Vulnerability Discovery for All: Experiences of Marginalization in Vulnerability Discovery

Kelsey R. Fulton*, Samantha Katcher†, Kevin Song‡, Marshini Chetty‡, Michelle L. Mazurek*, Chloé Messdaghi⋆, and Daniel Votipka†
*University of Maryland, †Tufts University, ‡University of Chicago, and ⋆Stand Out in Tech

Abstract

Vulnerability discovery is an essential aspect of software security. Currently, the demand for security experts significantly exceeds the available vulnerability discovery workforce. Further, the existing vulnerability discovery workforce is highly homogeneous, dominated by white and Asian men. As such, one promising avenue for increasing the capacity of the vulnerability discovery community is through recruitment and retention from a broader population. Although significant prior research has explored the challenges of equity and inclusion in computing broadly, the competitive and frequently self-taught nature of vulnerability discovery work may create new variations on these challenges. This paper reports on a semi-structured interview study (N = 16) investigating how people from marginalized populations come to participate in vulnerability discovery, whether they feel welcomed by the vulnerability discovery community, and what challenges they face when joining the vulnerability discovery community. We find that members of marginalized populations face some unique challenges, while other challenges common in vulnerability discovery are exacerbated by marginalization

1 Introduction

As organizational reliance on technology — and incidence of cyberattacks from both criminal and nation-state attackers — continues to increase, so does demand for security review, intended to ensure early identification and mitigation of vulnerabilities. The White House's recent executive order on Improving the Nation's Cybersecurity, which emphasizes "modernizing federal government cybersecurity" and "enhancing software supply chain security" as priorities, highlights the need for improved vulnerability discovery capabilities [2].

To scale up vulnerability review, organizations adopt varying approaches, including internal security expert review, hiring penetration testers, and offering bounties—money, swag, or recognition—for responsible vulnerability disclosure [18, 24]. We refer to people working in these roles generally as the vulnerability discovery workforce and vulnerability discovery community, and individually as hackers.

Unfortunately, while the number of hackers has grown, the diversity of the vulnerability discovery workforce remains limited. In a survey of 3,493 hackers on their platform, Bugcrowd found they were almost all male (94%) and white or Asian[1] (90%), with few participants self-reporting as female (6%), Latinx (3%), or African American (3%) [4]. This is a common trend in hacker surveys [19]. Additionally, the vulnerability reports produced by the vulnerability discovery community are typically dominated by a few highly-active participants [3, 12, 17, 27], meaning that in practice there is very limited diversity of perspectives in security reviews. Further, a recent hacker survey by Synack found participants from marginalized populations were less likely to feel they belong in the vulnerability discovery workforce [31], indicating there are challenges for members of marginalized populations not only in joining the vulnerability discovery workforce, but also in remaining active participants.

This lack of diversity indicates an equity problem: limited opportunities for people from marginalized populations to participate in bug bounties and/or to transition into in-demand careers in information security more broadly. The lack of diversity is also a problem for vulnerability discovery as a field: many eyes with varied perspectives are necessary to avoid blindspots and discover as many potential vulnerabilities as possible before a malicious party does [23].

Of course, struggles to diversify the workforce are not unique to vulnerability discovery; this is a long-running chal-

USENIX Symposium on Usable Privacy and Security (SOUPS) 2022.
August 7–9, 2022, Boston, MA, United States.

[1] We define Asian broadly, as Bugcrowd did, but we recognize Asian-Americans remain marginalized in the vulnerability discovery community

lenge facing science, technology, engineering, and mathematics (STEM) disciplines in general [29] and computer science in particular [26]. There has been significant effort to understand [7, 8, 25] and mitigate [6, 13, 30] barriers to entry into these fields. However, we expect that some characteristics of vulnerability discovery will lead to unique instantiations of these common challenges, making it worthwhile to study separately. The inherently competitive nature of vulnerability discovery (i.e., only the first person to identify a vulnerability is rewarded) is likely to dissuade newcomers, potentially reifying existing inequalities [1, 14, 22, 26, 29].

