Engaging Students from Under-Represented Groups to Pursue Graduate School in Computer Science and Engineering

Ravindra Mangar
Ravindra.R.Mangar.GR@dartmouth.edu
Dartmouth College
Hanover, NH, USA

Cesar Arguello
Cesar.N.Arguello.Martinez.GR@dartmouth.edu
Dartmouth College
Hanover, NH, USA

David Inyangson
dinyang1@jhu.edu
Johns Hopkins University
Baltimore, MD, USA

Tina Pavlovich
Tina.Pavlovich@dartmouth.edu
Dartmouth College
Hanover, NH, USA

Karen Gareis
gareis@grginc.com
Goodman Research Group
Cambridge, MA, USA

Tushar M. Jois
tjois@ccny.cuny.edu
City College of New York
New York, NY, USA

ABSTRACT

The persistent under-representation of students from groups historically underrepresented in Computer Science and Engineering (CS&E) programs presents a significant challenge to achieving diversity within the field. A workforce with diverse experiences and perspectives is essential for creating innovations that serve all members of society. Existing documented efforts to broaden diversity in CS&E are time-intensive (multi-week programs) and do not quantify attraction to graduate studies.

This paper aims to bridge that gap by presenting and evaluating a detailed design for a *one-day* workshop that includes presentations from research professors, hands-on cybersecurity demos, a panel discussion with current and recent graduate students in CS&E, and a participation survey. By engaging students historically under-represented in CS&E in the topic of graduate school, we aim to increase the diversity of students who apply to and attend graduate school, and ultimately enter the workforce through industry or through the professoriate, thus making the field more diverse and representative of varied perspectives.

We held the aforementioned workshop at a Hispanic-Serving Institution in April 2024. The event successfully attracted members of historically under-represented groups. Our survey results show that 78% of the participants agreed or strongly agreed that the event increased their interest in graduate school, 72% were more likely to seek further information about attending graduate school, and 67% of the participants had an increased interest in CS&E research. Our experience shows that one-day events focused on engaging students in the topic of graduate school in CS&E can positively impact attendee's interest in graduate school and provide valuable information about the application process and graduate school experience.

CCS CONCEPTS

• Social and professional topics → Computing education; **• Applied computing → Interactive learning environments**; **• Security and privacy → Mobile and wireless security**.

KEYWORDS

one-day workshop, graduate school, diversity and inclusion

ACM Reference Format:
Ravindra Mangar, Cesar Arguello, David Inyangson, Tina Pavlovich, Karen Gareis, and Tushar M. Jois. 2025. Engaging Students from Under-Represented Groups to Pursue Graduate School in Computer Science and Engineering. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE TS 2025), February 26-March 1, 2025, Pittsburgh, PA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3641554.3701956

1 INTRODUCTION

Training a diverse workforce in Computer Science and Engineering (CS&E) will lead to a more adept society resulting in more opportunities for innovation. Research shows that research products in information technology that are created by mixed-gender teams are more frequently cited than other patents of similar type and age [15]. The U.S. government has also made the recruitment and retention of a diverse STEM workforce a national priority [19].

Despite the increasing number of students in CS&E [4], there is still a lack of diversity in the field. The percentage of women earning CS degrees is smaller than in the 1990s. Additionally, the proportion of Black students earning CS Bachelor's degrees has stagnated since the 2010s [18].

To support the creation of a diverse workforce in CS&E, we need more *students* with diverse backgrounds in CS&E education programs. There are documented initiatives to increase the number of high school students studying CS&E in college [1, 10, 16, 20, 33], and to support CS&E graduate students entering careers in academia or industry [7, 13, 27]. Existing programs that support undergraduate students in pursuing CS&E graduate programs are extended-duration [8, 12, 14]. By creating a one-day event, we fill this gap in short-term, high-impact programming focused on increasing the diversity of personnel in industry, academia, and government. In particular, increasing the diversity of academia is essential to the persistence of students in these areas of study [11].

Our one-day, hands-on workshop to provide historically under-represented and first-generation students with information about

SIGCSE TS 2025, February 26-March 1, 2025, Pittsburgh, PA, USA

ACM ISBN 979-8-4007-0531-1/25/02…$15.00
https://doi.org/10.1145/3641554.3701956

graduate school in CS&E strengthens this pipeline. We theme our workshop around cybersecurity, a subfield which lends itself to hands-on demonstrations [32] and has strong student interest [29]. Our experience suggests that one-day workshops can increase our intended groups' interest in and likelihood to learn more about graduate school, thus promoting diversity in education and downstream in the workforce.

Prior Efforts. Prior work shows that multi-week research programs for underrepresented students in CS&E are positively impactful and improve participants' research skills [34]. But, such programs are time and resource intensive for both facilitators and participants, requiring large and sometimes infeasible commitments. Additionally, recent efforts to broaden diversity in cybersecurity education have not quantified attraction to graduate studies [24].

