Cybersecurity Education through the Gamification of Capture the Flag Competitions

Ian Cook

Brigham Young University

WRTG 316: Technical Communication

Professor Lisa Johnson

December 8, 2021

**Abstract**

One of the biggest problems facing a very technical field is that training and educational efforts cannot keep up perfectly with all the cutting-edge advances. This is consistent as well with Cybersecurity education solutions, where there exists no single silver bullet. Capture the Flag competitions, however, have emerged as an impactful tool in teaching participants technical skills in competitive environments conducive to the deeply technical nature of Cybersecurity as a whole. This is in part due to aspects of gamification found in the competitions themselves, which increase overall participation and motivate participants to persevere through more difficult tasks. This literature review demonstrates the above outcomes, as well as the conclusion that Capture the Flags are both conducive and valuable in an educational environment, such as a college course.

key words: Cybersecurity, gamification, Capture the Flag, Competitions, education.

**Introduction**

When one thinks of Cybersecurity, they often imagine a hacker in a dark room, hoodie pulled over their face, and typing madly at a computer. However, the road to get to that “hacker” status is one that isn't well defined or established. Seeking opportunities to hone skills and learn new tricks of the trade, cybersecurity enthusiasts often turn to technical competitions called Capture the Flags. These are problem-solving events where various problems are presented with a flag or code at the end once the problem is solved. They cover a wide variety of topics and technologies and have quickly become a staple for any cybersecurity learner.

For my literature review, I aim to survey the current implementation of what makes Capture the Flags such useful mediums, as well as their specific application within the higher education sphere. I will also take a step back and dissect Capture the Flags in the context of gamified learning and those elements. This literature review will hopefully serve as a starting point for others who wish to dive deep into the structure, purpose, and implementation of Capture the Flag competitions and gamified learning concepts in cybersecurity.

Through the course of my research, I have come to identify three reasons as to why Capture the Flags are effective tools for teaching cybersecurity. First, they are adaptable and suitable for learners of all levels. Next through gamified elements, they provide great extrinsic motivation, often sparking a learner's intrinsic motivation which is valuable when dealing with such a technically rich field. Lastly, Capture the Flags are highly adaptable and deployable for various topics and environments, allowing them to be used to fit all sorts of educational and entertainment aims.

With the state of today's ever-increasing digital world, the need for qualified, security-literate professionals is at an all-time high. With that need, there exists a parallel need for quality education and methods for learning and keeping up with such cutting-edge topics. Capture the Flags fill this important niche and should be maximized to provide the most benefit.

Historically, CTFs have been hosted by hacking groups or in tandem with conferences. However, this has shifted over the last year as colleges have begun building out cybersecurity programs and in turn their competitions and groups. This shift is intriguing because a career in cybersecurity higher education is quite unappealing compared to working in the industry. This point is out of scope for the review but is important to note. As many have searched for ways to develop more traditional paths into cybersecurity, Capture the Flags have served as a great way to bridge the professional and educational realms.

**Current Cybersecurity Education**

Among many industries, there exist well-established paths of entry into that field. For the medical field, one applies to medical school, completes various residency programs, and then earns their medical license. Such a singular path does not exist for Cybersecurity. Over the course of the last few years, many new avenues have sprouted in this void, with desires to become the well-worn path to success. A few of these avenues include online e-learning platforms, competitions, and cybersecurity degrees in higher education. These all have their strengths and weaknesses and can vary on their effectiveness depending on an individual’s career goals. For example, university programs at the present moment are early in their maturation, and as such are not seen as the definitive option. To better understand the effectiveness of Capture the Flag competitions within the current landscape, research was reviewed on what general cybersecurity education means are used today.

Current online training for professionals and others seeking to learn more about cybersecurity takes the form of e-learning programs. These “awareness training programs” provide information, however, lack some of the hands-on experience to teach participants the necessary skills to be competent (Beuran, Chinen, et al., 2016). This highlights an important need to balance both deliveries of information and the opportunity to develop skills for those seeking to learn. In their research, Beuran, Chinen, et al., aim to survey the totality of cybersecurity education within the country of Japan as a whole and review all that was successful and what was not successful. They concluded that although easy to deliver, e-learning platforms and training programs that resembled PowerPoints that students would click through, were not effective ways at ensuring students were competent in cybersecurity topics.

