Capture the Flag Unplugged: An Offline Cyber Competition

Vitaly Ford, Ambareen Siraj, Ada Haynes, Eric Brown
Tennessee Tech University
110 University Dr.
Cookeville, TN
{vford, asiraj, ahaynes, elbrown}@tntech.edu

ABSTRACT
In order to meet the cybersecurity workforce demand, it is important to raise cybersecurity interest among the youth. Just like ACM programming competitions, Capture the Flag (CTF) competitions allow students to learn cybersecurity skills in a fun and engaging way. It is an effective platform to increase students' interest in cybersecurity and prepare them for defending against real cyber attackers. A typical CTF competition requires at least some basic technical security knowledge and months of diligent preparation. For this very reason, many computer science students do not feel qualified to participate in CTF competitions, and as a result, do not even try. To overcome this lack of confidence while at the same time raising awareness about the cybersecurity profession in a realistic fashion, we have developed the CTF Unplugged project, as inspired by the CS Unplugged project. The primary goal is to teach students with little or no technical knowledge about the different cybersecurity challenges that a cybersecurity professional must address and the problem-solving skills needed for a cybersecurity career, all without direct use of technology. The effectiveness of CTF unplugged project has been evaluated after exposing 36 high school students participating in the Tennessee Tech University GenCyber Camp to these activities this past summer. Students reported a significant gain in knowledge, confidence and comfort level after participation.

CCS Concepts
• **Applied computing→Education**

Keywords
Capture the Flag; unplugged; cybersecurity; education; competition.

1. INTRODUCTION
According to the recently published Cybersecurity National Action Plan, cybersecurity is "one of the most important challenges" that our nation faces right now [1]. Similar concerns are raised on a global spectrum. The worldwide shortage of cybersecurity professionals is projected to reach 1.5 million by 2019 [2].

SIGCSE '17, March 08 - 11, 2017, Seattle, WA, USA

ACM 978-1-4503-4698-6/17/03…$15.00
DOI: http://dx.doi.org/10.1145/3017680.3017783

In order to meet cybersecurity workforce demand, it is important to raise cybersecurity interest among the youth. In this regard the National Security Agency (NSA) and National Science Foundation (NSF) sponsors the Generation Cyber (GenCyber) [3] program, which is tailored towards K-12 students with a purpose of raising general awareness about the significance and influence of cybersecurity in this era of the Internet of Everything.

The Cybersecurity Education Research and Outreach Center (CEROC) [4] at Tennessee Tech University joined the GenCyber initiative by offering several student and teacher camps in cybersecurity awareness and education this year. One of these camps was a month-long student camp held June 2016. The camp was delivered as an integrated part of the Tennessee Governor's School for Emerging Technologies [5], which is designed to encourage high school students to get involved into science, technology, engineering and mathematics. Some of Tennessee's top high school students (50/50 female to male ratio) are selected for attending the Governor's School every year. This year, as an integral part of the Governor's School, a cybersecurity camp was designed to introduce participants to fundamental security concepts, problems, and solutions through a series of interactive lectures and hands-on learning lessons [4]. The camp delivered about 30 different activities including the NSA Day of Cyber [6, 7], social engineering exercises, Raspberry Pi-based cybersecurity exercises, team building exercises, and a novel CTF Unplugged competition.

Just like ACM programming competitions, CTF competitions allow students to learn cybersecurity skills in a fun and engaging way. The goal of a CTF is to capture "flags" that are hidden somewhere in a system; the participants must identify them via a variety of techniques. These flags can be anything from a string of letters to an image or data file [22]. CTF competitions are effective platforms to increase student interest in cybersecurity and prepare them for defending against real cyber attackers [19, 20, 21]. The game-like environment of CTF competitions engage students in solving complex cyber-challenges. With proper training and preparation, such competitions can produce high quality cybersecurity professionals [19, 23].

