Exploring the MITRE ATT&CK® Matrix in SE education

Rachel Bleiman[1], Jamie Williams[2], Aunshul Rege[3], and Katorah Williams[4]

[1] Temple University, Philadelphia PA, USA
Rachel.bleiman@temple.edu
[2] The MITRE Corporation, USA
jcwilliams@mitre.org
[3]Temple University, Philadelphia PA, USA
rege@temple.edu
[4]Temple University, Philadelphia PA, USA
Katorah.williams@temple.edu

Abstract. Cybersecurity is a multidisciplinary field that requires understanding of human behavior. To reinforce this idea and encourage non-technical students to participate in cybersecurity, an experiential learning project was implemented to an upper-level undergraduate criminal justice class. This paper is focused on a class project in which groups of students mapped a social engineering case study onto the MITRE ATT&CK framework to understand the adversarial mindset. The paper provides background information on the ATT&CK framework, compares groups' mappings to each other within the class as well as against a mapping done by an ATT&CK representative, and offers a discussion on the analysis. This paper demonstrates that while someone with more knowledge and experience using the framework may map a SE case study differently than multidisciplinary students who are experiencing it for the first time, there is not a single correct way to map onto the matrix. Having students experience this mapping project allows them to understand the breakdown of an adversary's behavior and interpret key tactics and techniques in a way that fits their mapping needs. This paper also demonstrates how a SE case study can be mapped onto the ATT&CK framework despite SE not being the focus of the framework, and that SE uses tactics and techniques that are also relevant to technical cyberattacks. The authors hope to encourage more interdisciplinary cybersecurity education by sharing this course project.

Keywords: cybersecurity education, social engineering, experiential learning, adversarial frameworks, MITRE ATT&CK.

1 Introduction

Cybersecurity is often thought to be a technical field, in which only those with technical knowledge, such as coding, can contribute. However, that is not the case. In fact, cybersecurity should be a holistic, multidisciplinary field. Cyberattacks are committed by humans, and thus, understanding human behavior is an important element in defending

against such security threats. Furthermore, according to the National Institute of Standards and Technology (NIST), which is part of the National Initiative for Cybersecurity Education (NICE), the global shortage of cybersecurity professionals is estimated to be 2.72 million [1]. As current students are the next generation workforce, it is vital that they learn the necessary skills to participate in the cybersecurity field, whether that be in a technical or non-technical position. While students in technical fields are typically aware of opportunities within the cybersecurity field, many non-technical students are not aware that cybersecurity is even a career option.

One way to promote and advertise cybersecurity careers to non-technical students is through education on social engineering (SE), which is the act of manipulating others into taking actions that may not be in their best interest [2]. This can include clicking on a link in a malicious phishing email, plugging in a malware infected USB stick, or allowing an unauthorized individual entry into a secure server room. SE is a non-technical tool that is used throughout cyberattacks and can be studied through understanding human behavior; in fact, understanding the human behavior of SE can better help to defend against it. Cyberattacks may be carried out with only the use of SE, or SE may only be used throughout the attack alongside technical measures. Regardless, if only technical skills are emphasized in cyber education, defenders are left in the dark on a major part of an attack, the side of the human element.

One way for non-technical students to study SE in a way that trains them to be better defenders is through experiential learning. Instead of learning about SE via a lecture, experiential learning allows students to have hands-on experience in learning about the topic. While there are several ways to implement hands-on SE exercises, both from the mindset of the offender and the defender, one ethical way is to map adversarial behavior onto an existing framework of cyber adversarial tactics and techniques, such as MITRE's ATT&CK® Matrix [3].

Indeed, this paper will detail such an implementation of an experiential learning project in which students map a SE case study onto the ATT&CK framework. The following section describes other frameworks that exist in the cybersecurity field and extensively describes the ATT&CK framework to justify its use in this project. Next, the authors provide a description of the current study, including an overview of the class in which it was implemented and a description of the assigned SE case and course project instructions. Afterwards, the authors analyze the results from the course project, and compare the results from the various groups with those of an ATT&CK representative, who also completed specific parts of the project. The authors conclude with a discussion of the implications of the results and limitations of this project.