While such e-learning platforms and other programs exist, higher education institutions bring a variety of solutions and mediums. The other angle Beuran and Chinen, et al. (2016) reviewed was the current implementation of cybersecurity programs in Higher Education institutions. They found similar concerns with Leune & Petrilli Jr., (2017), in which they discovered that Higher Education is not always best equipped to respond to the quickly changing demands in skills needed by the workplace. They also found that traditional teaching methods were not aligned with the needs and interests of the students and therefore do not always produce the best outcomes. To better understand why this is, there are a few points that merit mention. First, the nature of cybersecurity is a very technical one. Finding qualified professors to teach such technical topics is difficult, and it is constantly changing which means professors need to be adaptable to what is relevant. Next, to compete and retain such professors means paying at a more competitive level which is often hard to do with such a lucrative industry. The field itself has not fully embraced the higher education path as the best path or even a worthwhile path for potential cybersecurity professionals. There is much debate that still exists whether a formal degree is useful in the field of cybersecurity.

To address the point made by Leune & Petrilli concerning traditional teaching methods, I reviewed articles presented on various teaching methods of cybersecurity within higher education, such as the frameworks of Challenge Based Learning and Gamification of cybersecurity learning. Cheung, Cohen et al. (2011) presented research that focused on the application of the idea of Challenge-based learning in cybersecurity. Challenge-based learning is a student-centered learning approach where students apply their knowledge and skills to the solving of real-world problems as opposed to just theoretical or hypothetical problems. By placing students directly in real-world situations, the learning that takes place is much more effective and valuable to the overall student’s progress in becoming a competent cybersecurity professional. For higher education institutions to embrace such a shift in teaching methodology, it would require increased coordination between universities, public institutions, and businesses to provide the structure needed for real-world problems to be available for a challenge-based learning approach. In addition to these topics, much of the applied learning intersects with competitions and the use of gamification to go beyond traditional teaching methods.

**Gamified Learning**

Now with a basic understanding of how cybersecurity education is approached as a whole, to take the next step involves stepping back and obtaining a wider view on the topic of gamified learning. As was identified earlier, there exist many ways to present information or problems to be solved in a way that helps the student learn. Often, such as the case with cybersecurity, there is no one set way to teach a subject perfectly. Although it is not perfect, one method that has become increasingly popular and effective as of late, especially with younger generations, is that of gamified learning, a connection born out of this generation’s immersion in video games. However, van Steen and Deeleman (2017) in their work stated that gamification implementations follow the model of serious games, or games intended to not entertain but to teach and focus on learning outcomes, rather than traditional video games. With this idea in mind, we turn to what is exactly meant by gamified learning.

Gamified learning shares the use of specific elements and frameworks to the ends of incentivizing participation and augmenting participant motivation throughout the learning process. Elements such as scoring mechanisms and leaderboards and incentives are interwoven among problems to be solved or specific checkpoints to be achieved. This approach is used to facilitate a more involved learning experience and has been used in many fields, not just Cybersecurity. Through the following review of current literature, we will observe the merits and composition of gamified learning as well as its effectiveness. Gamified learning exists and has persisted due to its ability to engage its learners and aid in their learning process from start to finish, and as such is a valuable and effective learning mechanism.

For an exercise to be considered under the genre of gamification, elements found in traditional video games are applied to an educational exercise. This could take the form of assigning points to a question and adding theatrical or storyline aspects to a problem to further engage the student or providing content of various levels of difficulty. McDaniel, Talvi, et al. (2016) defined gamification as the use of game mechanics to incentivize and motivate participants in competitive experiences where progression is tracked. This focus on progression mirrors that of many popular video games and can take the form of a progress bar or the ability for the student to see how many questions remain out of the number of questions already solved. This position leads well into more recent discoveries made by Vykopal, Švábenský, and Chang (2020) that these elements also provide a more beneficial experience both to students individually, in group environments, and to the instructor from a logistical standpoint as well. Many gamified learning systems involve a central scoring engine that allows a universal scoring standard to be applied across the board to all participants, allowing for a streamlined grading system, ideal for a classroom setting where completion or accuracy is a key value. All these elements potentially combine for a greater learning experience overall.

