Investigating the Experiences of Female CTF Players

Submitted in partial fulfillment of the requirements for

the degree of

Master of Science

in

Information Technology - Information Security

Antonio Martorana

B.S., Mathematics - Computer Science, UC San Diego

Carnegie Mellon University
Pittsburgh, PA

April, 2022

Acknowledgements

Thank you to my advisor Dr.Hanan Hibshi for her mentorship and guidance, and motivating me to pursue a unique thesis topic. Special thank you to Dr.Nicolas Christin for the invaluable feedback and comments. I'd also like to extend acknowledgements to Alejandro Cuevas Villaba, Dianelys Soto-Cruz, and the picoCTF team for all their help during this project. Finally, thank you to the Information Networking Institute, CyLab, and support from Cisco Systems, Inc. (Award No. 00000341) for covering related WiCyS conference accommodations to execute this research project.

Abstract

There have been many efforts focused on improving the representation of females in cybersecurity. Capture the flag (CTF) platforms have primarily been the tool of choice to teach fundamental skills and spark interest in the profession. However most platforms aim to address the initial learning curve for newcomers, many have not focused on diversity and inclusivity as a goal. While some research evaluates CTF design to improve participation and retention, this thesis aims to provide a secondary perspective. Through interviews conducted with 13 female-identifying CTF players and an overview of 207 female competitors from a CTF event hosted at the 2021 Women in Cybersecurity Conference, this thesis highlights factors that might motivate a female player's willingness to continue with CTFs or cybersecurity education. Our findings: (i) suggest that collaboration provides an incentive for female players to participate through advanced stages of a CTF, (ii) suggest a more robust environment that engages women and beginners will help with recruitment and continued participation, and (iii) support previous findings that CTFs introduce a variety of technical and mental skills. This thesis provides some preliminary recommendations for future work, and suggestions to picoCTF to enable more performance analysis.

Table of Contents

Acknowledgements **ii**

Abstract **iii**

List of Tables **vi**

1 Introduction **1**

1.1 Project Motivation 1

1.2 Problem Statement 2

2 Related Work **5**

2.1 Expanding Diversity in Cybersecurity 5

2.2 CTFs in Cybersecurity Education 6

2.3 Peer Proximity in STEM Education 8

3 Research Design **10**

3.1 Step 0: Capture-the-flag Competition Design 10

3.2 Step 1: Scoping and Interview Guide 11

3.3 Step 2: Interviews 12

3.4 Step 3: Qualitative Analysis 13

3.5 Step 4: Competition Analysis 13

3.6 Limitations 14

3.6.1 Research Sample 14

3.6.2 Interview Analysis 15

3.6.3 Challenge Difficulty 15

4 Results **17**
4.1 Interview Participants 19
4.2 Impact of Collaboration in CTFs 19
4.2.1 Shadowing and Exposure 20
4.2.2 In Person vs Remote Collaboration 21
4.2.3 Team Structure 22
4.3 Issues that may Contribute to Low CTF Participation 23
4.3.1 Outreach 23
4.3.2 Confidence and Deception 24
4.3.3 Resources 25
4.4 Building Cyber-related (1337) Skills 26
4.5 miniCTF Analysis 27

5 Discussion **29**
5.1 Marketability 29
5.2 The Community Dilemma 30
5.3 miniCTF vs picoCTF 31

6 Recommendations for Future Work **33**

7 Conclusion **35**

Bibliography **36**

Bibliography **36**

Appendix A Tables **40**

List of Tables

Table 3.1 CTF Category and Challenge Overview 11

Table 4.1 Completion Rate per Challenge and by Category 17

Table 4.2 Background of 13 interview participants 20

Table 5.1 Undergraduate Female Completion Rate in 2021 picoCTF vs 2021 miniCTF 32

Table 1.1 Background of 13 interview participants 41

1

Introduction

1.1 Project Motivation

The original motivation for this project was derived from a literature review I did investigating diversity issues in online gaming, and searching for similarities in gamified education. As we will later discuss, impressions of gamified education have found that women were less receptive than men, but do not explore much further. Research surrounding low female participation in games is less clear, and mostly focuses on social norms around certain genres of games and online harassment. My initial impression was to focus on whether user attitudes toward CTFs were influenced by previous online experiences. The next step was to search for diverse online games and create a framework that could serve as a guide for CTF development. One particular candidate was Animal Crossing: New Horizons a highly-rated, social simulation game that offered single and multiplayer options. It is also very receptive to players from many different backgrounds. However, after some work in this direction I began to understand that it was not an excess of negative factors that drove away participation but a lack of supportive ones. Community, collaboration, and peer proximity elements appeared the most prominent to probe further.

1.2 Problem Statement

Over the past decade many efforts within industry and academia have been proposed to address the lack of diversity in STEM [28]. Narrowing the scope towards cybersecurity, in 2021 24.9% of the professionals hired identify as female [28, 1]. Many efforts to improve female-representation in security-related fields have focused early in the education pipeline, as much research has demonstrated that career preferences are chosen around the middle school and early high school levels. The introduction of gamified learning through capture-the-flag (CTF) competitions, have primarily been the tool of choice in promoting early interest in cyber-related fields [22].

Capture-the-flag competitions, introduces students to a variety of technical concepts in computer science and cybersecurity. CTFs have been successful in introducing new students with little or no technical background into computer science and cybersecurity related topics [21, 23, 8]. Additionally, CTF participation has shown positive trends in promoting security behavior, in addition to teaching participants about less intuitive exploits [33]. As a game-based learning mechanism they promote engagement through competition, and learning through collaboration and hands-on activities. This is quite helpful when introducing it to K-12 and college students. There have been numerous competitions geared toward high school and college students by various government and industry sponsors such as Cybersecurity Awareness Week (CSAW), MITRE eCTF, Northrop Grumman's CyberPatriot, Collegiate Cyber Defense Competition and Collegiate Penetration Testing Competition, and picoCTF. Unfortunately, there has been little emphasis on increasing the participation and retention of females in CTFs. Modern approaches to CTF platforms only attempt to address the initial learning curve for newcomers, how effectively they teach cybersecurity concepts, and whether they motivate individuals to pursue a cyber career. However they do not address some of the issues that influence

participation and retention among females and other underrepresented groups in cybersecurity education. In this regard, existing literature is unclear on the underlying factors that cause low female representation.

To better understand female experiences in this area, I conducted interviews with 13 CTF participants from the 2021 Women in Cybersecurity (WiCyS) Conference. Our research questions are:

RQ1: What is the impact of collaboration in succeeding in CTFs?

RQ2: What issues may contribute to low participation in CTFs?

RQ3: What educational resources have helped build cyber-related skills?

