Designing and Using Capture The Flag for Coordination and Interaction in Engineering Education

Kelei Zhang*†, Simeon Wuthier*, Kay Yoon‡, Sang-Yoon Chang*
*Department of Computer Science, University of Colorado Colorado Springs
†Department of Informatics, Fort Hays State University
‡Department of Communication, University of Colorado Colorado Springs
{jzhang5,swuthier,kyoon,schang2}@uccs.edu

***Abstract*—Capture the Flag (CTF) games improve learners' engagement and diversify pedagogy for education and training. We design and build a novel CTF game that includes coordination and interaction between the (virtually participating) participants to build fellowship and facilitate networking. Our work builds on the existing CTF components with educational benefits but differs from the traditional CTF approach which presents either an individual game with no participant interaction or a team-based game where the members already know each other and have formed teams. More specifically, we incorporate real-time interactions between participants who are new to each other and engage the participants to collectively solve the CTF challenges. We apply our CTF in both a cybersecurity scholarship program and an academic conference. This paper describes and explains the design, implementation, execution, and validation of our CTF, particularly focusing on the novel goal of including coordination and interaction in order to build fellowships with the participants. We validate our CTF design and build using multiple channels, including the real-time data provided by logging during the session, post-CTF survey, and interviews from the beta-testing session. Our evaluation results show that our novel CTF focusing on coordination and interaction aids in building fellowship and a collaborative environment. We envision our CTF design to help with the rapport building and collaboration among participants in classroom/course settings, workshops, conferences, or technical training sessions.**

***Index Terms*—CTF, Coordination, Interaction, Team Rapport and Fellowship Building, Cybersecurity Education**

I. Introduction

Capture the Flag (CTF) is an effective platform for improving the learners' engagement with the subject matter and diversify pedagogy within education and training. CTF presents a competition-based game where each participant/team solves challenges or *flags*. CTF is popularly used in cybersecurity and engineering education and training, including classroom and lab environments [1], [2], training security professionals [3], as well as for pedagogical theory research based on live CTF competitions [4].

CTF is traditionally either an individual game with no participant interactions or a team game with existing teams whose members are already well-acquainted with each other. While the utility of CTF as a learning tool for individuals has been well established, little is known about its potential to facilitate active coordination and interaction across participants/teams. In fact, in a traditional CTF game, coordination and interaction is not encouraged and may cause disqualification of the participant.

In this paper, we design a computer- and Internet-based, virtual, and synchronous CTF which facilitates live coordination and interaction among participants to build fellowship and relations. From the traditional CTF, we add the Coordination flags which are hands-on and knowledge-based flags requiring the collaboration and communication between the participants. Because such collaboration and communications are important for engineering workplace and projects, the engineering education has incorporated pedagogical practices to teach the collaboration skills and competencies [5]–[7].

We test our CTF effectiveness through real-world experiments on a university cybersecurity scholarship program and a cybersecurity research conference. Our results show that our CTF and the Coordination flags incentivize and improve the learner engagement, help the participants learn about each other, and promote fellowship building and further interactions after the CTF session.

II. Related Work

Gamification has been used in academic environments since the 1970s when two popular education games were produced: the Oregon Trail and Lemonade Stand. Gamification practice not only makes learning a fun and enjoyable experience but also enhances the effectiveness of education through instruction [8]. In particular, CTF as a gamification teaching platform has been widely successful for the cybersecurity and engineering field within classrooms and labs [1], [2] , as well as hiring pipelines for security professional talent attestation [3]. This is oftentimes in correlation to the pedagogical theory of research based on live CTF competitions [4].

In [2], the authors show how simplified material presentations can help to ease users into the understanding and process for CTF self-engagement as opposed to more complex CTF-based configuration alternatives. In addition to self-engagement, CTF also helps participants in building self-confidence, improve practical skills, enforce theoretical concepts from course work, and motivating them to dive deeper into the cybersecurity field [1], [9].

Similar to Clifton strength-focused teaching [10], [11], where teams are formed according to their assessment after answering various questions, educators can analyze the CTF results to learn and understand a student's skillset which can further aid in focused teaching in the cybersecurity. One step beyond education includes MITRE, which has been utilizing CTF for Science Technology Engineering and Mathematics (STEM) outreach, talent acquisition, and workforce development in the industry for several years [3]. Additional CTF-based programs include the National Cyber League in which student participants market themselves for job exposure by utilizing scouting reports [12].