Armed with the element of what constitutes gamification, the natural focus is now turned to the actual impact of that strategy. This subject was commentated greatly by Muntean (2011), who identified the area of participation as one with great potential for influence by gamified elements. Speaking on that further, Muntean added that these elements led to feelings of ownership and purpose. By progressing and recognizing their progress and achievements, the students felt propelled to finish. Another topic generally identified by Muntean is that of motivation. Beuran, Chinen, et al. (2016), commented on this by identifying a great increase in motivation by participants to complete gamified training, especially in cases where the user had little to no experience or interest going into the training. Leune and Petrilli (2020) identified that when gamification was most closely tied to real-world challenges or applications, the impact of intrinsic learning and intrinsic motivation grew exponentially.

On top of all these arguments, Mayer, Bekebrede, et al. (2014), confirmed these outcomes but also took it upon themselves to study more of the science of game-based learning. They recognized that while implementing a lot of these had positive outcomes, there did not exist a well-established framework for understanding the overall impact of this strategy. It identified important aspects to observe such as previous experience, skills, game performance, the experience and play that take place within the game, player satisfaction, first and second-order learning. All of these elements were reviewed in some shape or form by the other sources, which reinforced their results in identifying gamification as a quality medium for learning, within cybersecurity specifically.

With the focus on student learning, these papers have explained how various strategies involving gamification have been successful. In my opinion, as more research is done on this topic, especially with the newer generations being raised surrounded by video games, learning by gamification will be more prevalent. In no area is this more true than Cybersecurity and more specifically in the realm of Cybersecurity Capture the Flag competitions.

**Capture the Flag competitions in Cybersecurity**

With the introduction of current cybersecurity education trends and the medium of gamified learning, the two realms intersect at the third and final focus of this paper, which is the topic of Capture the Flag competitions in Cybersecurity. In the following section, we will examine what constitutes a Capture the Flag competition from a structural and a conceptual manner, addressing both the value and drawbacks that it brings to the table. With those discussed, the final aspect visited will be Capture the Flag’s implementation in education. Capture the Flags are one of the best tools for teaching cybersecurity concepts, especially when organized properly and focused on providing opportunities for participants to learn. This is proven by both beginners and those more experienced in cybersecurity. Current research also strongly supports the use of Capture the Flag learning experiences in the classroom setting, as the benefits for the technical type of learning are well documented.

As with many other technical challenges, some considerations must be made when planning and organizing a Capture the Flag event. Depending on the desired goals and audience participating, there may be a need for more resources or more structure to run the competition. Often competitions are run as a short-term event, maybe 36-48 hours at most. However, because of research completed in recent years, variations on this specific format have been discovered, implemented, and tested with success.

One vein of variations includes efforts by researchers to apply these competitions into an educational setting, with encouraging results. Chothia and Novakovic (2015) organized a course in which students were presented with their virtual machine files and had to find flags within their specific machine and turn them in alongside a written description of their solution. This approach was unique in that there was no central infrastructure. Thus the only work for the teacher existed in creating the virtual machine files and then grading any written solutions. This solution was more difficult for the students than traditional coursework but was overwhelmingly more popular and valuable to their learning.

Some pitfalls were identified by other researchers, with valuable insights into how to avoid or mitigate these without detracting from the educational experience of the students. Chung and Cohen (2014) analyzed Capture the Flag events and scrutinized various flaws and weaknesses. Their conclusions based on their findings included unclear or guess-heavy questions, overdependence on technical skills, poor infrastructure, and other faults. Various mitigations include more hands-on challenges over trivia-type questions. By incorporating those kinds of challenges, students immerse themselves in the problem-solving process and develop technical tenacity. Chung and Cohen also shared concerns that Chothia and Novakovic (2015) found, being that the challenges in Capture the Flags were an excellent indicator of a student's technical skills and basic understanding but did not accurately assess their foundational knowledge to the same degree that traditional assessments or coursework could. A synthesis of the two was highly recommended by both of these research parties for a comprehensive educational experience.

