5-2022

A STUDY OF SOCIAL ENGINEERING CONCEPTS WITHIN A DECEPTIVE DEFENSE

Jacob Glenn Oedekerk
California State University - San Bernardino

A STUDY OF SOCIAL ENGINEERING CONCEPTS WITHIN A DECEPTIVE DEFENSE

A Project

Presented to the

Faculty of

California State University,

San Bernardino

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

in

Information Systems and Technology

by

Jacob Oedekerk

May 2022

A STUDY OF SOCIAL ENGINEERING CONCEPTS WITHIN A DECEPTIVE DEFENSE

A Project

Presented to the

Faculty of

California State University,

San Bernardino

by

Jacob Oedekerk

May 2022

Approved by:

Dr. Jesus Canelon, Committee Chair

Dr. Conrad Shayo, Committee Member

Dr. Jay Varzandeh, Chair, Information and Decision Sciences Department

ABSTRACT

Organizations fall victim to costly attacks every year. This has created a need for more successful layers of defense. To aid in this need for additional defense, this study researches a way to bolster an underused defense style called deceptive defense. Researchers agree that deceptive defense could be the future of cybersecurity, and they call for more research in the deceptive category. The unresolved question from these researchers is what attack style could be used with a deception-based defense on an attacker. From this unresolved question, it was also determined that social engineering should be used in this culminating experience project as the attack style in question. This led to the question: “How can cyber defensive deception borrow concepts from social engineering to aid in bolstering a deception-based defense?” This project focused on researching concepts from both deceptive defense and social engineering, and to apply concepts from a popular attack style to a less popular defense style. This was done through a path of research into techniques, influence concepts, and two popular frameworks. It takes a 4-phased approach: researching deceptive defense techniques, researching social engineering concepts, researching two popular frameworks, and then applying one to the other. The findings are that: (1) there are similar concepts from both attack and defense styles; (2) there are techniques with similar applications but applied to the opposite parties (attackers or defenders); (3) and that it was possible to pull concepts from the social engineering framework to plan a deception-based defense. Further research would be desirable in an applied approach of how an attacker reacts to each persuasion principle. More research would also be recommended in the honeypot technique as an alerting and profiling technique.

ACKNOWLEDGEMENTS

I would like to thank my family for their support and understanding throughout this entire process. They were always there for me to complain to from the very beginning. Without them, I would not have gotten to this point, and I love them all. I would also like to acknowledge the friends who encouraged me to keep going or to be proud of the work I put forth. Finally, I would like to acknowledge my wife Estephania, who had to deal with me in the most stressful moments and always encouraged me forward.

TABLE OF CONTENTS

LIST OF TABLES

CHAPTER ONE:

INTRODUCTION

Background

“Oh, what a tangled web we weave...when first we practice to deceive.”

- Sir Walter Scott, *Marmion* (1891)

From the research of Zhang et al. (2021), deception is defined as the act of manipulating the perception of someone by exploiting psychological vulnerabilities through guile or deceit. The goal of deception is to fraudulently alter beliefs, decisions, or actions (Zhang et al., 2021). This study focuses on both defensive deception and offensive deception in the field of cybersecurity. Defensive deception comes in the form of a category of deception practices used by the defense, and offensive deception comes in the form of social engineering. A socially engineered attack does not require being in the digital realm, but for the purposes of this study, it will be referred to as a digital deception attack. Deception has been used in a wide spectrum of settings throughout the years, both offensively and defensively, in nature, battle tactics, behavioral studies, and as already mentioned, in cyber defense. To begin with, deception had its origin in nature.

Nature has multiple examples of deception, but two types of deception stand out that both have direct examples of being used offensively and defensively: mimicry and feigning death (Humphreys et al., 2018). These two types of deception influence the attacker or victim into believing a falsehood. We can see mimetic deception from species such as the Mimic Octopus (Thaumoctopous Mimicus), which can defend itself by mimicking other animals. Mimicking deceives its predator or its prey depending on the situation (Hanlon et al., 2007). This type of deception is both offensive and defensive, based on how the octopus reacts to the threat. Alternatively, another deception in nature that can be both offensive and defensive is the strategy of feigning death (Humphreys et al., 2018). Playing dead is practiced by animals such as insects, lizards, rodents, and birds. Lizards use feigning death as a defensive deception, causing predators that consume only freshly killed prey to avoid them (Humphreys et al., 2018). Spiders can use deception offensively, luring in their prey with a variety of traps built into their webs (Almeshekah, 2014). Understanding offensive and defensive deception at these base levels helps this study see that deception is not restricted to its current uses within a cyber defense. It has been around longer than cyber defense and inspiration has already been drawn from the natural world. Mimicry can be seen in current cyber deceptive defenses such as honeypots (Ferguson et al., 2018), and feigning death is present in stalling tactics involved in attacker engagement (Horak et al., 2017). These are but a few examples of deception that are visible throughout nature, and it was further emulated with the war tactics of societies.

Ancient military strategies pioneered deception in war through tactics such as the fabled “Trojan Horse” circa 1184. This type of offensive deception would have allowed an attacker to break through a defense while preserving resources and tricking the opposing defenders into letting their guards down (Sembos, 2021). Examples of both offensive and defensive deception are commonplace in war. Ever since men have been at war with other men, ruses, feints, and deceptive techniques have been used (Calder, 2016). In ancient China, 341 BC, researchers discovered deceptive techniques being used by general Sun Bin and his army. Sun Bin faced an enemy attack that underestimated his army's morale. Sun Bin used this underestimation to his advantage, luring in the enemy with a ruse that looked like his own army was deserting (Wasson, 2022). This defensive deception tactic played on the perceptions of his enemy to guide the adversary into defeat. These uses of deception were done creatively in a goal-oriented manner. This study is focused on the use of deception in an attack and defense scenario, and these examples of deception are pulled from militaristic tactics. Seeing deception used creatively allows for this study to understand that deception formulated by humans for a human's perception can be extremely effective. The study of deception and perceptions was broadened and delved into through behavioral studies in more current times.

Behavioral deceptions, and the motivations behind them, were presented in three taxonomies by Burgoon et al. (1996). These taxonomies describe the use of deception in interpersonal contexts. Interpersonal behavioral deception is a style of communication that can be used to make an individual look better within social contexts or influence another's behaviors (Calder, 2016). This behavioral deception is the foundation of social engineering, where people that want something from another person could use a form of social engineering. Forms of human manipulation to gain a resource can be considered a form of social engineering (CompTIA, 2022). It is an attack that has evolved with the times, but a modern conception of social engineering is a calculated set of human manipulations that methodically reaches the end target (Mitnick, 2022). Social engineering is a threat to privacy that is a form of psychological manipulation. This psychological manipulation is used to exploit people to gain a foothold in a network, glean information that has some sort of value, or used to reveal confidential information (Aldawood, 2020). At its core, social engineering takes advantage of human behavior to gain an advantage against its target. This form of attack relies on deception, and people are notoriously bad at detecting deceptions (Aldawood, 2020). For example, the ability of an untrained observer to detect lies was estimated to be 53% in a research study performed by Vrij et al. (2010). This study poised untrained observers against trained observers to detect lies after watching a person tell either a lie or a truth. The trained observers' success rate was estimated to be 57%, slightly higher than an untrained observer.

The behavioral studies of deception, and gaps in current security methods, led to studies of deception within cyber defense. Cyber defensive deception is rapidly evolving and becoming a part of an organization's defense strategy (Zhang et al., 2021). Cyber defensive deception is the act of defense that uses digital deceptive means to mitigate attacks. Deception used in the digital universe was first theorized forty years ago in a novel written by Cliff Stoll titled *The Cuckoo's Egg*. This novel uses the example of a "honeypot" to attempt to catch a hacker (Stoll, 1995). A honeypot is one of the earliest forms of useful digital deception, where a resource is made appealing enough for an attacker to engage with it and become stopped/delayed/tracked by falling into the trap (Almeshekah, 2014). The idea of a honeypot has developed over the years into different variants such as honeynets and honeytokens. This type of deception is an ad-hoc style of deceptive defense and has also been gaining popularity in recent years. We are seeing holistic forms of digital deception that utilize multiple forms of deception to mesh into a layered defense that can mitigate an attacker at levels as high as an advanced persistent threat (Zhu et al., 2021). Between social engineering and deceptive defense, it is apparent that deception can be actively used in both attacking and defending an organization (Levine, 2014).