III. CTF Design Overall

Our work builds on the standard CTF including technical flags in cybersecurity and engineering (both knowledge-based and hands-on-based) to incorporate coordination and interactions between the CTF participants. We briefly summarize the standard Jeopardy-style CTF in Section III-A and apply the novel CTF parts (coordination and interactions) for the rest of this work. Thus, our focus in coordination and interaction better defines the ideal scope and the target audience which we define in Section III-D, even though the CTF can be used for more general engineering and computer science students interested in cybersecurity.

A. Standard CTF Design

In CTF, participants register for the game and face various flag challenges in a limited time frame. Games can be synchronous (i.e. played simultaneously by many participants) or asynchronous (i.e. multiple instances spread throughout time and independent from one another) with such games lasting hours to days, during which, participants submit flags to earn points. Flags are simply strings of characters linked to a particular challenge, and challenges can be categorized for improved design organization. Within such a scheme, initial lower-difficulty flags can be set to unlock higher-difficulty flags within the same flag category, which can be used to further encourage participants to increase their depth of knowledge within a particular category. In the case where a participant may get stuck on a flag, the optional functionality may be added where the participant can spend earned points (from previously solved flags) in exchange for a hint in an unsolved challenge. Participant points reflect the participant's performance at the end of the CTF, e.g., the participant with the most points wins the game.

B. CTF for Teaching Cybersecurity

Our CTF implements the learning-by-doing principle and the gaming-based teaching pedagogy, which has the benefits of improving motivation, sense of achievement, social learning, and situated learning [8]. We specifically target the materials to be for engineering and cybersecurity and derive the flag materials from the Introductory to Computer Security course content, the first course in cybersecurity designed for junior- or senior-level students in engineering. Our CTF is designed to be a preview of the course content and highlights the diverse aspects in the cybersecurity field. Our CTF includes both knowledge-based and hands-on-based flags, the latter including those designed for learning the practical skills useful in cybersecurity [1], [2], [13]. More specifically, our CTF includes the more traditional traffic analysis, cryptography, and forensics flags. In addition, we include some unique flags, including those based on QR codes (from which they need to recognize the QR code and read the steganographic/hidden message) and video flags (in which participants decode streamed content to discover hidden Morse code flags).

Our CTF is a jeopardy-style CTF with categories derived from different tasks for designing security solutions and secure systems, as opposed to having the categories based on the sub-fields in cybersecurity (e.g., network security, forensics, and exploitation). Our CTF, therefore, includes the six categories of Investigation (search for information), Design (select the required security objectives/requirements and design the corresponding mechanisms and techniques), Analysis (process and interpret from data or results), Implementation (build and execute security mechanisms in software/programming and hardware), Testing and Evaluation (evaluations of the security mechanisms, rules, or solutions), and Coordination (communicate with other participants for collective solving).

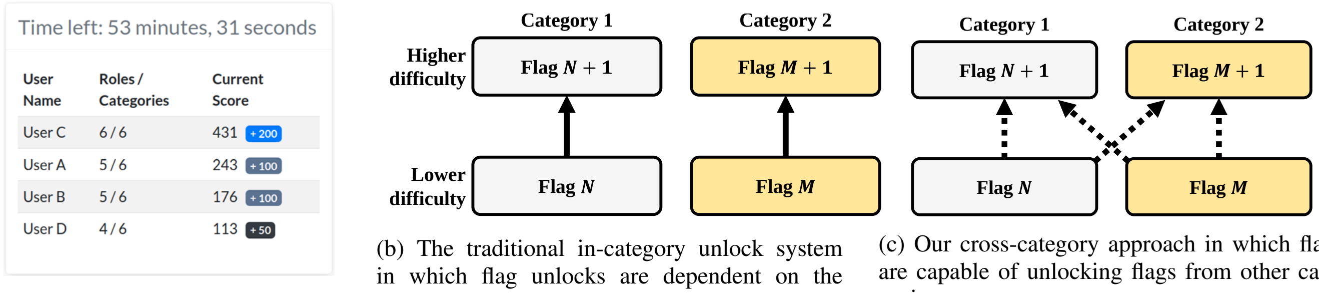
C. Broader Participation

We design the virtual CTF and host it online, i.e., the CTF server is hosted on a public IP and anybody with the link can join the synchronous/timed CTF session. We design the CTF so that there is minimal requirement for joining the CTF and only require a computer with Internet/browser connectivity and a smartphone. The CTF participation does not require additional downloads or tools. For example, instead of providing a packet capture (pcap) file for traffic analysis which would require software to deserialize (e.g. Wireshark), we provide a web-based interface for displaying necessary traffic analysis information.