Participants come from various career levels ranging from early undergraduate students to experienced professionals in various industries. During our interviews we explored collaboration experiences, early stages pursuing a cybersecurity education or participating in CTFs, and skill progression. Additionally to support and provide further insight into our research questions, we hosted a CTF event at the WiCyS Conference and analyzed the demographic/performance data of 200+ female players. This data includes the 13 participants we had interviewed. Our objective on this end was to find relationships between CTF performance and ethnicity/nationality, social-economic status, and academic standing (i.e. preparation) for female players.

Our findings from interviews indicate that collaboration further incentivized female participants to work on challenges, during later stages of CTFs and/or when progress was slow. We also found that among many female participants a combination of low confidence, lack of outreach and mentorship had made it difficult to engage with other peers from different backgrounds or participate in CTFs. However, on a more positive note many players suggested that CTFs was a primary resource used for building a broad domain of knowledge in cyber and would help

beginners/early-career professionals find their niche. An especially encouraging finding was that some participants noted they already had hands-on labs or CTF-style assignments embedded within their university curriculum.

In addition to my findings, I present recommendations for CTF and educational organizations to consider, and provide long-term research directions to improve the retention of female participants. Additionally, I will try and provide a set of recommendations for picoCTF to consider that can enable more data analysis for this type of research.

2

Related Work

In this section, we present an overview of the current efforts seeking to expand diversity in cybersecurity, how CTFs are used to further cybersecurity education including benefits and shortcomings, and how participation in STEM programs can be affected through peer proximity.

2.1 Expanding Diversity in Cybersecurity

To compensate for the growing shortage of cyber professionals universities, community colleges, and vocational programs have been tasked educating and training more talent, especially diverse talent. Not only are there too few students entering the talent pipeline, but there are remaining challenges in establishing quality cybersecurity educational programs that address the needs of students from diverse backgrounds. This negatively impacts the recruitment and retention of many upcoming professionals in cyber. Mountrouidou et al. describes some of the interventions and relevant research that have been used to mitigate these difficulties in cybersecurity. They specify (1) equitable access to education and resources, (2) present cybersecurity in multiple contexts, (3) hands-on and active learning, (4) student empowerment espe-

cially among minorities, and (5) student mentorship as components that should be used in a culturally responsive framework for education.

Two interventions of interest that Mountrouidou et al. outline are (3) authentic and active learning techniques, and (4) empowering and mentoring minority students to participate, engage, and stay in cybersecurity. In intervention (3) they specify active and hands-on learning techniques (especially gamification) having a favorable outcome for increasing student confidence and enthusiasm toward the cyber field. The second intervention mentions empowering and mentoring minority students in order to increase the participation and retention of those students. Organizations such as Grace Hopper, Women in Cybersecurity, SHPE, and NSBE have raised awareness among many underrepresented students in cybersecurity in addition to sponsoring community forums, career fairs, conferences, and mentorship that creates a supportive environment for those new to the field [28, 4].

2.2 CTFs in Cybersecurity Education

There has been evidence that poorly designed games discouraged novices from participating [28], and further evidence by a study involving a GenCyber summer camp that there are significant differences between the impressions of the games by male and female students [21]. This suggests that females are less receptive to gamified learning than their male counterparts. Comprehensive literature reviews also indicate that much of the research that looks into gamified approaches, makes no reported effort to recruit participants from underrepresented groups or assess the long-term effectiveness of the studies [28].

Gamification has especially been applied to cybersecurity education through capture the flag (CTF) competitions, which has been able to introduce students to a variety of technical concepts in computer science and cybersecurity. Capture the flag events come in two flavors, jeopardy and attack-defense. Jeopardy competitions

are challenge based, and organize specific challenges into knowledge domain categories. Participants receive a known number of points for completing each challenge. Attack-defense style CTFs attempt to recreate a live cyber-warfare environment for players, where teams have their own vulnerable services that must be protected and must simultaneously attack other teams' services and/or complete other tasks. Individuals and teams for each type gather points by finding flags through challenges or by attacking other services. The individual or team with the highest score wins. These games aim to improve engagement through competition and collaboration, in addition to learning relevant cybersecurity knowledge.

This game based training has been successful in introducing cybersecurity to students [6, 34]. They get hands-on training and simulated experience that is difficult to receive through traditional classroom settings. In group settings, students are able to leverage their teammates for knowledge and practice their collaboration skills, especially applicable to industry settings. In addition, CTFs have been good indicators of interest in pursuing a career in cybersecurity [2]. However, the same studies have also questioned whether CTFs specifically motivate beginners to pursue careers in cybersecurity or if they are best suited for reinforcing the interest of individuals with a depth of cybersecurity skills [31, 2]. More work has been done focusing on developing workshops and programs that specifically target novices with encouraging results [26]. Other issues revolve around the fact that many CTFs take time outside of the classroom and do not occur frequently enough to reinforce learned concepts. Finally, many studies looking to use CTFs to help improve gender diversity have acknowledged the lack of participation of female students and raise this as an important area of future work [31].

2.3 Peer Proximity in STEM Education

Some research has explored how peer proximity influences students choices in a STEM career during their early adolescent years [29, 3]. The foundation of rests on the proximity principle, defined by House as the effects of social structures, positions, or systems that are transmitted to individuals through stimuli that impinge directly on the individual [19]. We focus on its application to peer influence in STEM career participation and long term retention. Peers in this case can be defined as friends and classmates, or individuals who appear within another individual's educational environment.

Morgan et al. mentions inconsistencies that do not adequately address gender differences in the selection of educational or career choices, including college majors that may lead into STEM fields (the so called "leaky pipeline" issue"). They find that occupational plans of young women are less predictive of initial college major selection than that of males [27]. Young women not only disproportionately leave STEM fields, but abandon initial interest altogether. Instead there are more predictive factors that contribute to the early recruitment of females in various STEM fields, and while other explanations typically focus on academic performance/ability there is much research that shows the gender gap in STEM cannot be attributed to those metrics [20, 5, 24, 32].

One alternative hypothesis by Vleuten et al. explores how friends affect STEM choices, and ultimately to what extent the gender norms of class friends matter in male and female STEM choices after secondary education [32]. In their study they examined whether friends' characteristics were associated with STEM choices after secondary education, specifically for students in the STEM pipeline. This was done collecting data from 744 adolescents in secondary school and after secondary school in the Netherlands. The authors found evidence that gender normativity of

class friends influences the females' but not males' STEM choices. Additionally girls were substantially less likely to pursue STEM fields when their friends upheld more traditional gender norms, irrespective of their own norms [32, 3]. This study at least provides motive to explore conditions that enable more females to pursue a career in cybersecurity.