The Problem

Pawlick et al. (2019) states that defensive deception is an emerging and underused defensive layer that utilizes human behavior and trickery to attempt to defend a targeted cyber resource. The same researcher predicts that the future of cybersecurity "will leverage tools commonly employed by attackers for the purpose of defense." They state that future research is needed within the problem area of how leveraging an attacker's tools can aid the defense. Current research believes that deception, or specific defensive deception techniques, has more opportunity than discovered so far within cyberspace (Pawlick et al., 2019).

Further, an unambiguous attack environment has created a need to further the use of defensive deception through ambiguity and influence type tactics (Calder, 2016), which brings relevance to this project. Research from Almeshkah (2014) states that “deception can play a larger and more important role in cyber defense.” In the research of NITRD (2010, Networking and Information Technology Research and Development), recommendations for researching how to complicate and make an unpredictable attack surface through frustrating an attacker were presented. Based on the discovery of requested research by Pawlick et al. (2019), Almeshkah (2014), Calder (2016), and NITRD (2010), a question was partially formed regarding concepts within an attack style that could bolster a deception-based defense. To fully formulate this question, an attack style needed to be chosen to focus this research on. In game-theory research focused on deception-based defenses, the defenders were treated like social engineers, with a potential of altering an attacker’s moves. Social engineering is stated to be a form of deception that is comparable to a deceptive defense from the research of Ferguson-Walter et al (2019). According to a survey conducted by ISACA (Information Systems Audit and Control Association) in 2020, social engineering was the leading cause of compromised businesses at 14%. It was 40% more likely to be the reason of compromise than the next leading cause, advanced persistent threats. Social engineering is a prominent and successful attack type within a wide diversity of organizations (VPN et al., 2021). Social engineering attacks seek to use the act of human error, confusion, and trickery to perform various levels of successful malicious activity (Mitnick, 2022).

When justifying social engineering as the attack type to research with the intent of applying its concepts to a deceptive defense, we looked at the top attack types. In the ISACA (2020) report, the top six attacks that were reported on were social engineering (14%), advanced persistent threats, ransomware, unpatched systems, security misconfigurations, and Denial of Service attacks. Of these six, it is prudent to further narrow down to the top three for consideration as they are seen as more successful attacks according to this survey. In a study by Gallegos-Segovia et al. (2017), it was seen that social engineering can be used, and is used, as an attack vector for ransomware. Users in this study were sent fraudulent socially engineered emails and 85% of the users installed malicious ransomware on their computers. To further justify social engineering as the attack type to pull concepts from for a deceptive defense, APTs (advanced persistent threats) are successful due to social engineering (Bere et al., 2015). This same research shows that various forms of social engineering are used by over 50% of APTs to enter a network. It also suggests that an APT should be dealt with through behavioral methods, which is relevant to the advised research of the deceptive defense papers mentioned prior.

Questions

The question that emerged based on the areas of the previously mentioned research and the question that this project focuses on is: “How can cyber defensive deception borrow concepts from social engineering to aid in bolstering a deception-based defense?” This question led to the following question that this project addresses as well: “What influence concepts in cyber defensive deception match influence concepts in social engineering?”

Methodology

A route of research was determined to answer the question: “How can cyber defensive deception borrow concepts from social engineering to aid in bolstering a deception-based defense?” The route of research for understanding how digital deception could utilize more concepts from social engineering was taken through scholarly articles, research articles, propositions, reports, thesis, best practices, and conferences. These items of research were used to form an idea of four major principles. First, to understand what cyber defensive deception is and what techniques are currently being used by defenders. Second, an understanding of social engineering was formed through principles of persuasion and examples of social engineering within those principles. Third, frameworks of both defensive deception and social engineering were researched. And finally, the meshing of the techniques was explored. The final principle explores the ability for defensive deception to borrow concepts from social engineering, the difficulties that stem from this, and the advantages/disadvantages of how this could be done. This project will be based on research analysis using Google Scholar and sources pulled from scholarly journal websites, cyber security articles and cited sources within articles. The search was within the confines of

2010 or later for the major scholarly articles. Resources found within publications led to a large portion of the relevant research per category. Defensive deception scholarly articles led to more scholarly articles, allowing for a chain of relevant articles to explore the topic.

The second phase focused on understanding social engineering and principles of persuasion, which was used to help answer the secondary question: “What influence concepts in cyber defensive deception match influence concepts in social engineering?” These social engineering principles were researched through the perspective of the manipulation of human behaviors, and as such led to studies relevant to how an attacker alters the victims’ behaviors to successfully compromise the desired information. The path of research described here can be found in Table 1.

Table 1. Path of Research

<table>
<tr><td>Search Method</td><td>Category</td><td>Results</td><td>Selected</td><td>Key Words</td></tr>
<tr><td>Google Scholar
Question 1</td><td>Deception Based Defenses</td><td>95</td><td>7</td><td>“deceptive defense”</td></tr>
<tr><td colspan="5">Authors: Ferguson-Walter (2020), Ferguson-Walter et al. (2018), Calder (2016), Al-Shaer (2015), Horak et al. (2017), Schuh (2021), Zhu et al. (2021)</td></tr>
</table>

Selection and Keyword Choices: The “deceptive defense” keyword search was used to allow for selecting documents within a broad perspective of this research category. The 7 selected documents in the category of “deceptive defense” were selected based on forming a well-rounded current understanding of deceptive defense. They add up to the reasoning of why and how researchers believe deceptive defense is useful and in which scenarios it is currently being used. The actual selection was directed at those concepts presented by the researchers.				
Google Scholar Question 1	Deception Based Defenses	60	6	“defensive cyber deception”
Authors: Almeshkah (2014), Levin (2014), Pawlick et al. (2019), Pouget et al. (2003), NITRD (2010), Zhang et al. (2021)				
Selection and Keyword Choices: The “defensive cyber deception” keyword search was selected to create a focus on the use of deceptive defense within a cyber environment. There was some overlap between these two searches, but it allowed for research that included more cyber based deception reasoning, examples, and definitions.				
Google Scholar Question 1 & 2	Influence & Social Engineering	38	5	“social engineering influence”

<table>
<tr><td colspan="5">Authors: Mitnick (2022), Mouton et al. (2014), Hebert et al. (2021), VPN et al. (2021)</td></tr>
<tr><td colspan="5">Selection and Keyword Choices: The “social engineering influence” keyword search was desirable for this project since the predicted connection between defensive and offensive deception is the influence exerted on an individual’s behavior. The focus from the research of social engineering was then directed at influence which branched into the techniques used by the attackers. The relevant articles were selected based on the relevance to concepts of social engineering and how the concepts were described.</td></tr>
<tr><td>Google Scholar
Question 2</td><td>Influence & Social Engineering</td><td>80</td><td>4</td><td>“social engineering taxonomy”</td></tr>
<tr><td colspan="5">Authors: Mouton et al. (2014), Bere et al. (2015), Aldawood et al. (2020), Vrij et al. (2010)</td></tr>
<tr><td colspan="5">Selection and Keyword Choices: To research further into social engineering, it was useful for this study to explore social engineering taxonomies. A taxonomy was chosen from the above keywords. This research area also helped the paper find social engineering examples within various techniques.</td></tr>
<tr><td>Expert Recommendation</td><td>Influence & Social Engineering</td><td>N/A</td><td>3</td><td>“influence types”</td></tr>
<tr><td colspan="5">Authors: Muscanell (2014), Ferreira et al. (2015), Cialdini (2007)</td></tr>
</table>

Selection and Keyword Choices: Relying on the input of the researchers within the field of influence led to research articles and a book written by Dr. Cialdini referenced in those articles. The book was cited and referenced in a multitude of other studies that led it to being included in this research project as a guide for influence types and principles.