2 Adversarial Frameworks

In addition to ATT&CK, there are numerous other frameworks that exist within the cybersecurity community for various uses. Such frameworks are offered by the Open Web Application Security Project (OWASP), with both the OWASP Security Knowledge Framework and the OWASP Risk Assessment Framework [4,5]. Both of these frameworks created by OWASP are focused on coding and software security.

Another framework is MITRE's Common Vulnerabilities and Exposure (CVE) Framework, which identifies, defines, and catalogs publicly disclosed cybersecurity vulnerabilities [6]. MITRE's Common Attack Pattern Enumeration and Classification (CAPEC) is another framework that describes adversarial behavior and attack patterns, such as the common attributes and approaches known adversaries use [7]. Some well-known attack patterns that CAPEC describes is HTTP Response Splitting or SQL Injection. Another example of a useful framework is NIST's Mobile Threat Catalogue (MTC), which examines the mobile environment in particular [8]. The MTC contains a structured repository of threats against mobile information systems. While this list is not comprehensive of all adversarial behavioral frameworks, a final framework that the authors will discuss is the ATT&CK framework, which was chosen for use in this case study [3].

2.1 MITRE ATT&CK Matrix

The MITRE ATT&CK framework [9] enables practitioners to understand and track cyber adversary behaviors. The globally accessible knowledge base [3] is maintained by the MITRE Corporation as a means of organizing and analyzing the tactics, techniques, and procedures (TTPs) used by real adversaries. The content within ATT&CK is informed by real-world observations and is continuously maintained via analysis of publicly available cyber threat intelligence (CTI) as well as contributions from the community of ATT&CK users.

ATT&CK is appropriately structured around organizing adversary behaviors into TTPs. Specifically, for each included behavior ATT&CK captures and contextualizes the adversary's:

1. Tactic(s), or "why" the behavior was performed
2. Technique, or "how" the adversary attempted to achieve their tactical goal by performing the behavior
3. Procedure, or "what" the adversary specifically did to implement the technique

Fig. 1.

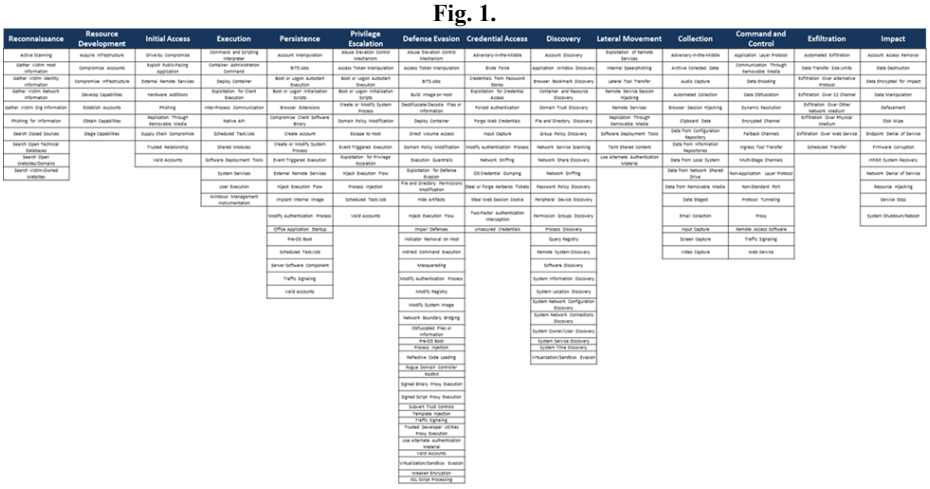

Fig.1: ATT&CK for Enterprise Matrix [10]

Fig. 2.

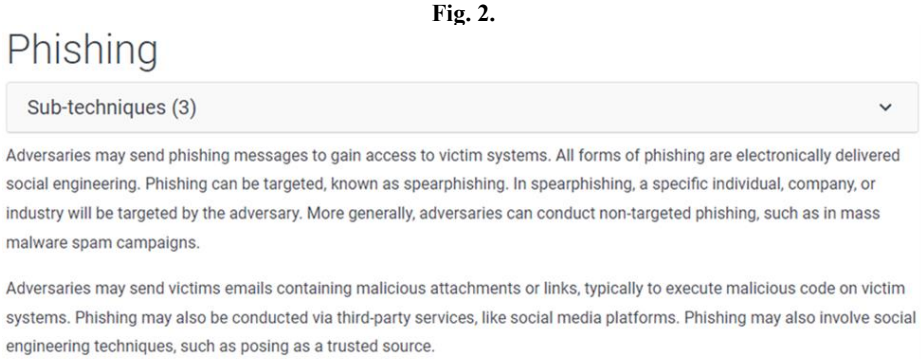

Fig. 2. Example ATT&CK Technique, Phishing (Technique ID T1566) of the Initial Access Tactic

ATT&CK also includes sub-techniques, which are functional equivalents to techniques but describe the specific behavior at a lower level than a technique (where applicable).

