ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #27796

Diversifying Pathways in Cybersecurity through the Design of Holistic Competitions

Dr. John Y Oliver, California Polytechnic State University, San Luis Obispo

Dr. Oliver is an assistant professor of Electrical Engineering and Computer Engineering and the director of Computer Engineering at Cal Poly, San Luis Obispo. His field of expertise is in computer architecture and system performance analysis with a growing interest in cybersecurity. His teaching activities focus on embedded systems and digital circuit design.

Cassidy Elwell, Cal Poly, San Luis Obispo

Diversifying Pathways in Cybersecurity through the Design of Holistic Competitions

Abstract

Cybersecurity competitions are touted as a good method for getting high school students interested in career paths in cybersecurity fields. From observations of high school cybersecurity competitions, we find that typical high school cybersecurity competitions focus narrowly on computer-technical competencies. A byproduct of these competitions is to create an intimidating atmosphere that rewards young adults who are already proficient in computer IT activities, but a discouraging environment to students who may have burgeoning interests in cybersecurity. Additionally, the skill set needed for cybersecurity professionals is much broader than purely computer-technical skills and include competencies like teamwork, communications skills and critical thinking, none of which are emphasized in typical high school cybersecurity competitions.

In this paper, we present a high school cybersecurity competition event called the Digital Forensics Challenge (DFC). The DFC is designed to reward cybersecurity competition teams that have a wider range of competencies than typical cybersecurity competitions and be more accepting of students who may not be singularly focused on the technical aspects of cybersecurity. We describe the elements that were added to emphasize critical thinking, global thinking, teamwork and communications skills. We find that by adding non-technical competencies to the DFC, competitors find that their holistic set of skills are more valued while at the same time competitors also claim that the amount of technical content of the DFC is greater than other cybersecurity competitions.

1 Introduction

There is a critical shortage of professionals in cybersecurity. As with the rest of the field of computing, this need is exacerbated by the lack of gender and racial diversity in the cybersecurity workforce. This problem has been recognized by NIST's National Inititative for Cybersecurity Education (NICE) working group, which has an objective of increasing the participation by veterans, minorities, and women in cybersecurity[1].

Cybersecurity competitions have been promoted to increase participation in cybersecurity-related fields among high school students. Typical secondary school-level cybersecurity competitions, such as the Air Forces CyberPatriot, currently focus on a very narrow set of computer-technical

related activities. These competitions require an array of preparation and coaching about the nuances of operating systems and computer networks. For instance, CyberPatriot teams are tasked with closing exploits on virtual machine snapshots of a pair of operating systems (OS), often Windows or Linux operating systems. Activities include adjusting user permissions, closing unnecessarily open ports, and modifying other operating system settings to close exploits. Leading up to the competition is where most of the learning happens for the competitors. Good teams have a strong coach with an understanding of OS or network configurations and the teams drill on closing a set of exploits as quickly as possible. During typical competitions, the best teams rarely need to communicate between their members. Rather, the members are running down checklists of settings to check in the OS and making necessary adjustments along the way.

While these competitions are popular (there are California high schools that have 250 students in their high school cybersecurity clubs), these competitions can be an intimidating environment for high school students new to cybersecurity, especially for those students who belong to a minority group[2], and only include students with a fairly narrow set of computer security skills. It is the hypothesis of this paper that if we want to increase the diversity of the cybersecurity workforce through cybersecurity competitions, it would be best to design entry-level competitions that have roles for students with a wider set of interests and to provide multiple avenues towards success[3].

Indeed, the field of cybersecurity draws upon a wide range of competencies. There are roles in cybersecurity for people with great communication skills, such as ethicists, lawyers, and compliance officers. Great critical thinking and teamwork skills are sorely needed. Also, the social engineering aspects of cybersecurity may be the largest challenge faced in the realm of cybersecurity. By designing cybersecurity competitions at the secondary school-level that focus only on great computer security skills, we may be filtering out many qualified individuals from the field of cybersecurity at the onset.

