**Using Voice Recognition to Defend Against Social Engineering**
**Understanding Social Engineering Attacks Using the Social Engineering Attack Framework**

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Owen Mitsinikos
October 27, 2022

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISORS

Kent Wayland, Department of Engineering and Society
Briana Morrison, Department of Computer Science

## General Research Problem

*How can we remove the burden of social engineering attacks from the everyday person?*

Social engineering is a rapidly increasing cyber-attack methodology that is constantly evolving and changing. The definition of a socially engineered attack is "a psychological exploitation which scammers use to skillfully manipulate human weaknesses and carry out emotional attacks on innocent people". (Aldawood and Skinner, 2018, p. 1) Common examples of social engineering attacks are baiting, scareware, pretexting, phishing, and spear phishing. In the framework of a company, any employee could be the entry point for a social engineering attack. A pretexting attack is defined as a "series of well-planned manipulations are crafted by an invader to acquire information of the victim". (Gupta & Mukherjee, 2019, p. 69) Pretexting attacks are a very trivial way to attack large companies, since it is very easy to pretend to be an employee that the victim has never interacted with. The main problem that I am trying to solve in my technical research is how to defend against a pretexting attack by eliminating this human weakness by having potential scam calls monitored by voice recognition software. Due to the ease of being able to perform this attack, finding a way to prevent and stop pretexting attacks is a very important problem in the world of cybersecurity.

The social engineering attack framework is a process that social engineers generally follow to perform an attack. The social engineering attack framework is portrayed as a flowchart, starting from researching and preparing for the attack, moving into developing and exploiting the relationship with the victim, and finally debriefing and potentially returning to the preparation phase (Mouton, Malan, Leenan & Venter, 2014). My STS research will study this social engineering attack framework in order to understand common ways people fall for attacks. Social engineering has always been a very difficult problem to solve by software engineers, since it is a social problem rather than one that can be fixed just by changing lines of code. By understanding this social engineering framework, we can detect social engineering attacks more easily and deploy preventative measures.

## Using Voice Recognition to Defend Against Social Engineering

*How can we defend against pretexting by using voice recognition software?*

Pretexting has been a problem for as long as the telephone has existed. Being able to get information from someone without needing anything but research and a voice makes it a very simple way to attack an unknowing victim. Due to how simple it is to set up and execute, pretexting has been at the forefront of cybersecurity professionals' minds ever since it has gained popularity. The leading theory of the best way to solve a problem like this is to use voice recognition software to monitor phone calls for common phrases that social engineers use to gain information. There are several other ways to use voice recognition as a defense, such as recording the voice of every employee saying their name and matching it to the attacker on the phone. These ideas build on Hoeschele and Rogers's work in *Detecting Social Engineering*

where they designed a system to solve this problem. While solving a problem like this, it is important to view it from a security mindset. Thinking with a security mindset requires a person to "think as an attacker and find ways to circumvent and exploit code flaws (Hooshangi, Weiss & Cappos, 2015, p. 1)". The plan for my research is to develop a voice recognition system and feed it common phrases that attackers use to hack people. I will perform tests on this system by acting as an attacker would and seeing if the system catches me. After these tests, I will refine the phrases to catch anything I missed, as well as look into testing it with former social attackers to see what they think can be improved.

## Understanding Social Engineering Attacks Using the Social Engineering Attack Framework

*How can the social engineering attack framework be studied in order to predict new advances in social engineering?*

The topic of my STS research is looking at the social engineering attack framework in order to understand how to predict new social attacks that the everyday person can't prepare for. We know that the framework consists of researching the victim that the attack is going to be performed on, using the research to influence and exploit the victim, and then exfiltrating the information, ideally with the victim knowing as little as possible. It is very useful that we know and understand each of the steps because we can use this framework to detect potential attacks that we don't know, such as new attacks that haven't been implemented that are still in the research phase of the framework. A consequence of this gap in knowledge is that we can only try to take preventative measures before a new attack, and we have to wait for the new attack to happen before we can take definitive steps to stop it. Therefore, it is very important to have as much information as possible to be able to detect new attacks before they can do significant damage to important systems around the world.

*Background*

As stated in the general question, I am studying the sociotechnical system of the social engineering attack framework in order to spot patterns that can help spot new social engineering attacks. Involved in this study are the people on both ends of the attack, the attacker, or social engineer, and the victim, in many cases an employee of a bigger company. Social engineering attacks often happen in workplaces, which is the main area in which I will be studying my research topic. Since new social engineering attacks can happen at any time, it is integral that STS researchers look into frameworks like the social engineering attack framework in order to better spot attacks in their inception before it is too late.

The social groups that I will investigate in my research will be reformed social engineers who understand everything about social engineering, former victims of social engineering, who will give critical insight in how they were exploited and when they realized they had been duped. There are some key cultural factors at play in the influence and exploit part of the social

engineering attack framework such as victims feeling sorry for a fake story the attacker made up, victims falling into social pressures like clicking a harmful phishing link from one of their acquaintances, or victims being rushed into giving information to a social engineer due to not wanting to waste the attacker's time. Cultural factors like these are important to look into because they are the most integral part of social engineering, having the attacker make the victim feel comfortable in helping due to societal norms.