A typical CTF competition requires at least some basic technical security knowledge and months of diligent preparation. For this very reason, often Computer Science (CS) students shy away from participating in CTFs based upon the assumption that it will require skills that they might not possess [19]. Also, it has been observed that students with soft skills such as investigative interests, openness to experience, rational and decision-making tend to be successful in CTF and consequently, in their cybersecurity career [20]. CTFs do require some time and effort on behalf of the instructor to groom those traits in students and prepare them for successful CTF participation. One of the most important aspects of such preparations is to nurture self-efficacy in students [20]. A stereotypical notion about CTFs is that participating in CTFs require significant technical preparation and access to a

technological platform. To overcome this misconception, raise awareness about the cybersecurity profession in a realistic fashion and increase confidence in participating in CTF competitions, we have developed the CTF Unplugged project. This has been inspired by the CS Unplugged project [8].

The "CS unplugged" concept refers to explanation of CS concepts through activities that do not require use of a computer. This approach has been highly successful and has been used by many in the CS community over the past twenty years. CS Unplugged was developed with the goal of providing some CS exposure for middle/high school students, who otherwise knew little or nothing about career opportunities in the field. Similar in intent, the primary goal of the CTF Unplugged project is to teach students, with little or no technical knowledge, about different cybersecurity challenges a cybersecurity professional would likely face at work. Additionally, CTF Unplugged addresses the problem-solving skills needed for a cybersecurity career without the direct use of technology.

The primary objectives of the CTF Unplugged project are as follows:

1. Familiarize students with cybersecurity concepts and incite interest in cybersecurity.
2. Increase students' knowledge about CTF and general cybersecurity competitions.
3. Increase confidence among students about participating in real CTFs. Students boost their confidence when they realize that their critical thinking skills are as important as their technical skills.
4. Increase students' comfort level in participating in CTF and general cybersecurity competitions. Students become more comfortable in CTF participation when they obtain practical cybersecurity knowledge through training that can be beneficial in a real CTF.

We have designed CTF Unplugged such that it can be easily used as a supplemental, active-learning exercise in a typical high school STEM curriculum. Each CTF Unplugged activity lasts for approximately 2 hours and students fulfilling the tasks require no assistance from teachers.

This paper's structure is as follows. First, we introduce related work. We will then describe the different activities in the CTF Unplugged project, concluding with the evaluation results and directions of future work.

2. RELATED WORK

CTF competitions have been widely used for raising awareness and increasing interest in cybersecurity among college students as well as middle and high school students. Such digital competitions as PicoCTF [28] and Cyber Security Awareness Week (CSAW) [29] were specifically developed for high school students. PicoCTF focuses on offensive side of security, engaging students in a web-based game. On average, students spend twelve hours playing PicoCTF. CSAW competition is a student-run CTF for high school and college students. It focuses on covering various aspects of software and hardware security in a competition form. CSAW has recently become an international event, involving high school students from India and the United Arab Emirates.

In addition to the digital competitions described above, there are some cybersecurity board games that teach participants the basics of security. For instance, *[d0x3d!]* is designed to familiarize students with the network security terminology and basic concepts related to attack and defense mechanisms existing in a typical network [30]. *Control-Alt-Hack* [31] is also a board game that exposes players not only to basic cybersecurity principles and concepts, but also to cybersecurity careers and applications.

The project CyberCIEGE uses a video game to teach computer and network security concepts [32]. Players can spend virtual money to defend their network against cyberattacks, purchase and configure network equipment, and observe the consequences of their decisions. CySCom [33] utilizes comics to educates the youth about cybersecurity related concepts and safe online practices.

3. CTF UNPLUGGED

In-house CTF exercises require some level of technological infrastructure setup, which can be a barrier to some institutions depending upon resource availability. There are some online CTF competitions [24], but these CTFs usually assume some prior technical knowledge. Additionally, online CTFs are generally timed, causing CTF beginners to feel stressed under the time pressure. Some universities have developed their own CTF infrastructure and provide pre-CTF training/workshops to familiarize their students with the competition [22, 25]. With dedicated investments in time and resources to design the CTF architecture, it may not be a viable option for K-12 teachers who do not have those resources and expertise.