One-day workshops, although short, are effective in increasing student interest in science and technology research [2]. We were unable to find scholarly work on one-day workshops focused on engaging students from historically underrepresented groups in CS&E (hitherto referred as HUGCSE) on the topic of graduate school. While such one-day workshops have likely been held, we were unable to find experience reports in the literature.

For this reason, our team sought to create and document a one-day workshop with presentations from research professors, hands-on demos led by current graduate students, and a panel session with current and recent graduate students in CS&E. We ran this program at The City College of New York (CCNY), a public, urban Hispanic-serving institution, as we felt our impact would be greater at an institution with more students from HUGCSE. We also engaged an external evaluator to create and administer a survey to understand the impact on students' interest in graduate school.

Contributions. In this paper, we present a report of our findings to evaluate the effectiveness of our unique combination of demos, panels, and research talks on attendees' interest in graduate school. We discuss the planning of the workshop, including descriptions of all segments, the advertisement strategies used to attract participants, and the selection and implementation of cybersecurity demonstrations. Additionally, we analyze the effectiveness of our workshop in fostering interest in graduate school among students from HUGCSE, using data collected through participant surveys.

We hope this report can be used to make the case for the effectiveness of one-day workshops in promoting diversity in CS&E. The reproducible materials from the workshop are publicly available for those interested in leading similar workshops.[1]

2 EVENT DESIGN

In this single-day workshop, we aim to present information about graduate school to students from HUGCSE in an engaging way. Our goal is to provide attendees with the information they need to consider pursuing graduate degrees in CS&E fields. We cover different aspects of graduate school through talks given by research professors, a panel discussion with current and former graduate students, and technical hands-on demonstrations. Despite being only one day, we aimed to include a diverse set of activities, featuring speakers from HUGCSE who share their experiences and pathways to pursuing a graduate degree. Additionally, our event includes discussions on funding opportunities and the application process for graduate school, as well as networking opportunities.

Objectives. Our objectives with the event are for students to:

- understand what graduate school in CS&E entails
- familiarize themselves with the graduate application process
- learn different ways graduate school can be funded
- discover possible career paths post-graduate school
- be more confident that graduate school is an option for them

2.1 Intended Audience

Our intended audience is students from HUGCSE, particularly Hispanic, Latino/a/e, women, Black, and first-generation students in the City University of New York public university system. We ran this event at CCNY, where 40.6% of undergraduate students in Fall 2023 identified as Hispanic/Latino, 52.3% of undergraduates identified as women, 15.4% of students identified as Black or African-American, and 37.2% identified as first-generation college students [25, 26]. We assume that event attendees have already taken introductory CS&E classes, and use this to guide the workshop's technical depth.

Team Demographics. Evidence suggests that seeing relatable "role model" individuals leads to increased motivation and likelihood of success for underrepresented populations in science and engineering [6]. So, we asked our research team members who were representative of our targeted student population to be panelists and facilitators. Additionally, our panelists and facilitators were from eight institutions: three private universities, two non-profit/not-for-profit research institutions, and three public universities, one of which is CCNY and one that is a Historically Black University.

2.2 Structure

We design this event to be four hours and thirty minutes long.

Professors' Presentations. The workshop starts with research presentations from four professors. Our presenters focused on the benefits of attending graduate school, what research looks like, using research to make real-world change, and how students can get involved in research as undergraduates.

Hands-on Demos and Lunch. After the presentations, students engage in hands-on research demos led by graduate students in CS&E, whose work focuses on cybersecurity. Often, students who initially lack interest in CS&E gain interest when it is applied in a context appealing to them [22, 28]. Therefore, the demonstrations focus on CS&E topics such as software, hardware, and networking as they apply to cybersecurity. The demos are also hands-on so students can tinker with the technology themselves.

We use large display screens to ensure that demos are well-presented, and we use graphical interfaces to present technical information intuitively. For the demos, we employ a research-fair style set up in a high-traffic area, to engage passersby as well as students who explicitly come for the event. We plan three demonstrations, each piloted by two graduate student facilitators. Students are encouraged to experiment with the demonstrations and interact with the facilitators. Through organic interactions, students gained insight into graduate-level work and graduate school life.

[1] https://github.com/SPLICE-project/bpc-workshop

Panel. The final portion of the event is a graduate student panel discussion. Our panelists spoke about their experiences and the impact their education had on their career prospects.

Networking and Check-out. As students depart, they receive pamphlets and QR codes for graduate programs at team members' institutions. Students are also asked to hand in their surveys.

The event lasted approximately four and a half hours. Due to the availability of external funding, we provided free food throughout the event. Additionally, we provided students who registered for the event a $10 cash travel stipend upon sign-in, to eliminate the barrier of transportation costs to attendance.

