Collegiate Social Engineering Capture the Flag Competition

Abstract

Social engineering (SE) is an essential, yet often overlooked, field within cybersecurity, particularly in the context of education, training, and awareness. While there are investments in cybersecurity education programs, they tend to have a primarily technical focus, including within classroom curricula and Capture the Flag (CTF) competitions. Because the current technical CTFs do not emphasize the relevance of the human-socio-psychological aspects of cyberattacks and cybersecurity, the researchers organized and hosted a Collegiate SECTF grounded in the social sciences, which offered a timely and unique platform for students to learn about social engineering topics, such as OSINT, phishing, and vishing, in a hands-on, engaging, and ethical manner. This paper details the planning and logistics of the virtual SECTF event which took place October XX, 2020 at XXXXXX XXXXXXXXX and hosted 6 teams of undergraduate students from across the world. Students' experiences while participating in this event are described in detail, with insight on teams' preparations, group formation and dynamics, strategies and adaptations, learning benefits, and thoughts on each individual flag. The success and positive student responses from the inaugural SECTF provide a proof of concept, demonstrating that experiential learning can be used to teach students about SE.

1. Introduction

Social engineering (SE) is defined as "any act that influences a person to take an action that may or may not be in his or her best interests" [1, p. 23].SE is a technique that often provides the foundation for 50-75% of the background work before a cyberattack. Cybercriminals use this human-centered vulnerability to conduct reconnaissance (identify systems operating at target facilities), obtain information intended to secure electronic systems (passwords), or to encourage targets to inadvertently provide access to electronic systems and information (downloading and executing malware files that are disguised as familiar or benign) [2, 3, 4]. The Federal Bureau of Investigation's 2019 Internet Crime Report noted that the total financial loss from the SE tactics of business email compromise, phishing scams, and confidence fraud/romance scams totaled more than $2.23 billion [5]. The human factor is often regarded as the weakest link in cyberattacks, making SE a major concern for cybersecurity [6]. Despite the significant threat posed by SE attacks, most organizations do not address SE topics during employee security training classes [7-9]. Furthermore, a review of 11 commonly followed information assurance curricula found that less than 25% of the curricula specifically included SE and none of the curricula mentioned social engineering education, training, awareness or auditing [10]. Education, training and general awareness of SE as a tool for cybercrime is low, as it is seen as less important in comparison to technical information security topics; is considered to be outside the scope of the technical domain and thus should be addressed by other disciplines; and requires research in diverse and converging areas, including psychology, criminology, sociology, and technology [7, 11]. Furthermore, research has been limited by the ability to design and implement training programs, as effective research would need to include and target human subjects, which raises ethical concerns [12].

This paper discusses one such education and training effort, the inaugural Collegiate Social Engineering Capture the Flag competition (SECTF henceforth), which was held in October XX, 2020 at XXXXXX XXXXXXXXXX. The next section sets the foundation by situating the SECTF amidst existing technical CTFs and arguing for its necessity. The third section discusses the planning behind the event, emphasizing the ethics and risk management protocols that were followed to ensure the event was safe, ethical, and fun for students. The fourth section details the three flags of the competition: Open Source Intelligence (OSINT), vishing, and phishing. The fifth section details student experiences via informal discussions with the winning teams and also responses from open-ended surveys. The paper concludes with a discussion about the relevance of an academia-nonprofit-industry nexus in making this SECTF a meaningful and engaging experience for students.

2. The current CTF landscape

The engineering and computer science disciplines are already investing heavily in cybersecurity education programs that have a primarily technical focus.

2.1. Abundance of technical CTFs

There are many existing Capture the Flag (CTF) competitions that are used to educate students in the area of cybersecurity (Table 1). While each of these is undoubtedly important in training the next generation, *they are all highly technical in nature and cater exclusively to technical STEM students*. Furthermore, there is a *saturation of focus areas,* such as reverse engineering, hacking, cryptography, and exploitation.

Table 1: Current Capture-the-Flag (CTF) Competitions for Students (* for online CTFs)

Name	Host/Developer	When	Focus
PicoCTF*	Carnegie Mellon	All year	Reverse engineer, break, hack, decrypt
PlaidCTF*	Carnegie Mellon	Apr	Web hacking, binary reverse engineering, exploitation, forensics, cryptography
CSAW CTF	NYU-Poly	Nov	Reverse engineer, web, crypto, and forensics
UCSB iCTF*	UC Santa Barbara	Mar	Attack other teams while defending self
US Cyber Challenge	Center for Internet Security	Summer	Identify vulnerabilities, forensics analysis, packet capture analysis
Panoply	UT San Antonio	Sep	Network defense competition; control & operate critical services (SMTP, DNS, etc.
CPTC	RIT	Oct	Pentest; attack & find vulnerabilities
CCDC	UT San Antonio	Apr	Detect and respond to outside threats, maintain availability of existing services, respond to business requests, and balance security needs vs. business needs
CyberPatriot*	Air Force Association	Nov-Feb	Find and fix security vulnerabilities in Windows and Linux operating systems
CyberAcademcy*	MITRE	All year	Web hacking, binary reverse engineering, exploitation, forensics, cryptography

For cyber-defense to be effective in the general population and with future cyber-professionals, students across *all* STEM fields need to learn about SE and its relevance to cybersecurity. While it is possible to partner with the existing competitions noted above, doing so would dilute the relevance of SE and make it a minimal part of a larger, technical competition.

2.2. Existing SE Awareness and Training Programs

DefCon hosts a SE village where participants can attend conference style SE talks and partake in a hands-on SE competition, during which they can attempt vishing, a SE technique that occurs via the phone [13]. The first conference that exclusively showcases SE and intelligence gathering is the Layer8 conference [14]. Attendees at this conference can participate in SE talks, hands-on workshops, and small-scale competitions [14].