It should be noted that the above study mostly focuses on the initial recruitment into the STEM pipeline, but raises a follow up question: what are the effects of peers on retaining STEM careers? There is strong evidence that adolescent students adjust their preferences to those of their friends, and in particular females typically retain their STEM preferences when other girls in their classroom also enjoy STEM (peer exposure) [29]. This notion would make sense since friends tend to select or persuade others into selecting similar classes and attitudes [16]. The researchers also emphasize that social influence mostly came from same-sex friends, which then reinforce the gender-norms discussed in the previous studies above. Since STEM classes still contain an overwhelming male to female ratio [9], it seems that a) increasing the presence of females in classrooms and b) similar gendered support groups are especially important when retaining students in STEM education.

3

Research Design

This is exploratory research about the female participants experience in CTFs, using a hybrid (qualtiative and quantitative) approach. We conducted participant interviews from competitors that competed in the miniCTF event at the WiCyS Conference. Simultaneously, we analyzed performance and demographic data from our CTF competition to draw insight and support findings from the interviews. Our research design has five phases: (0) designed the layout and challenges of our CTF event, (1) prepared interview questions based on an early literature review, (2) conducted interviews, and (3) analyzed interview transcripts following thematic analysis approach [10] and (4) comprehensively reviewed the 2021 picoCTF performance and demographic data across all female competitors.

3.1 Step 0: Capture-the-flag Competition Design

The CTF competition, named the WiCyS Conference miniCTF, was a 48 hour event. We anticipated and intended it was for beginners or as an introduction to CTFs. To promote a higher turnout we included a few intermediate and advanced challenges as well. There were five categories included that are typically in line with other

CTFs and previous iterations of picoCTF: Cryptography, Web Security, Forensics, Reverse Engineering, and Binary Exploitation. This is done to provide an overview of the relevant domains in cyber and build skillsets that each player should have in a particular category. The breakdown of challenge difficulty can be seen in **Table 1**. We added challenges that were primarily easy or medium difficulty level to promote engagement, and provided some form of skill progression. Difficulty was assigned to each problem based on feedback from testers and challenge developers. Prior to the event we also released tutorial videos to help navigate the platform, and walk individuals through the process of capturing and submitting a flag.

Category	Challenge	Difficulty	Description
Cryptography	Mod 26	Easy	Solve a Rot13 cipher
	La cifra de	Medium	Cracking vigenere ciphers
Web Exploitation	Where are the robots	Easy	Web crawlers and robots.txt
	Picobrowser	Easy	HTTP Headers
	Irish Name Repo 1	Easy	SQL Injection
Forensics	Glory of the Garden	Easy	Hexadecimal and binary numbers
	Disk, disk, sleuth! II	Medium	Introduction to Sleuthkit
Reverse Engineering	Let's get dynamic	Medium	Dynamic analysis tools
	Rolling My Own	Hard	Reverse engineering
Binary Exploitation	Cache me outside	Easy	Heap memory exploitation

Table 3.1: CTF Category and Challenge Overview

3.2 Step 1: Scoping and Interview Guide

To scope this research and prepare for interviews, I reviewed existing literature on diversity in STEM education. From here I progressively narrowed the field of view by looking at research in cybersecurity, cybersecurity education, gamified learning, and finally CTFs. Some topics that came up were teamwork, collaboration, pedagogical practices, and inclusive UI practices. I explored papers that investigated diverse playerbases in gaming or gamified learning to further identify similarities, and paths

of exploration. This search culminated on improving participation and retention of female players in CTFs, by exploring the current environment and identifying any potential barriers faced. Once settled on this research topic I searched for and randomly selected 15 papers through keyword searches and my existing knowledge of the field. I labeled all sections in those papers that explored gender diversity in relation to participation and retention, teamwork and collaboration, and peer proximity. For some papers that did not talk about those topics in CTFs, I labeled sections that indicated similar problems in cybersecurity, STEM education, and gaming. Those papers were used to help formulate my interview questions, which can be found in the **Appendix**.

3.3 Step 2: Interviews

We conducted semi-structured interviews with 13 participants from WiCyS Conference. Interviews were approximately 30-60 minutes long and all participants were competitors in the CTF event or had joined "Both Sides of a CTF workshop"[1]. In **Table 1**, we show the demographics of the interview participants and their backgrounds. A table can also be found in **Appendix A**. To recruit participants, we had multiple research staff walk around the venue, asking individuals if they would like to participate in the study. Once individuals filled out the consent form we either conducted an in-person interview at the venue or followed up by email and scheduled an interview over Zoom. Participants were given $10 gift card for participating in an interview and $5 gift card if they completed a survey, that was used for a follow up study to this project. After this process, we transcribed all audio recordings utilizing Otter.ai and corrected transcriptions when necessary.

[1] This was a workshop held at the WiCyS Conference that presents a CTF from the perspective of an organizer and a player

3.4 Step 3: Qualitative Analysis

To better understand various themes in our data, we qualitatively analyzed the responses of our 10 open-ended questions using thematic analysis. [10]. This was an iterative and reflective process, where we constantly moved back and forth between stages of reviewing the data, coding, searching for themes, and then refining as typically recommended during qualitative analysis [12].

The analysis consisted of several phases in this regard. Since interviews were semi-structured, we segmented responses from each participant by question and began carefully reviewing our data. At first we focused on a subset of questions and then iteratively engaged with others. This helped us progressively understand some of the viewpoints, experiences, and skill progressions that different players encountered. We created an initial set of codes during open coding, constructing them line by line. This took about 45 minutes to 1 hour per question on average.

At this point we sorted and collated the codes we had assigned so far into a codebook. Excerpts were grouped properly with their corresponding codes. Afterwards, we revisited the subset of questions using focused coding to: a) ensure our codes were applied consistently, and b) synthesize and group larger amounts of data. A single researcher then analyzed and coded the remaining questions in the same way, involving others in difficult or ambiguous cases. We extended / modified the codebook for new observations or insight when needed. Lastly, we systematically searched for relationships between emerging themes in buckets and across questions in our codebook. We reviewed and revised these themes as necessary.

3.5 Step 4: Competition Analysis

After the CTF competition, we analyzed the performance and demographic data of all 234 competitors. More specifically we reviewed the completion rates between

challenges and across categories, attempt vs. success ratings, and demographic data of competitors (i.e. race, school level, school zip codes). Challenges were assigned difficulty based on input from experienced CTF players, challenge developers, and testers (most of whom were beginners). This gave us insight into measuring the difficulty of challenges vs. the intended difficulty, skill acquisition within a category, and studying potential relationships between ethnic/race-related underrepresented groups and challenge completion.

3.6 Limitations

I identified three main limitations in regards to this thesis and the implications of my findings: the participant sample, stability in the interview analysis, and potential inconsistency in CTF challenge difficulty ratings.