Note that we focus this paper on the creation and implementation of the hands-on demos, as faculty presentations and panel discussions include personal experiences and advice, whereas the demonstrations are reproducible and usable in various contexts.

2.3 Communicating with Stakeholders

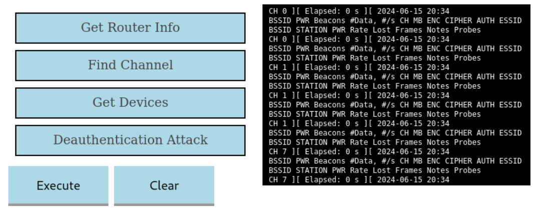
The CUNY system includes 25 colleges. We collected administrative and faculty contacts from the 20 with relevant programs. We grouped contacts by institution and area of study, so that for each outreach, one email would be sent to each structural unit. Our multi-phased communication approach included an initial email to identify key contacts and gather event suggestions. The second phase, 1.5 months before the event, included electronic flyers. The final phase was a reminder email sent the week of the event. This cold email method yielded a 45% response rate.

3 HANDS-ON DEMOS

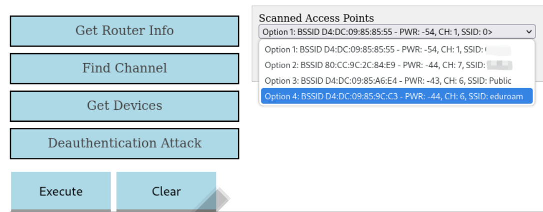
The event includes hands-on demonstrations created by current graduate students. While the demos are not directly aligned with the graduate students' specific research projects, which focus on security and privacy in smart homes, they leverage the students' expertise in cybersecurity. The demonstrations cover general cybersecurity threats, including Wi-Fi de-authentication, inference, and machine-in-the-middle attacks (MITM). These demos are broadly relevant, engage a diverse audience, and are interactive. Additionally, the creation of the demos highlights aspects of graduate work: building upon others' research to make it accessible and developing a deep understanding of state-of-the-art tools and techniques. At our event, attendees discussed this relevance to graduate study with the presenters.

Each demonstration starts with a short presentation to visualize concepts related to the attack. Participants receive a brief overview of the theory behind each exploit, are guided through executing the attacks, and then discuss potential defense mechanisms. To ensure accessibility for a broad audience with some computer science background, we include interactive web-based and command-line interfaces that abstract the low-level details of the attacks.

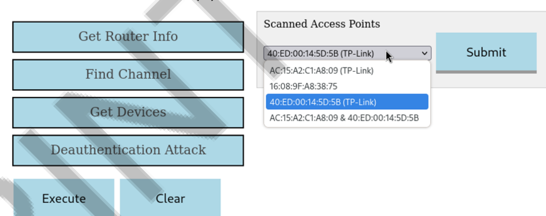
We differentiate our demos from others by designing the source code with minimal dependencies and using simple programming techniques. Our goal is easy-to-use demos that still showcase important aspects of graduate work. As a result, our demos are uniquely designed to get students thinking about graduate school. We have made a GitHub repository available, containing all the resources needed for the community to replicate these demonstrations [31].



(a) "Get Router Info"



(b) "Find Channel"



(c) "De-authentication Attack"

Figure 1: Output from Buttons in Web Client's GUI for Deauthentication Attack Demo.

3.1 Wi-Fi De-authentication Attack

In a Wi-Fi de-authentication attack, an adversary attempts to terminate the connection between a client and an access point (AP) [30], posing a significant security risk for smart home residents by disrupting monitoring devices like cameras and sensors. This demonstration aims to provide participants with a high-level understanding of the attack, familiarize them with the tools adversaries use, and encourage consideration of device security and privacy from an adversarial perspective.

At our event, participants actively performed a de-authentication attack on two vulnerable cameras live-streaming the event room. Given that many smart devices either only support or default to Wi-Fi versions vulnerable to this attack, attackers don't need to compromise a device in advance. This demonstration seeks to raise awareness about smart device selection and configuration and to generate interest in addressing real-life security issues.

Architecture. We use the Aircrack-ng suite [5] to create a server on a Raspberry Pi 4. The server scans for Wi-Fi APs, identifies the channel a target AP is on, and lists devices associated with the target AP. Furthermore, it sends de-authentication frames appearing to originate from an associated device to a target AP.

