Thesis Project Portfolio

Defending Against Social Engineering Attacks Using Voice Recognition

(Technical Report)

An Ethical Analysis of White-Hat Hacking

(STS Research Paper)

An Undergraduate Thesis

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

University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Owen Mitsinikos

Spring, 2023

Department of Computer Science

Contents of Portfolio

Executive Summary

Social Engineering is a common cyber attack that consists of using a human as a vulnerability to gain access to a system or information. Due to the lack of resources and training needed to perform a social engineering attack, they have always been a thorn in the side of cybersecurity specialists everywhere. The largest issue with social engineering attacks is that there isn't an easy way to defend against them. While companies like Microsoft and Apple can patch a vulnerability that gets discovered, companies can't just "patch" social attacks. My technical research consists of a way to increase the likelihood of detecting a social engineering attack before the attacker gains access to sensitive information. I solved this by designing a voice recognition software that detects common phrases that are used in social engineering attacks and alerts the victim if they are at risk of an attack being performed on them. My STS research consists of looking into white-hat hacks, which occur when a company hires a certified hacker to try to hack them. My research determines whether white-hat hacks are ethical or not, particularly when they use social engineering strategies to achieve the hack.

As stated in the introduction, my Technical Research involved using voice recognition software to detect social engineering attacks. The rationale behind this project was that human beings are always susceptible to social engineering attacks, since regardless of how alert they are, there is always a chance of slipping up, particularly to things like lack of sleep, boredom, or other human elements. My research intends to take this responsibility partially out of the human's hands by having the voice recognition system alert the person of danger. The methods in building and designing the software were to create a dictionary filled with the most commonly used phrases in social engineering attacks, test the system with real social hackers to build the dictionary more and to see how well the system holds up, and then refine the system to where it

is able to detect the hackers consistently. I came across several limitations with the research, mainly privacy issues occurring when the system is used in the workplace, as the system will be integrated through a company's phone lines. Overall, I conclude that a voice recognition system would be very useful in large companies looking to bolster their defense against social engineering attacks.

My STS Research Question, "Is white-hat hacking ethical?", delves into the common practice of using white-hat hackers to test a company's cyber defenses. As stated previously, white-hat hackers are "ethical" hackers that are hired to hack into a company to test their security. My research looks into how ethical this practice is when it comes to the white-hat hackers deploying social engineering techniques to unsuspecting employees. White-hat hacking is a common practice in cybersecurity, but I could not find any research on if it is ethical or not. I looked through the Association of Computing Machinery's Code of Conduct to determine what their stance on white-hat hackers is. The main section that I looked at was the section titled, "Avoid Harm". This section explains that it is important that the harm is ethically justified, and that the white-hat hacker is obliged to undo the harm as much as possible. I also looked into the comparison between white-hat hacking and performing deceptive psychological research. Overall, I found that white-hat hacking complies with the Association of Computing Machinery's Code of Conduct, as long as the white-hat hacker debriefs the employees after performing the hack.

I found that my research is valuable to the field of computer science, and more specifically cybersecurity. Both the voice recognition system and white-hat hacker research improve the defenses against social engineering and help make clear the stance of the Association of Computing Machinery when it comes to white-hat hacking. I achieved almost all

that I set out to do. In my prospectus I originally wanted to interview white-hat hackers while looking into them, but I found that I did not know where to find white-hat hackers to interview and quickly ran out of a timeframe to make it possible. I was a little disappointed in the technical research, as I would have liked to work on a physical project with a group, but the limitations of the computer science capstone requirements made designing the system the next best thing. Overall, both research projects have room to grow and be improved, with the technical project still needing to be created and applied to different software like Zoom and Microsoft Teams, and the STS project pushing to close the gap between software testers and white-hat hackers so we can defend against cyberattacks efficiently using non-deceptive practices.