Quality of the challenges was identified previously by Chung and Cohen as a potential flaw in the delivery of Capture the Flag competitions, whereas other researchers identified this as a CTF’s area of greatest potential. This is due to the flexibility in what an organizer or educator can do with challenges to meet the needs of the participants. For example, McDaniel and Hay (2016) dove into the subject applying solely to beginners and those with little to no exposure to the field of cybersecurity. Their findings were overwhelmingly positive, noting that in small training exercises, CTF formats were much more efficient in engaging participants in topics that they often had little to no interest in beforehand, and a noticeable increase of interest afterward because of their experience. When challenges were structured in the form of introducing a topic, followed by a hands-on exercise by way of a harder challenge of the same topic, students applied their knowledge learned in earlier problems, thus solidifying that knowledge. This also addresses the common difficulty in teaching cybersecurity to beginners due to the highly technical nature of the subject.

Another method noted by Chung and Cohen that increased the quality of the content was that of creating challenges that lent themselves to multiple angles of learning the same technique or skill. To be successful in solving a CTF problem, one needs to submit the flag found at the end of the problem. Often that means there are few restrictions in the way that one can solve it, meaning competitors can exercise creative thinking, and reward those who are perseverant in their study and efforts.

As shown in the above sections, Capture the Flag competitions provide great opportunities and means for students to learn technical skills and cybersecurity knowledge in a creative, hands-on approach. Although the competitions can take time to establish and develop, once a system is in place that meets the needs of the students, it is an incredible tool that aids both students and teachers. The flexibility in challenges allows teachers to fit the content best to their needs, whether it be in a specific subject or to a more beginner group of learners. Overall, the research at hand shows the value in pursuing methods of education beyond traditional ways.

**CONCLUSION**

In reviewing the sources provided above, it is clear that Capture the Flag competitions are successful in their aim to better educate participants in the topics of Cybersecurity, both in educational settings and non-traditional settings. The success of these CTFs can be attributed to the ingrained elements of gamification and flexibility. As I studied this topic, each publication included their aims for future research which collectively touched on a few various topics. Future aims include completing a deeper dive into the way technical problems are presented in Capture the Flags, identifying the most optimal way to handle questions that lend themselves towards more subjective answers, and whether CTFs truly aid in long-term learning. One effort to further shed light includes my efforts in the Brigham Young University Cybersecurity Research Lab. Our team is looking at the emotional experience of a student within a Capture the Flag, by applying Carol Kulthau’s Information Search Process framework to the equation. In this effort, we are seeking to better understand how students feel throughout the learning process of a Capture the Flag environment. All in all, these competitions, improved with the additional understanding that comes from the research completed, will make for more comprehensive cybersecurity education, and in turn, a safer online world for us all.

**References**

Beuran, R., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2016). Towards effective cybersecurity education and training.

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge based learning in cybersecurity education. Proceedings of the *International Conference on Security and Management* (SAM)

Chothia, T., & Novakovic, C. (2015). An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. 2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)

Chung, K., & Cohen, J. (2014). Learning obstacles in the capture the flag model. 2014 {USENIX} *Summit on Gaming, Games, and Gamification in Security Education* (3GSE 14)

Leune, K., & Petrilli Jr, S. J. (2017). Using capture-the-flag to enhance the effectiveness of cybersecurity education. Proceedings of the 18th *Annual Conference on Information Technology Education*

Lo, J., Mayer, I., Bekebrede, G., Harteveld, C., Warmelink, H., Zhou, Q., van Ruijven, T., Kortmann, R., & Wenzler, I. (2014). The research and evaluation of serious games: Toward a comprehensive methodology. *British journal of educational technology*,*45*(3), 502-527.

McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the flag as cyber security introduction. 2016 49th *Hawaii International Conference on System* *Sciences* (HICSS)

Muntean, C. I. (2011). Raising engagement in e-learning through gamification. Proc. 6th *International Conference on Virtual Learning* (ICVL)

van Steen, T., & Deeleman, J. R. (2021). Successful Gamification of Cybersecurity Training. *Cyberpsychology, Behavior, and Social Networking*

Vykopal, J., Švábenský, V., & Chang, E.-C. (2020). Benefits and pitfalls of using capture the flag games in university courses. Proceedings of the 51st *ACM Technical Symposium on Computer Science Education*