CHAPTER TWO:

LITERATURE REVIEW

The research for this project focused within two primary areas: digital defensive deception and social engineering tactics. Creating this focus in these given areas was done by selecting literature found using the key phrases: “deception defense” and “defensive cyber deception”. A second search was then done for “social engineering influence.” Each article within the search results was selected based on its relevance to the problem being addressed for this project. There is a large amount of research done in both categories, and abstracts were read for relevancy. The relevant articles were selected based on their research into the principles of digital deception or social engineering and their ability to expand on the principles of either subject. A holistic understanding of both principles needed to be established to apply one concept to the other.

A taxonomy of defensive deception for cybersecurity was conducted by Pawlick et al. (2019). This taxonomy covered the various types of deception while attempting to quantify the results with game theoretic mathematics. The researchers aimed to define these types of deception using game theory to refine the definition of deception outside of the previously broad use of the term. They applied relevant models to many deceptive techniques in cyber security to construct a taxonomy of the concepts: perturbation, moving target defense, obfuscation, mixing, honey-x, and attacker engagement. This research is relevant to the project because they define the separation of deceptive techniques. This separation will allow the focus to be on a specific defensive deception technique as needed.

Zhang et al. (2021) compiled three decades of cyber defense deception techniques with the design of giving cyber defenders a tool to develop a deception-based defense. These researchers state that they are the first to compile such a representative, systematic guide for deception techniques. The guide will allow for a certain defense to be applied to a certain type of attack. The research introduces and expands on the idea of a “deception stack,” “deception in depth,” and “deception lifecycle.” This paper is directly related to applying a deception technique to a specific problem and how to evaluate the success of that approach. It is going to be used as a tool, as the researchers intended, exploring the addition of an influence concept to a deceptive defense technique. This process will potentially aid in the mitigation of an attack.

In 2018, Ferguson-Walter et al. published the Tularosa Study. The Tularosa Study was undertaken by testing 130+ red team hackers. The study tracked personalities, psychological intent, and cognitive tests of these participants while they navigated through an attack on a network. The attackers were told that there were either deception practices at play or that there were not deception practices at play. The sample network was studied with and without the deception technique. The study was done utilizing decoys within the network as the primary form of deception. Ferguson-Walter et al. (2018) went on to publish theses, summaries, and scholarly articles related to their findings in this study. This research project found useful information in much of the research surrounding this case study since it is current research into the effectiveness of deception as a defense. The research done by Ferguson-Walter et al. is vital to the research done moving forward as they proved multiple facets of how attackers can be influenced in an environment laced with decoys.

The MITRE Corporation (2015) released an article titled “Denial and Deception in Cyber Defense.” This article laid the groundwork for an organization’s “active” cyber defense with the “deception chain.” The deception chain is an adaptation of the kill chain model utilized in cybersecurity (Heckman, 2015). The kill chain model follows the stages of a cyber-attack, and the deception chain is meant to help integrate denial/deception, cyber intelligence, and security operations into an organization. They lay out the deception chain in eight phases: purpose, collect intelligence, design cover story, plan, prepare, execute, monitor, and reinforce. This specific article and the research put forth by The MITRE Corporation will be vital to the exploration of implementing a defensive deception technique in the confines of this research project. An offshoot of this article is “Military Cyber Affairs” by Calder (2016), which makes a case for deceptive defense. They treat the deception techniques in a more utilitarian style, with the idea that the techniques can be framed from a military style of deception. It is a grounded approach that makes an argument for deception in the form of “increasing adversarial costs” outweighing the cost of defense. The research provided by Calder (2016) frames deception tactics as an attack on attackers. The author’s discussion of the deceptive style of defense is relevant to this research project as they include concepts from MITRE’s eight-step deception process that will also be referenced in this paper.

In a research paper written by Almeshekah (2014), a plan for implementing deception into current security defenses was presented. The research paper takes current systems and goes through how deception could be integrated, similarly to The MITRE Corporation, but with more emphasis on the practical application of applying deception techniques into an existing set of systems. The researchers analyzed the components that make up any type of deception presented through prior studies and then applied it to a computer’s security. This paper also presents how to set up a deception defense in environments that lead to success and then how to evaluate the success. An attacker’s biases will also be extracted from this research paper to aid in understanding why an attacker may fall for the deception.

Up to this point of research, the focus has been on deceptive defenses within a defense plan. After building up the toolbox of methodologies, tactics, and support for cyber defensive deception, the research led into the details of social engineering. This project will use the work from Muscanell (2014) called “Weapons of Influence Misused” to understand how social engineering is successful. The research done by Muscanell applies social influence tactics to the scams used by social engineers. Muscanell (2014) gives examples of social influence attacks in the context of internet scams used to gain information. For these purposes, he uses concepts from an expert psychologist: Cialdini. Cialdini (2007) published a book titled “Influence: The Psychology of Persuasion.” This book goes through the principles of influence, laid out in six concepts: reciprocity, commitment/consistency, social proof, liking, authority, and scarcity. These concepts will also be used within this project to be applied to current defensive deception techniques. Cialdini’s principles of influence are a cornerstone of studies that researchers have focused on social engineering, being the source of many other studies as well. This project will explain the principles, including examples from social engineering using the principles, and show constructive ideas of how they may be used within a deception-based defense.

One last piece of the puzzle this project will be relying on is the structure put in place by Mouton et al. (2014) regarding a social engineering attack. These researchers broke down Kevin Mitnick’s stages of a social engineer attack and expanded on the content within each stage. After Mouton et al. created an attack framework, there was a structured way to not only evaluate and map a social engineering attack but to also create one. The framework they created allows us to utilize it within the deceptive defense to see how it may be paired with the planning and execution of a deceptive defense.

CHAPTER THREE:

DECEPTION TECHNIQUES AND INFLUENCE

A defensive deception technique (DDT) attempts to influence an attacker's perception of their target. An effective DDT either hides, confuses, or misleads an attacker causing them to waste resources (time, energy, or processing power) and attack in a complicated or wrong direction. This causes an attacker to be delayed, exposed, or disoriented (Zhang et al., 2021). This type of defense relies on manipulating human behavior and attempting to apply deceptive behavioral illusions on the attacker. Defenders can understand an adversary's attack, apply deception techniques, force attackers to move slow, take greater risks, and use more resources allowing the defender an advantage in preventing an attack (Heckman et al., 2015). A defense that seeks to mitigate reconnaissance efforts is considered passive, while interactively engaging with an attacker is considered active (Horak et al., 2017). The categories of DDTs that this project will limit itself to are honey technologies, moving target defenses, and attacker engagements. The limitation to these three techniques is due to the wide range of interaction possibilities within each category. This chapter will be covering the categories and the amount of interactivity per category, followed by an analysis of the influences at the interactivity levels.

Honey Technologies

The term “honey technology” is an umbrella term covering a DDT that attracts an attacker to a resource set up by a defender that mimics an actual resource. It then tracks, traps, or slows down an attacker. If a honey technology is being interreacted with, it is an anomaly and should not be happening unless a malicious actor is the cause (Spitzner, 2003). Honey technologies can be seen in three major categories: honeypots, honeynets, and honeytokens (Pouget et al., 2003).

A honeypot is a system that is designed to attract an attacker to use exploits against it (Calder, 2016). When implementing a honeypot, the indicators that there is a honeypot should be concealed in most cases (Heckman et al., 2015). Defined by a public forum of security professionals in 2003, a honeypot is “an information system resource whose value lies in unauthorized or illicit use of that resource” (Spitzner, 2003). Honeypots evolved into other technologies such as honeytokens and honeynets. Each of these ideas work off the same principle as a honeypot: something that is appealing to an attacker to either be targeted, attacked, or interacted with (Pouget et al., 2003). A honeypot ranges from low interaction where the resource is there to be probed, or high interaction such as a fully mimicked system that an attacker could interact with. In a 2017 survey of organizations, it was hypothesized that honeypots would be the most popular form of honey technology, but the results show that the most widely used honey technology was honeytokens because they are more widely available and more easily deployed (Dominguez, 2021).