The server is controlled by the web-client shown in Figure 1. This web-client runs on the same Raspberry Pi as the server; the client's graphical user interface (GUI), however, makes visualizing the server's data and issuing commands much easier. The "Get

Router Info" button, instructs the server to scan the area for Wi-Fi APs. After the scan is complete, the user clicks the "Find Channel" button to select one of the APs from the scan and get the channel it uses (see Figure 1b). After finding the channel, the user retrieves the devices associated with the selected AP by clicking the "Get Devices" button. Finally, clicking the "De-authentication Attack" button, the user selects one or more devices to impersonate (see Figure 1c), and send 50 de-authentication packets to the target AP (appearing to come from the spoofed device).

Student Involvement. Participants are asked to identify the BSSID, channel, and brand of devices (based on MAC addresses) connected to a target AP. The target AP is a Raspberry Pi 3 configured with the default settings commonly found in off-the-shelf routers: Wi-Fi 4 support, WPA2 encryption, and disabled management frame protection. The presentation and AP name provided as a clue are sufficient information for students to execute the attack. Participants select the BSSID of the vulnerable AP and the MAC address of a connected device from the GUI's drop-down menus and send de-authentication frames to disrupt the connection. At our event, security cameras live-streaming the demo room were connected to the AP, so the de-authentication attack dropped the live feed, providing a visual representation of the exploit. After the exploit, we discuss mitigations to prevent such attacks.

This demo gives students an insight into graduate research by showing how to leverage and extend the functionality of popular networking tools. By sometimes having to guess the MAC address for devices in the demo, students see that graduate research involves trial and error and that not all solutions are straightforward.

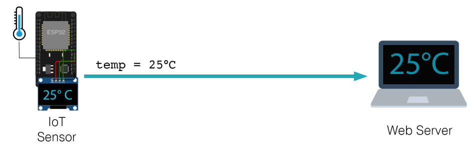
3.2 Machine-in-the-Middle-Attack

A machine-in-the-middle-attack is a cyberattack where an adversary intercepts and alters data traveling between two devices [21].

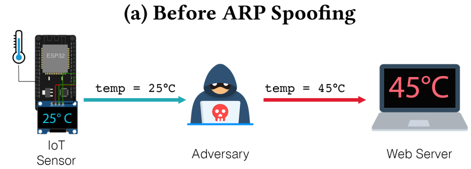
Architecture. To demonstrate the MITM attack, we create an IoT device using a Wi-Fi equipped ESP32 microcontroller paired with a temperature probe. A shown in Figure 2a, this device acts as the IoT sensor, periodically sending temperature data over a Wi-Fi connection. We develop a custom protocol for transmitting this temperature information. On the receiving end, we set up a web server using Flask, which accepts the temperature updates and displays them through a website. The ESP32 has an onboard display that continuously showed accurate temperature readings.

To execute the machine-in-the-middle-attack attack, we use Address Resolution Protocol (ARP) spoofing, a technique where an attacker sends falsified ARP messages over a local network to associate their MAC address with the IP address of another device, typically the router, causing traffic intended for that IP address to be sent to the attacker instead. Using this method, we intercept the communication between the IoT device and the web server. We use mitmproxy [3] to manipulate the data packets. By altering the packet filtering rules with iptables, we redirect the network traffic through mitmproxy, allowing modification of the temperature data being sent to the web server (see Figure 2b).

Student Involvement. Our brief introductory presentation covers the key components of this attack, including the ESP32 microcontroller, the web server, and the attack platform. We explain how the attack platform intercepts and manipulates data packets.



(a) Before ARP Spoofing



(b) After ARP Spoofing

Figure 2: Machine-in-the-Middle Attack Scenario. The student, in the role of the adversary, modifies data before forwarding it to the web server.

For this demonstration, users engage with the command line interface while viewing the temperature display website and the onboard display of the IoT (see Figure 2a). To make the commands more user-friendly, we create aliases that resembled high-level natural language. After executing the attack, participants see the altered temperature data on the website, which contrasts the true temperature continuously displayed on the IoT device's screen as shown in Figure 2b. This demonstration highlights skills such as hardware prototyping, integrating hardware and software, and analyzing security vulnerabilities.

After the participants execute the attack, we discuss the broader implications of such vulnerabilities, particularly in the context of smart homes. We illustrate a scenario where an attacker could exploit this vulnerability to manipulate smart home devices. For example, if a smart home system has an If This, Then That (IFTTT) rule set to automatically open windows at a certain temperature, an attacker can use this attack to falsely trigger the rule, opening the windows and gaining unauthorized entry into the house.

This demonstration aims to present students with the power of the command line interface and expose them to aspects of research through analyzing network protocols. We follow the order often seen in cybersecurity research papers: analyze the attack, discuss its implications through scenarios like IFTTT, and discuss mitigations.

3.3 Inference Attack

In an inference attack, an adversary attempts to deduce sensitive information by analyzing seemingly useless data [9]. In a smart-home, a successful inference attack can leak information about routines, occupancy, and behaviors of the home's inhabitants [23].