"Unplugged" exercises can enable similar skill-building activities without the need for a live computing. For students that may be intimidated by the technical nature of traditional CTF exercises, CTF Unplugged presents both technical and logical activities in a less "threatening", offline environment while still supporting critical thinking.

Students participating in CTF Unplugged exercises gain a greater appreciation for investigative critical thinking by learning how to break a complex problem into basic units of work. They experience iterative successes at each level that ultimately contribute to building their own confidence level to tackle larger problems in steps. Students begin to develop an appreciation for the logical aspect of problem-solving without going through traditional technical exercises.

All the exercises are built upon a story that serves as the context; the students become a part of the storyline from the very beginning until the end as they assist the investigators to capture an adversary. For Example:

Collaborative Enterprise for Replicable and Organized Countermeasures (CEROC) helps people to mitigate cyber-attacks. Recently, CEROC has been working closely with the FBI to track down a notorious hacker (pseudonym Hax0r) skilled in removing all traces after cyberattacks have been completed. Recently, Hax0r has become overconfident and has begun leaving clues for the FBI to demoralize the investigative team and demonstrate his/her superiority. After all, a hacker is only as important as his/her fame and legacy. The investigative team is hoping to capitalize on this lack of attention to detail. Your goal is to help the FBI close this case and track down Hax0r.

Each exercise is given as a "mission" to teach a particular set of skills by solving a specific problem with every mission having a set of tasks. As students complete those tasks, they capture "flags" that represent information sought. The following is an overview of the missions:

1. Mission 000: (Beginnings) Establishes the background information needed to complete the other missions.

2. Mission 001: (Reconnaissance Part 1) Allows students to conduct an investigation to gather intelligence.
3. Mission 010: (Forensics) Allows students to apply critical thinking to captured post-incident data and discover information about the incident and its source.
4. Mission 011: (Cryptography) Allows students to decode incomprehensible data into meaningful information.
5. Mission 100: (Reverse Engineering) Allows students to analyze code to determine its behavior.
6. Mission 101: (Steganography) Allows students to analyze image/data to uncover hidden information.
7. Mission 110: (Reconnaissance Part 2) Allows students to use data from standard infrastructure utilities to obtain information about a target.

There are many tools that are mentioned throughout CTF Unplugged, such as nmap [9], volatility [10], nikto [11], and Wireshark [12]. While the students never use the tools directly, they use printed data generated by the tools. The students are encouraged to search and learn about those tools on their own after the CTF Unplugged competition.

3.1 Background Information Exercise

The Background Information introduces students to the plot. The students learn that they have been hired by the FBI to investigate cyberattacks performed by an adversary. It has been shown that interesting stories presented side-by-side with exercises tend to draw students' interest and attract their attention [13].

After an introduction to different number formats, the initial tasks consist of understanding hexadecimal numbers and the ASCII table [14]. A sample of questions that the students answer is similar to the following:

1. Convert 105BF16 to decimal. What is the value?
2. What message is encoded in hex: 77 65 5F 6A 75 73 74 5F 68 65 78 61 6C 69 6E 5F 68 65 78 61 6C 69 6E?

To fulfill the assignments, the students have to understand the hexadecimal system and ASCII table.

3.2 Reconnaissance Part I Exercise

This exercise focuses on teaching students about intelligence gathering and its role in cybersecurity. The exercise uses a physical object to which the students can relate in order to personalize their experience. In particular, they must determine the name of a building on the school campus, given a picture of its back side. They must also find a flyer with an encrypted message, located somewhere on the second floor of the student hall. The activity is particularly engaging for the students because it uses relatable places and characters.

In the second part of the activity, the students learn about IP addresses, ports, and operating systems. They are provided with the output from an nmap [9] scan of the computer that the adversary used on campus. Analyzing the scan history, they must answer questions such as:

1. What is the IP address of the machine that Hax0r's used?
2. What is the service's version on port 21?
3. What operating system is installed on this system?

