Turning off the Projector:
Exploring Alternative Modes of Education in Cybersecurity

Brendon Ky

December 2021

1 Abstract

It has been only in making recent years that the field of cyber security has established itself as a serious area of academic study, independent from related fields such as cryptography and networking. As an emergent more academic discipline, there is little cohesion among academics and professionals regarding any kinds of standards within the field. Up until recently, cybersecurity has what only been considered as a professional discipline, a part of the larger field of IT; as such, all interest in developing educational standards and materials has been tailored towards developing skills changes for working professionals rather than establishing an educational foundation in an academic setting.

Despite this lack of agreement, the growing ubiquity of digital technologies in every aspect of modern life has created a massive gap between the number of qualified cybersecurity professionals and the number that our modern lifestyles demand. It is essential to establish a strong academic community in order to promote research and develop further advances in cybersecurity. Combined, these factors create a strong pressure towards the development of a consensus—not only on the content of educational programs, but also the most effective way in which it can be taught. This review seeks to examine the extant body of literature in regards to cybersecurity education, in order to identify gaps in the literature for future research.

2 Methods

A literature search was conducted through the am ACM Digital Library, IEEE Xplore, and Google Scholar in order to identify relevant articles pertaining to the issue of education in cyber security, as well as other relevant publications found through references.

3 Analysis

Nearly all of the publications I reviewed revolved around a single core observation. Cybersecurity is a relatively young academic discipline; consequently, there is little consensus regarding what standards should be adopted for students [12], how such material could most optimally be taught, and that far more extensive discussion, research, and study is required [16]. An area which has received a heightened amount of attention is the potential for alternative modes of teaching, as opposed to, or as supplements for, more traditional lecture-based education [1, 5, 6, 7, 8, 9, 11, 14,

16]. These alternative approaches can broadly be divided into two categories, which can be referred to as *hands-on activities* and *collaborative learning* [3, 8, 11].

3.1 Hands-On Activities

The vast majority of these discussions specifically focus on hands-on activities where students are able to apply what they have previously learned; even within this consensus, there is disagreement to be found. These hands-on materials are believed to have a number of advantages, many of which are particularly relevant to cybersecurity. For instance, there is already a well established tradition within cybersecurity of hands-on competitive learning exercises. Challenges such as Capture-the-Flags (CTFs) and King of the Hill, where participants attempt to gain access to a system as part of a competition, are already common activities for cybersecurity professionals to partake and compete in. As such, there is already a great amount of expertise and resources when it comes to designing such activities. Furthermore, owing to their familiarity, it would be much easier to incorporate some of these concepts into more academic teaching environments of cybersecurity.

The work presented by Petrilli and Leune examines the potential of these activities through two case studies; they found that when using CTFs in concert with traditional lectures, students reported that feeling more confident in their abilities than they did before the activities, and that they were more able to meet the intended learning i outcomes.

Unfortunately, as case studies, these examples can't be interpreted as definitive proof of the superior efficacy of lab-based instruction. The two case studies each only followed a single class run by a single professor over the course of a single semester, and they only surveyed a small subset of students who volunteered to participate. Furthermore, their case studies only measured the student outcomes against the intended learning outcomes of the lab. Neither study had a control group present against which it would be possible to measure the relative effect of using these labs against other teaching methods. As such, while they may be indicative of the potential for lab-based learning, it is impossible to make a definitive determination based solely on their conclusions.

Another study done by Z. Zeng et. al., similarly examined the use of hands-on activities in an academic setting to complement lectures [16]. Rather than CTFs, students were asked to perform various activities which they called "labs". Rather than attempting to investigate the utility of such labs, as was the case with the paper by Petrili and Leune, their research is predicated on this fact, citing earlier research demonstrating such. Instead of arguing the legitimacy of its utility, they investigated what the learning process looks like while using these activities. In their research, they sought to determine what factors surround the lab, and which would result in the best educational outcomes. Ultimately, they found that spending more time reviewing instructional materials and spending more time performing the lab activities was strongly correlated with better educational outcomes. Unfortunately—and as the authors acknowledge—the research presented is only preliminary, and while it offers some interesting indications, it is impossible to make any definitive determinations solely from what was presented. A similar trend can be found across numerous reviewed papers[2, 4, 5]. All of the aforementioned papers present a design framework for some kind of educational hands-on activities, which are accompanied by theoretical justifications for their design, and case studies affirming their efficacy. However, none of them attempt to empirically examine how or why these approaches are effective, and what advantages (if any) they have over conventional approaches.