Architecture. We simulate a smart home environment using an IR-controlled RGB lamp, a Raspberry Pi Model 3 with an IR transmitter, and two Apple M2 MacBook Pros. Participants use a graphical interface on the first MacBook (MB1) to send commands via a secure shell connection to the Raspberry Pi, which controls the lamp. The graphical interface shows all possible light configurations and states. When a user chooses a lamp state, an IR command is sent via the Raspberry Pi, updating the lamp and status.

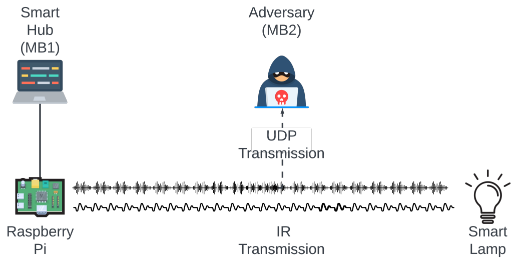


Figure 3: Inference Attack Scenario. The student, in the role of the adversary, passively eavesdrops on the obfuscated data.

The adversary in this demo is a local network eavesdropper using the second MacBook (MB2) and placing it on the same network as the Raspberry Pi. When the Raspberry Pi sends an IR command, an obfuscated UDP packet is sent to MB2, which is running Wireshark. Participants capture real-time traffic of the obfuscated commands corresponding to the lamp state. The scenario is shown in Figure 3.

We associate each lamp state command with a string value. The commands are of the form *"Turned<attribute>"*. Attributes are colors and actions, such as "orange" or "off". Commands are obfuscated by first determining the plaintext length, then base64 encoding it. The final representation of the lamp state command is generated by repeating the base64 encoding for the length of the original plaintext, preserving a relationship between the UDP payload's repeated sections and the plaintext command. By recognizing this relationship, similar to other types of inference attacks, an adversary can derive meaning from the obfuscated traffic.

Student Involvement. This demonstration highlights the complexity of building secure systems and exposes students to research strategies and intuitions. We provide students with a reference sheet as they interact with the demo and ask them to determine the state of the lamp by observing obfuscated commands. The sheet includes a description of inference attacks, the goal of the demonstration, and two packet captures of obfuscated payloads with their corresponding plaintext commands. To make the demo interactive, we model it after a chosen plaintext attack scenario [17]. The student takes the role of MB2 shown in Figure 3. In addition to the packet captures they already have, students can ask for up to two specific inputs to the lamp. Knowledge of the input and the obfuscated output allows students to gain information about the obfuscation mechanism. When students are ready to attempt inference, a facilitator takes control of the lamp via MB1 shown in Figure 3 and hides the lamp from students' view. The facilitator chooses a lamp state and asks the students to infer it.

Regardless of whether participants are able to successfully correlate commands to obfuscated payloads, this demo exposes participants to strategies for implementing and mitigating inference attacks, and the complexities of building secure systems. These strategies are applicable in real-world situations where data transmission by smart devices has compromised individual's privacy [9, 23].

4 PANEL

At our event, the panel discussion included three PhD students and an early-career research scientist; it was moderated by a faculty researcher. The panelists and moderator were from HUGCSE. This deliberate selection aimed to foster a discussion that would be relatable to the workshop participants. The panel began with brief introductions from the panelists and moderator, who shared personal and career highlights. Afterwards, the moderator directed questions to panelists based on their career stages. Questions were organized into four stages of a graduate student's journey: contemplation, application, acceptance, and graduation. In the *contemplation* stage, panelists discussed funding opportunities and factors to consider when selecting a graduate program. Moving to the *application* stage, they addressed selecting recommenders and writing a statement of purpose. During the *acceptance* stage, they commented on the obstacles, support systems, and responsibilities in a graduate program. Finally, in the *graduation* stage, panelists shared career aspirations post-graduation. The panel concluded with the moderator opening the floor for questions from workshop participants.

Table 1: Percentage of respondents who *Agree* or *Strongly Agree* with evaluation questions. * and † respectively indicate lower ($p < .05$) and marginally lower ($p < .10$) means for first-generation students.

Survey Item	**Percentage** (N = 17–18)
I enjoyed this event.	83%
This event:	
increased my interest in:	
CSE research.†	67%
graduate school.	78%
made me more likely to look for information about:	
becoming involved in CSE research.*	56%
attending graduate school.	72%
gave me a better understanding of:	
what CSE research is.†	56%
what graduate school entails.	59%
the application process for graduate school.†	39%
how graduate school can be funded.	34%
possible career paths after graduate school.	50%

5 EVALUATION

Our evaluation plan received institutional review board (IRB) approval prior to the event. To not disrupt the flow of the event, but still gather attendee feedback, we used paper surveys. As attendees arrived, team members positioned throughout the event space handed out surveys. The brief 1-page survey asks for impressions of the event and for demographic information.