As a first step to address this gap in the literature, we conducted 16 semi-structured interviews with members of the vulnerability discovery community from marginalized populations. We asked participants to describe their work and personal identity and then walk us through their career in vulnerability discovery. During this walkthrough, we asked them to describe resources they used (both helpful and unhelpful), mentors they had, and their interactions within the vulnerability discovery community. Through these interviews, we aimed to answer three main research questions:

R1: How do people from marginalized populations come to participate in vulnerability discovery?

R2: Do people from marginalized populations feel accepted and supported by the broader vulnerability discovery community?

R3: What challenges do people from marginalized populations face in becoming a vulnerability researcher and participating in the workforce?

We find that most of our participants found the field on their own and learned about it using primarily unstructured resources, independently and outside of work hours. While our participants considered mentors critical to navigating this learning process and making community connections, many reported that without a pre-existing job in vulnerability discovery, mentors can be difficult to find.

While not all of the challenges our participants faced were unique to members of marginalized populations, most were exacerbated by minority status and structural disadvantages (e.g., gender wage gaps). Further, we identified some challenges unique to people from marginalized groups, often related to discrimination and impostor syndrome. Drawing on our findings, we offer recommendations for lowering barriers to entry and cultivating an inclusive environment.

2 Background & Related Works

Surveys of participation and motivation In SynAck's short, informal Cybersecurity Diversity and Inclusion survey, 300 participants were asked about feelings of belonging in the community and challenges faced in entry and participation. This survey showed marginalized populations were significantly more likely to feel excluded from the vulnerability discovery community and more likely to believe there was a glass ceiling on their success. Our work investigates these results in detail to understand why these feeling of otherness exist in marginalized populations and identify specific challenges faced [31].

Interviews with security experts about development and culture Most related to our research are two hacker interview studies. First are Turkle's ethnographic studies of early hacker culture at the Massachusetts Institute of Technology in the 1980s [32, pg. 183–218]. Turkle observed how security experts in this community operated together and how new individuals joined the community. She found an insular culture of perceived differentness in this community that required others to demonstrate their worth and fit prior to joining the group. The world and vulnerability discovery itself has changed dramatically since Turkle's work. The Internet is now an integral part of many people's daily lives and vulnerability discovery itself has become more accessible and acceptable through the ever-growing adoption of bug bounty programs, possibly altering the counter-culture and insular ethos of this community. Our work investigates the impact of these changes in modern vulnerability discovery with a focus on marginalized populations.

3 Method

To understand the experiences of marginalized populations in vulnerability discovery, we conducted semi-structured interviews with members from the vulnerability discovery community who also identified as members of marginalized populations. We interviewed participants until we stopped hearing substantially new ideas, resulting in a total of 16 participants [5]. This approach was validated when no new codes were created when analyzing the final 5 participants. This sample size aligns with qualitative best practices [15].

Once interviews were complete, we used an automated transcription service to transcribe the audio recordings. After transcription, two researchers cooperatively coded the interviews using iterative open coding [10]. The study was approved by the University of Maryland, Tufts University, and University of Chicago institutional review boards. We obtained informed consent before the pre-screening survey and again before the interview. Given the personal and sensitive nature of the questions we asked, we informed every participant that they could skip a question or stop the interview at any time.

4 Results

This section details challenges faced by our participants when joining and continuing in the vulnerability discovery community. Specifically, we discuss challenges unique to marginal-

ized populations and those common to all members of the vulnerability discovery community, but exacerbated by participants' marginalized identity. For brevity, we do not report here on participants path into vulnerability discovery or positive experiences in the vulnerability discovery community.

4.1 Challenges unique to marginalized populations

Participants identified challenges unique to marginalized populations; most center on navigating and feeling unwelcome in the community with their marginalized identity.

Difficulty being taken seriously Some participants felt, when interacting with other security experts, they were not taken seriously (N = 4). When discussing a hacking group meetup she attended, P5 said "*When I talked to people, I could tell they weren't taking me seriously... they saw me and were like, 'What is she doing? What's she trying to do here?'*"

Reluctance to share information Participants also mentioned difficulty acquiring information from others in the community (N = 6). When trying to learn new things, several participants mentioned it seemed like other security experts did not want to share information. Our participants reported working extra hard to get the training and support that was more readily shared with their less marginalized colleagues.