Fig. 3.

Figure 3: Sub-Techniques of the Phishing ATT&CK Technique (Technique ID T1566)

The organization provided by ATT&CK not only captures the adversary perspective of malicious cyber operations, but also facilitates the creation of a common, shared language for tracking these behaviors. This enables users to apply ATT&CK towards many operational use cases, including (but not limited to):

- Tracking and organizing new as well as known behaviors observed in threat intelligence/case studies
- Developing and aligning defensive countermeasures for specific behaviors
- Prioritizing and communicating behaviors used by a red or other form of offensive assessment team
- Engineering and documenting an organization's current defensive posture, including strengths and potential gaps relative to specific adversary behaviors

Though ATT&CK is selectively scoped to cyber activities (i.e., those directly involving victimized systems modeled into the framework as platforms), the structure and way of organizing TTPs is applicable to wider domains. This structure -- specifically modeling behaviors into why (tactics), how (techniques), and what (procedures) -- is conducive towards modeling and connecting behaviors to defensive countermeasures. Researchers have explored and used the blueprint of ATT&CK to create similar ATT&CK-like representations of differing adversary behaviors [11].

Concepts such as social engineering are not directly captured in current version of ATT&CK as an individual technique/object, though the application of social engineering is relevant to many technical behaviors. For example, T1566 Phishing as well as many other behaviors exist where the "human-element" associated with the targeted system is exaggerated. These techniques specifically incorporate or even rely-on elements of persuasion, manipulation, elicitation, and impersonation for successful execution.

Utilizing the ATT&CK framework in an educational setting, specifically within a class largely focused on social engineering, allows students to explore adversarial

behavior through experiential learning and understand how social engineering is relevant within cybersecurity. The structure of the framework allows students to see and describe each behavior from the perspective of the adversary, motivating them to compile and question "why" and "how" each individual action contributes to the operational objectives. ATT&CK also creates a common language to describe these behaviors - which is a vital requirement of the greater goal of understanding, tracking, and measuring each behavior against potential defenses.

The following section provides an overview of a multidisciplinary undergraduate cybercrime class and experiential learning project in which students mapped a SE case study onto the ATT&CK framework.

3 Current Study / ATT&CK Mapping Project

3.1 Cybercrime Class Overview

The current case study project was implemented in an undergraduate upper-level criminal justice elective during the Spring 2021 semester and the Fall 2020 semester. The Cybercrime class consisted of students from multidisciplinary backgrounds including liberal arts and technical fields. Throughout each semester, students were divided into groups to engage in experiential learning projects, covering a range of SE topics such shoulder surfing, pretexting, and open-source intelligence, among others. Groups consisted of 5-7 students; some groups were multidisciplinary (from both College of Liberal Arts and College of Science and Technology), while others had students all from the same disciplinary background. One such project that the students were assigned was the MITRE ATT&CK mapping course project. The logistics, results, and discussion of this project are discussed in the following sections.

3.2 Project Description

For the ATT&CK mapping course project, student groups were each assigned a SE case study to read and map onto the ATT&CK framework. This paper will examine and compare the project completed by 3 of the groups across two semesters who were each assigned the same case study: Mission Not Impossible, from chapter 8 of the book "Social engineering: the art of human hacking" by Christopher Hadnagy. This case study detailed a story of a professional social engineer, Tim, who was tasked with infiltrating a server containing sensitive information that was highly protected due to the potential dangers associated with it falling into the wrong hands. The case study detailed a step-by-step account of Tim's planning and actions, allowing students to map techniques he used onto the ATT&CK framework.

The students were given a 2-part project and had about two weeks to complete each part. In Part 1, students had to identify the techniques and subtechniques that mapped onto the case study, providing excerpts from the case study as evidence. They also had to identify techniques from the case study that they could not map to the framework. In Part 2, students had to identify the proportion of techniques for each tactic that they were able to map and explain what their proportions may indicate about the ATT&CK

framework or the case study. Further, students had to redesign the framework in a way that they could attain a better mapping.