Our design for broader participation also includes the following among others. First, our flags are many in number (88 in total) diverse in difficulty to support a range of participants from those who just took introductory programming course to those who have a few years of cybersecurity R&D experience. Second, before starting the CTF session, we provide a live introduction and include introductory flags to familiarize the participants with the CTF platform. Third, our CTF is lightweight and short, i.e., the duration is one hour, so that there is less commitment and psychological barrier for participation.

D. Target Audience for Our Research

Target Audience by Design Thanks to our goal for fellowship building, the ideal target audience are the participants with which fellowship building and improved communication can benefit team productivity or the class rapport. Therefore, we recommend our CTF use toward the beginning of a course



Time left: 53 minutes, 31 seconds

User Name	Roles / Categories	Current Score
User C	6 / 6	431 +200
User A	5 / 6	243 +100
User B	5 / 6	176 +100
User D	4 / 6	113 +50

(a) Our floating scoreboard display.

(b) The traditional in-category unlock system in which flag unlocks are dependent on the category.

(c) Our cross-category approach in which flags are capable of unlocking flags from other categories.

Fig. 1: Comparison between the traditional flag unlock system and our approach. We denote arrows as "unlock", and the yellow boxes represent flags from an external category, for example, a Coordination flag can unlock an Analysis flag.

in a classroom setting, training workshop, and remote working environment.

Participants for Our CTF Research: CWSSP, SVCC, and Beta Testing For execution and validation, we apply our CTF in two engineering education/training environments to fit with the target audiences. First is the Colorado-Washington Security Scholars Program (CWSSP) which is an NSF-funded scholarship program for cybersecurity students at the bachelor, master's, and Ph.D. level at the computer science department at our institution. The scholarship includes financial support, including tuition, stipend, and professional allowances, and opportunities for training/education and conferences beyond that from the host institution's degree programs. The CTF session was in September 2021 and included the scholarship recipients of fourteen participants including one female participant. The CWSSP had a networking session immediately after the CTF session and the CWSSP program continues for the remaining academic year.

We also applied our CTF to the student audience of an academic virtual conference, Silicon Valley Cybersecurity Conference (SVCC) in December 2021. The CTF for SVCC involved nine participants, one of which is female. Our CTF was held on the first day of SVCC to facilitate the interactions and the networking of the conference participants for the remainder of SVCC.

In addition, we tested our CTF with a beta-testing group involving four participants (unrelated to this research) in August 2021 as we were developing the CTF before executing them for CWSSP and SVCC. We discuss more about our improvements from beta-testing in Section VI-A.

Because our CTF's main purpose is for education and teaching, our research does not require approval from the Institutional Review Board (IRB).

IV. CTF Design for Coordination and Interaction

As mentioned in section I, the standard and existing CTF games do not encourage coordination and interaction among participants/teams that have not been well associated with one another. However, in our design, we implement the coordination flags for real-time interactions among all participants which involves asking questions, learning more about each other, or using pre-shared codes to collectively solve a problem. Our CTF also displays the real-time scores of the participants for improved engagement and a competitive game/exercise experience. Here are our contribution designs to the existing CTF games.

A. *Incentive for Diversifying Across Flag Categories*

Prior to beginning the CTF, we briefly demonstrate how the controls work as well as the underlying mechanism to control the scoreboard. We include a bonus point system in which participants can earn extra points, with the intention of encouraging participants to explore further categories and diversify the flag categories. Upon diversifying their solutions, bonus points are awarded and displayed within the floating scoreboard, as shown in Fig. 1a, which we incorporate into the CTFd source code.

