

A COMPARISON STUDY OF TWO CYBERSECURITY LEARNING SYSTEMS: FACEBOOK'S OPEN SOURCE CAPTURE THE FLAG AND CTFD

*Rhonda G. Chicone, Purdue University Global, rchicone@purdueglobal.edu
Susan Ferebee, Purdue University Global, sferebee@purdueglobal.edu*

ABSTRACT

There is a high demand for innovative and smart technologies to improve cybersecurity education and produce skilled cybersecurity professionals in a faster, more engaging manner. Gamification, in the form of Capture the Flag (CTF) platforms, are increasingly being used by educational institutions and in private and public industry sectors. A previous 2018 study by Chicone and Burton investigated Facebook's CTF platform as an open source inexpensive learning and assessment tool for undergraduate and graduate IT/cybersecurity adult students for an online university. In this comparative expansion study, the 2018 study was replicated but this time examining and comparing Facebook's CTF platform with another CTF platform called CTFd. The studies were evaluated on assessment capability. It was found that Facebook's CTF had very little to aid with assessment while CTFd provided many formative assessment features that were valuable for students as well as for faculty in determining needs for future learning.

Keywords

Cybersecurity, Information Security, Capture the Flag, Cybergames, Cyber Range, Gamification, Assessment, Learning Outcomes

INTRODUCTION

Moving toward 2020, demand for cybersecurity professionals continues to increase. Casesa (2019) points to five positions, specifically that are in the highest demand in 2020. These positions are Cybersecurity Manager/Administrator, Cybersecurity Consultant, Network Architect and Engineer, Cybersecurity Analyst, and Cybersecurity Engineer. All of these positions require a broad knowledge of cybersecurity risk, threats, breaches, and mitigation strategies. In addition to the demand for cybersecurity professionals is also the need for non-information technology employees to raise their awareness of cybersecurity so that as end users they are prepared to prevent phishing scams and social engineering attacks. Additionally, there is a need for cybersecurity awareness training in elementary school through career professionals working at all levels of business (Roepke, R., & Schroeder, U., 2019). With the broad training requirements described, unique teaching and training methods are needed.

Gamification is seen as one method to teach cybersecurity to the broad range of people that require this training (Lee & Hammer, 2011). Gamification is defined as using game frameworks, game elements, and game mechanics and dynamics to promote desired learning outcomes. Capture the Flag for cybersecurity education began in the 1990s and its purpose was to allow players (students) to learn new concepts and skills in a hands-on environment where there were a variety of challenge levels. It is a game in which the players compete against each other and can be played by teams or individuals (Kaplan IT Training, 2019).

In this study, two Capture the Flag systems are compared in terms of their effectiveness in learning outcome achievement, assessment capability, ease of use, and student engagement.

Background

Sound cybersecurity practices and computer security practices are vital for protecting users, systems, applications, and data; however, there remains a large gap in the need for cybersecurity professionals and those that are adequately educated and available. Current training and education techniques include web classrooms, instructor-led training, virtual labs, and hands-on simulations (Jordan, Knapp, Mitchell, Claypool & Fisler, 2011). The effectiveness of all of these types of training is not clearly understood (Roepke & Schroeder, 2019). Immersive and interactive cybersecurity training could increase engagement and speed the learning. One method to train all employees and organizational leaders is gamification, which allows everyone to play the roles of various types of attackers. This method can enable

employees to reduce the number of attacks that occur due to human susceptibility exploits (Adams & Makramalla, 2015).

Training through Gamification. Gamification as a learning tool incorporates game elements such as competition, team collaboration, leaderboards to show comparative points, and rewards. Jordan et al. (2011) posits that these game elements contribute motivational factors of recognition and achievement which contributes to continued engagement. According to Jordan, et al. (2011) gamification typically starts with a current assessment of the learner's knowledge in order to guide the learning process for optimal efficiency and speed of learning. Capture the Flag (CTF) competitions are one way to implement gamification for cybersecurity education and training. Students compete against one another, earning points as challenges are completed with these points displayed on a leaderboard to further the competitive aspect of the game. CTF competitions are implemented domestically and internationally and available to a wide range of students in an online virtual environment. CTF competitions are sponsored by companies like Facebook, Microsoft, Raytheon and IBM.