To add to the analysis of the results of the project, one of the authors, who is a representative from MITRE focusing on the ATT&CK framework, also completed a mapping of the tactics, techniques, and subtechniques onto the same case study. Their mapping is compared to the student group mappings throughout the following results section.

4 Results

4.1 Part 1 (Sub)Techniques Identified, Excerpt Evidence

Each tactic had at least one group map a technique to it; however, while there were some similarities and overlaps among the mappings, not all groups identified techniques from every category, and the techniques that the groups identified varied. For example, under the tactic of Reconnaissance (see Table 1), Group A mapped the following 5 techniques: Gather Victim Identity Information, Gather Victim Network Information, Gather Victim Organization Information, Search Open Websites/Domains, and Phishing for Information (Vishing). While mapping from the exact same case study, Group B a identified a set of 5 slightly different techniques: Active Scanning, Gather Victim Identity Information, Gather Victim Organization Information, Phishing for Information, and Search Open Websites/Domains. Their mappings were fairly similar, overlapping in 3 of the techniques and differing in 2 techniques. Still within this tactic of Reconnaissance, all 3 student-groups along with the ATT&CK representative agreed on the mapping of 3 techniques: Gather Victim Identity Information, Gather Victim Org Information, and Search Open Websites/Domains.

Interestingly, three techniques under the Reconnaissance tactic that were mapped were only mapped by a single group: Active Scanning, Search Open Technical Databases, and Search Victim-Owned Websites. While all groups read the same case study, these three techniques were each only identified by one of the groups. Two of these three unique techniques were mapped by Group C, who had the highest proportion of techniques mapped from the Reconnaissance tactic as well as total techniques from all tactics. Perhaps they were able to interpret these techniques to better fit the case study and their mapping.

Further, within each technique, groups identified various subtechniques. For instance, within the technique of Gather Victim Identity Information, under the tactic of Reconnaissance, Group B identified all the subtechniques, which were Credentials, Email Addresses, and Employee Names. Meanwhile Group C only identified the subtechniques of Email Addresses and Employee Names (but not Credentials). As with the mappings at the tactic and technique levels, the subtechnique mappings show again how groups interpreted the case study differently and how certain groups were able to identify subtechniques to a much greater extent than other groups.

Table 1. Reconnaissance techniques mapping distribution

Reconnaissance Techniques	Total	Group A	Group B	Group C	ATT&CK
Active Scanning	1		X		
Gather Victim Identity Information	4	X	X	X	X
Gather Victim Org Information	4	X	X	X	X
Phishing for Information	3	X	X	X	
Search Open Websites/Domains	4	X	X	X	X
Gather victim Host Information	2			X	X
Gather victim Network Information	3	X		X	X
Search Open Technical Databases	1			X	
Search Victim-Owned Websites	1			X	
Total		5	5	8	5

In instances where the groups identified the same technique, the excerpts they provided had similarities and differences. For example, Groups B and C both identified the subtechnique of Gather Victim Identity Information under the tactic of Reconnaissance, and both groups used the same excerpt as evidence: "Tim went full-bore, collecting information such as the e-mail layout scheme, open requests for quotes, all employee names he could find, plus any social media sites they belong to, papers they wrote and published, clubs they were part of, as well as service providers they used." In contrast, Groups B and C had different excerpts they used as evidence of identifying the technique of Gather Victim Org Information under the Reconnaissance tactic; the excerpts from both groups each demonstrated the technique sufficiently.

In Part 1 of this project, Groups B and C were also tasked with identifying techniques in the case study that did not map onto the ATT&CK framework. Group B identified the subtechniques Improvised Pretext and Dumpster Dive as part of the Gather Victim Org Information technique and the technique Method of Obtaining Physical Access with a subtechnique called Shove Knife. Meanwhile, Group C also identified Dumpster Diving that would belong to the tactic of Reconnaissance and the technique improvisational pretext that would fall under the tactic of reconnaissance, initial access, or a "much-needed social engineering tactic."