Social Engineer Inc, and the SANS Institute also offer specialized SE courses and trainings. During these events, participants can learn about Open Source Intelligence (OSINT), communication styles, psychological manipulation techniques, reconnaissance, and phishing [15, 16].

Another type of SE awareness program that has recently gained popularity is video podcasts. One such podcast series is hosted by the Layer8 conference, which discusses SE in the context of professional social engineers' experiences and stories [17]. OSINTCurio.us is another project that provides a variety of videos and podcasts [18]. Their programs offer case studies that demonstrate the successful implementation of tools used to conduct OSINT [18].

The aforementioned SE programs and events provide participants with awareness and hands-on experiences in SE through podcasts, conferences, and trainings, and serve as an inspiration for this SECTF.

2.3. A purely Collegiate SECTF grounded in the social sciences

The current technical CTFs (§ 2.2) do not emphasize the relevance of the human-socio-psychological aspects of cyberattacks and cybersecurity. Existing SE awareness and training programs are expensive and remain outside the reach of the typical student and educator. Furthermore, they do not cater to the additional requirements of dealing with student populations, ethics boards, and connecting theory and practice via an academic curriculum. As such, a pure Collegiate SECTF grounded in the social sciences offers a timely and unique platform for students to learn about social engineering in a hands-on, engaging, and ethical manner.

The human factor has often been identified as the weakest link in cyberattacks, which can be exploited via SE. Studying the human and behavioral aspects of cyberattacks is the particular forte of the social sciences, and as such this discipline is ideally positioned to lead the efforts in cybersecurity awareness and training.

3. SECTF planning

The authors had to manage several components for the SECTF to function smoothly.

3.1. Flag development

The authors worked with the XXXXXXXXX XXXXXXXXX, the XXXXX to be focused on social engineering and intelligence gathering. The XXXXXXXXX is an official 501(c)(3) non-profit organization. This partnership formed the organizing team, which was instrumental in identifying SE flags (tasks) that were realistic and ethical.

The SECTF had three flags: OSINT, vishing, and phishing. The first flag was OSINT. Open Source Intelligence (OSINT) involves gathering information that can be "obtained legally and ethically from public sources" [19]. Selected teams were given a target local to their geographic location. Teams then had to identify a checklist of items for that target; each item was worth a predetermined set of

points. Some of these items included: employee email addresses, visiting hours, name of parking company, name of receptionist, name of cleaning company, name of food services company, and photo of employee badge. Students could identify these items using OSINT alone and had to provide replicable URLs and screenshots as proof. While OSINT was conducted on a real company and its employees, students were not permitted to go beyond these reconnaissance stages (§ 3.4).

The second flag was phishing, which was based on the first flag. Phishing occurs when a target is contacted via email by "someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords" [20, p. 1]. Each team was required to submit one phishing email that was based on the information obtained via OSINT. Thus, this email had to be framed in such a way that it was addressing someone at the target organization the team was assigned. This email had to be sent to the organizing team's email address (and not a real organization/ individual) by a preassigned time. The grading for this flag was subjective and based on the phishing email's believability and email signature.

The third flag was vishing, which was also built on the first flag. Vishing occurs over the phone, and "appears to be from a trusted source, but isn't. The goal is to steal someone's identity or money" [21, p.1]. Teams had to provide the names and titles of individuals (identified during OSINT) they planned to target. The judges posed as these individuals, so that students could 'target' them via a vish call. Teams were given 20 minutes to place three vishing calls; however only one team member could engage with a judge during each call. Here, teams had to extract information such as the type of operating system, the browser type and version, and email client that were used by the 'target'. The grading for this flag was subjective and based on student confidence, ability to build rapport, ability to adapt to any hurdles introduced by the judges, and the amount of information they were able to extract from the judges successfully.

3.2. Judges

Six professional social engineers were recruited to serve as judges for the event. Their role was to select the competing teams from the application pool (§ 3.6), fine tune the structure of the flags, engage with the students during the live SECTF, grade their performance, and debrief with students at the end of the competition. The judges also hosted 1-hour workshops for each of the three flags to ensure that new and seasoned students received an introduction and refresher respectively on the topics of OSINT, vishing, and phishing. These workshops, which occurred during the live SECTF, were also open as a free resource to students and educators not participating in the competition, but still wanted to benefit from the educational content.

3.3. Ethics

Each of the three flags listed above were vetted by the ethics board at the authors' home institution. The authors began engaging with the ethics board in March to ensure that careful consideration was given to each flag and corresponding student engagement. Given that the flags did not target real companies or their employees, but rather the competition judges, the SECTF project was reviewed and determined as not constituting human subjects research.

Pre and post event open-ended surveys were also designed and reviewed by the ethics board. The pre-event survey asked teams how they prepared for the event, what their expectations were, how their groups were formed, and what type of cybersecurity experience they had. The post-event survey asked specifically about the SECTF and its structure/logistics, as well as their opinions and experiences on each of the flags, including a summary of their strategies, division of labor, and how effective they thought their strategies were.

3.4. Risk management

To ensure that teams would engage in ethical behavior during the competition, the authors worked with the risk management unit at their home institution to design several waivers. Like the conversations with the ethics board, the authors engaged with the risk management unit in March to ensure that waivers were designed with careful thought on ethical code of conduct that ensured student safety and that no targets assigned for OSINT would be harmed.