The rest of this paper is organized as follows. First, we will share observations of cybersecurity competitions held in California for high school students. We next will describe a cybersecurity competition that was designed for high school students that addresses many of the shortcomings from our observations. Then, we will review survey results from a competition of 120 competitors. We conclude that by designing cybersecurity competitions for high school students that have roles for a wide array of students, we can not only create cybersecurity competitions that are technically deep, but also have places for students with diverse interests and skill sets.

2 Observations from high school cybersecurity competitions

Prior to the design of the California Cyber Innovation Challenge (CCIC), members from the CCTC observed and/or designed six high school cybersecurity competitions in the state of California. We are very impressed with cybersecurity competitions and the competitors appear to enjoy these events while learning many cybersecurity fundamentals. At these competitions, we have made several observations that are also supported by others who have designed and/or observed prior high school cybersecurity competitions[4],[5],[6],[7]. The following observations are generalizations of the competitions observed. We recognize that there is high variability in the

objectives and outcomes of competitions, but the observations apply nearly universally to all high school cybersecurity competitions that we attended.

Observation 1: Many competitions are arranged where students are organized into teams (typically 3-6 students) and teamwork is highly encouraged. However, we observed that many teams are really co-working by contributing to a team score rather than exhibiting high-levels of teamwork. As a result, many competitions observed do not show tell-tale signs of collaboration, such as having animated discussions or students working on the same problem at the same time.

Observation 2: Student competitors learn much in preparation for the competition about the use and design of computer-related technologies as well as computer system vulnerabilities and threat vectors. However, students often are not applying critical thinking skills during the competition. At some competitions observed, students at the competition are either completing a prescribed checklist of exploits to close; or even more simply, using the internet to search for answers. We classify these competitions on the static-side of the spectrum.

Some competitions include more dynamic components of the competition, for example active adversarial components, such as a "red team". We believe that these dynamic components result in higher levels of critical thinking in cybersecurity competitions. These dynamic components require far more critical thinking skills, but can be very difficult for teams without a deep practice of computer security.

Observation 3: Some competitors are very advanced in their knowledge of cybersecurity, even at the high school level. This results in some very lopsided competitions. We view this as a threat to novice players. Our conclusion is that the disparity of skills in an unbalanced game environment creates a hostile, inaccessible environment for students with budding interest in cybersecurity who have limited computer-technical skills.

Observation 4: Many competitions do not emphasize the tangential competencies of cybersecurity careers such as ethical, legal, and privacy concerns inherent to cybersecurity. Additionally, most competitions also don not explore the need for demonstrating good communication skills as part of the competition. Ethical, legal, and communication skills are necessary for any proficient cybersecurity professional. One could argue that one of the biggest challenges of cybersecurity is to find a way to effectively communicate the threats of cybersecurity to an increasingly cyber-based population who do not possess a good command of computer systems.

Observation 5: Most competitions involve a room full of competitors sitting around tables working constantly on computers for three-hour blocks at a time with little collaboration. In addition, parents, mentors, and coaches must leave the facility to ensure fairness among teams and therefore are unable to observe the competition themselves.

Observation 6: Competitors are ranked by an automated scoring system in real time and sole success being recognized to the teams or individuals who have already mastered such technical skill sets. Most competitions were found to be technical-only resulting in critical thinking, intuitiveness, communication, and presentation skills not being considered criteria in scoring. Additionally, new teams and individuals interested in improving their computer technical skills

are often intimidated and discouraged due to these criteria.

When considering the problem of diversity in cybersecurity competitions, we argue that stakeholders should think more completely about the students who do not compete in competitions and how to attract those students. Is the atmosphere of cybersecurity competitions at the high school level welcoming to students with a variety of interests beyond computer skills? Is the environment welcoming to students who are new to cybersecurity?

Furthermore, we should also recognize that many of the competitors of cybersecurity competitions will not pursue cybersecurity in post-secondary school. Therefore, understanding the characteristics of these students would also be helpful in building a pipeline to cybersecurity careers from K-12 schools.