We further motivate the "coordination" flags by making them the pre-requisites for other flag categories. To enable such an approach, we implement a mechanism that unlocks more advanced flags between the flag categories ("cross-category"), in contrast to the traditional approach having pre-requisites within a flag category ("in-category"). This is done by diversifying the flag unlock structure to work across categories, for example, solving a flag from Coordination may unlock an additional flag in Investigation. In a traditional CTF game, the unlock system is shown in Fig. 1b, which states that in order to proceed to a higher difficulty level flag, $N + 1$, the participants are required to finish the lower-difficulty flag N in the same flag category. Since our work is aiming for greater diversity across flag categories, we adapt the unlock system to have cross-category prerequisites as shown in Fig. 1c. To unlock the higher-difficulty level flag $N + 1$, participants will need to finish a lower-difficulty level flag, which may be either flag N from Category 1, or flag M from Category 2. We initiate all cross-category flags in the low-difficulty challenges so that as a participant progresses, they can encounter medium- and high-difficulty flags through a smoother and more diverse transition. Likewise, medium-difficulty and high-difficulty flags can utilize the in-category unlocking system for greater progression and depth in a specific flag category. In total, we have 88 flags to make sure the CTF does not run out of flags in the one-hour duration for the live, synchronous CTF game session.

B. New Flags for Coordination and Interaction

1) Meet-The-Others Flag: In this type of flag, the participants need to go out and chat with each other to uncover fact-based information about the other participants which is set to be straightforward and quick to acquire. For example, we use the information collected from preliminary questions and change it to a flag such as whose birthday is in the month of September. This will encourage communication among all participants. For the participant whose birth month is in September, there will be other participants talking to him/her. So, everyone will have the chance of talking to others.

2) Combining-Code Flag: To facilitate the pre-registration of participants and their data incorporation into the custom CTF flags, we provide participants with an 8-bit binary "code" in which we apply across the CTF. This is a unique flag as we design user-specific coordination flags for improved interaction and communication. At the beginning of the CTF, we will assign each participant a string of binary codes. During the CTF game, the participants will see flags asking them to find two binary strings from other participants, XOR the two strings, the result will be the flag. This type of flag serves the same purpose as the Trivial flag but in a different format, so the participant can pick the flags they feel comfortable doing.

3) Talk-With-Host Flag: We do not only want the participants to learn from each other via the Meet-The-Others flags but also want to interact with the hosts, for example, the faculty/senior students for CWSSP and the fellow conference participants for SVCC. During the game, flags in this type ask participants to talk to one of the hosts. When they do that, the host will ask a few questions about the participant, for instance, what the participant likes to do in leisure time, the name of game they play, their hobby, etc. The purpose of this flag is to build rapport between the CTF hosts and participants.

V. Implementation and Execution

We leverage our previous experience developing and using CTF for engineering education and build the game on the open-source CTFd platform, which enables fine-tuning and customization and lows the barrier for beginners to engage and presents the flags in a clear and readable way [14].

Fig. 2 shows our CTF execution process. While the Pre-registration and the Analyze are before and after the CTF session, respectively, the rest of the steps (Registration/Introduction, CTF Session, and Survey Evaluation) are during the session where the CTF Session is timed (i.e., to start and finish the race/game) while the others are not.

Pre-registration We do several things in this step. We first ask the participants to fill out the pre-registration questionnaire for information collection purposes. The questionnaire asks the facts about a participant, for instance, email address, full name, birth month, etc. We use the information to identify the winner and send awards. Meanwhile, our automated flag generator will use some of the information to generate Combining Code flags. Then the generator add the flags to the server. At last, we mass email the participants their codes.

Registration/Introduction Registration takes place after we announce the link to the participants. In this step, participants register their player accounts on the CTF game server. Then, we read the rules and start with demonstrating a few preliminary questions. Those preliminary flags serve two purposes: (1) teach the participant how to navigate the game; (2) teach them how to submit flags.

CTF Session CTF session starts after the registration/introduction step. Participants will do their best to solve as many flags as they can before the game ends. Each CTF game lasts for one hour.

Survey Evaluation When the CTF ends, we send the participants to take the post-CTF survey. The survey asks about their experience, thoughts about the game, and suggestions for future improvements. The survey takes place immediately after the game, thus the result better reflect participants' experience.

Analyze We take the CTF server log and survey results for analysis. This step can also involve the use of the CTF data after the CTF session, for example, CWSSP used the CTF results to construct the teams for its course activities.