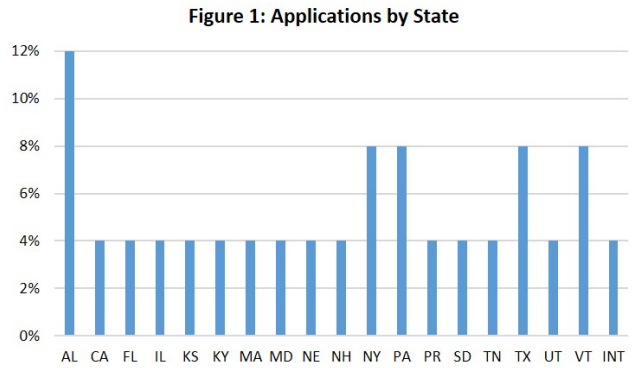
Each member of the selected teams had to complete three waivers to maintain participation eligibility. The first waiver ensured that students would not contact the target or its employees and that they not disclose any information found during the SECTF for an indefinite period of time via any platform. The second waiver ensured that students would not cheat or use external/professional assistance. The third waiver included an audio-visual release that would allow the authors to use images, audio, text, and video generated during the SECTF for event promotion and dissemination via conferences, publications, and podcasts by the authors.

3.5. Advertising

The SECTF was advertised on two platforms: the National Initiative for Cybersecurity Education (NICE) Competitions Subgroup listserv and the Women in Cybersecurity (WiCyS) forum. Additionally, the organizing team used its own social media accounts to promote the event.

3.6. Applications

The SECTF was open to undergraduate students across all disciplines. A total of 25 applications were received, 24 of which were from the United States, and one was international (see Figure 1).



Students entered the competition with their team composition details, their designated mentor information, and a team essay that expressed their interest in participating in the SECTF. Teams ranged from 1 to 6 members.

Majority of the applications featured seniors (41%), which was closely followed by juniors (36%), as seen in Figure 2. Sophomores made up 17% of the applications and freshmen had the least presence (6%). This indicates that advanced students were more interested to compete in the competition.

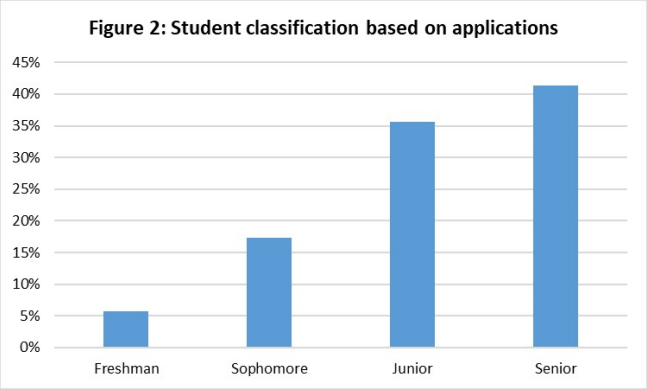
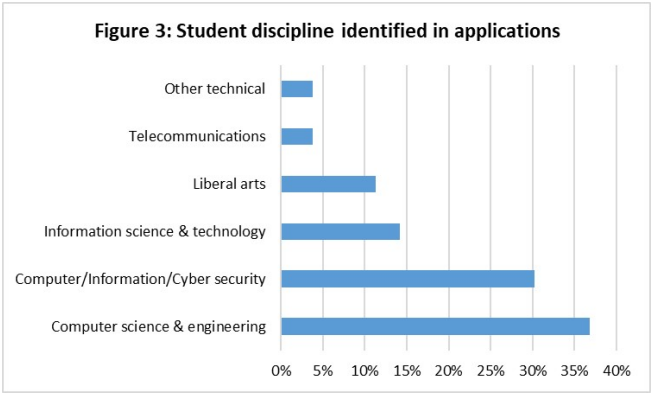


Figure 3 shows that the majority of the applications featured students from the technical domain: computer science & engineering; information science & technology; cybersecurity; and telecommunications made up for 85% of the student disciplines as listed in the applications. Liberal arts students, featuring English, Criminology and Psychology majors, made up for 12% of the student disciplines. Interestingly, 4% of the students majored in an assortment of fields, such as neuroscience, spatial science and biomedical engineering.



3.7. Selection criteria

Judges selected 6 teams based on two main criteria. First, they chose teams that stood out in terms of their passion and desire to compete as expressed in their application essay. Second, judges chose teams that were diverse in their composition with regards to gender, race, and discipline. This second criterion ensured that the selection process aligned with the National Science Foundation's commitment to broadening participation. The selected teams varied in size and composition, featuring 77% technical students and 23% liberal arts students. A majority of the students were seniors and juniors with a handful of sophomores; there were no freshmen across the six teams. All six teams had to complete the three waivers identified in § 3.4.

4. The inaugural Collegiate SECTF

The 2020 SECTF was initially scheduled to be in-person at the authors' home institution. The Covid-19 pandemic, however, required the organizing team to shift the SECTF to an entirely virtual format.

4.1. SECTF platform

The SECTF employed the zoom platform for real-time 'face-to-face' interaction, shared google drives which housed competition instructions and the final reports completed by the teams, and the organizing team's email address to interact with the teams and/or address their inquiries during the live competition. Selected teams also completed test runs with the authors to ensure that they could access the zoom platform and shared drives.

4.2. Psychological persuasion techniques

Each team was given a one-page information sheet on various psychological persuasion techniques that are often used in SE, such as authority, commitment, consistency, reciprocity, likeness or commonality, scarcity, social proof, and a natural inclination to help [22]. Attackers who utilize authority as a principle of persuasion rely on the victim's will-

ingness to comply with authorities, despite their own personal ethics [22]. Commitment is used to persuade victims by targeting their beliefs and commitments, and consistency relies on the fact that people act and behave in a manner consistent with their beliefs [22]. Reciprocity relies on the fact that people are likely to return favors when one is given to them [22]. Likeness or commonality is used when perceived similarities between the attacker and victim enhances the victim's compliance [22]. Scarcity persuades people through offering opportunities or objects that are seen as less available or highly valuable [22]. Social proof exploits the tendency that people are more likely to comply with a request if others have already done the same [22]. Lastly, attackers can persuade their targets to help them execute their attack by posing as someone in need of assistance, as people have a natural inclination to help others who are in need [22].