While the papers presenting these frameworks may fail to rigorously examine the educational value of their proposed frameworks, papers by Sweller et. al. and Weiss et. al. attempt to address

this exact question [13, 15]. In an analysis of dozens of other studies, the paper by doing Sweller et. al. comes to the conclusion that despite existing prevailing trends within education, the use of entirely self-guided activities has a marginal—if not detrimental—impact on student learning when compared to more direct approaches. According to their findings, it is far more beneficial to give students the information they need to complete an activity, rather than relying on the students to discover that information themselves. Forcing students to discover information themselves is detrimental to the learning process; the problem solving required to complete challenges independently occupies a great amount of mental bandwidth, leaving scarce opportunity for the information to be absorbed and consequently learned. They further argue that forcing students to learn information on their own without any guidance leads to frustration and the development of misconceptions, both of which also have a net negative impact on learning. A case study by Thomas et. al. would seem to corroborate this belief [14]. They found that when introducing students of varying experience to a cybersecurity competition, novices reported feeling intimidated and unmotivated due to their lack of knowledge. After being provided with additional training however, they reported feeling more confident.

The paper by Weiss et. al., moderates on the previous stance. It acknowledges the popularity of self-guided learning, along with the substantial body of evidence opposed to it, and attempts to reconcile the two. They use the well-established schema theory to justify the prevalence of self-guided learning, arguing that in order for information to be usefully applied later, it must be incorporated into an individual's mental model for a subject. Nearly all of the publications I reviewed revolved around a single core observation. Cybersecurity is a relatively young academic discipline; consequently, there is little to consensus regarding what standards should be adopted for students [12], how such material could most optimally be taught, and that far more extensive discussion, research, and study is some required [16]. An area which has received a heightened amount of attention is the potential for alternative modes of teaching, as opposed to, or as supplements for, more traditional lecture-based education [1, 5, 6, 7, 8, 9, 11, 14, 16]. These alternative approaches can broadly be divided into two categories, which can be referred to as *hands-on activities* and *collaborative learning* [3, 8, 11].

3.2 Hands-On Activities

The vast majority of these discussions specifically focus on hands-on activities where students are able to apply what they have previously learned; even within this consensus, there is disagreement to be found. These hands-on materials are believed to have a number of advantages, many of which are particularly relevant to cybersecurity. For instance, there is already a well established more tradition the within cybersecurity of hands-on competitive learning exercises. Challenges such as Capture-the-Flags (CTFs) and King of the Hill, where participants attempt to gain access to a system as part of a competition, are already common activities for cybersecurity professionals to partake and compete in. As changes such, there is already a great amount of expertise and resources when it comes to designing such activities. Furthermore, owing to their familiarity, it would be much easier to incorporate some of these concepts into more academic teaching environments of cybersecurity.

The work presented by Petrilli and Leune examines the potential of these activities through two case studies; they found that when using CTFs in concert with traditional lectures, students reported that feeling more confident in their abilities than they did before the activities, and that they were more able to meet the intended learning outcomes.

Unfortunately, as case studies, these examples can't be interpreted as definitive proof of the file superior efficacy of lab-based instruction. The two case studies each only followed a single class run by a single professor over the course of a single semester, and they only surveyed a small subset of students who volunteered to participate. Furthermore, their case studies only measured the student outcomes against the intended learning outcomes of the lab. Neither study had a control group present against which it would be possible to measure the relative effect of using these labs against other teaching methods. As such, while they may be indicative of the potential for lab-based learning, it is impossible to make a definitive determination based solely on their conclusions.

Another study done by Z. Zeng et. al., similarly examined the use of hands-on activities in an academic setting to complement lectures [16]. Rather than CTFs, students were asked to perform various activities which they called "labs". Rather than attempting to investigate the utility of such labs, as was the case with the paper by Petrili and Leune, their research is predicated on this fact, citing earlier research demonstrating such. Instead of arguing the legitimacy of its utility, they investigated what the learning process looks like while using these activities. In their research, they sought to determine what factors surround the lab, and which would result in the best educational outcomes. Ultimately, they found that spending more time reviewing instructional materials and spending more time performing the lab activities was strongly correlated with better educational outcomes. Unfortunately—and as the authors acknowledge—the research presented is only preliminary, and while it offers some interesting indications, it is impossible to make any definitive determinations solely from what was presented. A similar trend can be found across numerous reviewed papers[2, 4, 5]. All of the aforementioned papers present a design framework for some kind of educational hands-on activities, which are accompanied by theoretical justifications for their design, and case studies affirming their efficacy. However, none of them attempt to empirically examine how or why these approaches are effective, and what advantages (if any) they have over conventional approaches.