VI. Result Analysis

After beta-testing our CTF, we host it in CWSSP and SVCC and evaluate its design and implementation effectiveness through multiple channels, which include interviews (for beta-testing), CTF log data analysis, and post-CTF surveys.

A. Beta-Testing Interview and Improvements

We beta-test our CTF design during its development before hosting it to CWSSP and SVCC, which was able to provide significant improvement directions to the final implementation and execution, as discussed in Section V. The beta-testing (as discussed in Section III-D) was drafted as an initial version, after which, in-person formal interviews took place with each soliciting feedback for improvement. In this section, we explore our beta testing results and analysis.

The in-person interviews with the beta-testers aid in improving the CTF to its current version. In the interview, we set nine pre-established questions to learn about participants' experience about the notification system, thoughts on coordination and flag structure/difficulty, as well as feedback on the underlying CTF design through open-ended questions to solicit unanticipated and more meaningful feedback.

The beta-testing session interviews were able to provide critical improvement pointers, including information about our current prototype lacking demonstration and clear guidance, and a flawed notification system that occurs too frequently. This feedback influenced the existing presentation and the decision to add a live demonstration/play-through on preliminary flags (e.g. the Registration/Introduction step in Fig. 2) to accommodate the former problem. For the latter, our initial intention is to help the competition/live aspect of the CTF. The notification was designed to accomplish this; however, beta testing results show that it occasionally would become distracting due to the high frequency. To accommodate this,

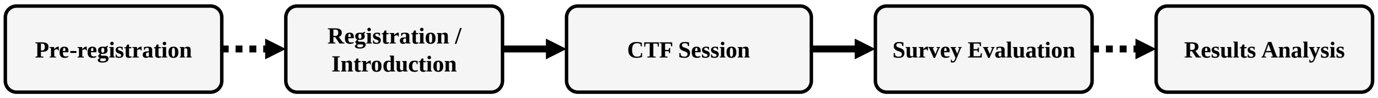


Fig. 2: Our CTF implementation and execution process. The solid line denotes *during-the-session* while the dotted lines denote the processes *outside-of-session*.

we create the scoreboard Fig. 1a to show the live score and highlight the extra points silently.

Other changes resulting from the beta-testing include the removal of extra point notifications because our interactive scoreboard interface removes this need. The pre-existing notification system to notify remaining time, we found to be useful in synchronizing awareness about the CTF state. We also find that adjusting the difficulty of the flags and re-weighting the points for every flag normalizes the categories to a fixed aggregate maximum score. Similarly, decreasing point costs when exchanging them for hints were found to improve the performance and enjoyment factors of the game.

B. Analyzing the Log Data

We share the two CTF data analysis results in this section. There are 14 participants in the CWSSP CTF and 9 in the SVCC CTF. There are in total 88 flags, within all six categories, the coordination flags take about 14.77% given the mean of 16.67%. The total submission numbers are consistent across two CWSSP CTF and SVCC CTF (731 vs. 733) given the same time frame and the correct rate is relatively close (42% vs. 34.79%). The CTF confirms our design on enforcing coordination and interaction with coordination submission ratio of 8.76% in CWSSP CTF and 8.09% in SVCC CTF.

Due to our implementation of the unlocking system, we find that some flags remain hidden from the participants at the end of the game, and are never seen or attempted. We visualize this with Table I showing the average participation rate. To calculate this, we divide the number of participants who submit any (correct and incorrect) flag by the total number of participants. By averaging this value for all flags within their respective category, we are able to compute participation rate, which serves as a direct indicator of how active participants are in each category. The participant rate for Coordination flags in CWSSP CTF is 12.14% compared to 36.67% in SVCC. The increase in participation is due to a greater incentive to move higher in the leaderboard since rewards were given to the top participants. When comparing the results to improvements in other categories (highest being 44.68% with a mean of 25.89%), the coordination category shows a significant improvement since smaller groups of participants imply less potential connectivity between each user. When there are fewer participants, the communication becomes more efficient thus eliminating the need to maintain more communication connections.

C. Survey Results

We share the two CTF survey results in this section. Immediately after the CTF games, we ask the participants to fill out the survey about their CTF experience. There are total of 13 replies in CWSSP CTF survey and 8 replies in SVCC CTF survey.