4.3. The live SECTF

The SECTF took place from October 2-4, 2020. Day 1 started with opening ceremonies, where the organizing team introduced the event, and the judges and the participating teams introduced themselves. The opening ceremony was followed by the first workshop, which focused on OSINT, after which the competition officially began. Each team started with the first flag, OSINT, and was given its respective target. Teams had 19 hours to complete their OSINT and generate a report which was due by 9am on Day 2. Students documented which of the checklist items they were able to find, and also provided the names of individuals (and their details, such as job title/description) identified through the OSINT that they planned to target for the vishing flag.

After the OSINT reports were due on Day 2, two more workshops, focusing on vishing and phishing, were offered. Teams were then given specific time frames during which they had to vish the judges (who posed as targets identified in the OSINT reports) and send out the phishing email to the organizing team. Vishing occurred over the zoom platform. To simulate a phone call experience, only the audio format of zoom was utilized. As noted in § 3.1, each team was given 20 minutes to place three separate vishing calls. While one of the team's member had to extract specific information from the judge, the latter introduced several hurdles, such as asking the student to repeat the question or placing the student on hold, to not only simulate realistic situations, but also to test the student's ability to adapt in real-time, and the quality of that adaptation. Each team was given similar resistance and obstacles to ensure experience consistency and fairness. When the teams were not scheduled to vish a judge, they worked on designing a phishing email that utilized the information generated through the OSINT flag. The phishing and vishing components of the competition occurred for 4 hours, after which teams had to work on their deliverables for the next day.

On Day 3, teams had to give formal 15-minute presentations to the judges about their findings for all three flags, which was followed by a 5 minute Q&A round, where judges asked specific questions that teams had to answer. After the formal presentations, judges graded the reports, vishing, and phishing flags. The judges then held one-on-one informal debriefing sessions with each team, where students could get feedback from, and ask questions of, the judges; students were not told of their ranking during these informal debriefings. Day 3 concluded with the closing ceremonies, where the winners were announced.

5. Student Experiences

We captured student experiences primarily via the open-ended surveys and debriefings of all participating teams, and podcasts that the authors recorded with the winning teams. As noted in § 3.3 and § 3.4, the participating teams signed waivers allowing us to share their experiences as a contribution to the cybersecurity education discourse.

5.1 Why compete in SECTF

Many teams reported wanting to compete in the SECTF because it was an experience they had never been offered before. Some of the teams were not familiar with SE and wanted to know what it meant in the context of cybersecurity. Teams also appreciated that the SECTF was not focused on technological aspects, so that they could use their social and interpersonal skills to compete. This competition also helped the teams understand that the human mind is the weakest link in cybersecurity: "you learn how to do the offense, and when you learn that, you learn about the defense, and you learn that people are susceptible to these things especially as technology advances." While this was out of the comfort zone of most teams, they wanted to "gain as much as [they could] from this competition…because in the classroom [they didn't] really learn too much about SE…That's just how it is because it's not very easy to teach." Teams took this SECTF as a learning opportunity to see how social engineering has an impact on cybersecurity.

5.2. Preparation

Before starting the competition, only one person reported that they were 'completely' prepared for the event. The rest of the participants were 'a little, 'fairly', or 'somewhat' prepared.

Groups did not know their tasks before the start of the competition, and some groups thought this made preparing for this competition difficult. Nonetheless, each team prepared differently. SE strategies that some teams prepared to use were OSINT, pretexting, phishing, and vishing. However, there were participants on some teams who were not pre-

pared to use any SE strategies, instead hoping to learn some during the event. These teams were hoping this competition would serve as an opportunity to learn, grow, and improve.

While some students took a passive approach to preparing for the competition, other participants actively trained. One student explained, "I started out by getting whatever my advisor gave me and watched extra lectures outside my studies because he gave me access to his lectures. So I watched those and did some tutorials and tried to build up my knowledge a bit more. Other than this general stuff, I thought I'd just go with an open mind because I wasn't sure what tasks I was getting."

Furthermore, instead of practicing specific SE strategies, other groups focused their preparation on teamwork. One group stated, "we are aiming to develop familiarity and comfort with each other so that we [could] work effectively as a group when it [was] time for the competition." Larger teams emphasized "building on each other's work and helping each other when [they got] stuck."

After the competition, several members from one team reported that they felt 'not prepared at all' while competing, whereas the rest of the teams reported feeling either 'a little' or 'somewhat' prepared. Many participants wish they had prepared more for conducting and compiling a report for OSINT. Other team members noted that they should have prepared more for vishing.

5.3. Group formation

The groups differed in terms of how well the members knew each other. Some teams consisted of members who knew each other for years beforehand, from being in the same cybersecurity club, working at the same research center, or having classes together. For example, one group explained that "We all had experience, we're all friends with each other, so we got a group of friends together that we know we would be able to work together with, and just have fun". Other groups had members who had only met for the first time in the months leading up to the competition, in which the teammates all responded to an email calling for participation. Often times, one or two team members would know each other but not the rest of the team, instead having mutual acquaintances with members in the group. While most teams seemed to readily accept team participants, one team had a stricter and more competitive formation, in which they had to write to the school's cybersecurity club explaining why they should be chosen to be on the team. As such, about 2/3 of the participants reported that they had not worked with their groups before in other cybersecurity exercises. So, it was important for team members to become familiar with each other before the start of the competition.