We believe that if cybersecurity competitions, especially at the high school level, could address these observations, not only would the students who are currently "good cybersecurity competitors" benefit through the cultivation of a broader set of skills, but the competitions would open new pathways for inclusion of a more diverse set of students.

3 Creation of a more diverse cybersecurity competition

Cybersecurity competitions for high school students cater to those students who are already very interested in learning more about computers. To engage a broader set of youth in cybersecurity in a welcoming and holistic manner, we designed cybersecurity competitions with elements that would be attractive to students who have interests beyond computing. We want to design competitions that are attractive to "computer geeks," "theater geeks," and all of the students in between.

The California Cyber Innovation Challenge (CCIC) can be thought of as the state-level high school championships for high school cybersecurity competitions and is sponsored by the State of California's governor's office. For the last two years, we have designed this competition with the express goal of being a cybersecurity competition that requires a broad set of competencies to score well and which rewards competition teams for having a diverse skill set in addition to strong computer-technical skills.

For both the 2017 and 2018 CCIC competitions, we designed computer forensics challenges we call the Digital Forensics Challenge (DFC). Competition teams each made of six students were tasked to solve a crime that was situated in an immersive environment using a complex digital and physical evidence trail. In both competitions, student teams had to assemble a timeline of evidence and then present their findings to a panel of judges. This competition could be considered similar to a computer-security game of Clue with a presentation at the end supporting the teams' findings. During the competition, team members were often divvying up the work between the team members, as multiple digital and physical pieces of evidence were provided. Once teams had a body of evidence to work from, many teams chose to assign select team members to begin analyzing the forensics data and synthesizing a timeline of events. Throughout the analysis process, we often observed team members arguing over the relative importance of the

evidence found, as it pertained to the case, and crafting their presentation for the judging panel.

The judging panel for each team consisted of three cybersecurity or law enforcement professionals. Teams had to craft an eighteen-minute presentation describing the who, what, where, when, why, how(s) of the crime as well as discussing privacy or moral issues. Judges were able to then ask the teams questions for two minutes.

For the 2017 competition, each of the sixteen teams were given a vehicle to search and seize physical items and digital devices. A laptop was placed in an obvious location, as well as other digital devices such as an external hard drive, Ring doorbell, and Amazon Echo device. Other digital devices, such as an SD card, were placed in much more difficult places to find, but often were hinted at by the digital evidence trail, such as Windows device connection logs. Digital evidence was often encrypted and/or partially deleted or obfuscated through file renaming. Other pieces of physical evidence were placed in the vehicles as well, including paper notes with passwords scribbled on them and paper invoices. The crime for the 2017 competition was about a former disgruntled employee who worked at a water treatment plant and desiring revenge on his former boss. This employee was acting in conjunction with a second criminal who was not in the center of the evidence trail, but had more nefarious intents.

The 2018 competition built off the 2017 competition and had students not only perform forensics on a Windows OS, but also an Android mobile device. The twenty competing teams were to gather and organize evidence from both an apartment and medical office, instead of a vehicle. Similar to in 2017, digital and physical evidence was hidden in their designated locations to a varying degree. However, additional digital hurdles were placed on the digital evidence, such as stronger encryption. We were also able to use GPS location information from the Android device to hide further physical evidence at nearby locations. The scenario for the 2018 competition put a ransomware attack at the forefront of the crime. Teams were told that the ransomware attack could be diffused by entering a series of six passwords into the competition website, which also acted as a live scoring engine that was displayed prominently on the competition floor. The passwords could be attained through computer forensics on the laptop, Android device, SD card, and external hard drive and through physical puzzles and ciphers left at the different search locations. Some of the puzzles and evidence in the 2018 competition required not only critical thinking skills, but familiarity with Spanish language and also relied on team's ability to read and synthesize Chumash native American poems. The twist in the 2018 scenario was that the ransomware was designed to be a decoy from the real crime of a data theft. Figures 1 and 2 show competitors from the CCIC 2019 performing a search of the medical office and performing computer forensics on the evidence they found as part of the search.