Types of Capture the Flag Systems. There are three forms of CTF gamification systems. They are jeopardy style, hardware challenges, and attack and defense. Jeopardy-style consists of a challenge in a particular category like cryptography, forensics, web or networking. A CTF allows students to answer quiz questions in a timed environment. Capturing the flag represents finding the correct answer. After the player captures the flag, he or she earns points. Jeopardy-style CTF events usually take place over 72 hours (Miller, 2015).

The Attack and Defense type CTF asks a team to get a server up and running and they then have to keep it functional while the server is being attacked by another team. This requires an extreme amount of multitasking as players examine source code for holes, simultaneously monitor network traffic for malicious exploits, and performing patches or other defense mechanisms. This all occurs in a timed scenario and the highest score is given to the first team to take down a server. Attack and Defend CTF events usually take place over 24 hours (Miller, 2015).

The Hardware Attack type of CTF gives the team an unknown hardware element and they need to determine how to bypass some element of the hardware element's security.

Facebook's CTF. Facebook has hosted competitions since 2013. In 2016, Facebook released an open-source version of its CTF platform to assist with security education. Facebook's CTF system is a web-based jeopardy style system that currently runs on the Ubuntu operating system version 14.0 or greater. The researchers decided upon using Amazon's Web Services (AWS) as the infrastructure for the system (Marinescu, 2016).

CTFd. CTFd is an open-source version of the CTFd platform. It is web-based and can be used as a jeopardy style system. The developers of CTFd also offer a hosting option that is cost-effective.

Problem

In 2020, 53% of companies reported facing a shortage of cybersecurity personnel, which represents a 10% increase from 2016. Although cybersecurity graduates have increased, educational systems still cannot keep up with the rapid increase in a number of attacks leading to continually increasing demands for cybersecurity professionals (Matthews, 2020). Matthews reports that current cybersecurity training does not reflect the reality of the field and that classroom learning is not always an effective method of learning for this field. The report also finds that companies are increasingly reluctant to spend more dollars on employee training in this field (Matthews, 2020). Gamification may provide improved learning and more rapid training of cybersecurity professionals.

Purpose

The purpose of this comparative study was to determine the differences in the open-source Facebook Capture the Flag system and the open-source CTFd Capture the Flag system. The two systems were compared based on the following criteria 1) administrative functionality 2) student assessment functionality, 3) system navigation and 4) users' perceived experience. Additionally, Appendix provides a complete specification comparison for both systems.

The content for each system was the same set of challenges to include web application security, reverse engineering, networking, digital forensics, cryptography, and general security topics (Kerner, 2016). This study included a group

of volunteers from the online university's student body who used the CTFd system as a learning tool. The process used in the original Facebook Capture the Flag study was replicated identically. Comparative results were provided for the two systems.

LITERATURE REVIEW

Gamification

Technology development provides more innovative education and training methodologies, including gamification and other computer-related training methods. Clark Abt (1970) described gamification as games with an explicit learning purpose rather than the purpose of amusing users (Sørensen, Meyer, & Egenfeldt-Nielsen, 2011; Tsekleves, Cosmas, & Aggoun, 2016). It is only in the last ten years that the value of 'serious games' has been acknowledged. Serious gamification technology is now used by many organizations, including the military, healthcare, and corporate training environments concerning cybersecurity education (Michael, 2006; Tsekleves, et al., 2016). Gamification and simulation environments allow learners to experiment without presenting a risk to other individuals, organizational assets, or situations (Damewood, 2016; Koukopoulos & Koukopoulos, 2017). Gamification supports experiential learning, which appeals to adult learners who prefer to have an immediate application of their learning and to self-direct their education (Damewood).