3.3 Forensics Exercise

The students analyze printed image metadata and are tasked to identify the exact location of the adversary based upon the analysis of the image. They learn about different pieces of information that can be extracted from the image data.

Additionally, students analyze Wireshark [12] logs, provided to them in clear text, and answer several questions like the following:

1. What is the username that the attacker used?
2. What is the password?
3. What file was uploaded on the victim's machine?
4. What is the IP address of the attacker?

The students conduct a thorough investigation of the Wireshark logs in order to understand the information flow and search for keywords to develop their answers.

3.4 Cryptography Exercise

Students begin with simple ASCII encoding techniques. Next, they are introduced to basic ciphers such as Caesar [15] and Rail Fence [16]. Students work with alphabet wheels like the one shown in Figure 2 to explore how letter shifting works in the Caesar cipher. They are also exposed to Morse code and how to decipher it.

It should be noted that while the students are shown how the ciphers work, they themselves must figure out how to decipher the cipher texts on paper providing an opportunity for students to work closely with one another in solving the challenges.

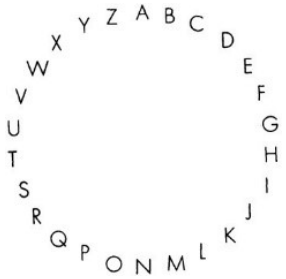

Figure 2. English Alphabet.

Examples of the questions asked are:

1. What is the original message that is enciphered as "PREBAODRAGASWIBKNDSSI"?
2. What is the message "--- ..- .-. -. . -..- - - .- .-. --. . - .. ... -... .- -. -.- --- ..-. .- -- . .-. .. -.-. .-"?

To find flags in this category, the students must apply appropriate decryption techniques. For example, the first string is enciphered using the Rail Fence cipher with a key of 4. The second string represents a Morse Code, and the students are given a code table to find the correct answer.

3.5 Reverse Engineering Exercise

In this exercise, the students are provided with printouts of two source codes of a program which generates passwords for the adversary. The code is heavily commented to explain each line. The students must determine how the code logic executes and compute the passwords based on simple math and ASCII table.

3.6 Steganography Exercise

The steganography exercise teaches students about the art of hiding messages inside of other objects. While without access to technology it is not possible to demonstrate the concept traditionally, we found an alternative way to highlight the idea by logically hiding messages inside of other objects. An example would be the image below (Figure 3) that hides the word "Root".

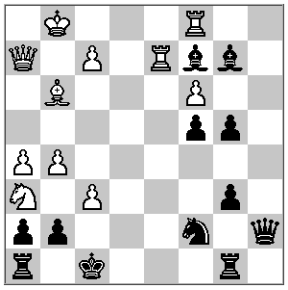

Figure 3. Chessboard assignment.

Another example is displayed on Figure 4. It apparently hides the name of an offshore bank that the adversary uses to keep the stolen money. To understand the actual text, the image has to be viewed through a mirror.

Figure 4. Mirrored text.

3.7 Reconnaissance Part II Web Exercise

The exercise uses a webpage's source code analysis, a web scanning tool output, and a WHOIS [17] service report. The web reconnaissance teaches students that both observation and attention to detail are important. They learn that there are simple yet powerful tools to discover essential information about web sites.

4. CTF UNPLUGGED EVALUATION

The effectiveness of CTF Unplugged project has been evaluated after exposing 36 high school students to these activities during the GenCyber student camp in summer 2016. The students were divided into twelve teams consisting of three persons each. All the teams completed all tasks in the exercises successfully in time. The team which finished first received an award.

For the evaluation, students were asked about their knowledge, comfort level and confidence about CTF, and cybersecurity competitions in general, prior to and immediately following participation in the CTF Unplugged exercises.