Demographics. We received 18 completed surveys. Of those who answered the question about race/ethnicity (n = 17), 24% are Asian, 29% are Black or African American, 24% are Hispanic or Latino, 12% are white, and 12% preferred not to respond. Of those who answered the question about gender (n = 15), 60% are male and 40% are female. And of those who answered the question about parental education (n = 17), the highest level of education for their parents was: less than a high school diploma for 12%, a high school diploma or GED for 12%, some college education for 18%, a bachelor's degree for 18%, a graduate degree for 24%, and 18% preferred not to respond. Thus, the event was successful in attracting members of HUGCSE to attend.

Survey Results. Survey results are summarized in Table 1. Overall, students rated the event highly, with the majority *agreeing* or *strongly agreeing* that they enjoyed the event (83%) and that it met the organizers' goals, including increasing their interest in graduate school (78%), making them more likely to look for further information about attending graduate school (72%), increasing their interest in CS&E research (67%), and giving them a better understanding of what graduate school entails (59%).

Because the N was small, findings of group differences should be interpreted with caution. There did not appear to be any differences by gender (6 women vs. 9 men) or by identification as a member of a HUGCSE (9 identifying as Black/African American or as Hispanic/Latino vs. 6 identifying as White or Asian).

First-generation college students (4 first-generation vs. 10 not first-generation) gave lower ratings to the event in various ways. First-generation students were significantly less likely to agree the event increased their likelihood of looking for ways to become involved in CS&E research (3.8 vs. 6.2 on a 7-point scale; $t(12)=3.5$, $p=.004$). They were also marginally less likely to agree the event: increased their interest in CS&E research (3.8 vs. 6.5 on a 7-point scale; $t(3.2)=2.9$, $p=.060$), improved their understanding of what CS&E research is (4.3 vs. 5.8 on a 7-point scale; $t(12)=1.9$, $p=.079$), or helped their understanding of the application process for graduate school (4.0 vs. 5.6 on a 7-point scale; $t(12)=2.0$, $p=.071$). As noted above, these results are suggestive given that they are based on responses from only 4 first-generation college students. As with the rest of the event materials, our survey template is publicly available [31].

Feedback on the Demos. We received mixed feedback from attendees through verbal conversations. Many participants, lacking smart home devices, found some demonstrations challenging to fully appreciate. Those with smart devices, however, grasped the broader implications and found the demos insightful. The deauthentication attack, due to its generality, was appreciated by a larger percentage of the audience.

6 REFLECTION

Guided by our evaluation and experience, we reflect on what went well, what did not, and changes for future versions of this workshop.

Successes. As our survey results in Table 1 show, this event was largely positively impactful in increasing student interest in research and graduate school. With well-planned presentations from faculty, student-led demonstrations, and student-panels, participants got to learn about graduate school from all facets – applying, getting funding, life as a graduate student, post-graduate school opportunities. Having a diverse team of graduate students and faculty from private and public institutions across the US with varied gender and racial/ethnic identities was also essential in connecting with students from various backgrounds.

Areas for Improvement. We found that the demonstrations we chose for this workshop were not as applicable to attendees as we had hoped. The Wi-Fi de-authentication attack was well-received because most participants have wireless routers and are familiar with the basics of Wi-Fi. However, the machine-in-the-middle attack was not fully appreciated as it requires familiarity with multiple smart devices, and some audience members did not own any. The demonstrations leveraged the presenters' expertise, which is cybersecurity. This allowed the presenters to use materials from their domain, reducing preparation effort. If this event were to be reproduced by teams with other focuses in CS&E, it would benefit students, presenters, and other practitioners in those fields to create demos that highlight aspects of those fields.

Future Work. Future demonstrations should be tailored to ensure they resonate more with the participants' experiences and knowledge. For example, while the Wi-Fi deauthentication attack was well-received due to participants' familiarity with Wi-Fi, more complex attacks like the machine-in-the-middle or inference attack could be adjusted to be fully appreciated by all attendees. For instance, the machine-in-the-middle demo could be adapted to a more relatable scenario such as spoofing a web page. The inference attack reference sheet could include more obfuscated commands to plaintext mappings to help students develop intuition for inference.

Attendees used the demos as an opportunity to learn more about the facilitators' work. They frequently asked if the demos were part of the facilitators' research, and upon learning they were not, inquired further about the specifics of their projects. Therefore, we believe future iterations of this workshop could benefit from presentations and demos on research conducted by the facilitators.

We had 95 sign-ups, and about 30 attendees. Since, by design, this event was in a high-traffic area, some attendees did not receive surveys. A personalized reminder and preview of workshop content might retain more students from sign-up to event attendance.