TABLE I: Average participation rate with respect to category.

Flag Category	CWSSP Participation	SVCC Participation	Number of Flags
Analysis	28.57%	32.22%	12
Coordination	12.14%	36.67%	13
Design	44.81%	50.93%	12
Implementation	33.04%	44.44%	19
Investigation	39.29%	48.61%	16
Test and Evaluation	22.45%	32.48%	16

TABLE II: Post-CTF assessment questionnaire mapping.

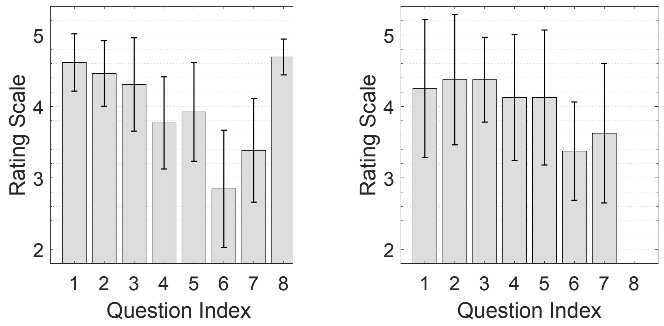
Index	Question
1	I found the CTF informative and relevant to cybersecurity.
2	I enjoyed the CTF.
3	I felt that I was participating in the CTF with others.
4	Other participants' presence helped me better engage with the CTF.
5	I found the Coordination-category flags helpful in making the CTF immersive/engaging.
6	I know the other CTF participants better after the CTF, i.e., better acquainted with the other participants.
7	I know who is better in what tasks/categories after seeing the CTF scoreboard.
8	I look forward to working with the participants moving forward (after the CTF session).

From satisfaction-related questions, the survey results in Fig. 3a and Fig. 3b show that the participants are aware of participating with others with a mean of 4.31 (out of 5) in CWSSP CTF and 4.375 in SVCC CTF, and others' presence helps the participant better engage with the CTF with a mean of 3.77 in CWSSP CTF and 4.125 in SVCC CTF. The participants also find the coordination category flags helpful in making the CTF immersive/engaging with a mean of 3.92 in CWSSP CTF and 4.125 in SVCC CTF. These three aspects indicate that the participants are aware of the other participants competing in the CTF and the engagement level was high.

From rapport-building-related questions, the survey result in Fig. 3a and Fig. 3b show the mean of 2.85 in CWSSP CTF and 3.375 in SVCC CTF on question "I know the other CTF participants better after the CTF" in Table II. We consider these to be a strong number given the fact that few participants use a different strategy that targets the flags that are "easy to rack up points" and two participants feel negatively about being ignored when "others don't answer" them. The participants do know who is better in what tasks/categories after seeing the scoreboard with a mean of 3.38 in CWSSP CTF and 3.625 in SVCC CTF. At last, the participants are looking forward to working with the others with a mean of 4.69 in CWSSP CTF (this question only exist in CWSSP because of the after-CTF activity).

VII. Conclusion and Recommendations

We design and use a novel CTF incorporating real-time coordination and interaction to build fellowship and forming collaborative environment. This paper describes our design, build, and the execution (including beta-testing) for the CTF.



(a) Survey results for CWSSP.

(b) Survey results for SVCC.

Fig. 3: CTF survey results after all participants have completed the game. Confidence intervals are included at 95% confidence. Table II maps "Question Index" into their corresponding questions. Fig. 3b lacks index eight due to a different competition context.

Testing it in a university cybersecurity scholarship program and an academic conference, our results show that our design makes the participants better engaged when getting help from others (means of 3.77 and 4.125 out of 5) and the participants feel the game is immersive (3.92 and 4.125 out of 5). The Coordination flags encourage coordination and interaction.

We recommend the use of our cybersecurity CTF in an environment which can benefit from fellowship building or facilitate networking and relationship building. For example, the CTF execution for this research project involved CWSSP (followed by the networking sessions between the new cohort of scholarship recipients) and SVCC (at the first day of the conference). Such environments can also include an engineering or computer science course or technical training sessions. Our CTF source code as well as instructions for hosting the CTF (e.g., recommendations for hardware, OS, networking bandwidth) is on GitHub [15] and is available to anyone interested.