These questions were asked using a 5-point Likert Scale with 1 representing Not Knowledgeable and 5 representing Very Knowledgeable. Students' average response for Prior Knowledge of Cybersecurity Competition was 1.5 and the average response after participating in CTF Unplugged was 3.4. The average response for Prior Knowledge of Capture the Flag Competition was 1.7 and the average response for Prior Knowledge of Capture the Flag Competition after participating was 3.9 (Figures 5 and 6).

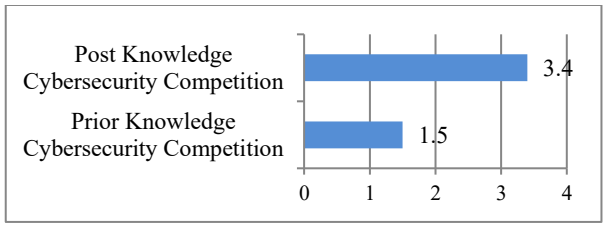

Figure 5. Knowledge of cybersecurity competition.

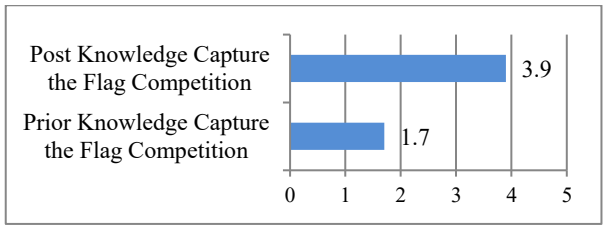

Figure 6. Knowledge of Capture the Flag competitions.

Regarding their comfort level prior to participating in CTF Unplugged and after participating in CTF Unplugged for both cybersecurity competitions and the Capture the Flag competition, the question was asked on a 6-point Likert Scale with 1 representing Very Uncomfortable and 6 representing Very Comfortable. The average response for comfort participating in a cybersecurity competition prior the CTF Unplugged was 3.5. The average response for comfort participating in a cybersecurity competition after participating the CTF Unplugged event was 4.5. Likewise, students made gains in comfort participating in a Capture the Flag Competition. Their average comfort level prior to participating in the CTF Unplugged was 3.5 while their comfort after participating was 4.8 (Figures 7 and 8).

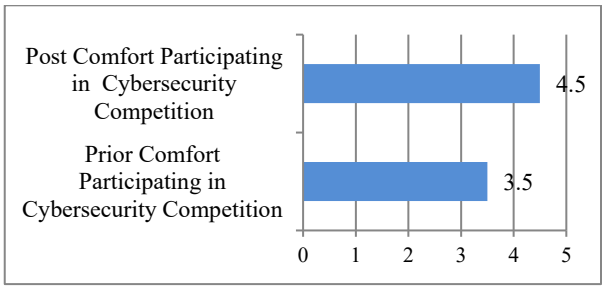

Figure 7. Comfort participating in cybersecurity competitions.

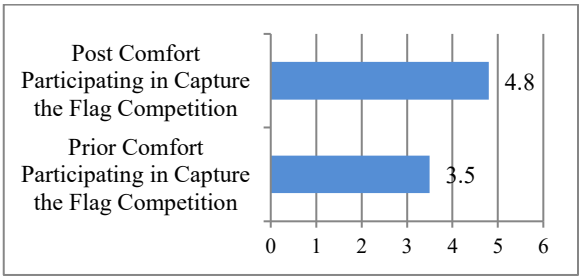

Figure 8. Comfort participating in Capture the Flag competitions.

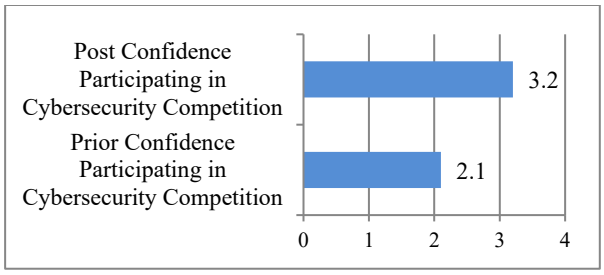

Figure 9. Confidence participating in cybersecurity competitions.