A honeytoken is defined as “a digital or information system resource whose value lies in the unauthorized use of that resource” (Spitzner, 2003). An example presented by the researcher Pouget et al. (2003) is a medical record stored in a database called “John F. Kennedy.” This would be a false record that if interacted with would be highly suspicious. Security has been using the idea of honeytokens for as long as security has been around, but honeytokens in the widely used context refer to a wide collection of deception techniques based on being bait resources (Zhang, 2021). The attacker “picks up” the honeytoken and “uses it.” The “pick-up” or the “use” triggers the defense mechanism, such as an alarm that it was “used.” Just like honeypots, honeytokens can also range from low interaction to high interaction. In the presented example of the medical record, just accessing the record may be all the defender wants to track and is the extent of the honeytoken. If the medical record also has further information in it that further influences the attacker, the interaction level with the honeytoken goes up.

A honeynet is a network of honeypots, mimicking a real network to be explored by an attacker. The act of exploring this honeynet leads to a higher level of interaction (Pouget et al., 2003). The interaction level with each style of honey technology ranges from low to high, depending on the goal of the defense. In the research done by Pouget (2003, p. 9), he offers the definition by Won-Seok Lee where honeynets are “…nothing more than a high involvement honeypot within which risks, and vulnerabilities are the same that exists in many organizations today.” A defender can see how the attacker moves from honeypot to honeypot, through the network, attempting to exploit the various systems and set ups. A honeynet can be seen as a high interaction honey technology, as it is more complex with more desire placed on an attacker moving through the environment. This leads to reasoning that having a honeynet can be used to watch and or engage with the attacker interacting with it, much like a spider’s web is there to specifically attract and/or trap an insect. While the honeynet may be useful for research and engagement purposes, Zhu et al. (2021) describes a highly usable version of a honeypot he termed “minefield honeypots”. The minefield honeypot can be used to begin the offensive deception from the deceptive defense by disrupting the reconnaissance and delivery of the attack. In addition, a minefield honeypot can be used to either act as an alarm for the defense or to provide more chances of studying the attacker. By studying the attacker, a deceptive defense can better understand how to treat the upcoming attack (Zhu et al. 2021).

Moving Target Defense

Moving Target Defense (MTD) is defined by the Networking and Information Technology Research and Development (NITRD) website as a defense technique for “cyber agility.” The defense works “by randomizing or mutating the system configuration to invalidate the attackers’ goal” (Al-Shaer et al., 2015). While the research presented by NITRD categorizes MTD as an agile defense strategy, it fits the definition of a deceptive defense by “disrupting attacker plans via changing adversarial behaviors” through means the attacker is not expecting. MTD is meant to be a proactive defense strategy that can alter defense strategies and move system parameters during or prior to an imminent attack. MTDs increase the cost for attackers by creating a more fluid and complex defending platform…taking more time, energy, and expertise to navigate the attack landscape (NITRD, 2010). While a moving target itself is a deceptive defense, a deception on top of the movement of the target increases the effectiveness (Cohen, 2009). The way a target can be moved is broken into two categories: randomization and Markov decision processes, where the Markov decision process has an outcome with some control and some non-control (Pawlick et al., 2019).

Attacker Engagement

The attacker engagement technique of deceptive defense is a higher level of interaction between both the attacker and the defender. It is squarely in the “active” consideration for deceptive defenses because an attacker is trading moves with the defender (Horak et al., 2017). The defender has more control of when and where to employ a deception once an attacker is identified. When looking at this defense from the perspective of a game where moves are being traded, the defender can employ different deceptive strategies depending on their goal. In this “game” of defense, it is found that when engaging and blocking the attacker, it is best to be delayed from the initial attack (Horak et al., 2017). The idea is that an attacker that is deceptively led further into an attack can be learned from and give up on their own accord, rather than being blocked right away and then re-entering to cause an extensive amount of damage.

Influence Chance and Deception Chain

As mentioned before, a defender could have different goals for implementing a defensive deception. The goal of a defender alters the course of the influence that the defender will be attempting to place on the attacker (Horak et al., 2017). If the defender's goal is to learn about what the attacker is doing within a honeynet, the defender may want to try and keep the attacker busy and waste as much time as possible. With this issue for evaluating influences and the goals of a defender, influences can be broken into interaction amounts. A defender can pick techniques with ranges from low interactivity to high interactivity. Based on game theory studies of deceptive defenses, each time an attacker interacts with a defense is a chance for the defender to alter the next move an attacker is going to make (Pawlick et al., 2019). For the purposes of this research, a chance to alter an attacker's move (even if it is their first move) will be considered an influence chance. Between these two concepts of interaction amounts and influence chances, we see how deceptions can attempt to influence an attacker and how many times an attacker is being influenced.

In a low interaction honeypot technique, a decoy firewall (aka honeywall) could be set up to alert if scanned in a certain way. If a port on the honeywall is scanned, then the DDT can alert the defender that there is interest in their network. The extent of this technique is low interaction with one influence chance. The influence chance is contained within how the defender set up the honeywall and what was seen by the attacker based on their scans. It is the opening move of a potentially short game. Alternatively, there is a high interaction DDT through attacker engagement. Attacker engagement involves a plethora of potential influence chances (Heckman et al., 2015). Engaging an attacker begins with the same level of interaction as most other deception techniques, but then gets carried to each move the attacker makes and the defense continues to try and deceive to reduce damage and/or learn from the attack.

By following the deception chain presented by MITRE, the interactions and influence that deceptions place on an attacker is laid out through purpose, collecting intelligence, designing a cover story, planning, preparation, execution, monitoring, and reinforcing (Heckman et al., 2015). Since this deception chain is used to determine the depth of the deception, it can also be used to align the influence chance with the defensive deception. For example, following the MITRE deception chain to create a deception based moving target defense, the interaction level of the defense is crafted, and by proxy the influence chances are created:

1. Purpose: A defender will be determining the goal of the deceptive defense and defining the requirements for success (Heckman et al., 2015). The

depth of the deception will be decided, so the amount of interaction will also be decided. This is where the number of chances to influence can be determined, and it will be solidified in the planning phase. A MTD purpose stage may include forcing the attacker within the network to be distracted with a confusing attack area to stall for them to be removed (Zhang et al., 2021). A success level for this example may be set at removing the attacker before they are able to execute a successful exploit.

2. Collecting Intelligence: This is referred to as the prediction stage, where the defender will be putting together the known history of the expected threats. This intelligence can come from the Structured Threat Information eXpression (STIX) or elsewhere, but research can be done for the expected threats. STIX is a partner developed language that aids in this stage. To apply this to a MTD example, the potential threats can be gathered to understand what will be affecting the attack landscape (STIX, 2021). This stage could be an indicator for potentially useful influences depending on direct attacker engagement opportunities.
3. Designing the cover story: An effective deception alters an attacker's perspective (Almeshekah, 2022) and this phase focuses on what would cause an attacker to fall for the deception. Hiding and showing certain pieces of information to allow for an illusion is done here. In the Tularosa study (Ferguson-Walter, 2022), it is shown that an attacker in a network full of decoys that is aware of the decoys, is still slowed down or

hampered by the deception of fake systems around them. The influence type can be determined here, even if it is as simple as causing an attacker to believe there is deception at play. An attacker will be pressured, or influenced, by a deception based on what they do and do not know about it (Ferguson-Walter, 2022).

4. Plan: The technicalities of the deception are determined in this stage. For this moving target defense example, a defender opted to utilize a form of MTD with dynamic systems. These dynamic systems can cause attackers to not know what type of target they will be applying exploits to (Zhang et al., 2021). This potential confusion is an influence chance introduced by the defender and can be adjusted with the style of systems chosen, the vulnerabilities left open, or the rotation speed of the systems changing their information.
5. Preparation: The effect of the deception is explored within this stage. The actuality of the influence chance would be another way to phrase this. The direction that an influence chance takes is going to be focused on by the defense. This supports the cover story, and the resources at hand are considered for creating the deceptive defense (Schuh, 2021).
6. Execution: Execution of the plan, the deceptive cover story, and the preparation is coordinated between the deception planners and the security operations.

7. Monitoring: At this point, the planners and operators are observing the culmination of their efforts. In this MTD example, there is no direct attacker engagement, human to human, so the success is based on the deceptions already laid out. There will be alarms alerting as to when the dynamic system was attempted to be breached and where the attacker pivoted next. When an alarm is sounded, the deception traps are triggered, along with a classic measure of alerting the defenders. Findings from Cohen et al. (2009) suggest that a human added on top of the deceptive traps adds to the layers of defense, allowed for by the deceptive trap triggering the alarm. This same researcher found that deception allows a defender more options for their reactions as the attackers are slowed or less effective. The success of the influence may be judged at this point through logs or from the perspective of a live defender.
8. Reinforcing: This process is iterative and based on the results of the monitoring, and the defense will be cycled through, adjusting to meet the goals. Alternative influences could be attempted and judged, building towards success if not currently successful.

