# Investigating the Experiences of Female CTF Players

Antonio Martorana
*Carnegie Mellon University*

Emily Chang
*University of Virginia*

Hanan Hibshi
*Carnegie Mellon University*

Alejandro Cuevas
*Carnegie Mellon University*

## Abstract

There have been many efforts focused on improving the representation of women in cybersecurity. Capture-the-flag (CTF) platforms have become an attractive tool of choice to teach fundamental skills and spark interest in the profession. However, while most platforms aim to address the initial learning curve for newcomers, many do not focus on diversity and inclusivity as a goal. In this paper we present our results from interviews conducted with 13 CTF players and the performance results of 207 competitors from a CTF event hosted at a Women-focused conference for cybersecurity. The participants in this study consisted of individuals who solely identified as a woman. Our paper 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 cognitive skills. This work discusses some preliminary avenues for future research and offers suggestions to educators and organizers of CTF platforms.

## 1 Introduction

Over the past decade, many efforts within industry and academia have been proposed to address the lack of diversity in STEM. Narrowing the scope towards cybersecurity, as of 2021, only 24.9% of cybersecurity professionals identified as women [1, 2]. Many efforts to improve the representation of women in security-related fields have focused early in the education pipeline, as much research has demonstrated that career preferences are chosen around middle school and early high school levels. The introduction of gamified learning through capture-the-flag (CTF) competitions has been the tool of choice in promoting early interest in cybersecurity-related fields. [3].

CTFs have been successful in introducing students with little or no technical background to computer science and cybersecurity-related topics [4–6]. Additionally, CTF participation has shown positive trends in promoting security behavior, in addition to teaching participants about less intuitive exploits [7]. As a game-based learning mechanism, they promote engagement through competition, and learning through collaboration and hands-on activities.

Unfortunately, there has been little emphasis on increasing the participation and retention of women in CTFs. Modern approaches to CTF platforms only attempt to address the initial learning curve for newcomers, their effectiveness in teaching cybersecurity concepts, and thier ability to motivate individuals to pursue a cybersecurity career. While there has been upcoming work in this area, there has been a lack of evaluation and follow up to how various interventions affect individuals from underrepresented groups in CTFs. Consequently, it is unclear based on existing literature what underlying factors contribute to the low representation of women in CTFs. To gain some clarity in this area, we identified the following research questions to be addressed:

**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?

To address the research questions above, we organized an in-person CTF during the 2021 Women in Cybersecurity (WiCyS) Conference. We analyzed the performance of 207 participants who identified as a woman using statistics and data collected through the picoCTF platform. Then, we held follow-up semi-structured interviews with 13 CTF participants to provide insight into our research questions. During our interviews, we explored collaboration experiences, the early stages of pursuing a cybersecurity education or participating in CTFs, and skill progression. Participants in our

sample came from various career levels ranging from early undergraduate students to experienced professionals in various industries.

Our findings from interviews indicate that collaboration incentivized participants to work on challenges and persevere, especially during the later stages of CTFs or when progress was slow. We found that among many participants a combination of low confidence, lack of outreach, and lack of 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 playing CTFs was a primary resource used to build a broad domain of knowledge in cybersecurity and would help beginners/early-career professionals find their niche. An especially encouraging finding was that some participants noted hands-on labs or CTF-style assignments were already embedded within their university curriculum.

Driven by our findings, we present recommendations for CTF organizers and cybersecurity educators to consider. We also provide suggestions for future research directions to improve the retention of women in this area.

## 2 Related Work

In this section, we review related work on expanding diversity in cybersecurity, the role of CTFs in cybersecurity education, and the effect of peer proximity in STEM education.

### 2.1 Expanding Diversity in Cybersecurity

To address the growing shortage of cybersecurity professionals, universities, community colleges, and vocational programs have been tasked with educating and training more talent, particularly from diverse backgrounds. However, challenges persist in establishing high-quality cybersecurity educational programs that meet the needs of students from diverse backgrounds. These challenges adversely affect the recruitment and retention of many aspiring professionals in cybersecurity [8]. Bagchi-Sen et al. investigated the challenges and needs of women in cybersecurity who hold manegrial and higher-ranked roles [9].