For instance, a team member from one school stated, "[We] didn't really know each other and.. I don't think there was ever a time when we all actually met or talked before." The team continued, "So I had the novel idea of making group meetings with all of us, … other teams [have members] that know each other, and they've worked with each other before and … we didn't really know each other's personalities, so I reached out to everyone to see if we could have these weekly meetings leading up to the SECTF to build up comradery". During these meetings, the team members combined their skillsets to practice working together, hoping to apply their team's unique skillset to the competition.

5.4. Group dynamics

As the competition was virtual, most teams' members were not in physical proximity of each other. Instead, teams connected virtually so that they could still work together efficiently. For instance, one team said, "Luckily we all had iPhones, so we used Facetime and that was really convenient, but we also had a google doc opened. If we had any questions, we could just facetime – it was faster." In addition to Facetime, other teams used Zoom or Google Docs to stay connected to each other.

However, it was harder for teams to collaborate on certain flags, such as OSINT. One team explained how "We didn't have a systematic approach; we just stumbled upon [the flags] haphazardly. We didn't have a set agenda. We knew [what to] look for, but we didn't have dedicated routes to discover them," further explaining how "it was definitely a free for all."

The group dynamics also played a factor in deciding which team members would complete the live vishing calls. One team explained that their team members chose on a volunteer basis, requiring group members to step forward if they thought the task aligned with their strengths. It was important for teams to understand each other and their skill sets. If one person had prior experience with a specific flag, then they could take the lead on that flag.

A theme in successful group dynamics during this competition was constant communication among team members. One of the winning teams explained that "we did a zoom session all weekend. We were collaborating at the same time and playing to each other's strengths and weaknesses." This team also explained how they frequently worked independently but would also work collaboratively at times if one member needed help.

Another winning team took shifts to complete the flags, so that some team members worked through the night while others slept and woke up early.

5.5. Strategy and adaptations

One of the key strategies that teams reported using was focusing on OSINT. Finding sufficient information and organizing it well in this part of the competition helped the

teams create their pretexts for phishing and vishing. Additionally, using their OSINT in the phishing and vishing components made their pretexts more credible and believable.

Another key strategy was constant communication among team members. Teams reported doing well because they were able to collaborate and divide up work well. Because of their communications, team members could avoid finding repetitive information during OSINT and could help each other create the pretexts for phishing and vishing.

Teams reported doing well because they were able to collaborate and divide up work well. Thus, letting an experienced team member take the lead on a certain flag was an important strategy. On some teams, group members, had specialized experience in creating OSINT reports, writing phishing emails, working in the same industry as the target, or serving as IT support (a common vishing pretext). Letting these team members take the lead on the corresponding flags helped direct the teams and divide the labor more easily.

To adapt to some of the challenges thrown at the team members during the vishing flag, the caller would have OSINT ready to provide more information, and a general note sheet with answers to common questions. Other teams even did mock calls in the time leading up to the live vish to rehearse and practice. Generally it was important that teams, "[were able to] think flexibly… change what [they were] doing if it [was] not working, and [realizing} that [it was] okay [to] just go a different way." For instance, if the vishing call was not going well, the caller would stall to try to get around the obstacle. One team member even employed 'crying' while targeting the judge to elicit sympathy to obtain information to complete the flag successfully.

5.6. Likes, dislikes, and favorite flags

Many of the groups reported enjoying the OSINT flag, despite feeling overwhelmed while engaging in it. Groups also stated that this flag was took the longest amount of time but was useful in completing the two subsequent flags, as it provided information on which they could base their pretexts. While frustrated at times, teams felt high levels of excitement after finding a flag that they had spent time searching for. Teams also reported that this flag was easy to collaborate on as there was so much information to find. Overall the teams seemed to like completing this flag and were generally surprised by how much sensitive information could be found by using open-source resources.

Some groups thought that the easiest flag to do as a deliverable was phishing. Although most of the groups felt rushed and constrained for time during the flag, they enjoyed the simplicity of the flag as a "direct assignment where [they] knew the outcome." Teams reported that they relied on their OSINT results to complete this flag and create a believable pretext, combining this information with psychological persuasion principles such as urgency. One participant noted, "I thought that [flag] was a really interesting [one] and see how much OSINT you can put behind it to gain trust. The phrase 'the devil's in the details' [really captures] it. You cannot use your tone of voice or pauses. There are a lot of elements that just disappear by writing [the phishing email]. So it was interesting to see how to SE by just writing." Team members also drew on their personal work experiences to create their phishing emails, as they explained that phishing emails are common occurrences in the work environment.

The vishing flag was often described as an adrenaline rush, and while it was intimidating, it was still fun. This was generally reported as the most stress inducing flag for the groups, as they did not know what to expect: "We did not know if the other person on the phone would be an easy target or be reluctant to give us flags." Generally, the callers reported that they felt overwhelmed during the performances and that this was the most difficult part of the competition. Unlike the other flags, vishing required live interactions with their targets/judges, with no time to hesitate or receive help from their team members after the call started. In creating the pretext for the vishing call, groups relied again on their OSINT, but still, people found creating the pretext to be hard "because there are so many different ways to approach it. [You were told what information to extract], but you had to create on your own the pretext that you had to do… there was a lot of freedom given to us for that vish, which was daunting." Participants felt especially stressed and overwhelmed during the live vish because "at times where I was getting stuck, I was panicking because I didn't know what to do, I don't know what to say because there wasn't a predetermined script – it was intimidating". To prepare for this, groups made documents envisioning how the call would go and trying to plan answers to questions they might be asked.