3.6.1 Research Sample

This work contains common threats and issues consistent with this type of qualitative research. Any generalized statements or assumptions made with this sampled group should be taken with care. For example, due to the nature of the conference which encourages more female representation in cybersecurity, more participants might have been educated on issues that various minority groups in STEM encounter. Observations may be different if we had gathered participants from more advanced CTFs or a non-diversity focused conference. Self-selection of participants may also be an issue; for example, male attendees more frequently declined an interview despite originally consenting to participate in the study. Survivorship bias may also be present in our sample since some interviewees might have not stayed for the entire duration of the CTF After Dark[2] event (or have shown up at all). For example,

[2] CTF After Dark was a session dedicated to the concluding hours of the miniCTF event, it allowed participants to receive help from tutors who were CTF students or picoCTF staff

some might have left because they felt they were no longer making progress on CTF challenges. Thus, our sample pool might consist of more participants with an experienced background.

3.6.2 Interview Analysis

Due to time constraints, we were unable to find another researcher who had the bandwidth to establish inter-coder and intra-coder reliability. This may impact the confidence in my coding process and our interpretations of our findings. However, since the coding process was reflective much of the data was reviewed and re-coded a few times, with input from other research collaborators.

3.6.3 Challenge Difficulty

Additionally, a possible avenue of exploration is a reevaluation of how challenges in CTFs are assigned difficulty. Problem developers often assign difficulty of each challenge based on their intuition and knowledge of various security concepts, in conjunction with input from testers. Thus, problems are assigned a lower difficulty than the true rating. Similar issues exist when instructors or teachers develop exams, many able to detect an increase or decrease exam to exam. Though unable to properly calibrate how much easier or harder a specific exam will be [11]. Based on this knowledge, it presents a possible explanation to higher completion rates between categories and across individual challenges in certain categories (i.e. web exploitation or cryptography) compared to Binary Exploitation or Reverse Engineering problems with similar difficulty. Future work could consider using additional or alternative dynamic measurements to assign difficulty to problems, perhaps by the players themselves during the competition.

Ethical Considerations This study was reviewed and approved by the Institutional Review Board (IRB) of our institution before any data collection began.

Prior to beginning the interviews, participants were once again briefed on the study, the data collection and retention policies, and ways for withdrawing from the study. Participation was voluntary.

4

Results

We first provide an overview of our 13 participants (Section 4.1). Then, provide some of our findings from our interviews starting with our first research question (Section 4.2), we want to study the impact collaboration has in CTF competitions and possibly identify any skills that result. While addressing our second research question we identify culture and environment issues that contribute to low participation in CTFs (Section 4.3). Finally, we present educational resources that have helped build skills

Challenge	Difficulty	C.R. per Challenge	C.R. by Category
Mod 26	Easy	86%	67.3%
La cifra de	Medium	48%	
Where are the robots	Easy	58%	45.7%
Picobrowswer	Easy	45%	
Irish Name Repo 1	Easy	37%	
Glory of the Garden	Easy	70%	45.4%
Disk, disk, sleuth! II	Medium	21%	
Let's get dynamic	Medium	10%	10.6%
Rolling My Own	Hard	11%	
Cache me outside	Easy	16%	15.9%

Table 4.1: Completion Rate per Challenge and by Category

necessary for CTFs (Section 4.4). Finally, we present performance and demographic statistics from the miniCTF competition (Section 4.5). Our aim on this end was to provide some additional insight into the nature and context of our study. Due to sample size we do not draw any statistical conclusions, but instead highlight trends to be explored in future work.

These findings were especially encouraging, given a similar study by Cuevas et al. that explored how CTF teams collaborate, organize, and what their technology needs require [13]. A key distinction was their study primarily focused on CTF team dynamics, this thesis tended to focus on the ecosystem / environment that female players would experience which includes CTF teams. For example they also examined team leadership qualities, tools and platforms used, and applications to security teams from the context of crowd sourced work.

One similar result found that teams would place depth and specialization at the core of their decision-making processes ranging from group formation to task distribution. Defined roles in this sense would enable other players to learn from senior members, distribute accountability to members working in a particular category, and allow team members to decide how to incorporate others into their work. One interesting observation in this study reported that individuals had expressed concerns regarding diversity and their "social identity self-presentation". Since competitions and collaboration primarily took place in an online setting, individuals could hide their self-presentation behind an avatar or online handle. Some individuals felt pressured to compensate their abilities once they could no longer limit this self-presentation. One female in that study noted how they were more aware of the comments they made and how it might validate stigmas or misconceptions of females in computer science [13]. One noted difference in their study was that among many motivators to participate in a CTF team, participants also mentioned the ability to earn prizes and measure performance of other potential teammates [13]. In our study

motivators mainly focused on learning and incremental improvement. 2 participants (P6,P13) did specifically note however that they were not interested in winning as it either detracted from having fun or the learning process (though P13 did mention they placed very well in one competition). Another noted finding upon reviewing the paper was that participants in their study did not further elaborate how newcomers were further incorporated into teams, beyond traditional mentorship aspects as an experienced CTF player [13].

4.1 Interview Participants

All participants were informed of the procedures of the survey and provided consent. The informed consent notified participants that they would be asked to complete 30-45 minute interview with a research member, discussing their experiences with online gaming, CTFs, and professional growth in cybersecurity. After the interview participants were sent a $10 e-gift card to a store of their choice.

We interviewed 13 female participants from the CTF event. Five were 18-24 years of age, three were 25-34, one was 35-44, one was 45-44, and two stated older than 40 years of age but did not specify. Exactly half the participants completed a Master's degree and the remaining half are enrolled in a 4-year institution studying a related technical field. We tried to interview a more representative sample, but we encountered difficulty finding and recruiting those who did not have a degree or had joined the industry through alternative means. **Table 4.2 and Appendix 1** summarizes the demographics of our sample.

4.2 Impact of Collaboration in CTFs

I asked participants on their experiences collaborating on CTFs and in comparison to independent work. There were three key themes that emerged from this analysis. Participants raised relevant benefits from collaboration (**Section 4.2.1**), noted

P#	Industry Area	CTF Experience (years)	Degree Area	Highest Degree	Employment Status
P1	software/security engineering	3	Computer Science	Masters	full time
P2	risk and compliance, vulnerability management	3	Information Systems	Undergraduate	student
P3	information technology	4	Computer Science	Undergraduate	student
P4	teaching assistant,	3	Computer Science	Undergraduate	student
P5	SAP Security Administration	Education	Computer Science w/ specialization in cybersecurity	Masters	research internship,new grad seeking full time
P6	vulnerability management, education, incident response	2	N/A	Masters	full time
P7	vulnerability management	3	Cybersecurity - Information Assurance	Masters	full time
P8	information technology	2	Information Technology - Cybersecurity	Bachelors/Masters	part time,student
P9	education	<1	Information Technology - Cybersecurity	Masters	full time
P10	network admin	1	Information Technology - Information Security	Bachelors	seeking full time
P11	nurse	0	Healthcare	Masters	full time employed, part-time student
P12	project management, security engineer	<1	Information Technology	Masters	full time
P13	n/a	2	Cybersecurity with specialization in Enterprise Cloud Computing	Bachelors	student

Table 4.2: Background of 13 interview participants

reasons they would not collaborate (**Section 4.2.2**), and identified different models of collaboration in CTFs (**Section 4.2.3**). Much of our analysis seems to support findings from existing literature.