Gamification also appeals to adult learners' desire for achievement. Earning immediate points and badges engage the adult learner as they achieve incremental goals. Learners are motivated to persist in gameplay as they accomplish incremental goals and feel intrinsically motivated. Additionally, learners feel extrinsic motivation as they visually see their score, receive recognition of their peers and instructors as they place on a leaderboard showing comparative results. Effective gamification provides participants with challenging but achievable goals that are incremental and lead to persistence playing (Fengfeng, Kui, & Ying, 2016). Gamification rested on Game theory originating from the field of economics and provided a way to evaluate the economic market competition. Game theory allowed at two or more participants to develop their skills performance by performing interdependent decision-making. The developing decision-making confidence prolongs engagement with learning (Hamman, Hopkinson, Markham, Chaplik, & Metzler, 2017).

CTF, as a gamification implementation, allows the learner to think like a hacker while competing in some CTF events. The game requires a team of individuals where attack and defense strategies must be designed and carried out making the game more realistic (Harmon, 2016).

Learning Assessment in Gamification Systems

How student learning is assessed is a critical factor for successfully achieving learning objectives. Technology has provided new approaches to formative assessments and gamification plays a role in formulating these new assessment approaches. Formative assessment is important as a trigger to stimulate ongoing student engagement as they use continuous feedback to plan future learning directions (Faten & Nouf, 2019). Formative assessment provides feedback that informs decisions about future teaching and learning activities (Faten & Nouf). Importantly, formative assessment has shifted from being teacher-focused to student-focused. Students now actively engage in and interact with the assessment process and learning decisions (Nicol & Macfarlane-Dick, 2006). Wang (2008) suggests that using game design and game elements including rules, challenges, clues, score collection and leaderboard display, and rewards produces significantly improved learning and motivation to learn.

Cybersecurity Education and Training Needs

Cybersecurity education and training is a core need in businesses today due to the growing number of cyberattacks and system intrusions. How to effectively teach students the cybersecurity information they need to protect against cyber threats, as well as the broad range of procedures, policies, and laws that must be understood and complied with, is a challenge faced both by businesses and educators. In the field of cybersecurity, typical classroom training is not ideal; for such a rapidly changing area, a more dynamic environment is necessary to keep practitioners current on the latest trends and technologies (Hammerstein & May, 2010). Learners need a combination of hands-on experience, content knowledge building, and practical skill-building, and experience building to become valuable members of the cyber workforce. While knowledge building can occur via traditional methods such as readings and lectures, the skill-

building needs to include experiential learning with an immediate application (Hammerstein & May). According to Conklin (2006), the use of a Cyber Defense Competition (CDC) can be an excellent way to give students the hands-on opportunity to test their knowledge. Often the skills acquired in a CDC experiential learning environment align with the experience needed for employment and military careers (Woszczyński & Green, 2017). While gamification provides strides in experiential learning, the ability of a learning system to assess the learning that occurs is also important. Less focus has been placed on learning assessment in these systems than focus on engagement. Future evaluations of gamification systems need to include an examination of assessment capabilities.

Conceptual Framework

While the original 2018 Facebook Capture the Flag study focused on gamification for learning, the evaluation of the CTFd platform revealed many new assessment opportunities so it is important to apply an assessment theory to form the foundation for the platform comparison. Assessment for Learning (AfL) is one such theory that can be applied. The theory looks at where the learner is now, where the learner is going, and how can the learner get there (Cambridge Assessment, 2019). The theory aligns with Vygotsky's (1978) social constructivist learning theory, meaning that learners learn by constructing from prior experiences and relationships with others. Formative assessment is an important part of this learning. Here assessment is used to form a student's learning and allow the student to see forward to what will be learned next. This differs from summative learning which provides an assessment of actual learning (Cambridge Assessment, 2019). AfL focuses on optimizing the feedback process both from student to teacher and teacher to student. In AfL feedback includes informal, immediate and oral feedback to the more formal, written feedback after having been given a test. Peer and self-assessment feedback are also important components of AfL (Cambridge Assessment, 2019). The two systems in this study will be evaluated on the components of assessment provided by the AfL.