4.2 Mapping ratios, indications, redesign

In Part 2 of the project, students identified the proportions of each tactic they used (see Table 2). Interestingly, the proportions that each group was able to map show that even within the same case study, some groups mapped drastically different numbers of

techniques within each tactic. For example, within the Collection tactic, Group A identified 11 techniques, while Group B only identified 1 technique.

In some cases, groups differed over whether a tactic was present in the case study at all. For example, The ATT&CK representative did not map any techniques in 5 of the tactics; comparatively, Group A mapped at least one technique in every tactic, Group B did not map any techniques in 6 of the tactics, and Group C did not map any techniques in 3 of the tactics. Groups also varied in the tactics in which they did not map any techniques; for example, of the 3 tactics that Group C did not map to, only 1 of those was the same as any of the 6 that the ATT&CK representative did not map to.

The 'Total' ratio in the bottom row of Table 2 shows some stark differences in how many total techniques groups were able to map, including differences both within the course groups and compared to the ATT&CK mapping. Group A had the highest mapping proportion with 44/205 techniques identified. Meanwhile, Group B had the lowest mapping proportion with only 16/205 techniques identified. The ATT&CK representative's mapping proportion is much closer to Group B, with a proportion of 24/203, and Group C's mapping proportion is closer to Group A's proportion, with 33/205 techniques identified.

Among all the tactics, the 'Count #' column shows that the most frequently mapped tactics were Reconnaissance, Collection, Initial Access, and Exfiltration. However, in some instances, there is only one group that is skewing the count column, making certain tactics seem more frequent just because of one group. For example, the Collection tactic is the second most frequently mapped tactic; however, breaking down the mapped techniques across each group, it is clear that Group A, who mapped to Collection 11 times, is carrying the weight of that variable's frequency, as groups B, C, and the ATT&CK representative only mapped to it 1 time, 5 times, and 2 times, respectively. This is similarly seen with the tactic of Exfiltration. Group A mapped to it 7 times, while groups B, C, and the ATT&CK representative only mapped to it 2, 0, and 3 times, respectively. In this case it is interesting that one of the most frequent tactics when looking at the count, was not mapped at all by one of the groups.

While there are some stark differences in the mappings, there are some tactics in which all the groups were in agreement. For example, the Tactics of Execution, Privilege Escalation, and Impact all had less than 3 mappings, each with multiple groups identifying either zero or one applicable techniques. As noted earlier, Reconnaissance has slight variation in the mappings between the groups, but for the most part shows agreement among each group, including the ATT&CK representative. Looking at the differences in the ratios of the student-groups compared to those of the MTIRE representative, tactics such as Resource Development are interesting to examine. For example, under the tactic of Resource Development, the ATT&CK representative identified 0 techniques. However, group A identified 2, which is a third of all techniques in that tactic, and group C identified 3, which is half of all techniques in that tactic. Perhaps those two student groups have a different understanding of the techniques in that tactic than the ATT&CK representative has. Additionally, the similarity between Group B and the ATT&CK representative in this example (both with 0 mappings to Resource Development) might stem from Group B having low ratios of techniques mapped for nearly every category, apart from Reconnaissance.

Table 2. Group Mapping Proportions[1]

Tactic	Group A	Group B	Group C	ATT&CK	Count #
Reconnaissance	5/10	5/10	8/10	5/10	23
Resource Development	2/6	0/6	3/6	0/7	5
Initial Access	2/9	4/9	3/9	3/9	12
Execution	1/10	0/10	1/10	0/12	2
Persistence	1/18	1/18	2/18	2/19	6
Privilege Escalation	1/12	0/12	1/12	1/13	3
Defense Evasion	2/37	0/37	0/37	4/34	6
Credential Access	1/14	1/14	3/14	1/14	6
Discovery	1/25	0/25	3/25	0/24	4
Lateral Movement	2/9	1/9	2/9	0/9	5
Collection	11/17	1/17	5/17	2/15	19
Command and Control	6/16	0/16	2/16	3/16	11
Exfiltration	7/9	2/9	0/9	3/8	12
Impact	2/13	1/13	0/13	0/13	3
Total	44/205	16/205	33/205	24/203	

After identifying the proportion of tactics that the groups could map onto the ATT&CK framework, the groups offered insight on what their mappings might indicate, both about the case study and about the ATT&CK matrix. Group A reported that

> the attacker in our case study did not rely on many technical methods to complete his job, therefore only a small proportion of the techniques mapped onto the matrix … he relied on more hands-on tactics to conduct the attack … Since he had to rely on more hands-on approaches, there is only a small proportion of the MITRE ATT&CK techniques that map over.