Both of the competitions were designed with the initial introduction of the crime as a decoy from the actual crime. This was done purposefully because, from our observation, well-practiced cybersecurity teams often chase the next computer-technical task rather than using their critical-thinking skills when in competition. This rabbit hole was particularly effective in 2018 as the most experienced teams did solve more of the ransomware passwords, but many missed that the ransomware was a diversion.

To recap, the ways in which our competition emphasized the use of a broader skill set than typical

Figure 1: Competitors searching the medical office space for the CCIC 2018

Figure 2: CCIC 2018 competitors performing computer forensics

high school cybersecurity competitions included: diversionary plot lines requiring global thinking, intertwining of digital and physical evidence, high levels of teamwork, ability to work with cultural and foreign language artifacts, presentation skills, and ability to argue moral and ethical issues all in addition to computer forensics and security skills.

4 Development of the Digital Forensics Challenge (DFC)

There were a number of stages necessary to successfully create a DFC for the CCIC to ensure the inclusion of both technical and soft skills and a realistic digital forensics investigative scenario.

4.1 Stage 1: Create forensics training materials

With the goal of the competition to attract a broader representation of participants and emphasize investigative skills, critical thinking, and teamwork, it is crucial for participants to prepare. Therefore, the materials provided should assist the students in establishing the proper skill sets in conjunction with a step-by-step guide of how to use particular tools to accomplish forensics analysis.

In the materials created for 2017, training material was obtained from the California Department of Justice based on a specific vendor's tools. This training was refactored to use open-source and freeware tools to ensure accessibility for all high school students. This training walked students through a Windows-based digital forensics investigation, and provided three additional training scenarios, each with a decreasing amount of scaffolding for self-guided education. Additionally, training videos were also created to assist in the dissemination of Windows-based digital forensics training.

For the materials in 2018, the Windows Forensics training from 2017 was accompanied by Android Forensics materials. In addition to training students on the use of the industry-standard tool Cellebrite, the materials explained step by step how to properly secure a device, extract the data, and then find hidden artifacts. The students were provided a Cellebrite UFED Reader allowing them to view and tag all of the extracted evidence through an Android-based digital forensics investigation while completing the training. This training is now freely available at : http://redactedForBlindReview.

4.2 Stage 2: Establish a realistic, engaging scenario

For students to successfully build technical and soft skills significant to a cyber professional and to supply excitement and interest to the field, the scenario behind the evidence must be concrete and realistic. A sense of drama and importance was deemed necessary to captivate the competitors.