After looking at these eight stages, influence chance is considered in the purpose and determined in the design of the cover story. It is then planned for in the preparation, applied in the execution, judged in the monitoring, and improved in the reinforcement stage.

CHAPTER FOUR:

SOCIAL ENGINEERING INFLUENCES

Social engineering is based on the idea that humans can be exploited into doing the bidding of the social engineer (Mitnick, 2022). These exploited characteristics take advantage of an existing vulnerability (Pawlick et al., 2019). These exploits are not necessarily taking advantage of software vulnerabilities, but instead are built from influencing human behavior (Mitnick, 2022). Influences can be categorized into six principles of persuasion, which are defined and assembled by Cialdini (2007): Reciprocation, Commitment and Consistency, Social Proof, Liking, Authority, and Scarcity.

Cialdini’s Social Influence Principles

1. Reciprocation: The basic idea of reciprocity plays on the feeling of obligation people feel when an exchange is made. People are going to be more apt to return a favor if a perceived favor was done for them.
    a. Social engineering example: In 2021, the FTC (Federal Trade Commission) issued a warning regarding a tech support fraud utilizing reciprocity. Attackers manipulated targets into believing they did them the service of “removing” a virus or fixing a different non-existent technical problem. The attackers then charged a fee for their fraudulent services (Hebert et al., 2021).

    b. Deceptive defense use: Understanding reciprocation is vital for a defense to understand that an attacker feels no desire to return a favor to a defense. Attackers have a target and timeframe to plan for reaching their goal, and if a defense mechanism helps the attacker to achieve the goal, then the attacker will still feel no reciprocity to the defense (Schuh, 2021).

2. Commitment and Consistency: This principle describes when people are committed to perform the task. In this case, the peoples' social norms align with them doing what they said they are going to do.
    a. Social engineering example: An organization that relies on email correspondence could fall into a situation where an employee is exploited by commitment and consistency. This scenario could be seen from an accountant that pays their vendor through an account number and has constant contact with the vendor. Typically, she sends money to a vendor monthly, and an attacker could insert themselves into the middle of the email chain with the accountant. They would then ask for the payment to a new account and the accountant could fall back on consistency and commitment to pay the attacker. It may not be discovered for weeks or until the vendor requests payment again (Anonymous, n.d.).

    b. Deceptive defense use: Attackers will have different levels of commitment to their attack. For the defense to understand how to use the concept of commitment and consistency against an attacker, the level and type of commitment may need to be determined. This determination could be discovered at the beginning stages of an attack. Sensors will be employed by the defenders, and based on the initially sensed attack, a blocking attempt could be aimed at the attacker. If partially blocked, and then circumnavigated, the defense will know the attacker is committed to the attack enough to continue even after encountering a hurdle. In research presented by Horak et al. (2017), it is discovered that an attacker is easier to deceive if they have already devoted resources and effort towards an attack. These researchers term this phenomenon “demise of the greedy” but it falls into the influence category of commitment and consistency. Based on the same research, this is an influence concept that defensive deception designers will be able to use to influence the direction of an attacker.

3. Social Proof: Social proofing works on the assumption people make that if others are doing it, the action is more correct. This assumption leads to an influence on perception based on other people performing the same action the person is about to do.

a. Social engineering example: Social proofing is the least used principle in phishing emails (Ferreira, 2015). While less used in phishing emails, it is used in fraud advertisements. In 2020, Facebook added a warning to their FAQ section of their website that included information on ways to avoid ads that claim a user is among many other winners of a contest (Facebook, 2020). This type of ad is pulling at an individual's perception that if other people won, it might be valid that they won too.

b. Deceptive defense use: A successful honey X technology can be bolstered with the concept of social proofing. If an attacker observed a honey-based deception that appeared to be used by the users within an enterprise, it could lull them into a false sense of security. Creating a honeynet that is closer to a realistic network involves emulating traffic moving across the network stack (Zhang et al., 2021). This action is playing on the attacker's desire to see others moving in a network, to try and deceive an attacker into believing it is a true network, and not a decoy network.

4. Liking: The "liking bond" is created by pulling at a victim's desire to say yes to someone or something that they know and or like. The desire to know or like someone could be based off attractiveness, similarity, compliments, or amount of contact.

a. Social engineering example: The “liking” principle is the most common principle of social engineering through phishing emails. A phishing email is a way for a social engineer to reach out their influence on a user to gain information or access through deception and persuasion (Ferreira, 2015). A phishing email that relies on the liking principle builds on social relationships with the victim. For example, when an attacker gets access to a user’s contact list, they would be able to spoof themselves as one of the user’s friends. This builds on the social relationship and the fact that a user is more likely to trust someone they already know and like to further exploit the user.

b. Deceptive defense use: The liking principle can be seen in the Tularosa Study conducted by Ferguson-Walter et al. (2018). It was indirectly applied to a decoy system by crafting targets that were appealing to an attacker. This attractive target was made appealing by utilizing exploits that would be seen as common or easy. These decoys looked more vulnerable and hence drew the attacker to attempt to breach the given targets. Eighty-three percent of the exploits launched in the study were towards the decoys, proving the value of the liking principle in a deceptive defense. Although it was not stated by the researchers that a principle of influence was used, this building of a more attractive target can be seen as an influence principle and has potential to be carried through to other deceptive defenses.

5. Authority: A person can become conditioned over their lifetime to respond in a certain way to an authoritative figure. The response becomes conditioned, and this conditioning is preyed on by social engineers.
    a. Social engineering example: Pulled from Cialdini's set of experiments, an experiment was performed where a false physician called nurses to attempt to get them to give an incorrect dose of medication. Ninety-five percent of nurses fell for the use of authority over the phone call with the false physician (Cialdini, 2007). The nursing role is trained to rely on the expertise and experience of a doctor, and this leads to an environment where the user is primed to fall victim to the authority principle.
    b. Deceptive defense use: The authority principle can be crafted for a deceptive defense in specific scenarios. These specific scenarios come from creating the conditions that an attacker believe an authority of the organization's security is alerted to their attack. For example, after an attacker compromises a system, a message may be set to trigger that the security team has been alerted (Zhu et al. 2021). This type of influence would

need to predict the attacker’s next move based on prior moves, but the goal could be to cause the attacker to abandon their attack.

6. Scarcity: A situation with scarcity implies that there is a perception of missing resources. This influence principle plays on a person’s desire to have something because of the perceived lack of resources.
    a. Social engineering example: A social engineer creates urgency through scarcity. Moving the decision process up for a victim lends to the victim making a decision that benefits the social engineer. In another example from Facebook, a popular phishing message went around in 2011 utilizing the scarcity principle (Cluley, 2012). This message told users that Facebook was closing that day and they only had 15 minutes to retain their account by logging in. The link in the message was malicious and stole account information after the user tried to log in.
    b. Deceptive defense use: For the defense to apply the scarcity principle to their benefit, there must be a resource the attacker needs from the defense. For example, this resource could be the amount of time perceived available to the attacker for the attack. Assuming the defense is using sensors to detect when the attacker begins their attack, the resource “time” could be controlled by the defense. This control exerted by the defense

could be through a stated upcoming maintenance. Allowing the attacker to know how long their attack is going to be, and shortening it, creates scarcity of the resource "time".