Confidence was measured on a 5-point Likert Scale with one being Not Confident to five being Very Confident. On each of these measures, students gained over one point on the five-point scale. Confidence in Participating in Cybersecurity Competition increased from 2.1 to 3.2. Confidence in Participating in Capture the Flag Competition increased from 2.2 to 3.5 (Figures 9 and 10).

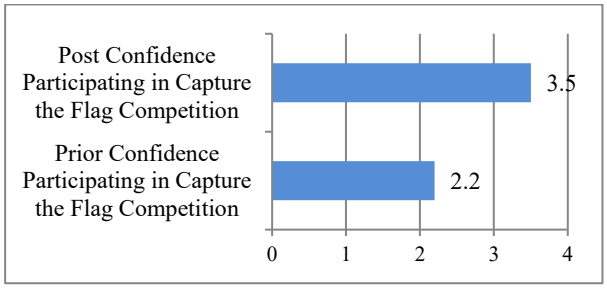

Figure 10. Confidence participating in Capture the Flag competitions.

Participants rated their knowledge level in six areas both before and after CTF Unplugged. Knowledge level was measured on a 5-point Likert Scale with 1 denoting Not Knowledgeable and 5 denoting Very Knowledgeable. These areas are Reconnaissance, Cryptography, Steganography, Cyber Forensics, Network Traffic Analysis, and Reverse Engineering. In each of these knowledge areas, students reported gains by participating in the program. For Reconnaissance the average knowledge level prior to CTF Unplugged was 1.9. The average post score for Reconnaissance was 3.3. Prior to the CTF Unplugged program the average score for Cryptography was 2.3 with a post score of 3.5. The average post score for Steganography was 1.5 with a post score of 2.9. The lowest starting average was for Cyber Forensics with a score of 1.4. The post score for Cyber Forensics was 3.0. Network Trafficking began at 1.7 and ended at 3.0. Finally, Reverse Engineering began at 2.3 and ended at 3.0 (Figures 11-15).

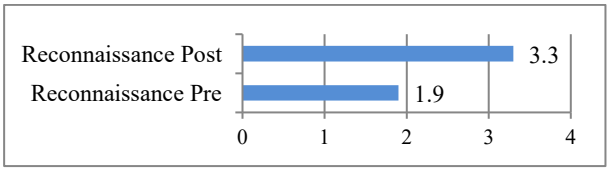

Figure 11. Reconnaissance pre and post.

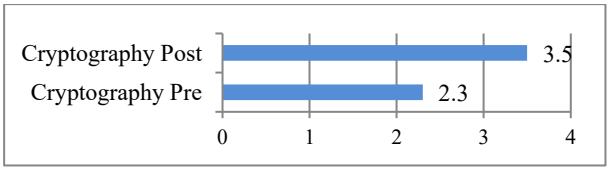

Figure 12. Cryptography pre and post.

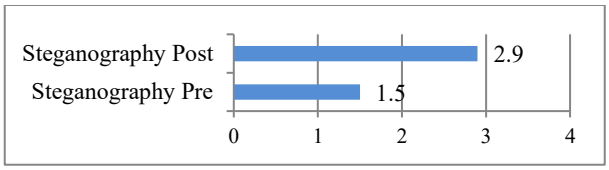

Figure 13. Steganography pre and post.

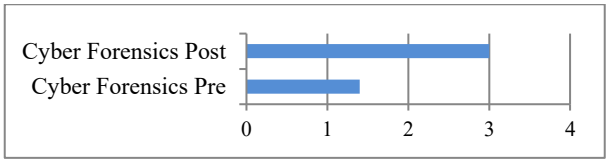

Figure 14. Cyber forensics pre and post.