To create a culturally responsive educational framework, Mountrouidou et al. recommend authentic and active learning techniques as well as empowering and mentoring students from underrepresented groups to engage and stay in cybersecurity. The authors specify gamification as an active learning technique that increases student confidence and enthusiasm towards the cybersecurity field. Conferences, such as the Grace Hopper Celebration of Women in Computing [10], and the Women in Cybersecurity (WiCyS) [11], create a supportive environment as they sponsor community forums, career fairs, and mentorship for women and underrepresented groups [1].

### 2.2 CTFs in Cybersecurity Education

One way of applying Gamification to cybersecurity education is through the use CTFs, which have been successful in introducing cybersecurity to students [12, 13]. As a team-based competition, students can leverage their teammates for knowledge and practice their collaboration skills, which are especially applicable in industry settings. In addition, CTFs have been good indicators of interest in pursuing a cybersecurity career [14]. The same studies have also questioned whether CTFs specifically motivate beginners to pursue cybersecurity careers or if they are best suited for reinforcing the interest of individuals with a depth of cybersecurity skills [14, 15]. Many studies looking to use CTFs to help improve gender diversity have acknowledged the lack of participation of students who identify as a woman and raised this as an important area of future work [15]. The lack of women participating in CTFs could cause a lack of diversity in the security and privacy workforce.

Poorly designed games have discouraged novices from participating [1], and further evidence by a study involving a GenCyber summer camp indicates that there are significant differences between the impressions of the games by students who identify as a man versus students who identify as a woman [4]. This suggests that women are less receptive to gamified learning than their male counterparts. 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, underscoring the importance of research in this area [1].

### 2.3 Peer Proximity in STEM Education

Vleuten et al. found evidence that gender normativity of class friends influences women's but not men's 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 [16, 17]. This study provides motive to explore conditions that enable more women to pursue a STEM career, such as one in cybersecurity.

This study raises the question: what are the effects of peers on retaining STEM careers? Peer exposure occurs when adolescent students adjust their preferences to those of their friends. Women demonstrate this characteristic in that they typically retain their STEM preferences when other girls in their classroom also enjoy STEM [18]. The researchers emphasize that social influence mostly came from same-sex friends. Since STEM classes still contain an overwhelming men-to-women ratio [19], it seems that a) increasing the presence of women in classrooms and b) similar gendered support groups are especially important when retaining students in STEM education.

## 3 Research Design

This exploratory research about the participant experience of women in CTFs adopts a hybrid (qualtiative and quantitative) approach. We interviewed competitors of the WiCyS Conference's miniCTF event. To draw insight and support findings from the interviews, we analyzed performance and demographic data from the miniCTF.

**Step 0: Capture-the-flag Competition Design.** As a CTF designed for beginners, the event primarly included easy and medium-difficulty challenges. Advanced challenges were included to provide a form of skill progression. Challenges were assigned difficulty based on input from experienced CTF players, challenge developers, and beginner-level testers. To provide an overview of cyber domains and build players' skillsets, we provided five categories that are in line with other CTFs: Cryptography, Web Security, Forensics, Reverse Engineering, and Binary Exploitation. The breakdown of challenge difficulty can be seen in **Table 1**.

**Step 1: Scoping and Interview Guide** To study the current CTF environment and identify potential barriers, we randomly selected 15 papers through keyword searches. We labeled all sections in those papers that explored gender diversity in relation to participation and retention, teamwork and collaboration, and peer proximity. We also labeled sections that indicated similar problems in cybersecurity, STEM education, and gaming. Those papers were used to help formulate our interviews questions, which can be found in the **Appendix**.

**Step 2: Interviews** We conducted 30-60 minute long semi-structured interviews with 13 participants from the WiCyS Conference. We show the demographics of the interview participants and their backgrounds in **Table 3**. Individuals filled out the consent form, participated in an in-person or Zoom interview, and were given gift cards for completing the interview and follow-up survey. Using Otter.ai [20], we transcribed all audio recordings. We reviewed and corrected transcriptions when necessary.

**Step 3: Qualitative Analysis** Since interviews were semi-structured, we segmented responses by interview question. These questions were grouped into subsets. To better understand various themes in our data, we qualitatively analyzed the responses of our 10 open-ended questions using thematic analysis. [21]. During open coding, we created an initial set of summaries, applied a preliminary set of codes, and collated these codes into a codebook. Using focused coding, we revisited the subset of questions to ensure our codes were applied consistently. At the end of this process, we systematically searched for relationships between emerging themes in our codebook and across interview questions.