To better understand our impact, we can add an optional survey question for students to provide their email addresses. This would enable us to reach out and see if students apply to graduate school.

The majority of direct costs for this event were for food, team member travel, and lodging. Although beneficial to have facilitators from eight universities, this event would be just as successful and less costly if planned with local colleagues. We see a hybrid or virtual event decreasing the efficacy of the hands-on demos.

7 CONCLUSION

This paper describes and evaluates a *one-day* workshop aimed at engaging students from HUGCSE on the topic of graduate school. Our findings indicate that one-day events focused on the topic of graduate school in CS&E can positively influence attendees and provide valuable insights into the application process and the graduate school experience. The evidence suggests that this program can be successful in a future iteration at an urban college or university with a high percentage of students from HUGCSE. To facilitate the organization of similar workshops, the guiding materials for each portion of the workshop, with the exception of the research professors' presentations, are publicly available [31].

ACKNOWLEDGMENTS

The authors thank Louis Hernandez, Kevin Kornegay, Michel Kornegay, Susan Landau, Lea Manglicmot, Michelle Mazurek, Beatrice Perez, Timothy J. Pierson, and Cora Ruiz for assisting with our workshop. This paper is supported by NSF under award numbers 1955805, 1955172, 1955228, 1955231, as well as by VeChain. The views and conclusions contained herein are those of the authors.

REFERENCES

[1] [n. d.]. Computer science higher education pipeline | Journal of Computing Sciences in Colleges — dl.acm.org. https://dl.acm.org/doi/abs/10.5555/1040196.1040209. [Accessed 15-07-2024].

[2] [n. d.]. Interactive youth science workshops benefit student participants and graduate student mentors — journals.plos.org. https://journals.plos.org/plosbiology/article?id=10.1371/journal.pbio.3000668. [Accessed 12-07-2024].

[3] [n. d.]. mitmproxy - an interactive HTTPS proxy — mitmproxy.org. https://mitmproxy.org. [Accessed 16-07-2024].

[4] 2020. Bachelor's degrees conferred by postsecondary institutions, by field of study: Selected years, 1970-71 through 2018-19 — nces.ed.gov. https://nces.ed.gov/programs/digest/d20/tables/dt20_322.10.asp. [Accessed 13-06-2024].

[5] Aircrack-ng. 2024. Aircrack-ng. https://github.com/aircrack-ng/aircrack-ng.

[6] Nir Aish, Philip Asare, and Elif Eda Miskioğlu. 2018. People Like Me: Providing relatable and realistic role models for underrepresented minorities in STEM to increase their motivation and likelihood of success. In *2018 IEEE Integrated STEM Education Conference (ISEC)*. 83–89. https://doi.org/10.1109/ISECon.2018.8340510

[7] Computing Research Association. 2024. Grad Cohort for IDEALS Workshop. https://cra.org/cra-wp/grad-cohort-ideals/. [Accessed 09-11-2024].

[8] Computing Research Association. 2024. NSF Distributed Research Experiences for Undergraduates. https://cra.org/cra-wp/dreu/. [Accessed 09-11-2024].

[9] Ravishankar Chamarajnagar and Ashwin Ashok. 2019. Privacy Invasion through Smarthome IoT Sensing. In *2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. 1–9. https://doi.org/10.1109/SAHCN.2019.8824933

[10] Barbara Ericson and Tom McKlin. 2012. Effective and sustainable computing summer camps. In *Proceedings of the 43rd ACM Technical Symposium on Computer Science Education* (Raleigh, North Carolina, USA) *(SIGCSE '12)*. Association for Computing Machinery, New York, NY, USA, 289–294. https://doi.org/10.1145/2157136.2157223

[11] LORELLE L. ESPINOSA. 2011. Pipelines and Pathways: Women of Color in Undergraduate STEM Majors and the College Experiences That Contribute to Persistence. https://cafethorium.whoi.edu/wp-content/uploads/sites/33/2021/01/Espinosa_WomenOfColorUndergraduateExperience.pdf. [Accessed 20-06-2024].

[12] Institute for African-American Mentoring in Computer Sciences. 2024. iAAMCS. http://diversitycomplete.com/iaamcs/. [Accessed 09-11-2024].

[13] Center for Minorities and People with Disabilities in IT. 2024. Early Career Doctoral Student Academic Careers Workshop. https://cmd-it.org/early-career-doctoral-student-academic-careers-workshop/. [Accessed 09-11-2024].

[14] Center for Minorities and People with Disabilities in IT. 2024. Tapia Conference. https://tapiaconference.cmd-it.org. [Accessed 09-11-2024].

[15] National Center for Women's Information Technology (NCWIT). 2022. Who Invents IT? https://wpassets.ncwit.org/wp-content/uploads/2022/03/18185236/NCWIT_Patent-Report-2022_Final_WEB-1.pdf. [Accessed 20-06-2024].