In our study, 10 of the 13 participants reported that they had played within a team for at least one CTF in the past and 9 of the 13 participants had a stable team they would compete with. One participant stated that while they had not been with a team, they had an experience collaborating with other peers indirectly.

4.2.1 Shadowing and Exposure

A frequent talking point among participants (P2,P3,P4,P6, P7,P9,P11,P13) was the ability to shadow more experienced CTF players who often had a diverse set of tools and background knowledge ready at their disposal. Advanced CTF players were more capable of finding simple and sometimes innovative solutions. Depending on the category they could recommend a software program, online tutorial/tool, or library package that is helpful to solve a problem. For example, those with experience in reverse engineering would recommend others to learn how to use popular reversing applications like Ghidra or GDB.

More importantly an experienced player could provide and explain relevant background information needed to proceed in a challenge or category. For novices who become interested in a particular domain, this person could be a future source of support. Mentorship in this aspect was a highly desired side effect of shadowing.

Participants stated that mentorship early on would help with technical, communication, and professional networking skill growth. In addition, mentors from similar backgrounds are better suited to address the unique obstacles (professional and personal) that mentees might encounter.

The same participants also highlighted the importance of exposure to highly collaborative environments. Collaboration in CTFs would allow participants to develop their social skills, a highly requested asset for industry positions. Regardless of individual abilities, players will often be required to communicate at high level (i.e. tutoring others) or technical level (i.e. strategizing with peers).

4.2.2 In Person vs Remote Collaboration

Some participants also made the distinction between in person and remote collaboration. They expressed that during remote team collaboration sessions would take place on different messaging or video conferencing platforms like Discord or Zoom. These sessions would be used primarily for (1) knowledge transfer or (2) status updates. However, most of the actual progress made on challenges would be made offline, and typically on their own. P1 mentioned this was not optimal because progress was made asynchronously and coordination was difficult.

On the other hand in person teamwork and the "community factor" were potential mitigations to burnout. Participants (P2,P4,P5,P7) said that during some stages of a competition, progress became slower than expected and required a steady effort of trial and error. P2 stated that when they got frustrated early, working with others would help with retention and motivate them to put more hours into a CTF. This suggests that in person collaboration among peers provides incentive and motivation continue to try new approaches and contribute to the group's overall knowledge. In person collaboration would also present other opportunities to grow their professional (and sometimes personal) network, and enjoy downtime with teammates. To this

end in person events present an opportunity to increase participation and retention in CTFs.

4.2.3 Team Structure

The organization between teammates emerged as a potential indicator of how motivated players would be to contribute. For some participants (P1,P2,P3,P9), team structures were decentralized and individuals were free to take on any problem. For others (P13,P11,P8,P7,P4,P6) there was a hierarchical structure. Teams had a lead or captain who delegated problems (or in some cases categories) to players in order of most experience to least experience. In some cases multiple players would be assigned to a category with a de facto lead who could act as a source of expertise. Participants on established teams (P4, P11, P13) also ensured that write ups and documentation could be kept for future knowledge transfer. The remaining participants did not have a strong preference to play with a team.

Of the two dominant organization layouts, the hierarchical structure was preferred. P6 mentioned that structure and active participation was a deciding factor in choosing to work with a team: *"... if I had a choice, if I had a team that was really engaged was there for, you know, a good portion of the time, we agreed that we were all going to get together on voice for like, the evenings or something like that. Then I went a team. Otherwise, if I'm individual, just let me do my thing."* Moreover, structure enabled accountability and cohesion between teammates. Accountability enabled (some used the word forced) players to remain engaged during parts of the competition when they were directly assigned tasks. P13 explained that *"project management and setting expectations early on"* was an important element when working with a team. Finally, cohesion promoted or in some cases introduced an inclusive culture between teammates.

4.3 Issues that may Contribute to Low CTF Participation

My next set of questions aimed to identify the atmosphere that female players typically find themselves in. I identified three elements that participants repeatedly reported were important to CTF participation: outreach (Section 4.3.1), mindset (Section 4.3.2), and resources (Section 4.3.3). Further analysis suggests that each of these elements influence different stages of a competitor's overall experience. For example, a typical cycle will begin with outreach, where different entities act as the initial point of contact for those who do not already know about an event. Once registered a participant will compete. However, the support and final impressions will determine whether or not they decide to compete again. Two factors relevant in this decision are a player's mindset and the amount of resources they receive. Overall, these themes suggest that CTFs currently cater to more experienced audiences and should continue to refine toolsets for beginners.

4.3.1 Outreach

I asked how competitors were introduced to CTFs. Participants had primarily discovered CTFs through second hand sources and/or through their own research. 7 of 13 participants (P2,P3,P4,P6,P8,P9,P12) were introduced to CTFs by others. (P2,P3,P4,P6) were introduced via some form of mentorship and (P12,P8) had been introduced by coworkers/colleagues. P9 reported that because they were in a cybersecurity program, they were surrounded by it either through word-of-mouth or advertisements. 5 of 13 participants (P1,P5,P7,P10,P13) stated that they had discovered them on their own, taking self-initiative on how to get hands-on experience. In addition, one noteworthy finding was that all of the above participants already had a developed interest in cybersecurity, and were proactive in their growth. This might suggest that players who were sufficiently motivated (either through commitment or

curiosity) are more likely to find and therefore compete in CTFs.

A follow up question was asked to examine their experiences on outreach for CTFs or cybersecurity. Outreach could come from grade teachers, professors, industry professionals, CTF organizers, etc. 9 of 13 participants (P1,P2,P6,P7,P8,P9,P10,P12,P13) answered that CTFs and cybersecurity were not mentioned to them . For those who are new to computer science, information technology, and other related fields there is much less emphasis on entering security. Most who find and participate in CTFs already have interest in security or have a contact who is.

In the final follow up question, I wanted to probe how participants thought outreach to CTFs or cybersecurity could be improved. Responses varied, but with one common theme: it is a difficult problem to solve and probably harder to measure. For example, (P5,P11,P13) reported that representation in cybersecurity and CTFs are improving but due to the unique nature of the field, the growth is quite slow. P1 mentioned that preexisting inequalities in fields like computer science, trickle down into sub-disciplines like cybersecurity or machine learning. Thus, CTFs participation among females is traditionally lower.