Another aspect on which the two systems will be compared is the gamification factor of each system. The theory of gamified learning defines the advantage of using game attributes to support learning attitudes and behaviors. Gamification theory does not assume the game attributes are holistically intended to influence learning, but rather to be an unintended but effective result, possibly related more to user engagement (Landers, 2015).

Additionally, a major assumption of this study was that when individuals perform hands-on activities it can enhance their skill set related to that activity. Hammerstein and May (2010) developed a new approach for cybersecurity workforce development and found that hands-on activities were integral to skill-building. They also noted that these specific skills are more effectively honed in brief and narrowly focused activities to enable them to convert knowledge into the ability to apply it. The CTF systems in this study provide this type of learning experience.

RESEARCH METHODOLOGY

Population, Sampling, & Data Collection

This study consisted of two parts. First, the researchers did a comparative analysis of each CTF platform, comparing administrative and assessment capabilities. Second, student participants played CTF on both systems and provided qualitative responses to questions related to their user experience.

Population and Sampling

In the Facebook Capture the Flag study (Burton & Chicone, 2018) all levels of Information Technology and Cybersecurity students were invited to participate in the study; approximately 1750 students received the invitation. Initially, the required consent form was completed by a total of 23 participants and 23 participants actually played the game with 12 completing the survey.

In the current CTFd study, 3432 students received the invitation, 189 students signed the informed consent. All levels of Information Technology and Cybersecurity students were invited to participate in the study. Forty-six students played and 23 completed the survey.

Data Collection

A feature by feature comparison was made for each system and a checklist created to show what features were included in each system. For purposes of the study, features relevant to assessment were the focus, however, the Appendix provides the full specification of functionality for each of the CTF systems.

In order to obtain player input about their experience using the systems, players engaged in a CTF event and then answered 4 qualitative questions regarding their experience. The data collection process described here was identical for both the Facebook CTF study and for this comparative CTFd study. After the consent forms were received, participants registered and signed on to play at the designated time. The CTF questions included a variety of topic areas including Application Security, Cryptography, Reverse Engineering, Networking, Forensics and General security and the competition itself included 75 quiz questions and 5 flag questions conducted over 48 hours. The topic areas, questions, and multiple-choice options were identical for both studies. At the end of the CTF event, feedback on the players' experience was collected from students using both systems via the same online survey for each of the systems.

RESULTS

Table 1. Emails

Functionality	Facebook CTF	CTFd
Registration captures player's email address		x
Sends Registration Confirmation to Player		x
Allows Customizing emails for players		x

The administration functionality of CTFd provided important email capabilities not offered by Facebook's CTF. For tracking purposes, in CTFd, the player's email is captured and stored during registration. Also, the player receives a confirmation that they are registered in CTFd which is not done in Facebook's CTF. Additionally, emails sent to the players can be customized in CTFd but not in Facebook's CTF where there is no capability to send emails.

Table 2. Assessment Capability by Question Category

Functionality	Facebook CTF	CTFd
Shows question category with most solves		x
Shows question category with least solves		x

Both systems allow the creation of question categories, but only CTFd provides the ability to assess most and least solved for particular categories.

More player assessment statistics are provided in CTFd as compared to Facebook's CTF. Both systems show specific questions that were solved correctly and incorrectly, however, Facebook's CTF was not user friendly with regard to this. This type of information was under Game Logs and was sorted by time. No other sort options existed. Also, it was only available for administrators, not players. CTFd shows percentages for questions solved/not solved and categories solved/not solved as well as showing the length of time to solve the questions. CTFd also shows the challenges (questions) that players did not attempt, and awards won are provided for players and teams. For student feedback purposes, all statistics and charts are downloadable. All assessment statistics are easily available for both students and instructors. Players can also see a leaderboard of the top ten players. The Appendix contains a hyperlink to all relevant statistics.