To maintain inter-rater reliability, two researchers independently coded the remainder of the interviews and modified the codebook for new insights or to resolve disagreement. This process continued until all questions achieved a Cohen's Kappa score of $\kappa > 0.75$. Most questions achieved $\kappa > 0.8$, which is typically recommended for exploratory research [22].

**Step 4: Competition Analysis** We reviewed the completion rates across challenges and categories, attempt vs. success ratings, and demographic data of competitors (i.e. race, school level) of all 234 competitors at the CTF event. This gave us insight into measuring the actual difficulty of challenges versus the difficult assigned by a combination of developers, testers, and experienced CTF players. Further insight into skill acquisition within a category, and observing potential relationships between underrepresented groups and challenge completion.

### 3.1 Limitations

We describe below limitations of our research design.

#### 3.1.1 Research Sample

Because the conference encouraged more representation of women in cybersecurity, participants might have been educated on issues that minority groups in STEM encounter. Observations may be different if we had interviewed participants from a non-diversity-focused conference.

Self-selection of participants may also be an issue; male attendees more frequently declined an interview despite originally consenting to participate in the study.

Survivorship bias may also be present in our sample as some interviewees may have felt they were no longer making progress on CTF challenges and left during (or before) the CTF After Dark[1]. Thus, our sample pool might consist of more participants with an experienced background. The opinions of experienced individuals could differ greatly from novices.

While we tried to interview a sample with a diverse array of ages, educational experiences, and skill sets, we encountered difficulty recruiting those who did not have a degree or had joined the industry through alternative means. Due to the small sample size, we do not draw any statistical conclusions. Instead, we highlight trends to be explored in future work.

#### 3.1.2 Challenge Difficulty

Problem developers often assign the difficulty of each challenge based on their intuition and knowledge of various security concepts. Thus, problems are assigned a lower difficulty than the true rating. Similar issues exist when instructors or teachers develop exams [23]. Future work could consider using additional or alternative dynamic measurements to assign difficulty to problems, perhaps by the players themselves during the competition.

[1] 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

| 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 1: CTF Category and Challenge Overview

## 3.2 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 and participants are free to opt-out at any time.

# 4 Results

In this section we present our results. We will first discuss the role of collaboration in CTFs, since most CTFs rely on teams of players. Then, we highlight challenges and issues contributing to low participation in CTFs.

## 4.1 Impact of Collaboration in CTFs

Teams tended to place depth and specialization at the core of their decision-making processes. Specialization ranges from group formation to task distribution. Defined roles enabled players to learn from senior members and distributed accountability to members. 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 [24].

### 4.1.1 Shadowing and Exposure

A frequent talking point among participants (P2,P3,P4,P6, P7,P9,P11,P13) was the opportunity to shadow more experienced CTF players who often had a diverse set of tools and background knowledge. These experienced players came from similar backgrounds and were mentors who could address the unique obstacles (professional and personal) mentees might encounter. Pariticpants stated that mentorship early on would help with technical, communication, and professional networking skill growth.

### 4.1.2 In Person vs Remote Collaboration

Some participants expressed that remote sessions were used for (1) knowledge transfer or (2) status updates. 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.

In-person teamwork was a potential mitigation to burnout. P2 stated that when they got frustrated early on, working with others would motivate them to put more hours into a CTF. This suggests that in-person collaboration provides motivation to try new approaches and contribute to the group's overall knowledge. In-person collaboration offers a chance to grow professional networks as well as enjoy downtime with teammates. To this end, in-person events present an opportunity to increase participation and retention in CTFs.

### 4.1.3 Team Structure

For some participants (P1,P2,P3,P9), team structures were decentralized and individuals were free to take on any problem. Others (P13,P11,P8,P7,P4,P6) adopted a hierarchical structure where team leaders delegated problems or categories to players based on their experience level.

The hierarchical structure was preferred. P6 mentioned that structure and active participation were deciding factors in choosing to work with a team. Moreover, structure enabled accountability: when directly assigned tasks, players remained engaged during parts of the competition. This level of team cohesiveness promoted an inclusive culture among teammates.