Acknowledgment

This material is based upon work supported by the National Science Foundation under Grant No. 1922410 and by Colorado State Bill 18-086.

References

[1] M. Beltran, M. Calvo, and S. Gonzalez, "Experiences Using Capture The Flag Competitions to Introduce Gamification in Undergraduate Computer Security Labs," in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*. Las Vegas, NV, USA: IEEE, Dec. 2018, pp. 574–579. [Online]. Available: https://ieeexplore.ieee.org/document/8947769/

[2] H. W. Prabawa, E. Junaeti, and Y. Permana, "Using Capture the Flag in Classroom: Game-based Implementation in Network Security Learning," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 2017, p. 6.

[3] R. Cherinka, "Using Cyber Competitions to Build a Cyber Security Talent Pipeline and Skilled Workforce," in *Intelligent Computing*, K. Arai, S. Kapoor, and R. Bhatia, Eds. Cham: Springer International Publishing, 2019, vol. 857, pp. 280–289, series Title: Advances in Intelligent Systems and Computing. [Online]. Available: http://link.springer.com/10.1007/978-3-030-01177-2_20

[4] M. Katsantonis, P. Fouliras, and I. Mavridis, "Conceptual analysis of cyber security education based on live competitions," in *2017 IEEE Global Engineering Education Conference (EDUCON)*. Athens, Greece: IEEE, Apr. 2017, pp. 771–779. [Online]. Available: http://ieeexplore.ieee.org/document/7942934/

[5] I. Cabrera, J. Villablon, and J. Chavez., "Blending communities and team-based learning in a programming course," *IEEE Transactions on Education*, vol. 60, no. 4, pp. 288–295, 2017.

[6] L. Battestilli, A. Awasthi, and Y. Cao, "Two-stage programming projects: Individual work followed by peer collaboration," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE)*, February 2018, pp. 479–484.

[7] K. Yoon and S.-Y. Chang, "Teaching team collaboration in cybersecurity: A case study from the transactive memory systems perspective," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, 2021, pp. 841–845.

[8] S. Kim, K. Song, B. Lockee, and J. Burton, *Gamification in Learning and Education*. Cham: Springer International Publishing, 2018. [Online]. Available: http://link.springer.com/10.1007/978-3-319-47283-6

[9] K. Leune and S. J. Petrilli, "Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education," in *Proceedings of the 18th Annual Conference on Information Technology Education*. Rochester New York USA: ACM, Sep. 2017, pp. 47–52. [Online]. Available: https://dl.acm.org/doi/10.1145/3125659.3125686

[10] C. Seemiller and J. Clayton, "Developing the Strengths of Generation Z College Students," *Journal of College and Character*, vol. 20, no. 3, pp. 268–275, Jul. 2019. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/2194587X.2019.1631187

[11] S. Krutkowski, "A strengths-based approach to widening participation students in higher education," *Reference Services Review*, vol. 45, no. 2, pp. 227–241, Jun. 2017. [Online]. Available: https://www.emerald.com/insight/content/doi/10.1108/RSR-10-2016-0070/full/html

[12] "NCL Individual Game Scouting Report." [Online]. Available: https://static1.squarespace.com/static/5e13a4b584a68c775e362068/t/5f3c5888533a540ce85da2c0/1597790354053/NEW+Spring+2020+Sample+Scouting+Report.pdf

[13] J. Mirkovic and P. A. H. Peterson, "Class Capture-the-Flag Exercises," in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. San Diego, CA: USENIX Association, Aug. 2014. [Online]. Available: https://www.usenix.org/conference/3gse14/summit-program/presentation/mirkovic

[14] S. Karagiannis, E. Maragkos-Belmpas, and E. Magkos, "An Analysis and Evaluation of Open Source Capture the Flag Platforms as Cybersecurity e-Learning Tools," in *Information Security Education. Information Security in Action*, L. Drevin, S. Von Solms, and M. Theocharidou, Eds. Cham: Springer International Publishing, 2020, vol. 579, pp. 61–77, series Title: IFIP Advances in Information and Communication Technology. [Online]. Available: https://link.springer.com/10.1007/978-3-030-59291-2_5

[15] "CTFd for Coordination and Interaction," Sep. 2021. [Online]. Available: https://github.com/simewu/CTFd