Defending Against Social Engineering Attacks Using Voice Recognition

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Owen Mitsinikos

Spring, 2022

Technical Project Team Members

Owen Mitsinikos

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

Briana Morrison, Department of Computer Science

Defending Against Social Engineering Attacks Using Voice Recognition

CS 4991 Capstone Report, 2023

Owen Mitsinikos
Computer Science
University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
ocm7td@virginia.edu

ABSTRACT

Social Engineering attacks can be very damaging to large businesses with important information to keep private. The solution that I propose to defend against social engineering attacks is to use voice recognition to alert companies when suspicious parties are potentially attacking. I am planning to design a voice recognition system that detects common phrases that social engineers use to steal information from unsuspecting victims and using these red flags to alert them. These phrases can be asking for passwords, personal information, or other suspicious actions. The anticipated outcomes for my system are for tests to result in the phrases getting picked up and reported. The next steps for this project would be to fix any blind spots found in testing and to start implementing the software once testing is complete.

1. INTRODUCTION

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. Any employee could be the entry point for a social engineering attack, especially a pretexting attack, which is defined as a "series of well-planned manipulations crafted by an invader to acquire information of the victim". (Gupta & Mukherjee, 2019, p. 69) Pretexting attacks are a very simple way to attack large companies, since it is very easy to pretend to be an employee that the victim has never interacted with.

Finding a way to prevent and stop pretexting attacks is a very important problem in the world of cybersecurity. The main challenge is how to defend against a pretexting attack by eliminating the human margin for error by using voice recognition software to monitor potential attacks.

2. RELATED WORKS

Hoeschele and Rogers (2005) lay the groundwork for different problems and solutions to social engineering, with one potential solution being a voice recognition system similar to the one I am proposing. What makes my research different is that I am actually creating and revising this system while the article just proposes the idea.

Hooshangi, et al (2015) explain what it means to have a "security mindset." The second part of my research will involve compiling common phrases used by attackers and revising these phrases in testing. A security mindset consists of "thinking as an attacker and finding ways to circumvent and exploit code flaws." This mindset is critical to maximizing the usefulness of my system.

3. PROPOSED DESIGN

The general idea of my design is to create a system that uses voice recognition to parse speech into text in order to warn potential victims of an attack. The system relies on having company-wide phones in order to monitor potential threats.

3.1 Plans for System Architecture

The voice recognition system will be a program connected to a phone that uses a voice recognition library to parse through the speech that comes through the phone line. Once the words are received, they will be compared with a dictionary filled with common phrases that hackers use to receive information. If the program finds a match between the two, it will send an alert to the person receiving the call, warning them that they may be on the phone with a malicious party. This is the main use of the system and is what I will spend the most time improving.

A secondary part of the system that I have planned is creating a database of every employee saying their name into the phone. After this database is filled out, my system will integrate a check when someone is calling where it asks the employee to say their name before connecting them to the person they are calling. My system will then compare this to the matching voice in the database to add another layer of security in the process. If the voices do not match, an alert will be sent to the person who is being called.

3.2 Requirements and Limitations

The most important need that this system solves is adding another layer of security to a company. Other needs that are less important, but would be good to take note of are making the system both easy to integrate and use, as well as unobtrusive to the employees. In researching this, I found a major limitation that had to be addressed in privacy and monitoring phone calls. This is a very divisive subject and I had to make sure that the system does not overstep any boundaries that employees may have. Another limitation that came up during my research is that companies are moving away from having designated work phones, with many switching to using their personal cell phone or company-wide applications like Microsoft Teams. I had to take the limitations into account in my design, as I do not want to design a system that is obsolete in a few years due to technological advances.

The most important limitation that I had to solve was the privacy limitation, as it will be very difficult to get companies and employees to use the system if they do not trust it. My solution to this problem is using work phones instead of employee cell phones, allowing the system to monitor the calls while ensuring that the calls only deal with the company. The system will also delete all of the data it parsed from the call to ensure that it cannot be used maliciously. There may be companies that still do not trust this, but this was the best solution I could find to a very difficult issue in privacy.

Another limitation that I found difficult to solve is the issue of false positives, where a benign conversation could accidentally get flagged if a phrase is said in a different context. Unfortunately I could not find a good solution to this limitation that does not sacrifice the security of the system, so it will just have to be something the companies have to keep in mind when using it.

4. EXPECTED OUTCOMES

The main outcome that my system is expected to provide is a more secure feeling around getting unexpected and urgent calls as an employee. Knowing that they have this system behind them, employees can feel a lot safer taking calls from people that they do not know and do not have to constantly be second-guessing whether the person calling is malicious. Another outcome that I expect my system to have is that it will not be perfect on its first test. I plan on testing the system with white-hat social engineers, allowing me

to recursively add phrases to the system that I did not think of at first. After extensive testing, I expect the system to be a great solution to social engineering.

5. CONCLUSION

The voice recognition system is very important in the fight for security due to the prominence of social engineering and how vulnerable people can be to social engineering attacks. I found that it is very important to be careful with voice recognition, especially when implemented with phones, due to people understandably not wanting to be recorded by a system that they may not know the specifications of.

While the system is designed with a large company in mind, it can definitely be retooled to work for small companies and personal use, although it probably would not be as useful due to the nature of social engineering attacks. Security is very important and my system solves an often overlooked part of cybersecurity. While security programs can be tested and revised for bugs, a person cannot be expected to always make the correct decision in a situation which could lead to large problems for companies. With my system, I found that eliminating the human element of cybersecurity can be done.

6. FUTURE WORK

In the future, I would definitely like to edit my system to not only work for phone calls, but also Zoom, Microsoft Teams, or other potential programs that are common in the workplace. Workplaces are moving away from phones and these are blind spots in my system that attackers could use to work around it. Being able to keep up with new advances in technology in the workplace is key to keeping my system relevant.

REFERENCES

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

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