Table 3. Assessment Capability by Player/Team statistics

Functionality	Facebook CTF	CTFd
Provides question solved percentages		x
Provides solved by category percentages		x
Provides time to solve		x
Provides specific questions solved correctly	x	x
Provides specific questions solved incorrectly	x	x
Shows challenges that player did not attempt		x
Shows awards		x
Statistics and Charts are downloadable		x

Qualitative Responses

After the CTF competition and at the end of the post-assessment quiz, participants were asked five qualitative questions about their experience. These questions were identical for both studies. The questions and response summaries are shown below in Tables 4 and 5.

Table 4. Facebook CTF Study Qualitative Responses

Qualitative Question	Response Summary	Percentage
What was your experience with the Capture the Flag (CTF) competition? Was it difficult, fun, enjoyable, educational, etc.?	Enjoyable and fun	75%
	Technical issues made it less enjoyable	25%
Did you find that the competition allowed you to hone new skills and gain new knowledge	Learned new skills, gained knowledge	75%
	Technical issues inhibited learning	25%
Was the system technically easy to use? Did you experience any technical issues?	Easy to use, no technical issues	58%
	System lagged, difficulty with instructions	42%
For future competitions, would you prefer the event to be:	Over the weekend	67%
1. Over a weekend		
2. End of the week (Thurs.-Fri.)		
3. Early in the week (Mon.-Tues.)		
	Mon.-Tues. or Thurs.-Fri.	32%

Table 4. Facebook CTF Study Qualitative Responses

Qualitative Question	Response Summary	Percentage
How long do you think the competition should run? 1. 1 day 2. 2 days 3. 3 days 4. A week	Two days	50%
	Mon.-Tues. or Thurs.-Fri.	50%

Table 5. CTFd Qualitative Responses

Qualitative Question	Response Summary	Percentage
What was your experience with the Capture the Flag (CTF) competition? Was it difficult, fun, enjoyable, educational, etc.?	Enjoyable and fun	65%
	Challenging, motivational, like to see more hands-on labs	35%
Did you find that the competition allowed you to hone new skills and gain new knowledge	Learned new skills, gained knowledge	75%
	Technical issues inhibited learning	25%
Was the system technically easy to use? Did you experience any technical issues?	Easy to use, no technical issues	100%
For future competitions, would you prefer the event to be: 1. Over a weekend 2. End of the week (Thurs.-Fri.) 3. Early in the week (Mon.-Tues.)	Over the weekend	66%
	Mon.-Tues. or Thurs.-Fri.	34%
How long do you think the competition should run? 1. 1 day 2. 2 days 3. 3 days 4. A week	Two days	44%
	Mon.-Tues. or Thurs.-Fri.	64%

Cost-Effectiveness of the Platforms

The researcher who set up the competition did have to pay the hosting center (AWS) a small set up fee and incurred minimal usage charges during the competition. However, the additional ‘cost’ to consider is the time the researcher spent creating the challenges, including the quiz questions and flag challenges. Currently, Facebook doesn't have their master repository ready to share so users must customize the platform with their own content.

The researcher who set up the competition decided to go with the CTFd hosting option. The cost for a consumer is \$50/month (basics), \$100/month (enhanced), and custom pricing (special projects). For researchers/professors, the cost is \$10/month for the basics. The costs are for an unlimited number of players. The additional 'cost' to consider is the time the researcher spent adding the challenges, that came from the Facebook CTF competition to the CTFd system. The researcher did not seek for a master repository from CTFd since challenges were already created from the Facebook CTF study.

CONCLUSION

Discussion

The CTF gamification platform, in general, provides a good learning environment and both systems evaluated here, Facebook's CTF and CTFd provided the gamification factors that help a student see formative assessment is an important part of this learning. Here assessment is used to form a student's learning and allow the student to see forward to what will be learned next. This differs from summative learning which provides an assessment of actual learning (Cambridge Assessment, 2019). AfL focuses on optimizing the feedback process both from student to teacher and teacher to student. In AfL feedback includes informal, immediate and oral feedback to the more formal, written feedback after having been given a test. Peer and self-assessment feedback are also important components of AfL (Cambridge Assessment, 2019). The two systems in this study will be evaluated on the components of assessment provided by the AfL.