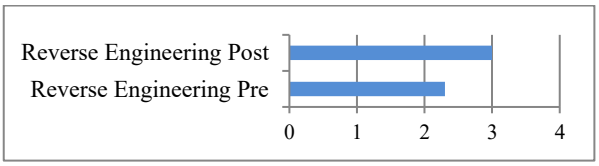

Figure 15. Reverse engineering pre and post.

Overall, after participating in CTF Unplugged, 91.7% of the students reported that they better understand how to investigate cyber incidents. Similarly, 97.2% reported that they better understand how Capture the Flag competitions work.

4.1 Suggestions for Improvement

Most of the recommendations for improvement centered around logistics of how the CTF games were executed or about the materials provided. Some students remarked "make it so we all have to start in the same place and follow the same order in the game structure"; "each person has their own copy, it was difficult to work on multiple tasks at once with only one copy". Others suggested that the copies be in color or be accompanied with more explanation of the concepts. Students recommended that the teams be made up of two individuals instead of three. Several students requested more time. These are all minor recommendations that can easily be considered to improve the program in the future.

5. CONCLUSION

The CTF Unplugged project has been demonstrated as a potential tool in educating high school students about the cybersecurity field in general. The CTF Unplugged activities immerse students into realistic scenarios walking them through different cybersecurity career tracks. By completing the exercises, students are exposed to simulated challenges and skills required for cybersecurity professionals. For example, the cyber forensics exercise familiarizes students with different challenges that forensics professionals may face and develop approaches to solve them. The reverse engineering activity introduces students to the analytical mindset that reverse engineers need in their job. Additional activities can be easily incorporated.

The CTF Unplugged project contributes to the K-12 cybersecurity/CS education as follows.

1. Students do not need access to a technology platform to participate.
2. Students do not require any prior knowledge or skill in cybersecurity to participate.
3. To organize CTF Unplugged in their high school classrooms, teachers need not have any prior cybersecurity experience or access to technical resources.

4. Students with different background and skills can collaboratively work solving challenges together. The team which finished first consisted of two girls and a boy who equally contributed to completing the exercises, nor did they have any prior interest or knowledge in cybersecurity.

While the CTF Unplugged project does not require the usage of any technology for playing the game, we wanted to make it feel like an actual CTF. In this regard, for score reporting purposes only, a free platform offered by Facebook CTF (FCTF) [18] was used that allows real-time visualization of the "flags" captured by the students as they submit their answers to the challenges. Remarks received from the students confirm that this arrangement allowed the students to "feel" like they were participating in real technical CTF, and it contributed increasing their motivation and confidence. If teachers want to use the FCTF with CTF Unplugged, it can be used as a virtual instance, allowing the teachers to access the web based platform within several minutes of a simple setup process.

The CTF Unplugged project builds a bridge for students with no cybersecurity knowledge and no access to technological resources to reach an understanding of CTF competitions through the use of offline paper-based activities. All the materials developed for CTF Unplugged are free to use and distribute [27]. Our current goal is to disseminate CTF Unplugged so that it could be used in GenCyber Student camps nationwide; also, we plan to build a community for improving and expanding the CTF Unplugged activities. We believe that crowdsourcing can drastically enhance both quality and quantity of the exercises as well as contribute to the growing interest in K-12 cybersecurity education.

6. ACKNOWLEDGMENTS

This research has been supported by the NSF Award# 1565562 and Office of Research, Tennessee Tech. We would like to thank the TNTech Governor's School and its director, Dr. Chris Wilson, for allowing us to embed CTF Unplugged exercises into the agenda.