## 4.2 Issues that may Contribute to Low CTF Participation

Now we present results from our interviews that highlight issues that could contribute to low participation of women in CTFs.

| 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 2: Completion Rate per Challenge and by Category

| P# | Industry Area | CTF Exp. (Yrs) | Degree Area | Highest Degree | Employment Status |
|---|---|---|---|---|---|
| P1 | Software/sec. engineering | 3 | Computer Science | Masters | FT |
| P2 | Risk & Compliance, Vuln. Mgmt. | 3 | Information Systems | Undergraduate | FT |
| P3 | Computer Science | 4 | Computer Science | Undergraduate | Student |
| P4 | Computer Science | 3 | Computer Science | Undergraduate | Student |
| P5 | SAP Security Administration | - | CS w/ spec. in Cybersecurity | Masters | New Grad |
| P6 | Vuln. Mgmt., Incident Resp. | 2 | N/A | Masters | FT |
| P7 | Vuln. Mgmt. | 3 | Cybersec. Inf. Assurance | Masters | FT |
| P8 | Information Technology (IT) | 2 | IT - Cybersecurity | Bachelors/Masters | PT Student |
| P9 | Education | <1 | IT - Cybersecurity | Masters | FT |
| P10 | Network Admin | 1 | IT - InfoSec | Bachelors | Seeking FT |
| P11 | Nurse | 0 | Healthcare | Masters | FT Job, PT Student |
| P12 | Project Mgmt., Sec. Engineer | <1 | Generalist IT | Masters | FT |
| P13 | Information Technology (IT) | 2 | Cybersec. & Enterprise Cloud C. | Bachelors | Student |

Table 3: Background of 13 interview participants

#### 4.2.1 Outreach

Twelve of 13 participants discovered CTFs through second-hand sources and/or through their own research. These participants already had developed an interest in cybersecurity and were proactive in their growth. This suggests that players who were sufficiently motivated were more likely to find and compete in CTFs.

In the final follow-up question, we asked participants how outreach to CTFs or cybersecurity could be improved. Some participants (P5,P11,P13) reported that representation in cybersecurity and CTFs was improving but the growth was slow. P1 mentioned that preexisting inequalities in computer science trickle down into sub-disciplines like cybersecurity or machine learning. Thus, the participation of women in CTFs and the cybersecurity workforce is traditionally low.

#### 4.2.2 Confidence and Uncertainty

A common consensus among nine participants (P1,P3,P4,P6,P7,P8,P9,P10,P12) was the notion that cybersecurity, and by extension CTFs, seemed more complex to break into. 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 [25].

Some participants admitted that they were not confident in their abilities. 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 belief of one's own ability to complete a task in cybersecurity [14]. Much of the anxiety to perform well in a competitive environment could possibly raise doubts about one's ability to succeed in the profession.

#### 4.2.3 Resources

Participants (P3,P6,P7,P8,P9,P10,P12,P13) highlighted a need for more resources for beginners. Beginners are often left to discover the vast amount of tools and information on their own. While competition organizers recommend that players work collaboratively, such an option disregards individuals who cannot find a team or prefer to work independently. The early struggle in a CTF may demotivate players, causing them not to participate 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 [15]. Many participants provided suggestions for increased mentorship via tutors or industry professionals and more technological resources to help those from low-income communities.

### 4.3 Building Cyber-related (1337) Skills

In the gaming community, "1337" means an extremely skilled player, and the term originated in the hacking community. Hence we ask participants a set of questions to understand how they advanced their cybersecurity and/or hacking skills. Six of the 13 participants (P5,P6,P7,P8,P12,P13) reported gaining exposure to a variety of cybersecurity skills such as in forensics, cryptography, and reverse engineering. In addition, participants reported gaining 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.

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 lack of clarity leads to repeated exposure to failure and the need to frequently reevaluate an exploit/defense strategies. P13 said these types of investigative skills are important *"[...] because you need to lose your fear of being wrong and...it can give you an idea of whether or not you want to be that analyst or engineer"*. This insight applies well to industry in a variety of settings where threat actors and exploits are adaptive, and vulnerabilities are unknown.