Group A believed that only a small proportion of techniques from the case study were able to be mapped onto the framework, but, interestingly, this group had the highest number of techniques mapped across all groups. This also indicates that Group A believed that the framework does not adequately cover hands-on approaches, which are commonly seen in SE behavior.

Next, Groups B and C provided implications of their mappings specifically for the ATT&CK framework. In regard to the ATT&CK framework, Group B reported that

> we are able to see a majority of the techniques reside during the Reconnaissance and Initial Access tactics. Based on that notion we can assume that … Tim … worked diligently to obtain the information he gathered … we are able to see the disparity in techniques used-starting more prevalent in the tactics regarding gathering information and becoming more scarce towards the tactics in which he could potentially be noticed and compromise himself.

[1] Note: ATT&CK representative denominators do not match the other groups' denominators for some techniques as a newer version of the ATT&CK framework was used.

As Group B noted, their mapping focused heavily on the early stages of the attack, specifically in the Reconnaissance and Initial Access tactics. In fact, of the group's 16 total techniques mapped, 9 of them are in the first 3 tactics in the framework. The group inferred that the attention to these two early tactics indicated that a much more careful approach was utilized during the attack. Thus, they believe that techniques toward the right-hand side of the matrix correlate with riskier behavior while tactics on the left-hand side of the matrix include behavior more focused on information gathering. Meanwhile, Group C's implications about the ATT&CK matrix were that

> the ATT&CK matrix more than sufficiently covered all of the technical aspects of this case study, which speaks to its strength. Our group had no trouble finding a technique or [subtechnique] for every technical maneuver. There were many techniques that exist on the matrix but were not applicable to our case study, which speaks to its depth and universal application. However, the matrix lacks depth when it comes to social engineering tactics. As social engineering is [a] critical [component] of cyberattacks, the framework could definitely improve in this area.

The thoughts expressed above imply that the matrix has a wide depth, especially in its technical measures, but lack in regard to social engineering related techniques. This is similar to the implications that Group A gathered from their own mapping. It is interesting that the 2 groups with the highest ratio of techniques mapped both spoke to the matrix not providing enough techniques regarding SE tactics; perhaps their large number of techniques mapped can be attributed to an attempt to make up for the lack of SE techniques by heavily mapping technical techniques.

Lastly, Groups B and C provided implications for the completeness and richness of the case study. Regarding the case study, Group B reported that

> the current ATT&CK Framework suggests that Tim had a good pretext and was able to adequately social engineer others without becoming compromised. The case study as presented dictates itself as very cautious ... In order to map this case study any better, more information would need to be provided.

Group B inferred that the ability to map this case study onto the ATT&CK framework implied that the behaviors of the adversary were well thought out, as techniques he used during his attack are techniques that are commonly used, as they are in the framework. They believe that being able to map behaviors to the framework makes for a sophisticated attack. Meanwhile Group C said that

> since we had no [difficulties] mapping the case study onto the matrix, the case study has shown [to] be of quality and complete. The amount of tactics and techniques that were able to be mapped shows the depth of the case study. The case study was not vague at any point and allowed our group to easily map every technical technique. If our case study contained more techniques, there would have been a stronger mapping, but that is not a fault of the case study as this was a [relatively] simple 'attack.'

Here, Group C acknowledges their strong technical mapping. However, they refer to lacking an even stronger mapping due to the task being 'simple'. This might be attributable to the lack of SE techniques on the framework. Because such SE behavior does not map onto the framework, it is being thought of as a 'simple attack'.

Groups B and C were also tasked with redesigning the ATT&CK matrix to achieve a better mapping (e.g., increase mapping proportion, improve simplicity, minimize redundancy) and justify how their redesign is better. Group C noted that

> the low proportion of one case study allows for many different kinds of studies to be easily mapped to the matrix. There are many different ways attacks can be carried out, and the [framework] reflects this well … we would not attempt to reduce redundancy because the places where techniques are repeated are purposeful and reflect the different stages of an attack where a strategy can be used.