4.3.2 Confidence and Deception

There was a clear set of mental obstacles that most encountered. A common consensus among 9 participants (P1,P3,P4,P6,P7,P8,P9,P10,P12) was the notion that cybersecurity initially seemed more complex and difficult to break into. CTFs themselves were an extension of that. Many stated themselves, friends, or classmates had been intimidated at the thought of attending CTFs. These feelings were motivated by a lack of technical knowledge or experience. This adds evidence to previous work by Cheung et al. who found that perceived knowledge levels were a significant barrier to using competitions to attract students to cybersecurity [7]. Remaining opinions focused on misconceptions or stigmas commonly held in general. For example, P1

explained how their conversations went with classmates when speaking about specific areas of focus in computer science, *"[...] it is just like this grimy industry to be in"*.

For those that did take the first step, some admitted they were not confident at their abilities outright. Lack of confidence was often associated with feelings of imposter syndrome or uncertainty when struggling to solve challenges. This finding runs in parallel to previous conclusions that women generally report lower self-efficacy, or the strength in the belief of one's own ability to complete a task in cybersecurity [2]. In addition, much of the anxiety to perform well in a competitive environment could possibly raise doubts on one's ability to succeed in the profession. In the previously cited study by Cuevas et al., a reported observation was that members may have felt pressured to perform better in order to prove their social identity does not inhibit their abilities [13]. Furthermore, this was especially true for beginners or newcomers who often were not sure where to look or whom to ask for help. During the CTF many participants had stated that a combination of trial and error and online resources were the primary methods used to approach unfamiliar challenges. However, as the number of attempts quickly reached a saturation point it became clear that they were no productive or maybe abandoned interest in doing challenges altogether.

4.3.3 Resources

Participants (P3,P6,P7,P8,P9,P10,P12,P13) highlighted a need for more resources that help beginners. Beginners are often left to discover the vast amount of tools and information on their own. Competition organizers typically do not provide to much assistance (either in the form of tutors or guides) because of the competitive nature of the event, which is also true for beginner friendly platforms. Most recommend that players join a team and work collaboratively. This is one valid option, but disregards individuals who either cannot find a team or prefer to work independently. This early struggle may act as one barrier that demotivates players from participating in future

events. A previous season of the National Cyber League, found substantial drop-offs in novice participation across three sequential events all of which were intended for individuals [31]. Many provided suggestions for increased mentorship via tutors or industry professionals, and more technological resources to help those from low income communities.

4.4 Building Cyber-related (1337) Skills

We asked participants to report on the methods used during CTFs. 6 of the 13 participants (P5,P6,P7,P8,P12,P13) spoke about the unique advantages of CTFs in comparison to other learning methods. They reported gaining exposure to a variety of cyber skills in forensics, cryptography, reverse engineering, web exploitation, open source intelligence, network and web security. In addition participants reported gained experience in security tools and operating systems such as Linux, Wireshark, and Ghidra. Finally, a virtual playground where individuals can experiment with tools and systems without consequences was a much desired component of CTFs. Ideally participants are able to learn a variety of tools in this casual environment.

A subset of participants (P2,P4,P5,P7,P13) mentioned that CTFs expose people to tasks where problems and solutions are not clearly defined. This applies well to industry in a variety of settings where threat actors and exploits are adaptive, and vulnerabilities are unknown. However, one consequence of this is repeated exposure to failure, and the need to reevaluate an exploit/defense strategies multiple times over. P13 said these types of investigative skills are important *"[...] because you need to lose your fear of being wrong and also because it can give you an idea of whether or not you want to be that analyst or engineer or something like that"*.

4.5 miniCTF Analysis

An initial overview of our competitors (n=234), shows there were 207 female competitors and 16 male competitors (others either did not specify or reported as non-binary). Our analysis concentrated on the 207 female participants. 61% (145) of competitors held an undergraduate academic standing, 22% (53) chose not to identify their academic standing, and less than 1% identified as high school students or teachers.

Next, we provide a performance summary from the CTF in **Table 2**. Our initial focus began with the overall completion rate per category, this value was calculated using the equation:

$$CR = \frac{total\ \#\ of\ correct\ \ submissions}{\#\ problems\ in\ category\ *\ \#\ of\ participants}$$

Cryptography had the highest number of correct solutions (67.3%), Binary Exploitation and Reverse Engineering (15.9% and 10.6% respectively) having the lowest number of correct solutions. Web Exploitation and Forensics were approximately the same in terms of completion (around 45%). This finding was not surprising as 8 of 13 participants had stated cryptography was one of their favorite categories, followed by 6 mentions of forensics, 3 of web exploitation, 2 for open source intelligence (which was not a category in our CTF, but is common in others like the National Cyber League), and 1 for Reverse Engineering.

Then, we look at the completion rate per challenge which was simply calculated using this equation:

$$CR = \frac{\#\ of\ correct\ submissions}{\#\ of\ female\ participants}$$

The results of these calculations can also be found in **Table 2**. Again, we see a low amount of completion in the Reverse Engineering and Binary Exploitation categories

in comparison to the others. If we look across the Web Exploitation category, we also notice a 20% drop off in completion numbers even though the relative difficulty stayed the same. Given the present sample size we cannot determine the exact reason but possibilities include tiredness, lack of interest, and expected vs. actual challenge difficulty. In addition, the our analysis efforts ended early because of some missing points of information that we could not yet grab from the picoCTF platform.

5

Discussion

We discuss some common stories that appeared along with our findings. **Section 5.1** discusses improving the marketability of CTFs. In **Section 5.2** we illustrate how barriers create a tug-of-war style scenario which inhibit supportive communities from positive growth.

5.1 Marketability

Our conversations about outreach (P1,P3,P7,P8,P11,P13) led to a common theme of marketability. Marketability could be defined as whether individuals find it worthwhile to participate in CTFs or pursue a cybersecurity education. This decisions is primarily influenced by its attractiveness to others. To this end we discovered two goals that participants stated we should focus on: targeted outreach and early intervention.

There is a lot of emphasis, both within industry and academia to improve the gender diversity gap in this space. Participants outlined the need to adapt how CTF platforms and cybersecurity are presented to female students. Generic methods are not enough, the appearance and message needs to resonate with the individuals

targeted by outreach. Existing literature already supports this notion [18].

Furthermore, crafting this message for younger individuals is especially crucial. Early intervention has been shown to be a major factor in the direction an individual will take their future careers [14]. For example P13 shared that it has to be *"[...]fashionable... I look at my nieces, for example. And I tell them, hey, let's like take apart a hard drive, when they were three years old, totally down, because they didn't think like, this is a gender activity. Right? As soon as they've hit puberty, that's a little bit different"*. Future work could investigate how to make CTFs more fashionable or specifically aimed at female students. There are existing initiatives in place for introductory programming such as Girls Who Code [30]. We believe the details and its impact are a good direction for future research. ‘

5.2 The Community Dilemma

Some participants (P1,P3,P4,P9,P11,P12) emphasized the value of self-initiative in learning and networking. A subset of those (P1,P3,P9,P11,P12) further said this was an imperative character trait that would enable success in CTFs and cybersecurity. Participants frequently stressed the importance of resilience and the ability to learn from previous experiences. In this regard, the broad set of sub-disciplines and interdisciplinary nature of the field caused many to feel overwhelmed, especially when trying to navigate their interests. A common side effect of this process is a mixture of success and failure, and for those that might participate in CTFs, frustration. Most participants (P1,P2,P4,P5,P6,P10,P11,P13) suggested joining a club or community, especially those that promote diverse/underrepresented backgrounds. However, this may not always be plausible due to geographical location, lack of awareness in diversity by other women, or bias (and in some cases harassment).