## 5 miniCTF Analysis

We observed the overall completion rate per category for 234 competitors, which was calculated using the equation:

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

We looked at the completion rate per challenge which was calculated using this equation:

$$CR = \frac{\#\ of\ correct\ submissions}{\#\ of\ participants\ who\ identify\ as\ a\ woman}$$

The results of these calculations can also be found in **Table 2**. We see a low amount of completion and correct solutions in the Reverse Engineering and Binary Exploitation categories. Given the present sample size, we cannot determine the exact reason but possibilities include tiredness, lack of interest, and expected vs. actual challenge difficulty.

## 6 Discussion

We summarize the results of our exploratory study into three takeaways that we discuss below: improving CTF attractiveness, the community dilemma, and focusing on systems education.

### 6.1 Improving CTF Attractiveness

Participants (P1,P3,P7,P8,P11,P13) stated we should focus on two goals: targeted outreach and early intervention.

Participants outlined the need to adapt how CTF platforms and cybersecurity are presented to students who identify as a woman. Generic methods are not enough, the message needs to resonate with the individuals targeted by outreach. Existing literature already supports this notion [26].

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 in their future careers [27]. For example P13 shared that it has to be *"fashionable...I [asked] my [three-year-old] nieces 'let's take apart a hard drive!' [They are] totally down, because they didn't think this is a gender activity...As soon as they've hit puberty, that's a little bit different"*. There are existing initiatives in place for introductory programming such as Girls Who Code [28]. Future work could investigate how CTFs can resonate with students who identify as a woman.‘

### 6.2 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. The broad set of sub-disciplines and interdisciplinary nature of the cyber field caused many participants 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 underrepresented backgrounds. However, this may not always be plausible due to geographical location, lack of awareness in diversity by other women, or bias and 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. a community like WiCyS or university club) to recruit women.

Who then becomes responsible for facilitating this intervention? This dilemma could be solved by accelerated partnerships and research from industry and academia respectively. We recognize the incentive to put in additional resources

| # of (undergraduate women) solves | Mod 26 | Disk disk disk sleuth! II | Cache Me Outside | Rolling My Own | Let's get dynamic |
|---|---|---|---|---|---|
| Annual CTF | 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 4: Completion Rate of Undergraduate Women in 2021 picoCTF vs 2021 miniCTF

may be difficult. 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).

### 6.3 Systems Education

Because the WiCyS miniCTF highlighted a significant drop in completion rates for reverse engineering and binary exploitation challenges, we investigated commonalities in picoCTF 2021 public competition that included participants from around the world. 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 at the WiCyS 2021 conference): Mod 26, Disk disk disk sleuth! II, Cache Me Outside, Rolling My Own, and Let's get dynamic.

While 70% of the WiCyS miniCTF competitors were undergraduate women, the annual competition had a much higher number of high school students than university students.

There was a higher completion rate percentage in the conference miniCTF than picoCTF for all 5 challenges that were present in both. Details are shown in **Table 4**. Several alternative explanations (i.e. larger variety of challenges present, lower overall academic standing) exist. We believe this secondary perspective should act as a signal for educators and academics alike to place emphasis on systems education.

## 7 Conclusion

In this paper we present the results of 13 semi-structured interviews and 207 players who identify as a woman from a CTF event we hosted at the 2021 WiCyS Conference. The interviews discussed their experiences in cybersecurity education and CTFs. This exploratory study aimed to identify motivations and barriers that have shaped their experiences in both CTFs and education, and identified CTF categories where players who identify as a woman struggle. 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. In diversifying the workforce, such an observation is applicable to the security and privacy industries.

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 broaden competitors' knowledge of the field and played a role in discovering core interests. Finally, our work provides directions for future research, and recommendations that cybersecurity or educational organizations may consider when aiming to improve the cyber-talent pipeline.

## 8 Acknowledgements

We would like to thank our study participants and the WiCyS organizers. In addition, we thank Dianelys Soto-Cruz, Hugrun Hannesdottir, and Sara B. Schwarz who helped run the CTF at WiCyS and gave a tutorial during the conference to introduce CTFs. This work is funded by Cisco Systems Inc. through award # 1012353 and 78068415.

## References

[1] Xenia Mountrouidou, David Vosen, Chadi Kari, Mohammad Q Azhar, Sajal Bhatia, Greg Gagne, Joseph Maguire, Liviana Tudor, and Timothy 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*, pages 157–176, 2019.