Unwelcoming environments While representation, and diverse work groups in general, helped our participants feel welcome, the lack thereof had the opposite effect (N = 6). For example, when asked to discuss whether she felt welcomed in the community, P13 describes "*The first time that I went to one of [this hacking organization's] networking events, I was appalled because I didn't see anybody like me, I didn't see very many women of color, or anything.*" Some participants (N = 3) avoid interacting with the community altogether due to negative prior experiences and fear of rejection.

Discrimination Perhaps most alarming is the discrimination faced by our participants. Our participants mentioned experiencing sexism (N = 8), racism (N = 3), sexual assault (N = 3), transphobia (N = 2), and homophobia (N = 1) either directed at themselves or someone close to them.

Our participants also faced discrimination that was less explicit. P15, an African American woman describes: "*They have other interns that came in. And I felt that those interns were, they like called on them more. But I can't say for a fact that it was because they were different color.*" These experiences caused our participants to feel a sense of otherness and rejection from the community.

Participants experienced enough discrimination that they had explicit coping mechanisms to avoid facing discrimination when joining and interacting with other hackers. Participants reported selecting online usernames to provide anonymity (N= 3) to avoid any discrimination.

4.2 Challenges exacerbated for marginalized populations

Not all the challenges participants faced were unique to marginalized populations. In particular, when first starting out in vulnerability discovery, they often faced challenges many or all new members of the community face. However, these challenges are often exacerbated for marginalized populations because of the inequalities that they suffer within and outside of the vulnerability discovery community.

Structure of learning materials and resources One example that may affect people new to vulnerability discovery is that learning resources often assume students come with a technical background (N = 3). While this challenge is not unique to marginalized populations, it can be especially harmful given that this assumption can worsen members' already existing feeling of otherness. One way to overcome this challenge is through support from more experienced members in the community. However, as described in Section 4.1, our participants reported being less likely to have this support. Our participants also noted that the inherent unstructured nature of the learning materials posed a similar challenge (N = 4).

Lack of opportunities Another challenge reported by our participants was the lack of attainable entry-level positions and opportunities (N = 3). While finding entry level positions can be challenging for all vulnerability discovery community members, it is especially difficult for members of marginalized communities, as echoed in the SynAck survey [31].

The lack of entry-level positions creates a secondary effect: making finding mentors harder (N = 5). Most of our participants found their mentors through a work position. While helpful mentors are essential to the success of every member of the vulnerability discovery community, they play a pivotal role for members of marginalized populations: Our participants overwhelmingly reported that having a mentor was essential in helping them navigate imposter syndrome pertaining to their membership in the vulnerability discovery community. This imposter syndrome is often exacerbated by the discrimination they faced within the community [16].

These factors interrelate and exacerbate each other in a vicious cycle: discrimination and imposter syndrome can make members of marginalized populations feel unqualified and therefore less likely to apply for an entry-level job, thus excluding them from the most likely source of mentorship, and therefore from a resource that could help to combat the discrimination and imposter syndrome.

Unhelpful mentoring Participants also reported unhelpful and unsupportive mentors as a key challenge they faced (N = 5). We expect the presence of unhelpful mentors is not unique to members of marginalized communities and is a prevalent problem within the vulnerability discovery community. However, the encouragement to mentor minorities through special funding [9, 28], special awards [11, 21], or workplace requirements incentivizes "token mentoring" within the community and leads to an overwhelming increase of "bad" mentoring for members of marginalized communities. Our participants noted that the existence of workplace requirements to mentor new employees resulted in being mentored by unwilling mentors, thus resulting in a negative mentorship experience that further exacerbated their existing imposter syndrome and inequities. P17 notes that they were "*promised mentorship*" at a new job, but their provided mentor "*felt threatened by their presence*," so they "*didn't quite get along quite well. So trying to work with him and trying to learn from him, it wasn't there.*" Further, research suggests that members of marginalized communities in many fields are often mentored differently, and less effectively, than their less marginalized colleagues [20].