7. REFERENCES

[1] The White House, "Fact Sheet: National Cybersecurity Action Plan". [Online]. Available: https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
[2] Cybersecurity Ventures, "Job Report". [Online]. Available: http://cybersecurityventures.com/
[3] GenCyber, "Summer Cybersecurity Camp Program". [Online]. Available: https://www.gen-cyber.com/
[4] Cybersecurity Education Research and Outreach Center (CEROC), Tennessee Tech University. [Online]. Available: https://www.tntech.edu/ceroc
[5] Tennessee Tech University, Governor's. [Online]. Available: https://www.tntech.edu/engineering/academic-programs/governors-school
[6] NSA Day of Cyber at Tennessee Tech University. [Online]. Available: http://dayofcyber.org/us/tennessee-tech-adds-nsa-day-of-cyber-experience/
[7] NSA Day of Cyber. [Online]. Available: http://www.dayofcyber.org
[8] T. Bell, et al. "Computer science unplugged: School students doing real computing without computers." Journal of Applied Computing and Info. Tech. 13.1 (2009): 20-29.
[9] Network mapper, free security scanner. [Online]. Available: https://nmap.org
[10] Volatility: memory forensics. [Online]. Available: http://www.volatilityfoundation.org
[11] Nikto: web scanner. [Online]. Available: https://cirt.net/nikto2
[12] Wireshark: network protocol analyzer. [Online]. Available: http://www/wireshark.org
[13] Marzano, Robert J., and Debra J. Pickering. *The highly engaged classroom*. Solution Tree Press, 2013.
[14] ASCII table. [Online]. Available: http://www.asciitable.com
[15] Dcode project, "Caesar cipher". [Online]. Available: http://www.dcode.fr/caesar-cipher
[16] S. Knight, "Rail Fence Cipher". [Online]. Available: http://www.cs.trincoll.edu/~crypto/historical/railfence.html
[17] Domain tools, "WHOIS service". [Online]. Available: http://whois.domaintools.com/
[18] Facebook, "Capture the Flag platform". [Online]. Available: https://github.com/facebook/fbctf
[19] R. S. Cheung, et al., "Effectiveness of cybersecurity competitions," in *Proceedings of the International Conference on Security and Management (SAM)*, the World Congress in Computer Science, Computer Engineering and Applied Computing, 2012.
[20] C. Wee and M. Bashir, "Understanding the Personality Characteristics of Cybersecurity Competition Participants to Improve the Effectiveness of Competitions as Recruitment Tools," Advances in Human Factors in Cybersecurity. Springer Publishing, pp. 111-121, 2016.
[21] R. S. Cheung, J. P. Cohen, H. Z. Lo, and F. Elia, "Challenge based learning in cybersecurity education," in *Proceedings of the International Conference on Security & Management*, vol. 1. Las Vegas, Nevada, USA: SAM 2011, Jul. 2011.
[22] J. Werther, M. Zhivich, T. Leek, and N. Zeldovich, "Experiences in cybersecurity education: The MIT Lincoln laboratory capture-the-flag exercise," Cybersecurity Experimentation and Test, vol. 8, 2011.
[23] C. Eagle and J. L. Clark, "Capture-the-flag: Learning computer security under fire," Naval Postgraduate School, Monterey CA, 2004.
[24] Capture the Flag competitions. [Online]. Available: https://ctftime.org/
[25] G. Vigna, et al., "Ten years of iCTF: The good, the bad, and the ugly," USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE). 2014.
[26] D. R. Krathwohl, "A revision of Bloom's taxonomy: An overview," *Theory into practice* 41.4 (2002): 212-218.
[27] CTF Unplugged. [Online]. Available: http://goo.gl/S4UEkO
[28] P. Chapman, J. Burket, and D. Brumley, "PicoCTF: A game-based computer security competition for high school students," USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), 2014.
[29] Cyber Security Awareness Week (CSAW). [Online]. Available: https://csaw.engineering.nyu.edu/about
[30] A Network Security Game d0x3d!. [Online]. Available: http://d0x3d.com/d0x3d/welcome.html
[31] T. Denning et al., "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security*, pp. 915-928, ACM.
[32] M. F. Thompson and C. E. Irvine, "Active Learning with the CyberCIEGE Video Game," USENIC Workshop on CyberSecurity Experimentation and Test, 2011.
[33] B. Ledbetter, et al., "CySCom: Cybersecurity COMics," in *Proceedings of the IEEE Intelligence and Security Informatics Conference (ISI)*, 2016.