[2] ISC [2]. Women in cybersecurity: Young, educated and ready to take charge, Accessed March 2022. URL: https://www.isc2.org/Research/-/media/67B23A98D3A54E878FF927748D8F3EF1.ashx.

[3] Tina Ladabouche and Steve LaFountain. Gencyber: Inspiring the next generation of cyber stars. *IEEE Security & Privacy*, 14(5):84–86, 2016.

[4] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, pages 68–73, 2018.

[5] Kees Leune and Salvatore 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*, pages 47–52, 2017.

[6] Tom Chothia and Chris 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.

[7] Daniel Votipka, Eric Zhang, and Michelle L Mazurek. Hacked: A pedagogical analysis of online vulnerability discovery exercises. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1268–1285. IEEE, 2021.

[8] Darrell Norman Burrell and Calvin Nobles. Recommendations to develop and hire more highly qualified women and minorities cybersecurity professionals. In *International Conference on Cyber Warfare and Security*, pages 75–81. Academic Conferences International Limited, 2018.

[9] Sharmistha Bagchi-Sen, H. R. Rao, Shambhu J. Upadhyaya, and Sangmi Chai. Women in cybersecurity: A study of career advancement. *IT Professional*, 12(1):24–31, 01 2010.

[10] About grace hopper celebration of women in computing, Accessed August 2023. URL: https://ghc.anitab.org/about/.

[11] Our Story | WiCyS - Women in Cybersecurity, Accessed August 2023. URL: https://www.wicys.org/about/our-story/.

[12] Ronald S Cheung, Joseph P Cohen, Henry Z Lo, and Fabio Elia. Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1. Citeseer, 2011.

[13] Joseph Werther, Michael Zhivich, Tim Leek, and Nickolai 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.

[14] Masooda Bashir, Colin Wee, Nasir Memon, and Boyi Guo. Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, 65:153–165, 2017.

[15] David H. Tobey, Portia Pusey, and Diana L. Burley. Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. 5(1):53–56, mar 2014. doi:10.1145/2568195.2568213.

[16] Maaike van der Vleuten, Stephanie Steinmetz, and Herman van de Werfhorst. Gender norms and stem: the importance of friends for stopping leakage from the stem pipeline. *Educational Research and Evaluation*, 24(6-7):417–436, 2018.

[17] Anne Ardila Brenøe and Ulf Zölitz. Exposure to more female peers widens the gender gap in stem participation. *Journal of Labor Economics*, 38(4):1009–1054, 2020.

[18] Isabel J Raabe, Zsófia Boda, and Christoph Stadtfeld. The social pipeline: How friend influence and peer exposure widen the stem gender gap. *Sociology of Education*, 92(2):105–123, 2019.

[19] Joseph R Cimpian, Taek H Kim, and Zachary T McDermott. Understanding persistent gender gaps in stem. *Science*, 368(6497):1317–1319, 2020.

[20] Otter.ai - Voice Meeting Notes & Real-time Transcription, Accessed October 2022. URL: https://otter.ai/.

[21] Victoria Clarke, Virginia Braun, and Nikki Hayfield. Thematic analysis. *Qualitative psychology: A practical guide to research methods*, 222:248, 2015.

[22] Mary L McHugh. Interrater reliability: the kappa statistic. *Biochemia medica*, 22(3):276–282, 2012.

[23] Robert Coe, Jeff Searle, Patrick Barmby, Karen Jones, and Steve 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*, 19:05–10, 2008.

[24] Alejandro Cuevas, Emma Hogan, Hanan Hibshi, and Nicolas Christin. Observations from an online security competition and its implications on crowdsourced security. *arXiv preprint arXiv:2204.12601*, 2022.

[25] Ronald S Cheung, Joseph Paul Cohen, Henry Z Lo, Fabio Elia, and Veronica Carrillo-Marquez. Effectiveness of cybersecurity competitions. In *Proceedings of the International Conference on Security and Management (SAM)*, page 1. The Steering Committee of The World Congress in Computer Science, Computer . . . , 2012.

[26] Julia Himmelsbach, Stephanie Schwarz, Cornelia Gerdenitsch, Beatrix Wais-Zechmann, Jan Bobeth, and Manfred 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*, pages 1–16, 2019.