During the live vish call, teams used different strategies to extract the required information. While some used a sense of urgency, others tried to take a calmer approach. One group explained how "I had watched a class delivered by a former FBI hostage negotiator and he puts a lot of emphasis on how to put an effective negotiation and frame it as a collaborative effort. So I [didn't] frame it as I'm the authority figure demanding all this information [but rather] I'm trying to do my job, you're trying to do your job, so how can we both arrive at this collaborative outcome?"

Another aspect, other than the live component, that made the vish call more challenging than the phishing email was that the nature of a vish call requires a deliberate tone of voice. One group explains that "Because this was a vishing

call you couldn't really tell someone's body language … so I tried to be a little more consistent and firm in what I was saying and sounding like I know what I'm saying." To do this, teams would have OSINT in front of them to reference if they needed more information. The team member continued: "I wanted to sound calm, I didn't want to create urgency in my voice [but rather] in the situation."

Participants explained that once they started on the vish calls they became easier, and that "a few minutes in, you just [got] into it and without even realizing that you're [not] you anymore." Teams emphasized that during the vish, the key to success was taking on the role of the pretext, which helped them to react quickly and engage with their targets smoothly.

5.7. SECTF Learning Benefits

All of the teams reported learning new information from competing in the SECTF. Outside the context of SE, this competition taught teams the importance of collaborative group work. For many teams, this competition was the first introduction to direct experiences in phishing and vishing. Teams also reported that this event enlightened them to the realities of OSINT. Overall, it taught the teams "how vital SE is to the future of cybersecurity," which they explained is not taught or emphasized much in their technical cybersecurity classes. One participant also explained that "I did not know that a career can be made from doing these sorts of tasks like OSINT, vishing, and phishing. I am eager to stay more updated in this field." Whether this competition served an introduction to SE or was additional practice, each participant reported receiving learning benefits from competing.

5.8. Why SE?

Teams reported wanting to be involved more with SE because it is the side of cybersecurity that is often overlooked in their classes. They were accustomed to learning the technical side of cybersecurity but now were aware that SE was just as important. A group member reported that SE was relevant to the extent that they would "apply it in everyday life and work." Another participant explained that "SE [was] important because the human element [was] the weakest link. And we are only as strong as our weakest link. It doesn't matter how much we are hardening our technical systems. If we still haven't hardened our human element…then the system will still be weak."

6. Discussion

6.1. Proof of concept, limitations and lessons learned

Overall, the inaugural SECTF was a success and ran smoothly without any technical glitches for zoom, shared drives, and email correspondences, and aligned with the structure logistics and allotted time.

The authors' biggest undertaking was to demonstrate that a safe and ethical platform could be developed to teach students about SE via the experiential learning process. Experiential learning is an active learning strategy, where students learn through action, learning by doing, learning through experience, and learning through discovery and exploration [23]. As detailed in § 5, the SECTF served as an experiential learning medium and allowed students to try their hand at SE, which they otherwise may not have been exposed to.

While the SECTF was implemented successfully, there were two limitations. First, the covid-19 pandemic forced the organizing team to make the competition virtual. The online platform prevented students from experiencing in-person SE flags, such as developing pretexts, shoulder surfing, etc. [24, 25]. The authors note that physical face-to-face SE is as important an experience for students as is virtual SE, which was addressed by the 2020 SECTF. Interestingly, this virtual delivery could also be viewed as a benefit. We found a good proportion of applications coming from smaller universities and community colleges. Students from these institutions stated in their applications that the virtual nature of the SECTF enabled them to participate as they did not have to worry about finances in general, and travel during the pandemic, while still getting a chance at learning about SE and engaging with SE experts.

A second limitation was that the authors did not do a pre-post study specifically using the SECTF as an *intervention*, to gauge student learning and their perceptions towards SE before and after participating in the competition. The authors, however, wanted to primarily develop a proof of concept and ensure that all the components addressed thus far (logistics, structure, ethics, risk management, establishing partnerships with nonprofits and industry) could be implemented. In short, the inaugural SECTF established the foundation and will serve as a stepping stone to delve further into student engagement and learning in the future.

In addition to these limitations, the authors learned two lessons, especially as this was the organizing team's first attempt at a national collegiate SECTF. First, teams provided feedback that some of the instructions for the flags could have been clearer, which would have avoided confusion during the live SECTF. While this was a minor issue, the authors will address it moving forward.

Second, while the judges interacted with the teams, the authors served as the backend infrastructure operators. They ensured that all the zoom meetings for the opening and closing ceremonies, webinars, vishing flags, formal presentations, informal debriefings, and judges' room worked efficiently. They were also responsible for ushering the teams and judges to the various zoom rooms as per the schedule. They also held virtual office hours, where teams could

email their inquiries during the SECTF and respond in a timely manner. While this two-person infrastructure team was successful, a larger team at the authors' home institution would help with coordination and scheduling.

6.2. Teaching students about ethics

Many CTFs are structured as attack/defense, which allow students to gain experience with both offensive and defensive related skills [26]. An equally important aspect that should be taught is the "ethical and legal implications of hacking others' machines, services, or networks, and the implications of misusing their skills" [26, p. 1]. The SECTF offered the offensive experience via the flags, but also the emphasized the ethical aspects via waivers that students signed agreeing to ethical conduct and not causing harm to OSINT targets and their employees. The judges, who were SE experts in the field, further echoed the relevance of ethical behavior during the opening and closing ceremonies, as well as the informal debriefings. One team stated that that SE should be "used for good rather than evil, use it for education rather than manipulation. It's good to expose these flaws, but that's a learning experience, not a monopolizing experience. You're not going to take advantage of these people".