The results of this comparative study revealed that Facebook's CTF, while offering real-time formative assessment through the use of immediate feedback and leaderboards, it is limited in a more granular form of feedback to further help the student understand their current knowledge level but to also help determine future avenues of learning that the student and instructor should focus on. Facebook's CTF provides information on categories of questions being responded to and how many correct answers are given for an overall category. CTFd provides more individual information for right and wrong answers within categories and for individual questions as well. This allows a student to self-assess their level of knowledge in specific areas and clearly shows their strengths and weaknesses. From an instructor's perspective, the instructor can look at an entire class and see where the class as a whole has strengths, and where the weaknesses exist, the instructor can use this information to inform future class lessons. Since Facebook's CTF does not capture user emails, it does not allow the teachers to communicate with the students directly from the game format. CTFd, on the other hand, does allow for this direct communication which further enhances formative assessment capabilities. Also, in terms of communication between student and teacher, CTFd provides downloadable charts and graphs. This allows the teacher to provide visual feedback of the student's results but also allows students to access these charts and graphs on their own. The visual display of statistical data is easier for the student to comprehend.

Another advantage of CTFd is that the vendor will host the system rather than making the instructor or administrator find their own hosting option. One of the biggest differences found in the open-ended answers from participants was that there were many technical challenges with Facebook's CTF platform compared to CTFd's platform. The lack of technical issues in the participants definitely created a more positive experience in the CTFd's platform and seemed to contribute to a more positive learning experience.

CTFd offered the instructor and/or administrator a lot of options for customizing content but also the look and feel of the game. This provides good creative opportunities for the instructors and provides a number of ways to improve student engagement. Additionally, CTFd can be expanded by adding web pages, which means the game might end up including a blog that both students and instructors can contribute to as well as web pages that contain supportive content that students could use within the game to research correct answers.

Recommendations for Future Research

There are a number of areas for future research that emerge from this comparative study. Obviously, continued research in comparing other CTF platforms, both proprietary and open source will yield new valuable data for those trying to decide on a CTF platform to implement. Additionally, studies that evaluate cybersecurity learning with the use of CTF and without the use of a CTF platform will provide valuable information on how well the CTF approach improves or does not improve actual learning outcomes and summative assessment scores. This research would involve a pre-assessment and post-assessment to measure learning outcomes. Included in this type of study would be

information gathered on how effective CTF platforms are for learning between gender, and different age and grade levels. Another area of future research would be to explore the different options for added features and added web pages to see which supporting options might be most engaging and most liked by the students.