This presents a circular issue in which women might not continue to participate in CTFs without a support system, yet there needs to be an existing support system

(i.e. community like WiCyS or university club) to recruit women. My follow up question is: who is responsible for facilitating this intervention? While it is important for members of a diverse groups to be the primary agents of change, it is difficult in the presence of the barriers highlighted above and in **Section 4.3**. I believe inclusive efforts should be promoted by a variety of stakeholders, especially in scenarios where underrepresented groups have a smaller population of individuals (i.e. due to geographic region, bias, and lack of awareness by other underrepresented individuals). In addition, this dilemma we suggest could further be solved by accelerated partnerships and research from industry and academia respectively. We recognize the incentive to put additional resources may be difficult, however we believe that engaging with many underrepresented groups will increase the quality of research and knowledge in this field.

As we have highlighted in **Section 2**, both the community intervention and peer proximity are both taken into account. In addition, it should be noted that the relevant factors to peer proximity in this case are geographical location (i.e. physical proximity) and mentorship (i.e. relevant parties that can engage each other as a positive influence).

5.3 miniCTF vs picoCTF

The WiCyS miniCTF highlighted a significant drop in completion rates for reverse engineering and binary exploitation challenges. So we decided to look at the most recent iteration of picoCTF (2021), and find any commonalities. To do this we looked at the five challenges that were present in both 2021 picoCTF (which is remote based) and 2021 WiCyS miniCTF (in person): Mod 26, Disk disk disk sleuth! II, Cache Me Outside, Rolling My Own, and Let's get dynamic.

Since 70% of the WiCyS miniCTF competitors were undergraduate females we only considered looking at the undergraduate female playerbase in the 2021 picoCTF.

The annual competition has a much higher number of high school students than university students, there were 2052 registered participants who identified as female in 2021 picoCTF, 17% (348) of who indicated they were undergraduate students.

There was a higher completion rate percentage in the conference miniCTF than picoCTF for all 5 challenges that were present in both. Details can be shown in **Table 3** above. The number of solves was lower for the annual event than for WiCyS for all challenges, even when accounting for a larger undergraduate female playerbase. The number of solves for each challenge were: Mod26 (189 solves), Disk disk disk sleuth! II (7 solves), Cache Me Outside (1 solve), Rolling My Own (0 solves), and Let's get dynamic (3 solves). Several alternative explanations (i.e. larger variety of challenges present, lower overall academic standing) exist, however we believe this secondary perspective should act as a signal for educators and academics alike to place emphasis on systems education.

# of (female undergraduate) solves	Mod 26	Disk disk disk sleuth! II	Cache Me Outside	Rolling My Own	Let's get dynamic
picoCTF	189 (54.3%)	7 (2.0%)	1 (0.2%)	0 (0.0%)	3 (0.8%)
miniCTF	124 (85.5%)	30 (20.6%)	20 (13.7%)	14 (9.6%)	15 (10.3%)

Table 5.1: Undergraduate Female Completion Rate in 2021 picoCTF vs 2021 miniCTF

6

Recommendations for Future Work

In this chapter I will provide an itemized set of recommendations for future research work. These recommendations will be based off of previous literature reviews, results and trends from interviews, and experiences while gathering data off of the picoCTF platform.

1. The effects of offline vs online collaboration and how it might promote engagement / factor into learning outcomes.

2. Explore the difference in skill acquisition between decentralized and centralized teams. Prior research has seen that players with varying levels of motivation will impact the team's outcome and success.

3. Explore the accuracy of pre-CTF/post-CTF confidence levels in retention.

4. We found there is much work needed to better asses how well CTFs motivate women and beginners to pursue a career in cybersecurity.

5. More work is needed to assess learning deficiencies in reverse engineering and binary exploitation categories (among males and females). One possible direc-

tion is developing challenges with a steady learning progression, or workshop development.

6. How to incentivize a variety of stakeholders to better support inclusive groups.

7. I had some difficulty combing through vast amounts of user data in the picoCTF platform, here are some feature development ideas that could be incorporated to better track engagement, participation, and retention:

    - Collect any user interactions with challenges (i.e. starting challenge instance, downloading a file, etc.)
    - For users that register around picoCTF, track engagement on picoGym before and after competition.
    - Data visualizations for a variety of metrics like demographics and completion rate.

7

Conclusion

In this Master's thesis we present the results of 13 semi-structured interviews and 207 female players from a CTF event we hosted at the 2021 WiCyS Conference. The interviews discussed their experiences in cybersecurity education and capture the flag events. This exploratory study aimed to identify motivations and barriers that have shaped their experiences in both CTFs and education, and identified CTF categories where female players struggle in comparison to their male couterparts. We learned that collaboration must be well structured, active, and in-person to help yield a positive CTF experience. This helps mitigate any negative environmental issues that players or students might have previously experienced. We discovered a significant drop in performance among Reverse Engineering and Binary Exploitation challenges, which highlights a need for future emphasis by educators on systems courses. However, CTFs overall have helped those broaden their knowledge of the field, and played a role in discovering core interests. Finally, we discussed recommendations that cybersecurity or educational organizations should consider when aiming to improve the cyber-talent pipeline, in addition to leaving possible directions of future research.

Bibliography

[1] [Online]. Available: https://www.isc2.org/Research/-/media/67B23A98D3A54E878FF927748D8F3EF1.ashx. [Accessed 03/25/22].

[2] M. Bashir, C. Wee, N. Memon, and B. Guo, "Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool," *Computers & Security*, vol. 65, pp. 153–165, 2017.

[3] A. A. Brenøe and U. Zölitz, "Exposure to more female peers widens the gender gap in stem participation," *Journal of Labor Economics*, vol. 38, no. 4, pp. 1009–1054, 2020.

[4] D. N. Burrell and C. Nobles, "Recommendations to develop and hire more highly qualified women and minorities cybersecurity professionals," in *International Conference on Cyber Warfare and Security*. Academic Conferences International Limited, 2018, pp. 75–81.

[5] S. J. Ceci, W. M. Williams, and S. M. Barnett, "Women's underrepresentation in science: sociocultural and biological considerations." *Psychological bulletin*, vol. 135, no. 2, p. 218, 2009.