6.3. Benefits of academia-nonprofit-industry nexus

As noted in [27], higher education institutions acknowledge the need for more "collaborative, multidisciplinary, entrepreneurial, and global education". The authors agree with this notion, which is why they partnered with XXXXX XXXXXX and brought in professional social engineers with multiple years of industry experience. The SECTF initiated a dialog between SE experts, social scientists (the authors), and students. This dialog is instrumental for the future workforce to learn about the relevance of the human factor in cybersecurity from experts with real world SE experience.

The collaboration between the judges, XXXX XXXXX, and the authors allowed for the creation of flags that were realistic. The OSINT, phishing and vishing SECTF flags were often used by professional SE experts during their reconnaissance operations and penetration testing activities. Furthermore, the judges used their own experiences to engage with the students in real-time during the vish, grade the flags, and debrief with the students; thus injecting SE field experiences into the competition. The academic component ensured that the flags remained within ethical and risk management bounds that kept students safe, did not cause harm to targets, and offered an engaging hands-on learning experience.

Many students expressed that they had never experienced an event like the SECTF and many felt that they were outside their comfort zone. They acknowledged that they did not get this experience in their undergraduate courses, and that the SECTF addressed this deficit. Technical students stated that while their coursework was important, it did not train them in the SE space. Non-technical students stated that the SECTF helped them understand and appreciate how their own disciplinary training was relevant in cybersecurity. All students (regardless of their discipline) said that having well-renowned SE experts as judges, knowing that they had designed and graded the flags, being able to engage with them especially for vishing and debriefing, made the SECTF experience memorable and realistic, further supporting the need for, and benefit of, an academia-industry-nonprofit nexus.

6.4. NICE Framework Mapping

The SECTF competition has been mapped on to the NICE Cybersecurity Workforce Framework (NICE Framework). The NICE Framework, National Institute of Standards and Technology (NIST) Special Publication 800-181, is a nationally-focused resource that categorizes and describes cybersecurity work [28]. The NICE Framework establishes a taxonomy and common lexicon that describes cybersecurity work and workers irrespective of where or for whom the work is performed. It is comprised of seven workforce categories with a subset of 33 Specialty Areas, as well as Work Roles, Tasks, and Knowledge, Skills, and Abilities (KSAs) [28].

Knowledge is a "body of information applied directly to the performance of a function" [28, p. 5]. The SECTF can be mapped to the following Knowledge IDs and descriptions:

K0110-Knowledge of adversarial tactics, techniques, & procedures. The workshops provided students with the basics of OSINT, vishing and phishing, which they would later apply towards the competition.

K0426-Knowledge of dynamic and deliberate targeting. Each of the workshops offered students with examples of real world OSINT, vishing, and phishing, allowing them to learn about current patterns and trends and how the threat landscape is evolving.

K0603-Knowledge of ways in which targets/threats use the internet. The OSINT workshop demonstrated how threat actors could use open source information available online to develop a detailed target profile.

Cybersecurity Skills involve the "application of tools, frameworks, processes, and controls that have an impact on the cybersecurity posture of an organization or individual" [28, p. 5]. The SECTF can be mapped to the following Skill IDs and descriptions:

S0052-Skill in the use of SE techniques. (e.g., phishing, vishing etc.). Students were able to apply the knowledge

obtained via the workshops to try their hand at three main adversarial techniques of vishing, phishing, and OSINT.

S0044-Skill in mimicking threat behaviors. Students experienced this best with vishing as they had a real-time dynamic interaction with the judges who served as targets. Students deliberately targeted the judges and had to adapt to any hurdles given by the judges. Students also mimicked phishers when they designed phishing emails that was based on the OSINT information they found.

Ability is "competence to perform an observable behavior or a behavior that results in an observable product" [28, p. 6]. The SECTF can be mapped to the following Ability IDs and descriptions:

A0107-Ability to think like threat actors. Each flag was structured to be attack-centric. Thus, students developed the ability to grow their offense skill sets and think like cyber-adversaries. They engaged in reconnaissance (OSINT), and designed specific attack vectors (vishing and phishing).

A0088-Ability to function effectively in a dynamic, fast-paced environment. The 2-day SECTF, like many Collegiate CTFs, was temporally compressed, thus requiring students to manage the flags in a dynamic environment. All teams strategized about how best to complete the flags, while adapting to any hurdles and challenges they experienced.

While technical CTFs can certainly be mapped to the NICE Framework, the authors demonstrated that a purely SE based CTF mapped effectively as well. According to [28], academic institutions are an essential part of preparing and educating the future workforce. Developing and delivering exercises, such as the SECTF, that align with the NICE Framework allows institutions to prepare students with skills needed by employers.

7. Conclusion

Technical CTFs catered to students are undoubtedly an important investment, however, this pool of students is *too small and homogeneous* to support the holistic development of the solutions needed in our technologically dependent society [29]. *Enlarging and diversifying* the pool of students learning SE will cast a wider net to recruit the most talented students as well as to foster their *creative potential* as they enter the cybersecurity workforce [29].

This paper has made the case for the need for a purely SECTF event. It has demonstrated a successful proof of concept, adhering to ethics and risk management, while simultaneously providing a fun and meaningful learning experience.

Technical domains should also incorporate SE in cybersecurity education and training programs. Computer science faculty should offer a basic discussion of SE in courses to bring awareness to the threat that SE poses to data confidentiality, which is ultimately guarded by humans (the weakest link) [30]. Businesses spend a significant portion of their annual information technology budgets on high-tech computer security (firewalls, biometrics, etc.), which make conventional hacking more difficult [31]. Cybercriminals are increasingly using SE to conduct cyberattacks, and as such, students and employees in technical domains must learn how to manage these types of attacks [31, 32].