*Literature Review*

There is a lot of information already known about how social engineers go about performing attacks. In *Reverse Social Engineering to Counter Social Engineering in Mobile Money Theft*, researchers were able to find a way to counter attack social engineers and report them to the authorities after they have performed the attack. Unfortunately, while this is a good solution for preventing future social engineering attacks from being committed, defenders need a successful attack in order to prevent the future attacks. *A critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications* did a study to find common ways attackers got the victim to let their guard down in order to perform the attack. While my research will build on this idea, the source mainly focuses on the social part of the system, while my research will look into the mutual shaping of society and technology in social engineering attacks. Although there is a lot of information already out there, my studies are focusing on new potential attacks rather than attacks that have already happened.

*Theoretical Framework*

The main theory that I am going to use to look at the sociotechnical system of the social engineering attack framework is Pacey's Triangle. Pacey's Triangle is very useful for understanding frameworks because it breaks the framework down into three important aspects: Cultural, Organizational, and Technical. I've already touched on the cultural aspect of the social engineering attack framework in the *Background* section of this paper, showing that there are many societal norms at play when a social engineer is performing an attack. There are many organizational groups that are in this framework. The two main actors are the social engineer and the victim, but other groups are the victim's acquaintances who may also suffer from a social engineering attack due to the victim's information being compromised, the victim's company if the attack was orchestrated in order to breach a large company, and other social engineers who may learn new techniques from each other. Finally, the main technical aspect of the sociotechnical system is the telephone, but there are other aspects such as software that the attacker can use to change their voice or defensive software like the voice recognition solution in my technical problem. Understanding these aspects is important as I collect data, as it lets me focus on the important actors in the system that were described in Pacey's Triangle.

*Methods*

In order to carry out my research, I will first gather information on the social engineering attack framework by looking into similar studies performed to understand the attacks better. For example, *How social engineers use persuasion principles during vishing attacks* has valuable information on how the social engineers go about performing attacks while also having good information on how they went about testing these attacks. After gaining more of this understanding on how they generally occur, I will look into the past and research how social engineering attacks have mutated with new technologies. This is where the mutually shaping occurrence of social engineering as a sociotechnical system appears most explicitly. As new technological advances come out, both the attackers and victims receive more options to attack or defend against the other. These new ways of attacking and defending shape our society as people become more aware of these attacks. Once one side is comfortable attacking or defending, the other side will be pushed to create new technology for their side, similar to my technical research above.

After studying this from academic research, I will interview former social engineering attackers of different ages to see their different mindsets of both social engineering and the social engineering attack framework to get a first-hand perspective of what the mutual shaping was like while working in the field. I will also get their opinions on where they believe the field is heading for the future. After these interviews, I will synthesize all of my findings to predict what part of the social engineering attack framework is poised for technological improvement, while also explaining what future defenses could consist of based on my interview findings.

## Conclusion

Through both my STS research and the technical research, I will find ways to unburden the everyday person from the risk of a social engineering attack. In my STS research, I hope to learn more about the social engineering attack framework in order to understand patterns in how social engineers go about performing attacks. I also hope to understand more of the things that work in social engineering attacks, through performing research like I stated in the *Methods* section. For my technical research, I hope that I can provide meaningful insight on a potential solution to using voice recognition to detect social engineers while also pointing out flaws in different theories, including my own. Overall, all of this will work will give solutions to preventing social engineering attacks for people in their everyday life.

## *References*

Al-Dablin, D., Al-hamad, A., Al-Bahlal, R. & Altaib Badawi, M. (2020). An Analysis of Various Social Engineering Attack in Social Network using Machine Learning Algorithm. 10.22937/IJCSNS.2020.20.10.7

Aldawood, H.A., & Skinner, G. (Eds.). (2018) A critical Appraisal of Contemporary Cyber Security Social Engineering Solutions: Measures, Policies, Tools and Applications.

Ariu, D., Frumento, E. & Fumera, G. (2017). Social Engineering 2.0: A Foundational Work. 10.1145/3075564.3076260

Cuchta, T., Blackwood, B., Devine, T., Niichel, R., Daniels, K., Lutjens, C., Maibach, S. & Stephenson, R. (2019). Human Risk Factors in Cybersecurity. 10.1145/3349266.3351407

Gupta, S. & Mukherjee, A. (2019). 4. Use of big data in hacking and social engineering. In S. Gupta, I. Banerjee & S. Bhattacharyya (Ed.), Big Data Security (pp. 47-74). Berlin, Boston: De Gruyter. https://doi.org/10.1515/9783110606058-004

Hassan Kilavo, Leonard J. Mselle, Ramadhani I. Rais & Salehe I. Mrutu (2022) Reverse Social Engineering to Counter Social Engineering in Mobile Money Theft: A Tanzanian Context, Journal of Applied Security Research, DOI: 10.1080/19361610.2022.2031702

Hoeschele, M. & Rogers, M. (2005). Detecting Social Engineering. Pollitt, M. & Shenoi, S. (Eds.), Advances in Digital Forensics (pp. 67-77). International Federation for Information Technology

Hooshangi, S., Weiss, R., & Cappos, J. (2015). Can the Security Mindset Make Students Better Testers? https://ssl.engineering.nyu.edu/papers/hooshangi_sigcse15.pdf

Jones, K.S., et al.: How social engineers use persuasion principles during vishing attacks. Information and Computer Security. 29(2), 314– 331 (2020). https://doi.org/10.1108/ics-07-2020-0113

Mouton, F., Malan, M., Leenan, L. & Venter, H. S. (Eds.). (2014). Social Engineering Attack Framework. *IEEE*.