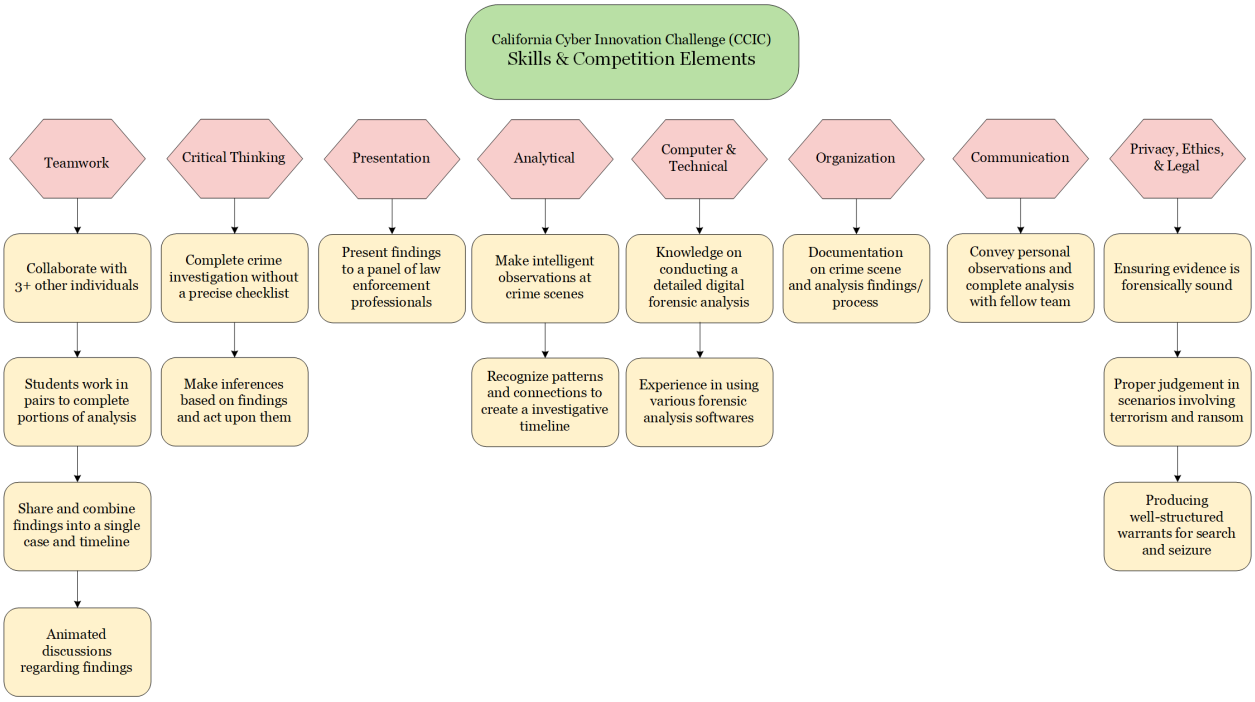

Figure 3: CCIC DFC Learning Skills Mapped to Corresponding Competition Elements

For the 2017 competition, the crime investigated by the competitors was a cyber threat against a municipal water supply. The crime included multiple criminals, with disparate motives. A non-linear evidence path was created where investigators (student teams) were led to believe that the initial suspect was the main criminal, but the mastermind of the crime was actually an accomplice whose digital evidence trail was more closely guarded. In the creation of this scenario, two criminal forensics examiners were consulted to ensure realism in the challenge.

For the 2018 competition, the students investigated a ransomware attack being utilized as a decoy for a data theft. The crime involved a variety of suspects and a extremely detailed evidence map incorporating pieces of evidence in a timeline amongst four digital devices, five puzzles, and a myriad of physical evidence such as bills and magazine articles. Investigators (student teams) were under the impression that the ransomware attack was committed by a single individual until discovering a series of letters written between the suspect and his accomplice after visiting the nearby location specified in the GPS of a photo.

The skills needed to perform the analysis is shown in Fig.3. Whereas typical cybersecurity competitions focus mostly on the computer technical skils, with some teamwork and critical thinking, the CCIC is designed with a much wider set of skills to be demonstrated.

4.3 Stage 3: Timeline and evidence creation

The digital evidence trail is time consuming to create as each activity on a digital system is logged in real-time. First, an evidence trail for our crime had to be planned out. This included emails,

Skype calls, web browsing, document creation, photos, and other such common activities on a computer. Some of these pieces of digital evidence were either hidden (placed on different hard drive partitions for instance) or encrypted (as a password protected .zip files). Then, to create this digital evidence trail, the authors had to use the digital device multiple times per day for planting this evidence trail along with other "non-evidence" activities, such as sending emails to friends and family members or browsing the web. This process was implemented over a three week period. It would ensure a correct chronology of evidence events, as well as make the search realistic.

In 2017, five digital device evidence pieces were created in our implementation: a laptop, an external hard drive, an SD card, an Amazon Echo device, and a Ring doorbell. In 2018, four digital device evidence pieces were created in our implementation: a laptop, an Android mobile phone, an external hard drive, and an SD card. The biggest challenge found in the creation of the 2018 competition was the detailed timeline required to ensure the evidence pieces incorporated across the laptop and mobile phone devices made logical sense and correctly portrayed the scenario.

4.4 Stage 4: Hold dry-runs of the training and elements of the DFC

Following the completion of the evidence creation, the authors host dry-runs with local high school students who were not participants in the CCIC. These dry-runs used the forensics images developed for the CCIC to identify any issues with realism and difficulty, receive feedback from students on the challenge set up and scenario, and estimate the amount of time taken for student teams to successfully analyze a majority of the evidence. Based on observations made and feedback received from these dry-runs, the competition evidence may need to be adjusted and the time constraints of the competition may need to be modified. Fortunately, we did not have to make any changes to the digital evidence trail as this process would have necessitated the complete rebuild of the digital evidence. The only changes made were in some of the physical evidence that was part of the competition and the training materials provided.