Thus, the group decided to strengthen the matrix by adding an additional tactic called 'Social Engineering', which would fit into the matrix between the tactics of resource development and initial access. They justify this placement with the pattern that creating a pretext and engaging in social engineering techniques typically occurs during the early stages of an attack. Their 'Social Engineering' tactic would contain 7 techniques: Phishing, Vishing, Baiting, Spear Phishing, Quid Pro Quo, and Farming.

Meanwhile, Group B's redesign did not create any new tactics or techniques, but they suggested other ways to improve the framework. First, they suggested that the framework keeps up to date with advancing technology and physical methods. They also suggested adding in an appropriate place in the framework for unplanned strategies.

Lastly, Group B suggested that the framework use language that is more digestible for readers who are not familiar with the terms from the technical domain, or to provide clear definitions for technical terms used. Perhaps the nature of the language might explain why groups interpreted techniques differently and had different mappings from each other.

5 Discussion

This section offers a discussion on the lessons learned from analyzing the results of the course project, student-suggested revisions for the ATT&CK matrix, biases to be mindful of when using mappings, and some limitations of this study.

5.1 Lessons learned

The authors learned or affirmed three lessons from implementing and analyzing this course project: (i) there is no 'wrong' way to map, (ii) tactics/techniques can be interpretable, and (iii) SE is relevant.

One of the most evident lessons learned is the notion that there is no single correct way to map adversarial behavior onto the ATT&CK matrix. Despite each group reading and mapping the behavior from the same SE case study, each group produced its own

unique mapping with evidence from the text as empirical support. Mappings can also vary depending on the target audience and the objective of creating the mappings, whether that is for industry, government, or education, and whether that is for better understanding a specific adversary, creating defensive protocols/playbooks, or general practice with understanding human adversarial behavior, among any other objectives. Regardless of the reason, each group was able to provide excerpt evidence as proof that the mapped technique was in fact present in the case study.

In looking at the selected text chosen to support the mapping to each tactic or technique, it also became clear that groups had different interpretations on each tactic and technique. Regardless of the official definition for tactic or technique that ATT&CK lists on their matrix, groups were able to interpret these terms to have definitions more relevant to their case study and to SE in particular. For example, ATT&CK's official definition for the technique of 'Trusted Relationship', which is under the tactic 'Initial Access' includes "Organizations often grant elevated access to second or third-party external providers in order to allow them to manage internal systems as well as cloud-based environments." This description indicates that the technique is in regard to using a trusted relationship to gain technical access; however, student groups interpreted this term differently in a way that fit the case study. This was often done in the context of social engineering behavior, which otherwise did not map onto the framework according to the official definitions. In this example, Group C also mapped onto the 'Trusted Relationship' technique and provided the following excerpt as evidence: "At this point a little friendly chit chat ensued and before you know it they were laughing and exchanging pleasantries." In this context, the group interpreted the technique differently than the description provided on the ATT&CK framework, so that it would be more applicable to SE adversarial behavior. Regardless of the interpretation, each group's use of a technique was able to be backed up with excerpt evidence from the text.

These interpretations lead to the third lesson from this course, which was the affirmation that SE is relevant, both in the ATT&CK framework and within cybersecurity as a whole. The various mappings demonstrate the focus of SE on the reconnaissance stage, but also that techniques used throughout a SE engagement can apply to techniques or tactics that are typically used for technical cyberattacks, and that techniques and tactics that are commonly used for technical attacks are also relevant in SE attacks.

5.2 ATT&CK Matrix Revisions

While teams were able to take different interpretations of some of the tactics and techniques to fit into a SE perspective, it was clear that there was a gap in some social engineering techniques. As noted in part 1 of the results, some teams discussed various SE tactics and techniques that they would add onto the matrix to make it more useful for SE case studies, including some behaviors that they found within their case study that they could not map onto the matrix (even with reinterpreting terms), with some groups going as far as suggesting tactics dedicated solely for SE. This reaffirms that the matrix is not specifically made for SE adversarial behavior; nonetheless, groups were able to successfully map an entire SE case study onto the framework.