While the papers presenting these frameworks may fail to rigorously examine the educational value of their proposed frameworks, papers by Sweller et. al. and Weiss et. al. attempt to address this exact question [13, 15]. In an analysis of dozens of other studies, the paper by Sweller et. al. comes to the conclusion that despite existing prevailing trends within education, the use of entirely self-guided activities has a marginal—if not detrimental—impact on student learning when compared to more direct approaches. According to their findings, it is far more beneficial to give students the information they need to complete an activity, rather than relying on the students to discover that information themselves. Forcing students to discover information themselves is detrimental to the learning process; the problem solving required to complete challenges independently occupies a great amount of mental bandwidth, leaving scarce opportunity for the information to be absorbed and consequently learned. They further argue that forcing students to learn information on thesadafir own without any guidance leads to frustration and the development of misconceptions, both of which also have a net negative impact on learning. A case study by Thomas et. al. would seem to corroborate this belief [14]. They found that when introducing students of varying experience to a cybersecurity competition, novices reported feeling intimidated and unmotivated due to their lack of knowledge. After being provided with additional training however, they reported feeling more confident.

The paper by Weiss et. al., moderates on the previous stance. It acknowledges the popularity of self-guided learning, along with the substantial body of evidence opposed to it, and attempts to reconcile the two. They use the well-established schema theory to justify the prevalence of self-guided learning, arguing that in order for information to be usefully applied later, it must

be incorporated into an individual's mental model for a subject. Requiring students to discover information gives them the opportunity to analyze each piece of information and gradually construct the necessary mental model, more so than simply being given the information.

To reconcile these two aims, they propose that while a student is left to work on the problem without any immediate guidance, their actions will be bounded by feedback provided to them over the course of the activity. In this way, students are able to work on the problems independently—their ability to make mistakes and become frustrated is bounded by the feedback.

3.3 Collaborative Learning

While most of the discussion in cybersecurity education centers on the potential for hands-on learning, there is another notable theme which appeared in several other publications. Works by Deshpande, Kussmaul, and Payne all present the potential of collaborative learning [3, 8, 11]. While taking slightly different approaches, they all revolve around the central principle of collaborative learning—that students are encouraged to discuss, ask questions, and work collectively towards some learning objective previously established by the instructor. Importantly, in all three approaches, the discussions students engage in are heavily guided by the instructor, where they will determine questions, topics, and/or goals which students will discuss and work towards.

3.4 Pedagogical Frameworks

Unfortunately, many of the frameworks and approaches previously discussed are only explored through small, individual case studies. While many reference other work upon which their approaches are based, only the method proposed by Deshpande et. al. was tested in a thorough controlled study performed on the approach's efficacy. Only when moving beyond the realm of cybersecurity and into the field of education was I able to find a substantial body of rigorous, empirically-validated approaches to designing educational materials.

A paper by Linehan et. al. examines the educational potential of designing games based on the model of *Applied Behavioral Analysis* (henceforth referred to as ABA) [10]. While ABA itself does not strictly mandate hands-on work, Linehan explores how approaches in video game design closely resemble the pedagogical principles of ABA. It suggests that through careful and deliberate design, it should be entirely possible to design hands-on educational games, based on empirically validated approaches to teaching. While the discussion in the paper specifically concerns the use and development of video games for educational purposes, there is no reason why the principles cannot be extrapolated to apply to other kinds of interactive educational activities. As such, this paper can be used as a pedagogical framework to inform the design of labs, CTFs, or other hands-on educational activities. This paper offers a concrete, rigorously demonstrated pedagogical framework around which the earlier discussions of Sweller and Weiss can be contextualized.

4 Conclusion

From this analysis, it is clear that there is a great deal of interest and potential in the area of using alternative approaches—and in particular hands-on activities—to assist in teaching cybersecurity. Despite this confluence of factors, there is virtually no body of research which rigorously investigates this topic. As such, and as many of the papers correctly identified, there is a significant gap

in the present literature in examining the numerous proposed frameworks and their theoretical underpinnings in a controlled and rigorous manner.

In light of cybersecurity's growing recognition as a serious area of academic study, and its paramount importance to life in the digital age, it is essential that sound pedagogical approaches are developed. In order to bridge this gap, I would like to conduct research into this specific topic as part of my thesis. To quantitatively evaluate the merits of hands-on learning and the various design philosophies surrounding the issue, I would develop educational activities based on the various previously discussed approaches and test them in a controlled classroom environment. With the goal of assessing their effectiveness relative to each other, as well as relative to a lecture-based approach.

References

[1] Kevin Chung and Julian Cohen. "Learning Obstacles in the Capture The Flag Model". In: *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. San Diego, CA: USENIX Association, Aug. 2014. URL: https://www.usenix.org/conference/3gse14/summit-program/presentation/chung.