Social Engineering Attack Framework

A social engineering attack can be displayed through an attack framework. This social engineering attack framework allows us to understand and investigate an attack of influence from beginning to end (Mouton et al., 2014). It takes the "art" of manipulating a person and breaks it down into a usable methodology that we will be looking at as an opportunity to bolster a deceptive defense. Each of the above principles of influence can be applied as the source of manipulation within this framework. According to Mouton et al. (2014), a social engineering attack is made from the types of communication, the social engineer, the goal, the medium, the compliance principles, and the techniques. A framework put together by the research of Mouton, based on Mitnick's social attack model, will give us the depth required to apply social engineering concepts. The Mouton et al. (2014) framework is laid out in six steps:

1. Attack Formulation: The attack formulation stage is meant to determine the goal and identify the target. This stage of the framework breaks the target into either individuals or groups. Determining what is desired and who it is desired from will guide future decisions.
2. Information Gathering: At this point a social engineer will gather as much information as possible related to the target and the attack. According to

Muscanell (2014), social engineers gain access to personal information with the intent to strengthen a principle of social influence.

a. An attacker wants to find where they will find the information that can further the attack.

i. Public information (websites, social media, and blogs) vs. Private information (medical records, and bank accounts)

1. After gathering the information, the information is assessed to determine what is relevant and what is non-relevant.

b. This stage is repeated until the attacker is satisfied that enough information has been gathered.

3. Preparation: The seasoned social engineer ensures everything is ready at this point.
   a. The information will be constructed into the bigger picture. This lays out the pretext, forming the attack vector, which formulates a plan to reach the goal.
4. Develop a Relationship: Develop a (good for the exploitation) relationship with the target.
   a. Developing a relationship is done through establishing communication.
      i. Example: An attacker could establish communication through digital means such as an email.

   b. Within the development of a relationship is the building of a rapport. This means that the form of communication must keep the victim within the bounds of the ruse. The prior mentioned email must be believable and not set off red flags within the victim's head.

5. Exploit the relationship:
   a. The target should be primed utilizing manipulation tactics with the means of pointing the victim to the desired emotional state suited for the plan.
   b. After the target has reached the desired priming, the elicitation can commence. Elicitation is the finale, where the attacker achieves their end, such as a user clicking on the malicious link in the email and the backdoor getting installed on their computer.
6. Debrief: In most cases, an attacker does not want to be caught, and it is in their best interest to ensure the target is able to be attacked again if more information is required.
   a. To that end, the victim should be returned to a normal state of mind.
   b. At this point, if the first goal was achieved and there are further goals, then it cycles back to the gathering information stage.

Analysis of How Influence Translates Defensively

The principles of influence laid out by Cialdini (2007) rely on the target to be in a state of emotions that allow for the influence to be successful. Each technique has a different set of requirements to be successful. For example, in Cialdini's studies the scarcity principle is more effective when the target believes there is competition for the scarce resource. In the case of attack vs. defense, a social engineer may introduce scarcity and then enforce it with competition. For example, in communication with a victim, a socially engineered attack may use an advertisement that states there are only two items available in stock and that the order needs to be placed immediately. This would be a ruse enforcing the scarcity principle, and there would in fact be plenty left in stock for the victim to buy (or none). They can then introduce competition for the resource with further communication. If the victim reaches out to the attacker, they may then state that the price has gone up because there is an imaginary bid on the last item. This scenario illustrates the freedom a socially engineered attack has. While the social engineer has this freedom, the deceptive defense may be extremely limited with how they could introduce scarcity. The limitation stems from how they can present deception to the attacker during an attack. In many examples, influence exerted by a social engineer towards a victim might not be directly translated to a defender using the same principle of persuasion on an attacker. An attacker will have various aspects of their mindset, emotions, characteristics, personalities, cultures, and knowledge base that alters the influence types used against them. Zhang et al. (2021) propose that "biases are a cornerstone component to the success of any deception-based mechanisms". This same researcher states that a major success factor is evaluating the progress of an attacker and how successful the deception was from the progress. As mentioned, the most popular principle of influence used in phishing emails was the “liking” principle. To implement this principle, an attacker will research their victim, or use common aspects of liking, to be successful in their attack. A victim will be primed for an attack because of the niceties in the email, the friendly greeting, the content that speaks of an acquaintance, or the back and forth with a friendly individual. After being primed for the attack and being in the correct emotional state, the social engineer swoops in with a malicious request. To attempt to apply the concept of liking against an attacker in the exact same way from the perspective of a deceptive defense may be difficult, but to take the idea of how a social engineer treats their victim to apply the concept of liking may have more success. The defense has little control over their attacker’s emotional state in the early stages of the defense, but if the concept of liking were applied during a MTD while the attacker was confused or frustrated, it may be the way to manipulate their behavior towards a target of your choosing (Pawlick et al., 2019). Understanding when an attacker is confused, applying pressure at the right time, and then giving them an out that commonly works for them during other attacks could give the defense a successful tactic. The defense may not be able to prime the target over the course of hours or days to the correct emotional state, but they will be able to tell when an attacker is mid attack and running across issues due to a deception chain based MTD.

This chapter addresses “How can cyber defensive deception borrow concepts from social engineering to aid in bolstering a deception-based defense?” In the discussion of how a deception-based defense could borrow concepts from social engineering, the prior chapter covered how a social engineering attack is successful along with examples of attacks that utilize successful concepts of social engineering. This success comes from the influence and persuasion they apply to their victims and the framework used to deliver their attacks to the victim. While looking at these successful attacks, we looked at lessons and concepts a deceptive defense may learn from, and they can use within specific defensive cases. We will continue looking at more fine-grained concepts to be borrowed from social engineering in the following chapter.

CHAPTER FIVE:
DISCUSSION TO MATCH INFLUENCE CONCEPTS

Social engineering attacks and deceptive defense techniques both influence human behavior to reach their goals. While one is an attack and one is a defense, the principles of influence can be seen in both. This section is meant to explore opportunities of influence a deceptive defense can utilize from the success of social engineers. This exploration will be looking at similarities between deceptive defenses and social engineering, the differences in influences to exert, how the frameworks can be used together, and what is successful in social engineering attacks that may be successful in matching deceptive defense techniques.

Analysis Methodology

We have already determined that both offensive and defensive deception can implement an influence chance, but there are fundamental differences between how a social engineer can use influence and how a deceptive defense can use influence. To work through these differences and applications, we will look at each stage of the deception chain and each stage of the social engineering framework paired with how principles of influence can be integrated within the mesh of these techniques. To propose this meshed framework, we will be selecting most similar deceptive defense techniques to set against most similar social engineering techniques. After selecting these most similar techniques, we will select the principles of influence being used within each technique. Next, we will treat the planning of the deceptive technique as if it were a social engineering attack and see how the planning would happen within those contexts set directly against the most similar social engineering attack.

Picking Techniques to Apply Influence

To select a similar social engineer attack technique to pair with a defensive deception, we will start by first classifying the form of communication that they use. To do this, we look to the research done by Mouton et al. (2014) who breaks social engineering tactics into two main classes: direct and indirect communication. If we bring this form of classification to deceptive defense techniques, honey technology would be indirect communication, where there is an intermediary of communication through the defense. The closer we get to the attacker’s engagement technique, the closer we get to what could be classified as direct communication. Next, we will pick a pairing of attack and defense that utilize a similar medium. The medium can be seen as how the interaction of communication is performed. A honey technique could use a network of decoys (honeynet) to communicate their deception to an attacker, and this medium would be communicated to an attacker’s scanning capabilities. Finally, the selection will also delve into the concepts of influence assembled by Cialdini (2007). Both social engineering and deceptive defense work within the bounds of what can feasibly influence a target in the chosen technique. Even if there is a similar communication style and a similar medium, there may not be a similar influence. For example, an attacker can utilize the authority principle in a phishing email, but authority may end up being ineffective by a defense utilizing a moving target defense which matches the communication type of a phishing email. In addition to the influence type similarity, we will be selecting a technique that extends, or through its goal opts to extend a similar amount of influence chances. To visualize the qualitative process of identifying a similar technique from both categories, the following two tables were assembled.

Table 2. Defensive Deception Qualitative Analysis

Category	Honeypot	Honeynet	Honeytoken	MTD	Attacker Engagement
Communication Type	I	I	I	I, D	D
Medium	DC	DC	DC, PC	DC	DC, PC
Influence Chances	L-M	M-H	M-H	H	H

The “Communication Type” category is labeled as I for indirect communication and D for direct communication. The “Medium” category is labeled as DC for digital contact and PC for physical contact. The “Medium” category will be judged and broken down further, after the initial selection of the most similar technique. The “Influence Chance” category is labeled as L for low, M for medium, and H for high. Low to high ratings are based on the amount of interaction the technique is likely to extend to the target.