REFERENCES

- Adachi, P. J., & Willoughby, T. (2012). More than just fun and Games: The longitudinal relationships between strategic video games, self-reported problem solving skills, and academic grades. *Journal of Youth Adolescence*, 42, 1041-1052. doi: 10.1007/s10964-013-9913-9
- Adams, M. & Makramalla, M. (2015, January). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, 5(1), 5-14. Retrieved from <http://timreview.ca/article/861>
- Balasubramanian, N., Wilson, B. G., & Cios, K. (2006). Innovative methods of teaching and learning science and engineering in secondary schools. *Journal of Systemics, Cybernetics and Informatics*, 4(6), 41-46.
- Cambridge Assessment. (2019). Assessment for learning. Retrieved from <https://www.cambridgeinternational.org/Images/271179-assessment-for-learning.pdf>
- Casesa, P. (2019). The 5 most in-demand cybersecurity jobs for 2020. Retrieved from <https://blog.focal-point.com/the-5-most-in-demand-cyber-security-jobs-2020>
- Chicone, R., Burton T. & Huston, J. (2018). Using Facebook's Capture the Flag Platform as a Hands-on Learning and Assessment Tool for Cybersecurity Education. *International Journal of Conceptual Structures and Smart Applications*, 6(1), 18-32.
- Clawson, J.G.S. (2006). *Adult learning theory: It matters*. 34-48. doi: 10.1017/CBO9780511617850.004. Retrieved from https://www.mnsu.edu/cetl/teachingwithtechnology/tech_resources_pdf/Adult%20Learning%20Theory%20and%20Online%20Learning.pdf
- Craigien, D, Diakun-Thibault, N., & Purse, R. (2014, October). Defining cybersecurity. *Technology Innovation Management Review* 4(10), 13-21. Retrieved from <http://timreview.ca/article/835>
- Damewood, A. (2016). Current trends in higher education technology: Simulation. *Techtrends: Linking Research & Practice to Improve Learning*, 60(3), 268-271.
- Faten, A., & Nouf, A. (2019). The effects of paper, web, and game based formative assessment on motivation and learning: A literature review. Available from <https://eric.ed.gov/contentdelivery/servlet/ERICServlet?accno=ED594189>
- Fengfeng, K., Kui, X., & Ying, X. (2016). Game-based learning engagement: A theory- and data-driven exploration. *British Journal of Educational Technology*, 47(6), 1183-1201.
- Hamman, S. T., Hopkinson, K. M., Markham, R. L., Chaplik, A. M., & Metzler, G. E. (2017). Teaching game theory to improve adversarial thinking in cybersecurity students. *IEEE Transactions on Education*, 60(3), 205-211.
- Hammerstein, J. & May, C. (2010). The CERT approach to cybersecurity workforce development. *Defense Technical Information Center*. Retrieved from <http://www.dtic.mil/get-tr-doc/pdf?AD=ADA537055>
- Hardy, C., & Tolhurst, D. (2014). Epistemological beliefs and cultural diversity matters in management education and learning: A critical review and future directions. *Academy of Management Learning & Education*, 13(2), 265-289. doi:10.5465/amle.2012.0063

- Harmon, T. (2016). Cyber security Capture the Flag (CTF): What is it? *Cisco Blog: Perspectives*. Retrieved from <https://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it>
- ITU-International Telecommunication Union. (2009). Overview of cybersecurity. *Recommendation ITU-T X.1205. Geneva: International Telecommunication Union (ITU)*. Retrieved from <http://www.itu.int/rec/T-REC-X.1205-200804-I/en>
- Jordan, C., Knapp, M., Mitchell, D., Claypool, M. & and Fisler, K. (2011, October). CounterMeasures: A game for teaching computer security. In *Proceedings of the 10th ACM Network and System Support for Games (NetGames)*. Retrieved from <http://web.cs.wpi.edu/~claypool/papers/security-game/>
- Kaplan IT Training. (2019). What is capture the flag? Retrieved from <https://www.kaplanittraining.com/resources/capture-the-flag-ctf-a-gamification-of-cybersecurity-learning>
- Kelly, D. (2017). The economics of cybersecurity. *International Conference on Cyber Warfare and Security; Reading, 522-XIV*. Retrieved from <https://search.proquest.com/central/docview/1897683119/abstract/726966149386421FPQ/1?accountid=34544>
- Kennedy, M. (2017). Connecting to things. *American School & University*, 89(5), 16.
- Kerner, S. M. (2016, May). Facebook open-sources its capture the flag competition platform. *eWeek*. Retrieved from <http://www.eweek.com/security/facebook-open-sources-its-capture-the-flag-competition-platform.html>
- Kessler, E. H. (2013). *Encyclopedia of Management Theory*. Thousand Oaks, California: SAGE Publications, Inc.
- Kimmerle, J., Moskaliuk, J., Oeberst, A., & Cress, U. (2015). Learning and collective knowledge construction with social media: A process-oriented perspective. *Educational Psychologist*, 50(2), 120-137.
- Koukopoulos, Z., & Koukopoulos, D. (2017). Integrating educational theories into a feasible digital environment. *Applied Computing and Informatics*. doi:10.1016/j.aci.2017.09.004
- Landers, A. (2015). Developing a theory of gamified learning: Linking serious games and gamification of learning. *Sage Journals*, 45(6), 752-768. doi:10.1177/1046878114563660
- Lee, J. & Hammer, J. (2011). Gamification in education: What, how, and why bother? *Academic Exchange Quarterly*, 15, 1-5.
- Lohrmann, D. (2012, November 9). Introducing the Michigan cyber range. *Government Technology*. Retrieved from <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Introducing-the-Michigan-Cyber-111212.html>
- Matthews, K. (2020). The state of the Cybersecurity skills gap heading into 2020. Retrieved from <https://securityboulevard.com/2019/11/the-state-of-the-cybersecurity-skills-gap-heading-into-2020/>
- Michael, D. (2006). *Serious games: Games that educate, train and inform*. Boston, Mass: Course PTR.
- Miller, D. (2015, November 2). Intro to CTFs. Retrieved from <https://www.youtube.com/watch?v=bxt-JidP3bU>
- Marinescu, P. (2016, June 15). #HITB2016AMS CommSec track D2 - Facebook presents capture the flag. Retrieved from https://www.youtube.com/watch?v=z_Xic03zor0