5.3 Biases

While it is important to note which tactics and techniques were mapped across this case study and any that are mapped in the future, it is also important to keep in mind biases associated with mapping adversarial behavior. These include novelty bias, visibility bias, producer bias, victim bias, and availability bias [12]. Novelty bias occurs when techniques that are newer, more interesting or more exciting tend to get reported more than standard techniques, which might get ignored. Visibility bias occurs when certain techniques are not available to the person mapping; some techniques might only be visible in a certain stage of the attack, whether that is before, during, or after. Others may not be visible at all. Thus, these issues with visibility may result in biased mappings. Next, producer bias is when reported mappings reflect a limited scope, due to what extent organizations choose to publish and what their objectives are. Another type of bias is victim bias, which holds that certain victim organizations might be more likely to report incidents or mappings than other victim organizations. The final type of bias is availability bias, which is that people are more easily able to recall certain techniques over others, so those techniques will have higher frequencies of being reported. Because of any or all combinations of these biases, it may be deceptive to only view the prevalence of certain techniques when examining a set of mappings. Further, as this paper provided mappings of the same technique by different groups that were backed by different case study excerpt evidence, certain techniques may reoccur during an attack, yet the frequency or repetition of certain techniques cannot easily be deduced. Thus, these biases must be kept in mind, especially when using these mappings to generate defensive operations.

5.4 Limitations

It is important to note that there were some limitations to this study. First, this analysis is based on mappings of a single case study that was short in length and not as thorough as it ideally could have been. Thus, these findings cannot be generalized, as they could be attributed to any attributes of the case study. A second limitation is the number of mappings that were compared in this analysis. The sample size is small with only three mappings, which also makes it difficult to generalize the findings. A final limitation is that this course project was implemented across multiple semesters during which project instructions and elements varied. This, along with variations in the version of the ATT&CK framework that was used across semesters complicated some of the comparisons. Along the same line, the comparisons between the student-groups and the ATT&CK representative were limited, as the ATT&CK representative was not asked to complete the entire course project, only mapping of the tactics, techniques, and sub-techniques.

6 Conclusion

The authors encourage others to use the findings and discussion in this article to inspire future work. This may include academics implementing similar projects in their

classroom with other case studies or more detailed case studies. Additionally, further research could be done with mapping other cybercrimes outside the realm of strictly SE, although SE is incorporated into various cybercrimes. Finally, the authors suggest future work to give a stronger focus to the possible mitigations associated with mapped tactics and techniques.

Educators could also encourage students to utilize their mapping of adversarial behavior and turn it into a defender mindset by identifying ways to stop or mitigate such behavior. For instance, some techniques students could delve into include Boot Integrity; Data Backup; Encrypt Sensitive Information; Limit Access to Resource Over network; Limit Hardware Installation; Multi-factor Authentication; Network Segmentation; Remote Data Storage; Restrict File and Directory Permissions; and User Training. However, educators should also allow students to develop their own mitigation strategies that may not be part of ATT&CK to allow for creativity and novel approaches.

By sharing the logistics, results, and benefits of this course project, the authors hope to help educators in developing their own course projects and teaching various aspects of cybersecurity (including human-factors) via experiential learning.

References

1. NICE: Cybersecurity Workforce Demand. Available at https://www.nist.gov/system/files/documents/2021/12/03/NICE%20FactSheet_Workforce%20Demand_Final_20211202.pdf (2021).
2. Hadnagy, C.: Social Engineering: The Science of Human Hacking. Wiley (2018).
3. ATT&CK matrix (same as [10]?) https://attack.mitre.org
4. OWASP Security Knowledge Framework, https://owasp.org/www-project-security-knowledge-framework/, last accessed 2022/31/3.
5. OWASP Risk Assessment Framework, https://owasp.org/www-project-risk-assessment-framework/, last accessed 2022/31/3.
6. CVE Overview Page, https://www.cve.org/About/Overview, last accessed 2022/31/3.
7. CAPEC Homepage, https://capec.mitre.org/, last accessed 2022/31/3.
8. NIST Mobile Threat Catalogue, https://pages.nist.gov/mobile-threat-catalogue/background/, last accessed 2022/31/3.
9. Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C.: MITRE ATT&CK: Design and Philosophy/ Available at https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf (2020).
10. ATT&CK Enterprise Matrix, https://attack.mitre.org/matrices/enterprise, last accessed 2022/31/3.
11. AMITT Design Guides, https://github.com/cogsec-collaborative/AMITT, last accessed 2022/31/3.
12. ATT&CK Sightings, https://attack.mitre.org/resources/sightings/, last accessed 2022/31/3.