[16] Joanna Goode and Jane Margolis. 2011. Exploring Computer Science: A Case Study of School Reform. *ACM Trans. Comput. Educ.* 11, 2, Article 12 (jul 2011), 16 pages. https://doi.org/10.1145/1993069.1993076

[17] Matthew Green. 2012. Wonk Post: Circular Security. https://blog.cryptographyengineering.com/2012/04/27/wonk-post-circular-security/.

[18] Elizabeth Grieco and Steven Deitz. 2023. Diversity and STEM: Women, Minorities, and Persons with Disabilities 2023 | NSF - National Science Foundation — ncses.nsf.gov. https://ncses.nsf.gov/pubs/nsf23315/report/science-and-engineering-degrees-earned. [Accessed 13-06-2024].

[19] https://ww2.aip.org/andrea peterson. [n. d.]. Workforce Diversity Initiatives in the CHIPS and Science Act — ww2.aip.org. https://ww2.aip.org/fyi/2022/workforce-diversity-initiatives-chips-and-science-act. [Accessed 20-06-2024].

[20] Patricia K Hunt, Michelle Dong, and Crystal M Miller. 2021. A multi-year science research or engineering experience in high school gives women confidence to continue in the STEM pipeline or seek advancement in other fields: A 20-year longitudinal study. *PLoS ONE* 16 (2021). https://api.semanticscholar.org/CorpusID:242805672

[21] Avijit Mallik. 2019. Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi* 2, 2 (2019), 109–134.

[22] Jane Margolis and Allan Fisher. 2002. *Unlocking the clubhouse: Women in computing*. MIT press.

[23] Yair Meidan, Michael Bohadana, Asaf Shabtai, Juan David Guarnizo, Martín Ochoa, Nils Ole Tippenhauer, and Yuval Elovici. 2017. ProfilIoT: a machine learning approach for IoT device identification based on network traffic analysis. *Proceedings of the Symposium on Applied Computing* (2017). https://api.semanticscholar.org/CorpusID:1928705

[24] Xenia Mountrouidou, David Vosen, Chadi Kari, Mohammad Azhar, Sajal Bhatia, Greg Gagne, Joseph Maguire, Nicoleta Tudor, and Timothy Yuen. 2019. Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. 157–176. https://doi.org/10.1145/3344429.3372507

[25] Jay Mwamba. 2023. U.S. Department of State again names CCNY Fulbright HSI Leader. *The City College of New York* (30 10 2023).

[26] Office of Institutional Research. 2023. The City College of New York Fact Sheet - Fall 2023 Undergraduates. [Accessed 22-05-2024].

[27] University of Michigan. 2024. NextProf Nexus. https://nextprof.engin.umich.edu/nextprof-nexus/. [Accessed 09-11-2024].

[28] American Association of University Women. Educational Foundation. Commission on Technology, Gender, and Teacher Education. 2000. *Tech-savvy: Educating girls in the new computer age.* American Association of University Women.

[29] Elaine Rowles. 2023. When Bad News Is Good News: Cyber Breaches Drive Demand For Cybersecurity Programs. https://www.graydi.us/blog/graydata/when-bad-news-is-good-news-cyber-breaches-drive-demand-for-cybersecurity-programs

[30] Domien Schepers, Aanjhan Ranganathan, and Mathy Vanhoef. 2022. On the Robustness of Wi-Fi Deauthentication Countermeasures. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (San Antonio, TX, USA) *(WiSec '22)*. Association for Computing Machinery, New York, NY, USA, 245–256. https://doi.org/10.1145/3507657.3528548

[31] SPLICE-project. 2024. bpc-workshop. https://github.com/SPLICE-project/bpc-workshop.

[32] Zouheir Trabelsi. 2021. IoT based Smart Home Security Education using a Hands-on Approach. In *2021 IEEE Global Engineering Education Conference (EDUCON)*. 294–301. https://doi.org/10.1109/EDUCON46332.2021.9454085

[33] Justice T. Walker, Amanda Barany, Alex Acquah, Sayed Mohsin Reza, Alan Barrera, Karen Del Rio Guzman, and Michael A. Johnson. 2023. Coding Like a Data Miner: A Sandbox Approach to Computing-Based Data Science for High School Student Learning. In *2023 IEEE Frontiers in Education Conference (FIE)*. 1–5. https://doi.org/10.1109/FIE58773.2023.10343283

[34] Dazhi Yang, Dianxiang Xu, Jyh-Haw Yeh, and Yibo Fan. 2019. Undergraduate Research Experience in Cybersecurity for Underrepresented Students and Students with Limited Research Opportunities — learntechlib.org. https://www.learntechlib.org/p/207536/. [Accessed 18-06-2024].