4.5 Stage 5: Finalize and 'build' scenario setting

To continue with adding realism and excitement to the competition, teams were given a scenario setting to search and seize evidence from. The digital props placed in the crime scene(s) need not be in working order (for more details, see Stage 6 below).

In 2017, the digital devices and physical items were then placed in a vehicle. We borrowed 16 vehicles from a local car dealership for the event. These devices were placed with "car garbage" purchased from our local Goodwill. The laptop was kept in plain sight on the passenger-side seat, while the rest of the digital devices were hidden in the vehicle.

In 2018, the digital devices and physical elements were placed in an apartment and medical office. We rented 10 barrack apartment rooms from across the street to be rotated for use by the 20 competing teams. We also built 10 medical offices in the competition space that was time-shared

by the competition teams. A laptop and mobile phone devices were in plain sight per their common normal use, however, the external hard drive and SD card were strategically hidden. The physical items complementing the digital devices included usual garbage, office and medical supplies, and magazines and books. Finally, the elements for each of the five ransomware password puzzles were hidden in a variety of locations throughout the two destinations.

4.6 Stage 6: Deploy the scenario on competition day

Following the authors' announcement of the premise of student teams' need to act as digital forensics investigators, each team is given a box containing background information about the suspect, latex gloves, notepads, and flashlights to perform their search. Also, included in the box was a USB drive with some pre-recorded (mp3) interviews with the initial suspects in the case. The teams were each then provided their location(s) to search and seize for both digital and physical evidence. Upon discovering a digital device, student teams were instructed to go to the 'forensics technician' table to exchange their digital device for a USB drive containing a forensics image of that digital device. This was done to avoid having competitors create their own forensics images, as this is a time consuming process that could take several hours or even days.

The students then would perform digital forensics analysis with the teams often having their members work in parallel: one student would look at the email evidence, while another would recover deleted files, while another would look at Skype chat logs. Student teams would put the evidence they found on a timeline and then craft an argument of who committed the crime, what their motivation was, when and how the crime was committed, and what should be done to remediate. In the 2018 scenario, teams were also asked to address any ethical or moral issues related to the crime(s) committed. This argument was then presented by each team to a panel of judges. The judges ranged from CIA and FBI agents to the county's assistant district attorney and other forensics examiners. These judging panels were given a 30-minute training on the case and the pieces of evidence involved. Each judge was then provided a scoring rubric and list of suggested follow-up questions to ask the student teams.

5 Critique of the Digital Forensics Challenge

Overall, we found both of the DFC events to be a success. Veteran high school cybersecurity competitors provided us glowing feedback on the quality of our events. Since the teams for our competitions were chosen either through automatic bids from the four different California regional competitions or through at-large bids chosen by the Governor's office, it is impossible to tell if the DFC improved the diversity of the cybersecurity teams. Nonetheless, our survey data of the competitors was overwhelmingly positive for all competitors, including gender and racial diverse competitors, that we feel we achieved our goals.

In our survey, we asked the competitors if their overall skills were valued more in the DFC or less in the DFC when compared to other cybersecurity competitions where a '1' was much more valued, a '3' was the same value, and a '5' indicated that the competitors felt their skills were much less valued, the average reply was a 2.0 (the competitor felt that their overall skills were

more valued in the DFC than other cybersecurity competitions) for the 52 respondents to the survey that had prior cybersecurity competition experience.

One concern about adding non-digital elements to cybersecurity competitions is the perception of "watering down" the computer-technical elements of the competition. In a survey question where competitors were asked to compare the amount of technical cybersecurity content in the DFC compared to other cybersecurity competitions, where '1' was the DFC had much more technical cybersecurity content when compared to other cybersecurity competitions, a '3' indicated equal amounts and a '5' indicated that the DFC had much less technical cybersecurity content when compared with other competitions, the DFC scored a 2.36 (the DFC had more cybersecurity content when compared with other competitions) for the same 52 respondents.