[6] 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 and Management (SAM)*. Citeseer, 2011, p. 1.

[7] R. S. Cheung, J. P. Cohen, H. Z. Lo, F. Elia, and V. Carrillo-Marquez, "Effectiveness of cybersecurity competitions," in *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer . . . , 2012, p. 1.

[8] T. Chothia and C. Novakovic, "An offline capture the {Flag-Style} virtual machine and an assessment of its value for cybersecurity education," in *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, 2015.

[9] J. R. Cimpian, T. H. Kim, and Z. T. McDermott, "Understanding persistent gender gaps in stem," *Science*, vol. 368, no. 6497, pp. 1317–1319, 2020.

[10] V. Clarke, V. Braun, and N. Hayfield, "Thematic analysis," *Qualitative psychology: A practical guide to research methods*, vol. 222, p. 248, 2015.

[11] R. Coe, J. Searle, P. Barmby, K. Jones, and S. Higgins, "Relative difficulty of examinations in different subjects," *Report for SCORE (Science Community Supporting Education) CEM Centre, Durham University. http://www. iop. org/News/file_30371. doc last accessed*, vol. 19, pp. 05–10, 2008.

[12] J. W. Creswell and C. N. Poth, *Qualitative inquiry and research design: Choosing among five approaches*. Sage publications, 2016.

[13] A. Cuevas, E. Hogan, H. Hibshi, and N. Christin, "Observations from an online security competition and its implications on crowdsourced security," 2022. [Online]. Available: https://arxiv.org/abs/2204.12601. [Accessed 04/27/22].

[14] M. Dark, "Advancing cybersecurity education," *IEEE Security Privacy*, vol. 12, no. 6, pp. 79–83, 2014.

[15] D. R. Forsyth, *Group dynamics*. Cengage Learning, 2018.

[16] S. Goel, W. Mason, and D. J. Watts, "Real and perceived attitude agreement in social networks." *Journal of personality and social psychology*, vol. 99, no. 4, p. 611, 2010.

[17] T. Goodman and A.-I. Radu, "Learn-apply-reinforce/share learning: hackathons and ctfs as general pedagogic tools in higher education, and their applicability to distance learning," *arXiv preprint arXiv:2006.04226*, 2020.

[18] J. Himmelsbach, S. Schwarz, C. Gerdenitsch, B. Wais-Zechmann, J. Bobeth, and M. Tscheligi, "Do we care about diversity in human computer interaction: A comprehensive content analysis on diversity dimensions in research," in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 2019, pp. 1–16.

[19] J. S. House, "Social structure and personality," in *Social psychology*. Routledge, 2017, pp. 525–561.

[20] J. S. Hyde, S. M. Lindberg, M. C. Linn, A. B. Ellis, and C. C. Williams, "Gender similarities characterize math performance," *Science*, vol. 321, no. 5888, pp. 494–495, 2008.

[21] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Game based cybersecurity training for high school students," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 2018, pp. 68–73.

[22] T. Ladabouche and S. LaFountain, "Gencyber: Inspiring the next generation of cyber stars," *IEEE Security & Privacy*, vol. 14, no. 5, pp. 84–86, 2016.

[23] K. Leune and S. J. Petrilli Jr, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proceedings of the 18th Annual Conference on Information Technology Education*, 2017, pp. 47–52.

[24] A. Mann and T. A. DiPrete, "Trends in gender segregation in the choice of science and engineering majors," *Social science research*, vol. 42, no. 6, pp. 1519–1541, 2013.

[25] L. McDaniel, E. Talvi, and B. Hay, "Capture the flag as cyber security introduction," in *2016 49th hawaii international conference on system sciences (hicss)*. IEEE, 2016, pp. 5479–5486.

[26] J. Mirkovic and P. A. Peterson, "Class {Capture-the-Flag} exercises," in *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[27] S. L. Morgan, D. Gelbgiser, and K. A. Weeden, "Feeding the pipeline: Gender, occupational plans, and college major selection," *Social science research*, vol. 42, no. 4, pp. 989–1005, 2013.

[28] X. Mountrouidou, D. Vosen, C. Kari, M. Q. Azhar, S. Bhatia, G. Gagne, J. Maguire, L. Tudor, and T. T. Yuen, "Securing the human: a review of literature on broadening diversity in cybersecurity education," *Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education*, pp. 157–176, 2019.

[29] I. J. Raabe, Z. Boda, and C. Stadtfeld, "The social pipeline: How friend influence and peer exposure widen the stem gender gap," *Sociology of Education*, vol. 92, no. 2, pp. 105–123, 2019.

[30] J. Stern, E. Reid, and K. Bancroft, "Teaching introductory computer science for a diverse student body: Girls who code style," in *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, 2015, pp. 705–705.

[31] D. H. Tobey, P. Pusey, and D. L. Burley, "Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league," vol. 5, no. 1, p. 53–56, mar 2014. [Online]. Available: https://doi.org/10.1145/2568195.2568213.

[32] M. van der Vleuten, S. Steinmetz, and H. van de Werfhorst, "Gender norms and stem: the importance of friends for stopping leakage from the stem pipeline," *Educational Research and Evaluation*, vol. 24, no. 6-7, pp. 417–436, 2018.

[33] D. Votipka, E. Zhang, and M. L. Mazurek, "Hacked: A pedagogical analysis of online vulnerability discovery exercises," in *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021, pp. 1268–1285.

[34] J. Werther, M. Zhivich, T. Leek, and N. Zeldovich, "Experiences in cyber security education: The {MIT} lincoln laboratory {Capture-the-Flag} exercise," in *4th Workshop on Cyber Security Experimentation and Test (CSET 11)*, 2011.

Appendix A

Tables

P#	Industry Area	CTF Experience (years)	Degree Area	Highest Degree	Employment Status
P1	software/security engineering	3	Computer Science	Masters	full time
P2	risk and compliance, vulnerability management	3	Information Systems	Undergraduate	student
P3	information technology	4	Computer Science	Undergraduate	student
P4	teaching assistant,	3	Computer Science	Undergraduate	student
P5	SAP Security Administration	Education	Computer Science w/ specialization in cybersecurity	Masters	research internship,new grad seeking full time
P6	vulnerability management, education, incident response	2	N/A	Masters	full time
P7	vulnerability management	3	Cybersecurity - Information Assurance	Masters	full time
P8	information technology	2	Information Technology - Cybersecurity	Bachelors/Masters	part time,student
P9	education	<1	Information Technology - Cybersecurity	Masters	full time
P10	network admin	1	Information Technology - Information Security	Bachelors	seeking full time
P11	nurse	0	Healthcare	Masters	full time employed, part-time student
P12	project management, security engineer	<1	Information Technology	Masters	full time
P13	n/a	2	Cybersecurity with specialization in Enterprise Cloud Computing	Bachelors	student

Table 1.1: Background of 13 interview participants