[27] Melissa Dark. Advancing cybersecurity education. *IEEE Security Privacy*, 12(6):79–83, 2014. doi:10.1109/MSP.2014.108.

[28] Jeff Stern, Emily Reid, and Kari 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*, pages 705–705, 2015.

# A Interview Questions

Interviews were conducted by one interviewer. Each interview was audio recorded, with permission from the research participant.

1. What background best describes you?
    - Computer Science
    - Information Systems
    - Electrical and Computer Engineering
    - Information Technology or Information Security
    - Other
2. Have you taken cybersecurity in a classroom environment?
    (a) If yes:

i. Type of classroom experience (university classes (in-person/online), workshops, seminar, etc.)
ii. Describe some of the assignments (assignments, on labs, individual/group projects)?
iii. Describe your experience in the classroom.
iv. Describe interactions with your peers, TAs, faculty.

(b) If no:

i. How did you go about learning cybersecurity?
ii. Describe what you wanted to learn and why(i.e. motivations, particular subjects, resources).

3. Describe some of your professional experiences.

- Cybersecurity
- Other STEM Field (non - Cyber)
- Non - STEM Field

(a) Did you work within a team environment?

i. If so, describe some of the team dynamics:
- Mentor? Primary contacts if you had a question or needed help. Are you a manager or a lead? [Follow ups]
- Team structure.

(b) Describe your work environment.

i. What is your role within the team? Day - to - day duties.
ii. Company/organizational/department culture.
iii. Diversity and Inclusion (D&I) Goals

4. Do you participate in CTFs?

(a) If yes:

i. Did you discover the game on your own or were introduced to it? If not on your own, who mentioned it/introduced it to you?
ii. How long have you been playing?
iii. What are your favorite types of challenges?
iv. Do you participate in CTFs within a community (i.e. clubs, professional network, online community) or group of friends?

A. If with a group or team describe:
- Team structure
- How are problems delegated?
- Knowledge transfer protocol or meetings?
- Are team sessions planned/spontaneous?
- How do you communicate (i.e. platforms such as Discord, Zoom, Slack, Teams, etc.)?

B. Advantages and potential disadvantages of group or team play?
C. Have you participate in CTFs on your own?
D. How do you approach difficult challenges?
E. Advantages and potential disadvantages of group or team play?

v. How has your knowledge of cybersecurity and career interests progressed with each CTF?
vi. New strategies? Technical or non-technical skills? Favorite or non-favorite categories?
vii. How have you approached increasingly difficult challenges?
viii. Describe some of the CTFs you have liked and disliked? What did they do or could have done better?

(a) If no:

i. Any reason in particular?
ii. What factors would have to be satisfied so that you would participate?

5. What advice would you give someone who wanted to get involved in cybersecurity or learn more about it?

6. From your personal experience, what barriers are there for women or other minorities in cybersecurity/STEM fields?

## B Coding Statistics

| Question | Column | Cohen's Kappa | p-value | Percent Agreement |
|---|---|---|---|---|
| | who | 0.859 | 0.000152 | 92.3 |
| | what | 0.902 | 6.5710-11 | 92.3 |
| | when | 1 | 3.1310-8 | 100 |
| 4A | how | 0.823 | 0 | 92.3 |
| | improved | 0.825 | 3.3510-5 | 92.9 |
| | growth_rate | 0.896 | 7.4410-8 | 92.9 |
| | growth | 0.889 | 5.5910-11 | 92.9 |
| 4E | approach | 0.848 | 0 | 85.7 |
| | play_style | 1 | 0.000311 | 100 |
| | team_benefit | 1 | 1.5410-13 | 100 |
| | structure | 0.813 | 9.6710-12 | 84.6 |
| | motivational_type | 1 | 8.9710-8 | 100 |
| 4F | platform | 0.885 | 6.1310-10 | 92.3 |
| | outreach | 1 | 1.7310-14 | 100 |
| | education | 0.809 | 1.0910-12 | 84.6 |
| 6 | information | 0.914 | 0 | 92.3 |
| | factors | 0.832 | 0 | 84.6 |
| | rejected_views | 1 | 2.9210-6 | 100 |
| 7 | information | 1 | 0.000311 | 100 |
| 8 | barriers | 0.832 | 0 | 84.6 |

Table 5: Cohen's Kappa and Percent Agreement of Two Raters