Lack of awareness Participants felt their lack of knowledge about vulnerability discovery as a career option contributed to their difficulty in getting involved (N = 6). P2 mentioned they "*did [vulnerability research] as a hobby" because they had "no notion that there existed a career option. Other than if you successfully hacked some big company, they might hire you to become a security person. Which I didn't think was that likely to work out.*" This lack of awareness can be further aggravated by the fact that members of marginalized populations are actively dissuaded from joining vulnerability discovery as described in subsection 4.1.

Uncertainty and resilience Uncertainty is inherent in vulnerability discovery. Effort analyzing a target may not pay off, as the security expert may not find a bug, or another security expert may "scoop" a bug before it is submitted. Ambiguity in bug bounty programs also contributes uncertainty, as the security expert may have to argue with bounty managers about the bug's existence or value. Participants cited frustration with this uncertainty about bug acknowledgement as one factor dissuading them from participation in the field (N = 5). P7, for example, joined a bug bounty program, but "*then I realized they don't really want to pay for it. You know, it's like, oh, we'll give you this much money. Just kidding [they backed out]. It was informational.*"

While this need for resilience applies throughout the vulnerability discovery community, it may be particularly challenging for members of marginalized populations who have less community support and face frequently hostile environments, as described above.

5 Recommendations

The unique and exacerbated challenges faced by members of marginalized populations in vulnerability discovery point to the need for improvements in community support. In this section, we conclude with recommendations for making these community improvements.

Mentoring members of marginalized populations Our results suggest mentoring can be critical to help members of marginalized populations succeed in vulnerability discovery, but quality mentoring is not always simple to achieve. Simply creating programs to encourage mentoring for marginalized populations can lead to instances of unhelpful, even "token" mentoring. This accords with prior work finding that members of marginalized populations, specifically women, are often mentored differently than less marginalized populations. In their work, Ibarra et al. find women are often over-mentored and under-sponsored: sponsors not only provide advice but actively work to advocate for their mentees and recommend them for new opportunities [20]. Mentors in the vulnerability discovery community should keep this distinction in mind; many of our participants indicated that their most successful mentoring experiences involve this kind of sponsorship. We recommend that programs designed to promote mentoring explicitly consider how to incorporate sponsorship.

Helping mentees reach mentors Finding a mentor and building a relationship over time is not always easy. We suggest that the vulnerability discovery community invest in creating systems that help facilitate mentoring for members of marginalized populations. A mentor matching system, in which people who are comfortable disclosing demographic information that identifies them as a member of marginalized populations self-select interests or needs could be beneficial. This one-on-one mentoring could allow new members to be matched with mentors and allow for sponsorship. If both parties opt in, such a system could specifically match mentors and mentees who are both from marginalized populations, offering a mentor who understands some of the specific challenges the mentee is likely to face. We note this does not mean the mentor and mentee have to be from the same marginalized population, as our results suggest mentees feel welcomed when a broad diversity is represented in the community.

Forming affinity groups with care One strategy that has been used to help marginalized populations in STEM generally has been to create various affinity groups, such as Women in Cybersecurity. However, our results suggest this approach needs to be undertaken with care. It is important not to rely on affinity groups to solve structural problems that must be tackled by people who already have representation and power.

References

[1] Lecia Jane Barker, Kathy Garvin-Doxas, and Michele Jackson. Defensive climate in the computer science classroom. In *Proceedings of the 33rd SIGCSE Technical Symposium on Computer Science Education*, SIGCSE '02, pages 43–47, New York, NY, USA, 2002. Association for Computing Machinery.

[2] Joseph Biden. Executive order on improving the nation's cybersecurity, May 2021. (Accessed 07-21-2021).

[3] Bugcrowd. The state of bug bounty. Technical report, Bugcrowd, June 2016.

[4] BugCrowd. Inside the mind of a hacker 2020, 2020. (Accessed 07-21-2020).

[5] Kathy Charmaz. *Constructing grounded theory: A practical guide through qualitative analysis*. sage, 2006.

[6] Sapna Cheryan, Allison Master, and Andrew N Meltzoff. Cultural stereotypes as gatekeepers: Increasing girls' interest in computer science and engineering by diversifying stereotypes. *Frontiers in psychology*, 6:49, 2015.

[7] Sapna Cheryan, Victoria C Plaut, Paul G Davies, and Claude M Steele. Ambient belonging: how stereotypical cues impact gender participation in computer science. *Journal of personality and social psychology*, 97(6):1045, 2009.