While this paper examined a Collegiate SECTF, the existing cybersecurity curriculum needs to be revamped to incorporate SE. This would provide an opportunity for technical students to become better developers and defenders, and social science students to realize the value of their discipline and appreciate their contributions. Additionally, more needs to be done to educate the educators. Oftentimes, educators are reluctant to try new projects because they have to develop the instructions and rubrics from the ground up, and they may not be familiar with how to receive ethics approval. Arming educators with these materials would result in a willingness to adopt innovative course projects that enhance the quality and diversity of cybersecurity education. The authors hope that this paper inspires educators and students to consider these efforts in the future.

Acknowledgements

References

[1] Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. Wiley.

[2] Rege, A. (2014). A criminological perspective on power grid cyber attacks: Using routine activities theory to rational choice perspective to explore adversarial decision-making. Journal of Homeland Security and Emergency Management, 11(4), pp. 463-487.

[3] Grassi, P., Garcia, M. & Fenton, J. (2017). Digital Identity Guidelines. NIST Special Publication 800-63-3. Online at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

[4] Rege, A. (2016). Incorporating the human element in anticipatory and dynamic cyber defense. In Cybercrime and

Computer Forensic (ICCCF), IEEE International Conference on, pp. 1-7.

[5] Federal Bureau of Investigation. (2019). 2019 Internet Crime Report. Retrieved February 2, 2021. Online at https://pdf.ic3.gov/2019_IC3Report.pdf

[6] Jakobsson, M. (2016). Understanding Social Engineering Based Scams. Springer New York.

[7] Mitnick, K., & Simon, W. L. (2002). The art of deception. Indianapolis, IN: Wiley.

[8] Rotvold, G. (2008). How to create a security culture in your organization. Information Management Journal, 42(6), 32-38. Retrieved from EBSCO database.

[9] Thornburgh, T. (2004). Social engineering: the dark art. Proceedings of the 1st Annual Conference on Information Security Curriculum Development, 133-135. Retrieved from ACM Digital Library.

[10] Twitchell, D. P. (2006). Social engineering in information assurance curricula. Proceedings of the ACM 3rd Annual Conference on Information Security Curriculum Development, 191-193. Retrieved from EBSCO database.

[11] Hauser, D. M. (2017). Status of Social Engineering Awareness in Business Organizations and Colleges/Universities (Doctoral dissertation, Baker College (Michigan)).

[12] Cyber Security Summer School (CSSS). (2017). Social engineering capture the flag summer school. (accessed September 28, 2018). http://www.studyitin.ee/c3s2017.

[13] Social-Engineer.org (2020). “SEVillage at DefCon”. Online at https://www.social-engineer.org/sevillage-defcon/

[14] Layer8.com (2020). “Layer8 Conference: About Us”. Online at “https://layer8conference.com/about-us/”

[15] Social-Engineer.org (2020). “Social Engineering Training”. Online at https://www.social-engineer.com/social-engineering-training/

[16] SANS (2020). “SEC567: Social Engineering for Penetration Testers”. Online at

https://www.sans.org/course/social-engineering-forpenetration- testers

[17] Layer8.com (2020). “The Layer 8 Podcast”. Online at https://layer8conference.com/the-layer-8-podcast/

[18] OSINTCurio.us (2020). “OSINT Videos and Podcasts”. Online at

https://osintcurio.us/osintvideosandpodcasts/

[19] R. D. Steele, “The importance of open source intelligence to the military,” International Journal of Intelligence and Counter Intelligence, vol. 8, no. 4, pp. 457-470, 1995.

[20] Phishing.org (2020). “What is phishing?”. Retrieved January 16, 2021. Online at phishing.org/what-is-phishing

[21] Norton (2020). “What is vishing? Tips for spotting and avoiding voice scams”. Retrieved January 16, 2020. Online at https://us.norton.com/internetsecurity-online-scams-vishing.html

[22] Uebelacker, S. & Quiel, S. (2014). The Social Engineering Personality Framework. Online at https://www.researchgate.net/publication/271135217_The_Social_Engineering_Personality_Framework

[23] Rege, A. (2015). “Multidisciplinary Experiential Learning for Holistic Cybersecurity Education, Research and Evaluation”. Proceedings of the 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education. (3GSE 15).

[24] Rege, A., Mendlein, A. & Williams, K. (forthcoming). "Security and Privacy Education for STEM Undergraduates: A Shoulder Surfing Course Project". Proceedings of the IEEE Frontiers in Education.

[25] Rege, A., Williams, K., Mendlein, A. (2019) “An experiential learning cybersecurity project for multiple STEM undergraduates”. Proceedings from the IEEE Integrated STEM Education Conference.

[26] Demetrio, L., Lagorio, G., Ribaudo, M., Russo, E., & Valenza, A. (2019). ZenHackAdemy: Ethical Hacking@ DIBRIS. In Proceedings of the 11th International Conference on Computer Supported Education (CSEDU). (pp. 405-413).

[27] Finnegan, J., & Llewellyn, D. C. (2020). Breaking Down the Silos: Innovations for Multidisciplinary Programs.

[28] NICE (National Initiative for Cybersecurity Education) Framework
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[29] Start-Engineering.com (2018). "In Cybersecurity, Change Describes Education and Threats Alike". Retrieved September 28, 2018. Online at http://start-engineering.com/

[20] Hauser, D. M. (2017). Status of Social Engineering Awareness in Business Organizations and Colleges/Universities (Doctoral dissertation, Baker College (Michigan)).

[31] Twitchell, D. P. (2006). Social engineering in information assurance curricula. Proceedings of the ACM 3rd

Annual Conference on Information Security Curriculum Development, 191-193. Retrieved from EBSCO database.

[32] Lineberry, S. (2007). The human element: The weakest link in information security. Journal of Accountancy, 204(5), 44+. Retrieved from Gale Business Collection.