Video game is sufficient	8	11.59%
2- Part 2 (VM) contribution to understanding is minimal	13	18.84%
3- Part 2 (VM) complements part 1 (Video game)	35	50.72%
4- Part 2 (VM) is essential	13	18.84%
Total	69	100.00%

5 Conclusions

In this paper, we studied the impact of removing a typical prerequisite course on computer networks from a cybersecurity course that includes network security. The objective of removing the prerequisite is to make the course accessible to more students, which is crucial to close the gap in cybersecurity education. Although more than half of the students did not have a prior course on networks, most students indicated that adding network security to the course enhanced their understanding of information security problems and practices. Some of the challenges were

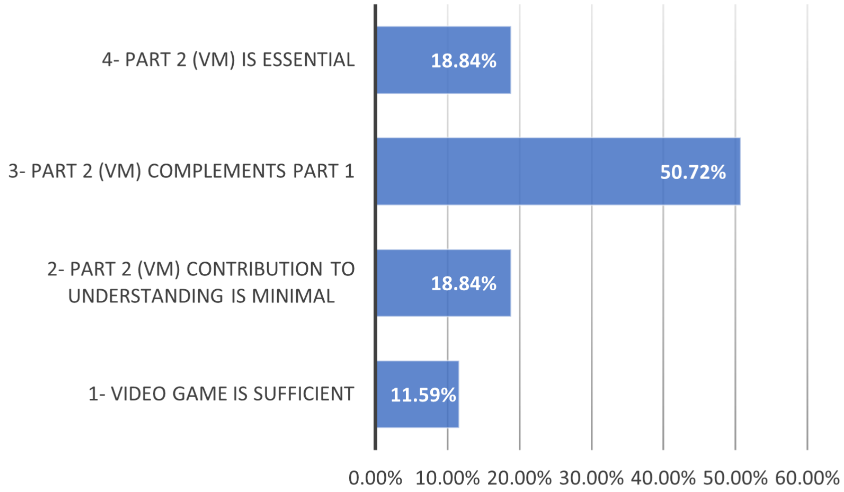

Figure 3: Students' rating of the impact of including Part 1 (CyberCEIGE video game) in addition to SEED VM (Part 2) in an exercise on network firewalls.

in developing hands-on assignments given the diverse background of students on computer networks. We studied two different approaches for hands-on activities on network firewalls, one is the CyberCIEGE video game and the other is using a virtual machine (SEED VM). The survey results indicated that the majority of students found that SEED VM complements the gaming assignment. This could be attributed to the fact that students were able to control more networking details, for example, related to IP addressing and port numbers. Overall, the results of this study show the feasibility and effectiveness of accessible cybersecurity education, and that a prerequisite of a computer networks course is not essential for students to learn network security in an information security course.

It is worth noting that many advanced topics in the network security domain will require adding a prerequisite to cover. However, the paper suggests not refraining from including some network security topics, with adjustable levels of depth, in a cybersecurity course that does not have a computer networks course as a prerequisite. This is motivated by the importance of the topic in the age of the Internet of Things and the pressing need for educating future engineers about the growing cybersecurity challenges that originate from connectivity. Educating students on network security, even at a basic level, is becoming a crucial step toward protecting various engineering systems and critical infrastructure.

References

[1] William Stallings and Lawrie Brown. *What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences*. Pearson, 2017. ISBN 9780137502875.

[2] (ISC)^2. Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens. Technical report, 2018.

[3] Computing Curriculum Efforts. https://www.computer.org/volunteering/boards-and-committees/professional-educational-activities/curricula.

[4] ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline. http://cybered.acm.org/.

[5] Valdemar Švábenský, Jan Vykopal, and Pavel Čeleda. *What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences*, page 2–8. Association for Computing Machinery, New York, NY, USA, 2020. ISBN 9781450367936. URL https://doi.org/10.1145/3328778.3366816.

[6] Tanner J. Burns, Samuel C. Rios, Thomas K. Jordan, Qijun Gu, and Trevor Underwood. Analysis and exercises for engaging beginners in online CTF competitions for security education. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, Vancouver, BC, August 2017. USENIX Association. URL https://www.usenix.org/conference/ase17/workshop-program/presentation/burns.

[7] C.E. Irvine, M.F. Thompson, and K. Allen. Cyberciege: gaming for information assurance. *IEEE Security Privacy*, 3(3):61–64, 2005. doi: 10.1109/MSP.2005.64.

[8] SEED Labs. https://seedsecuritylabs.org/.

[9] CyberCIEGE. https://nps.edu/web/c3o/cyberciege.

[10] Cynthia E. Irvine, Michael F. Thompson, and Ken Allen. Cyberciege: An information assurance teaching tool for training and awareness. 2005.

[11] Cynthia E. Irvine, Michael F. Thompson, and Ken Allen. Cyberciege: An extensible tool for information assurance education. 2005.

[12] Wenliang Du. Seed: Hands-on lab exercises for computer security education. *IEEE Security Privacy*, 9(5): 70–73, 2011. doi: 10.1109/MSP.2011.139.