- Munoz, L., Miller, R., & Poole, S. M. (2016). Professional student organizations and experiential learning activities: What drives student intentions to participate? *Journal of Education for Business*, 91(1), 45. doi:10.1080/08832323.2015.1110553
- Nicol, D. & Macfarlane-Dick, D. (2006). Formative eassessment and self-regulated learning: A model and seven principles of good feedback practice. *Studies in Higher Education*, 31(2), 199-218.
- Oktavia, T., Warnars, H. L., & Adi, S. (2017). Integration model of knowledge management and social media for higher education. *Telkomnika*, 15(2), 678-685.
- Peters, M. A. (2014). The shapes of theory in education. *Educational Philosophy and Theory*, 46(12), 1315-1319. DOI: 10.1080/00131857.2014.920975
- Rass, S.; König, S.; & Schauer, S. (2017). Defending against advanced persistent threats Using game-theory. *Plos One*, 12(1), e0168675.
- Roepke, R., & Schroeder, U. (2019). The problem with teaching defence against the dark arts: A review of game-based learning applications and serious games for cyber security education. *Proceedings of the 11th International Conference on Computer Supported Education (CSEDU 2019)*, 58-66.
- Sørensen, B. H., Meyer, B., & Egenfeldt-Nielsen, S. (2011). *Serious games in education: A global perspective*. Aarhus: Aarhus University Press.
- Statistics How To. (2017). What is a t-test? Retrieved from <http://www.statisticshowto.com/probability-and-statistics/t-test/>
- Trippe, D. M., Moriarty, K. O., Russell, T. L., Carretta, T. R., & Beatty, A. S. (2014). Development of a cyber/information technology knowledge test for military enlisted technical training qualification. *Military Psychology*, 26(3), 182-198. doi:10.1037/mil0000042
- Tseklevs, E., Cosmas, J., & Aggoun, A. (2016). Benefits, barriers and guideline recommendations for the implementation of serious games in education for stakeholders and policymakers. *British Journal of Educational Technology*, 47(1), 164-183.
- Vygotsky, L. (1978). *Mind in society*. London: Harvard University Press.
- Wang, T. (2008). Web-based quiz-game-like formative assessment: *Development and evaluation*. *Computers & Education*, 51(3), 1247-1263.
- Wenz, J. (2015, August 10). Human hackers will play digital capture the flag against AI. *Popular Mechanics*. Retrieved from <http://www.popularmechanics.com/technology/security/a16827/ai-capture-the-flag/>
- Woszczyński, A. B., & Green, A. (2017). Learning outcomes for cyber defense competitions. *Journal of Information Systems Education*, 28(1), 21-41.
- Xuesong, Z., Jibao, G., Hefu, L., Jyh-Chong, L., & Chin-Chung, T. (2017). An Experiential learning perspective on students' satisfaction model in a flipped classroom context. *Journal of Educational Technology & Society*, 20(1), 198-210.
- Yuan, D. (2017, May). Developing hands-on cybersecurity laboratory with virtualization. *Journal of Computing Sciences in Colleges*, 32(5), 118-124. Retrieved from <http://dl.acm.org/citation.cfm?id=3069649>