6 Future Work

There are several improvements being considered for the design of future DFC events. First, we plan to use a different variety of digital devices for the students to discover and investigate. By incorporating devices with various operating systems and user interfaces, the competitors would be further challenged in locating devices they may not expect to hold valuable information and extracting the data appropriately to ensure preservation. Second, we plan to include the use of social media to aid competitors in understanding the dynamic components of a computer forensics investigation. In addition, this is an opportunity for pieces of evidence to require psychological interpretation, therefore increasing the use of critical thinking and analytical skills. Third, we would like to continue incorporating a realistic, detailed timeline plot and evidence trail for the crime as these aspects were key to keeping the competitors engaged, making intelligent observations, and obtaining new investigative skills. Finally, a crucial aspect of the competition we want to continue and improve upon is the inclusion of both a forensics event and a cybersecurity event linked with the same immersive theme. In 2018, the healthcare scenario tied together the DFC event and a network cybersecurity event which allowed the competing teams to strengthen their skills in various avenues of challenges.

Outside of the CCIC competition, we are interested in working with our partner competitions across California in measuring the diversity of the participants and tracking to see if they pursue a cybersecurity field in post-secondary school. We also want to survey participants of high school cybersecurity competitions who do not continue with cybersecurity competitions to better understand what mechanisms provably work to attract a diverse set of students to cybersecurity.

7 Conclusion

Typical high school cybersecurity competitions cater to a very narrow swath of students: students who are already interested in the details of computer technology. However, to meet the demands for a cybersecurity workforce, we need to do a better job in attracting and retaining a broader number of students. The CCIC's DFC is one attempt at creating a high school level cybersecurity

competition that would appeal to students with a wider set of interests and potentially a growing interest in computer security.

8 Acknowledgements

We would like to thank the staff at the California Cybersecurity Institute (CCI) who were in charge of the logistics of the CCIC competition, including registration, tech support, and fundraising. This competition would also not have been possible without previous designers of the CCIC, Ciera Dixon and Lauren Pixley.

References

[1] NICE. Nice program updates, November 2017. Skype.

[2] Mark A. Gondree Portia Pusey and Zachary N. J. Peterson. The outcomes of cybersecurity competitions and implications for underrepresented populations. *IEEE Security & Privacy*, 14(6):90–95, 2016. doi: 10.1145/1188913.1188915. URL http://doi.acm.org/10.1145/1219092.1219093.

[3] David H. Tobey, Portia Pusey, and Diana L. Burley. Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. *ACM Inroads*, 5(1):53–56, March 2014. ISSN 2153-2184. doi: 10.1145/2568195.2568213. URL http://doi.acm.org/10.1145/2568195.2568213.

[4] C. Eagle. Computer security competitions: Expanding educational outcomes. *IEEE Security Privacy*, 11(4): 69–71, July 2013. ISSN 1540-7993. doi: 10.1109/MSP.2013.83.

[5] Jelena Mirkovic, Aimee Tabor, Simon Woo, and Portia Pusey. Engaging novices in cybersecurity competitions: A vision and lessons learned at ACM tapia 2015. In *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, Washington, D.C., 2015. USENIX Association. URL https://www.usenix.org/conference/3gse15/summit-program/presentation/mirkovic.

[6] Masooda Bashir, April Lambert, Jian Ming Colin Wee, and Boyi Guo. An examination of the vocational and psychological characteristics of cybersecurity competition participants. In *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, Washington, D.C., 2015. USENIX Association. URL https://www.usenix.org/conference/3gse15/summit-program/presentation/bashir.

[7] Clark Taylor, Pablo Arias, Jim Klopchic, Celeste Matarazzo, and Evi Dube. CTF: State-of-the-art and building the next generation. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, Vancouver, BC, 2017. USENIX Association. URL https://www.usenix.org/conference/ase17/workshop-program/presentation/taylor.