Table 3. Social Engineering Qualitative Analysis

Category	Phishing	Whaling	Tailgating	Reverse Engineer	Baiting	Pretext
Communication Type	I, D	D	I, D	D	I	D
Medium	DC, PC	DC, PC	PC	DC, PC	DC, PC	DC, PC
Influence Chances	M-H	M-H	H	M-H	M-H	H

Based on the initial qualitative analysis tables, the most aligned techniques are “Honeytoken” and “Baiting”. Both honeytoken and baiting use indirect communication (Mouton et al., 2014), digital or physical contact types, and have a medium to high influence chance amount (Aldawood et al., 2020).

These can be judged as similar, and examples show the logical similarity of each. A honeytoken is laid down by the defense to draw an attacker to it, to further the goal of the defense. The attacker then uses the honeytoken, either being misdirected to a trap or to give away what their attack is going to be. A baiting set by a social engineer can be seen as performing a similar task, with a different end goal. The baiting is laid down to draw a victim in, furthering the attacker’s goals. It could be in the form of a poisoned USB drive, where the attacker wants the victim to use it to gather more information from the victim or direct the victim to another influence chance, such as a malicious website. Now that a similarity has been established, the next stage is determining the types of influence a social engineer uses with the baiting technique and the types of influence a defender may use.

Influence Stacking

For a defense to choose a type of influence used within a honeytoken deception technique, we can look at the success social engineers have had with the poisoned USB drive. What makes the poisoned USB drive a viable tactic used by social engineers? According to Ferreira et al. (2015), social engineers utilize multiple concepts of influence together. This researcher studied phishing emails, but the results of stacking influences can be extrapolated to the baiting technique. Example: An attacker embeds a keylogger in a file on a USB drive and presents it to a target at a music festival. They do not just hand it to the victim and expect the victim to use it. They may present it saying something like:

“I am a singer and here is my latest song, only a few people have gotten to listen to it. Could you please let me know what you think? I feel like you have good taste in music since you’re here too.” This example is made up but demonstrates the stack of influence concepts in three sentences. Scarcity from the few people that have listened to the song, reciprocity from the act of picking the audience to give a gift of a song to and liking from the compliment in music are all at play in one influence chance.

So, what can the deception-based defense learn from this example of social engineering and baiting? The social engineer picked a song to give away at the music festival, matching the context of the environment. If the honeytoken were built for a hospital, the token could be a false patient file or a duplicate doctor’s credentials. The social engineer used a liking principle in their influence chance. A defender could utilize an influence concept such as liking to make the honey token appealing to the attacker, such as a false file labeled “classified”. On top of pushing and pulling with influence concepts, the honeytoken itself could lead to further deceptions and influence chances, just like the USB drive leading to a malicious keylogger.

Using the Framework in the Chain

Planning the deception chain and outlining the social engineering framework were both presented in prior sections. Similar techniques have been identified and influences have been considered, next we can see how social engineer attacks may add concepts to the deception chain for the defense. This section cross references the frameworks presented in the prior sections with the intent of finding an application of the social attack framework within the MITRE deception chain. As seen below, the deception chain can incorporate the idea of a social engineering attack if the defense chooses to focus on influencing the attacker and account for their reactions or emotional state.

1. Purpose: When a defender is planning their deceptive defense, the social attack framework can begin to be considered to find the purpose of the deception. Determining the attacker's goal will aid in deciding the purpose of the defense. A social engineering attack begins by defining the goal and the purpose of the defense aids in thwarting the goal.
2. Collecting Intelligence: Normally, a deceptive based defense puts together known attacks in this stage. In addition to this, they can add to this stage by profiling the attacker who composes the most current threats. This profiling matches the SE attack framework stage where an attacker gathers as much information related to the victim as possible. Public, private, and alternative methods of gathering information on attacker types can be utilized. This stage may include adding the first deceptive defense, a honey device that can detect if it is a human based attack or an AI based attack (Horak et al., 2017).
3. Designing the Cover Story: The deception chain speaks of influence at this point but based on the prior stage incorporating the SE attack framework, the profile of an attacker and the purpose of their attack

can be included in the choice of influence. A plan to return the attacker back to an emotionally ready-to-be deceived state may also be added within this stage as it will continue the ability for defenders to utilize influence chances.

4. Plan: Since this is where the technicality of the deception is formed, it should also be where the defense can decide on how they can do the equivalent of developing a relationship with the attacker. This “relationship” may be in the form of how the attacker interacts with the deception and what they expect the attacker to do based on the interaction.
5. Preparation: Like the prior stage, based on the attacker profile, the attacker goal, and the deception of choice, preparation can focus on the guidance of the attacker through the deception. This matches the SE attack stage of “preparation” where the engineer is trying to account for building the big picture of how an attack will happen.
6. Execution: The execution stage aligns with the SE framework stage of exploitation. The deception chain can borrow the idea of priming within this stage. Priming the attacker for a deceptive defense can come from the order of events, the deception in use, or the timing of the defense (Zhu et al., 2021).
7. Monitoring: A social engineer can monitor their attack, to determine how the victim is responding, to then adjust as needed. A deceptive

defense normally monitors for the culmination of their efforts as well. To borrow from a social engineer, a plan can incorporate multiple side shoots to account for how the attacker “may” react with guidance triggers to manipulate the attacker back on course to the goal of the defense (Zhu et al., 2021).

8. Reinforcing: Depending on the goal of the defense, it may be determined that the tracks of the deception should be covered. This is a play out of a social engineer’s playbook when they do not want to be caught. A deceptive defense covering their tracks similarly to a social engineer may resolve retribution or hide how the defense was successful to the attacker.

CHAPTER SIX:

CONCLUSIONS AND AREAS FOR FURTHER STUDY

This project researched the similarities between a deceptive defense and a socially engineered attack. This similarity is highlighted with the principles of influence and the manipulation of human behavior. By understanding how they work separately, we can see how these techniques are related and how the defense is supported by concepts borrowed from the social engineering framework. Not only can they incorporate some of the framework, but they can look to the success of socially engineered attacks for inspiration in the defense. Lastly, a defense can work to build up their influence chances to aid in applying influences on an attacker.

Defenders face hurdles of applying influence in the way that social engineers apply influence on their victims. There are specific techniques within both the offensive deception and the defensive deception that have striking similarities. These similar techniques are useful to identify and understand for alignment techniques social engineers use with techniques deceptive defenders use. Aligning similar techniques allows for less hurdles of influence uses and allows for inspiration to be extracted from a successful social engineering attack.

Further research into how an attacker reacts to specific influence principles during an attack would be useful in the field of understanding influence on an attacker. A study that attempts to influence a multitude of attackers with the same defensive item, such as a moving target defense, and uses multiple influence concepts to enforce the deception would be desirable. A study like this would allow for documenting the most useful influence concept in different situations during a deceptive defense. Finally, it may also be useful to explore how a honeypot could be strategically used as an initiator of an offensive deception attack for an aberrant guest.

REFERENCES

Aldawood, H., & Skinner, G. (2020). An advanced taxonomy for social engineering attacks. *International Journal of Computer Applications*, *177*(30), 1–11. https://doi.org/10.5120/ijca2020919744

Almeshekah, M. H., & Spafford, E. H. (2014). Planning and integrating deception into computer security defenses. *Proceedings of the 2014 Workshop on New Security Paradigms Workshop - NSPW '14*. https://doi.org/10.1145/2683467.2683482

Al-Shaer, E. (n.d.). Responses to RFI for the 2015 Federal Cybersecurity R&D Strategic Plan. *2015 Federal Cybersecurity R&D Strategic Plan*. https://www.nitrd.gov/documents/cybersecurity/2015stratplanrfi/NITRDCybersecRFI-Al-Shaer.pdf

Bere, M., Bhunu-Shava, F., Gamundani, A., & Nhamu, I. (2015). *International Journal of Computer Science Issues*, *12*(6). https://doi.org/10.20943/01201701

Burgoon, J. K. (n.d.). Interpersonal deception theory. *Encyclopedia of Deception*. https://doi.org/10.4135/9781483306902.n201

Calder, Spencer R. (2016). A Case for Deception in the Defense. *Military Cyber Affairs. 2*(1), Article 4. https://www.doi.org/http://doi.org/10.5038/2378-0789.2.1.1021

Cialdini, R. B. (2007). *Influence: the psychology of persuasion*. Collins.