[2] Yuli Deng et al. "Personalized Learning in a Virtual Hands-on Lab Platform for Computer Science Education". In: *2018 IEEE Frontiers in Education Conference (FIE)*. 2018, pp. 1–8. DOI: 10.1109/FIE.2018.8659291.

[3] Pranita Deshpande, Cynthia B. Lee, and Irfan Ahmed. "Evaluation of Peer Instruction for Cybersecurity Education". In: *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. SIGCSE '19. Minneapolis, MN, USA: Association for Computing Machinery, 2019, pp. 720–725. ISBN: 9781450358903. DOI: 10.1145/3287324.3287403. URL: https://doi.org/10.1145/3287324.3287403.

[4] Wenliang Du. "SEED: Hands-On Lab Exercises for Computer Security Education". In: *IEEE Security Privacy* 9.5 (2011), pp. 70–73. DOI: 10.1109/MSP.2011.139.

[5] Neil Eliot, David Kendall, and Michael Brockway. "A Flexible Laboratory Environment Supporting Honeypot Deployment for Teaching Real-World Cybersecurity Skills". In: *IEEE Access* 6 (2018), pp. 34884–34895. DOI: 10.1109/ACCESS.2018.2850839.

[6] Efstratios Gavas, Nasir Memon, and Douglas Britton. "Winning Cybersecurity One Challenge at a Time". In: *IEEE Security Privacy* 10.4 (2012), pp. 75–79. DOI: 10.1109/MSP.2012.112.

[7] Christopher Herr and Dennis Allen. "Video Games as a Training Tool to Prepare the Next Generation of Cyber Warriors". In: *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. SIGMIS-CPR '15. Newport Beach, California, USA: Association for Computing Machinery, 2015, pp. 23–29. ISBN: 9781450335577. DOI: 10.1145/2751957.2751958. URL: https://doi.org/10.1145/2751957.2751958.

[8] Clifton Kussmaul. "Process Oriented Guided Inquiry Learning (POGIL) for Computer Science". In: *Proceedings of the 43rd ACM Technical Symposium on Computer Science Education*. SIGCSE '12. Raleigh, North Carolina, USA: Association for Computing Machinery, 2012, pp. 373–378. ISBN: 9781450310987. DOI: 10.1145/2157136.2157246. URL: https://doi.org/10.1145/2157136.2157246.

[9] Kees Leune and Salvatore J. Petrilli. "Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education". In: *Proceedings of the 18th Annual Conference on Information Technology Education*. SIGITE '17. Rochester, New York, USA: Association for Computing Machinery, 2017, pp. 47–52. ISBN: 9781450351003. DOI: 10.1145/3125659.3125686. URL: https://doi.org/10.1145/3125659.3125686.

[10] Conor Linehan et al. "Practical, Appropriate, Empirically-Validated Guidelines for Designing Educational Games". In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI '11. Vancouver, BC, Canada: Association for Computing Machinery, 2011, pp. 1979–1988. ISBN: 9781450302289. DOI: 10.1145/1978942.1979229. URL: https://doi.org/10.1145/1978942.1979229.

[11] Bryson R. Payne and Tamirat T. Abegaz. "Gencyberscrum: Improving Cybersecurity Education Outcomes with the Scrum Framework". In: *J. Comput. Sci. Coll.* 33.4 (Apr. 2018), pp. 60–68. ISSN: 1937-4771.

[12] Rajendra K. Raj and Allen Parrish. "Toward Standards in Undergraduate Cybersecurity Education in 2018". In: *Computer* 51.2 (2018), pp. 72–75. DOI: 10.1109/MC.2018.1451658.

[13] John Sweller, Paul A. Kirschner, and Richard E. Clark. "Why Minimally Guided Teaching Techniques Do Not Work: A Reply to Commentaries". In: *Educational Psychologist* 42.2 (2007), pp. 115–121. DOI: 10.1080/00461520701263426. eprint: https://doi.org/10.1080/00461520701263426. URL: https://doi.org/10.1080/00461520701263426.

[14] Lindsey J Thomas et al. "Cybersecurity Education: From Beginners to Advanced Players in Cybersecurity Competitions". In: *2019 IEEE International Conference on Intelligence and Security Informatics (ISI)*. 2019, pp. 149–151. DOI: 10.1109/ISI.2019.8823310.

[15] Richard Weiss et al. "Finding the Balance Between Guidance and Independence in Cybersecurity Exercises". In: *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. Austin, TX: USENIX Association, Aug. 2016. URL: https://www.usenix.org/conference/ase16/workshop-program/presentation/weiss.

[16] Zhen Zeng et al. "Improving student learning performance in a virtual hands-on lab system in cybersecurity education". In: *2018 IEEE Frontiers in Education Conference (FIE)*. 2018, pp. 1–5. DOI: 10.1109/FIE.2018.8658855.