[8] Sapna Cheryan, John Oliver Siy, Marissa Vichayapai, Benjamin J Drury, and Saenam Kim. Do female and male role models who embody stem stereotypes hinder women's anticipated success in stem? *Social Psychological and Personality Science*, 2(6):656–664, 2011.

[9] CISA. Cisa awards $2 million to bring cybersecurity training to rural communities and diverse populations.

[10] Juliet Corbin and Anselm Strauss. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications, 2014.

[11] Alicia Dietsch. Winner of the at&t diversity and inclusion champion award 2021.

[12] Matthew Finifter, Devdatta Akhawe, and David Wagner. An empirical study of vulnerability rewards programs. In *Proceedings of the 22nd USENIX Security Symposium*, USENIX Security '13, pages 273–288, 2013.

[13] Cynthia E Foor, Susan E Walden, and Deborah A Trytten. "i wish that i belonged more in this whole engineering group:" achieving individual diversity. *Journal of Engineering Education*, 96(2):103–115, 2007.

[14] Kathy Garvin-Doxas and Lecia J. Barker. Communication in computer science classrooms: Understanding defensive climates as a means of creating supportive behaviors. *J. Educ. Resour. Comput.*, 4(1):2?es, March 2004.

[15] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough? an experiment with data saturation and variability. *Field Methods*, 18(1):59–82, 2006.

[16] Morey Haber. Do you suffer from imposter syndrome? https://www.forbes.com/sites/forbestechcouncil/2021/10/28/do-you-suffer-from-imposter-syndrome/?sh=760dc87d8f57, 2021.

[17] Hackerone. 2016 bug bounty hacker report. Technical report, Hackerone, San Francisco, California, September 2016.

[18] Hackerone. 2019 hacker-powered security report. Technical report, Hackerone, San Francisco, California, December 2019.

[19] HackerOne. The 2020 hacker report. Technical report, HackerOne, April 2020.

[20] Herminia Ibarra, Nancy M Carter, Christine Silva, et al. Why men still get more promotions than women. *Harvard business review*, 88(9):80–85, 2010.

[21] $(ISC)^2$. $(ISC)^2$ diversity award.

[22] Colleen M. Lewis, Ken Yasuhara, and Ruth E. Anderson. Deciding to major in computer science: A grounded theory of students? self-assessment of ability. In *Proceedings of the Seventh International Workshop on Computing Education Research*, ICER '11, pages 3–10, New York, NY, USA, 2011. Association for Computing Machinery.

[23] Thomas Maillart, Mingyi Zhao, Jens Grossklags, and John Chuang. Given enough eyeballs, all bugs are shallow? revisiting eric raymond with bug bounty programs. In *Proceedings of the 15th Workshop on the Economics of Information Security*, WEIS '16, 2016.

[24] Jonathan Marcil. Building an application security team, 2017. (Accessed 07-23-2020).

[25] Jane Margolis, Rachel Estrella, Joanna Goode, Jennifer Jellison Holme, and Kim Nao. *Stuck in the shallow end: Education, race, and computing*. MIT press, 2017.

[26] Jane Margolis and Allan Fisher. *Unlocking the clubhouse: Women in computing*. MIT press, Cambridge, MA, 2002.

[27] Adam Mein and Chris Evans. Dosh4vulns: Google's vulnerability reward programs. https://docs.google.com/presentation/d/1REYDohHohDhGAUfUq_Pyz5XFQL44Z3nfH9FnOvvTKBQ/htmlpresent, 2011. (Accessed 02-26-2017).

[28] Sam Mintz. Boston cyber training company gets $1 million from dhs for diversity efforts.

[29] Elaine Seymour and Nancy M. Hewitt. *Talking About Leaving: Why Undergraduates Leave the Sciences*. Westview Press, 2000.

[30] Daryl G Smith. *Diversity's promise for higher education: Making it work*. JHU Press, 2020.

[31] Synack. Synack cybersecurity diversity and inclusion report. Technical report, Synack, 2020.

[32] Sherry Turkle. *The second self: Computers and the human spirit*. Mit Press, 1984.