Cluley, G. (2012, September 17). *Facebook will close all accounts today? rogue app spreads virally*. Naked Security. Retrieved March 13, 2022, from https://nakedsecurity.sophos.com/2011/02/01/facebook-will-close-all-accounts-today-rogue-app-spreads-virally/

Cohen, F. (2009). *Moving target defenses with and without cover deception*. condor.depaul.edu. Retrieved April 17, 2022, from https://condor.depaul.edu/dmumaugh/readings/handouts/SE477/Black-Swan-2009-04.pdf

CompTIA. (n.d.). *What Is Social Engineering? The Human Element in the Technology Scam.* Retrieved April 16, 2022 from https://www.comptia.org/content/articles/what-is-social-engineering

Dominguez, A. (n.d.). *The State of Honeypots: Understanding the Use of Honey Technologies Today*. Egnyte. Retrieved April 16, 2022, from https://sansorg.egnyte.com/dl/HE62lPPvln

Facebook. (2020). *About Fact-Checking on Facebook*. Facebook. Retrieved March 13, 2022, from https://www.facebook.com/business/help/2593586717571940?id=673052479947730

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. *Lecture Notes in Computer Science*, 36–47. https://doi.org/10.1007/978-3-319-20376-8_4

Ferguson-Walter, K. J. (2020). *An Empirical Assessment of the Effectiveness of Deception for Cyber Defense*. (Publication 1823) [Doctoral Dissertations, University of Massachusetts Amherst]. https://doi.org/10.7275/z0rb-ek46

Ferguson-Walter, K., Fugate, S., Mauger, J., & Major, M. (2019). Game theory for Adaptive Defensive Cyber Deception. *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security - HotSoS '19*. https://doi.org/10.1145/3314058.3314063

Ferguson-Walter, K., Shade, T., Rogers, A., Trumbo, M. C. S., Nauer, K. S., Divis, K. M., Jones, A., Combs, A., & Abbott, R. G. (2018). The Tularosa study: An experimental design and implementation to quantify the effectiveness of cyber deception. *Hawaii International Conference on System Sciences 2019*. https://doi.org/10.24251/HICSS.2019.874

Gallegos-Segovia, P. L., Bravo-Torres, J. F., Larios-Rosillo, V. M., Vintimilla-Tapia, P. E., Yuquilima-Albarado, I. F., & Jara-Saltos, J. D. (2017). Social engineering as an attack vector for ransomware. *2017 CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON)*. https://doi.org/10.1109/chilecon.2017.8229528

Hanlon, Roger T., Conroy, Lou-Anne, & Forsythe, J. W. (2007). Mimicry and foraging behavior of two tropical sand-flat octopus species off North Sulawesi, Indonesia. *Biological Journal of the Linnean Society*, *93*(1), 23–38. https://doi.org/10.1111/j.1095-8312.2007.00948.x

Hebert, A., Hernandez, A., Perkins, R., & Puig, A. (2021, May 11). *How to spot, avoid, and report tech support scams*. Consumer Information. Retrieved March 13, 2022, from https://consumer.ftc.gov/articles/how-spot-avoid-report-tech-support-scams

Heckman, K., Stech, F., Schmoker, B., & Thomas, R. K. (2015). Denial and Deception in Cyber Defense. *Computer. 48*. 36-44. 10.1109/MC.2015.104.

Horak, K., Zhu, Q., & Bošanský, B. (2017). Manipulating adversary's belief: A dynamic game approach to deception by design in network security. Decision and Game Theory for Security - 8th International Conference, GameSec 2017, Proceedings. Springer, 273–294. DOI: 10.1007/978-3-319-68711-7_15

Humphreys, R. K., & Ruxton, G. D. (2018). A review of Thanatosis (death feigning) as an anti-predator behavior. *Behavioral Ecology and Sociobiology*, *72*(2). https://doi.org/10.1007/s00265-017-2436-8

IBM Security. (2021) *Cost of a Data Breach Report*. https://www.ibm.com/downloads/cas/OJDVQGRY

ISACA. (2020). *State of cybersecurity 2020*. Retrieved April 10, 2022, from https://www.isaca.org/go/state-of-cybersecurity-2020

Levine, T. R. (2014). *Encyclopedia of deception*. SAGE.

Mitnick, K. (2022). *The History of Social Engineering*. The History of Social Engineering. Retrieved March 13, 2022, from https://www.mitnicksecurity.com/the-history-of-social-engineering#top

Mouton, F., Malan, M. M., Leenen, L., & Venter, H. S. (2014). Social Engineering Attack Framework. *2014 Information Security for South Africa*. https://doi.org/10.1109/issa.2014.6950510

Muscanell, N. L., Guadagno, R. E., & Murphy, S. (2014). Weapons of influence misused: A social influence analysis of why people fall prey to internet scams. *Social and Personality Psychology Compass*, *8*(7), 388–396. https://doi.org/10.1111/spc3.12115

Networking and Information Technology Research and Development. (2010). *NITRD CSIA IWG Cybersecurity Game-Change Research & Development Recommendations.* Retrieved March 13, 2022, from https://www.nitrd.gov/pubs/CSIA_IWG_%20Cybersecurity_%20GameChange_RD_%20Recommendations_20100513.pdf

Pawlick, J., Colbert, E., & Zhu, Q. (2019). A game-theoretic taxonomy and Survey of Defensive Deception for cybersecurity and privacy. *ACM Computing Surveys*, *52*(4), 1–28. https://doi.org/10.1145/3337772

Pouget, F. & Dacier, Marc & Debar, Hervé. (2003). White paper: honeypot, honeynet, honeytoken: terminological issues. Rapport technique EURECOM. 1275.

Schuh, D. L. (2021, September 8). *The cyberspace advantage: Inviting them in!* The MITRE Corporation. Retrieved March 13, 2022, from https://www.mitre.org/publications/technical-papers/the-cyberspace-advantage-inviting-them-in

Scott, W., Norris, M. H., ed. (1891) Sir Walter Scott's Marmion. Boston and New York, Leach, Shewell, & Sanborn. Retrieved from the Library of Congress, https://lccn.loc.gov/12038504.

Sembos, P. (2021, November 8). *Greek-American Stories: History of the trojan horse*. The National Herald. Retrieved February 10, 2022, from https://www.thenationalherald.com/greek-american-stories-history-of-the-trojan-horse/

STIX. (2021). *Structured Threat Information Expression*. Retrieved March 13, 2022, from https://stix.mitre.org/language/version1.1/

Stoll, C. (1995). *The cuckoo's egg: Tracking a spy through the maze of computer espionage.* New York: Pocket Books.

VPN, A., Miller, C., & Cohen, G. (2021, August 26). *Social engineering attacks caused majority of business breaches in 2020*. Industrial Cybersecurity Pulse. Retrieved March 13, 2022, from https://www.industrialcybersecuritypulse.com/social-engineering-attacks-caused-majority-of-business-breaches-in-2020/

Vrij, A., Granhag, P. A., Porter, S. (2010). Pitfalls and opportunities in nonverbal and verbal lie detection. Psychological Science in the Public Interest, 11(3), 89–121. https://doi.org/10.1177/1529100610390861

Wasson, D. L. (2022, March 12). *Battle of Hydaspes*. World History Encyclopedia. Retrieved March 13, 2022, from https://www.worldhistory.org/article/660/battle-of-hydaspes/

Zhang, L., & Thing, V. L. L. (2021). Three decades of deception techniques in active cyber defense - retrospect and outlook. *Computers & Security*, *106*, 102288. https://doi.org/10.1016/j.cose.2021.102288

Zhu, M., Anwar, A. H., Wan, Z., Cho, J.-H., Kamhoua, C. A., & Singh, M. P. (2021). A survey of defensive deception: Approaches using game theory and machine learning. *IEEE Communications Surveys & Tutorials*, *23*(4), 2460–2493. https://doi.org/10.1109/comst.2021.3102874