Undergraduate Thesis Prospectus

Preparing for the Quantum Revolution

(technical research project in Computer Science)

The Psychology of Social Engineering Attacks

(sociotechnical research project)

by

Anmol Sandhu

October 27, 2023

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.

Anmol Sandhu

Technical Advisors: Brianna Morrison and Rosanne Vrugtman, Department of Computer Science

STS advisor: Peter Norton, Department of Engineering and Society

General Research Problem

How can cybersecurity measures be improved?

Computers are an integral part of people's lives today. People store much of their valuable information on their personal devices and institutions like hospitals and the government store important information on their patients and citizens on their own computers. While convenient, this creates massive vulnerabilities, as any information stored on a computer can be stolen through cyberattacks, a rapidly increasing threat (University of North Georgia, 2023). Cyberattacks can take a multitude of forms, from phishing scams to complex data breaches. The estimated cost of these attacks is in the trillions of dollars annually (University of North Georgia, 2023). There is a continuous arms race between cybersecurity professionals and cybercriminals, with each side finding new weaknesses to fix or exploit. The prevalence of cyberattacks and the importance of the data stored on computers necessitates continuous improvement in cybersecurity. By analyzing historical data and current scientific developments, it will be possible to determine existing flaws, how to fix them, future threats and how to counter them.

Preparing for the Quantum Revolution

What effects will quantum computers have on cybersecurity and what can be done to prepare?

Individual capstone project through the computer science department under advisement of Dr. Morrison and Dr. Vrugtman.

The basis of modern encryption techniques is the difficulty in finding prime factors of large numbers. For a large number, attempting to factorize it on a classical computer would take

longer than the lifetime of the universe. The numbers used for encryption are many times larger than this and would take, for all intents and purposes, infinite time and power to factor. However, on a quantum computer this problem could be trivialized and solved in a reasonable time frame. The algorithm to do this already exists (Shor, 1994). The only limitation is the lack of a functional quantum computer to run the algorithm. Once this computer exists, existing encryption techniques will become obsolete. Governmental institutions, universities, and corporations are all working to develop this computer. They are also developing encryption techniques that could be secure against quantum computers (Bernstein & Lange, 2017). The NSA has run competitions open to the public to create such an algorithm. Numerous algorithms have been proposed (NIST, 2022). The goal of this project is to analyze some of these algorithms and determine their efficacy and ease of implementation.

There does not yet exist a quantum computer that can outperform classical computers and, in most cases, it fails to perform at an equal level. The state of the art has recently been able to factor numbers in the millions (Dash et al., 2018), which does not begin to approach the scale of numbers used for encryption. Due to the importance of quantum computing technology, it is unlikely that all existing research will be made available to the public. These factors will limit the scope of this project to a purely theoretical domain. Using quantum mechanics, computing theory, and math, it will be possible to determine if these encryption techniques will be secure. However, a future mathematical or physical discovery could update existing theory, undermining the security of these algorithms. Additionally, theory can only do so much. Without a quantum computer to test on, there cannot be a guarantee that the algorithm with be secure. At the end of this project, several proposed algorithms will have been analyzed to see if they are theoretically secure. If any are found to be secure, that will be a big step in beginning the transition away from

current encryption to newer algorithms. This transition must be accomplished before an ideal quantum computer exists, to prevent the theft of data.

The Psychology of Social Engineering Attacks

How do malicious actors adaptively exploit human psychology in social engineering attacks?

The most common type of cyberattacks are social engineering attacks, such as phishing scams (Klimburg-Witjes & Wentland, 2021). These attacks rely on exploiting vulnerabilities in human psychology, such as trust or the promise of a large reward (Salahdine & Kaabouch, 2019). An iconic phishing scam is a wealthy foreigner who wants to give the victim a large sum of money and needs their banking information. The promise of a substantial reward was enough to make people overlook the warning signs. Variations of this scam are still popular today. Much like other types of cyberattacks, social engineering attacks are constantly changing as people adapt and attackers adapt to these adaptations. These attacks are effective, but how exactly do attackers exploit human psychology?

Participants include victims (among them naive users, risk-tolerant users, and savvy users), cybersecurity experts, cybersecurity vendors, and law enforcement agencies such as the FBI. Because social engineering attacks exploit vulnerabilities in human psychology, some people are more susceptible than others. Montañez et al. (2020) found that individuals who only infrequently deal with cyberattacks are more likely to fall for them. High workload and stress can also increase susceptibility to attacks (Montañez et al., 2020). An attacker who knows this would look for people who don't often deal with attacks, especially during times when the person is likely to be overworked. Attackers also often pretend to be figures with authority over the victim,

incentivizing compliance. In Goltz (2021), an intern fell for an attack pretending to be the CEO. Researchers are trying to understand how these attacks occur. There was no shortage of papers about this topic, Montañez (2020) was especially detailed, being one of the first to layout a view of human psychology through social engineering. The three basic categories of users are the naïve, the risk-tolerant, and the tech-savvy. Each of them is susceptible to different social engineering attacks. A naïve user may not think that someone would try to scam them, and a risk-tolerant user might consider the reward worth the risk. A tech-savvy user might seem resistant to these attacks, but some of the largest phishing scams have been performed on seemingly tech-savvy victims (Huddleston, 2019). Even corporations can be victims of these attacks and many spare no expense in pursuing cybersecurity measures (Aiyer et al., 2022). Cyberattacks can cost vast amounts of money in both data and reputation, so corporations naturally want to avoid them (University of North Georgia, 2023). Despite this, many leaders of corporations do not fully understand cybersecurity (Lohrmann, 2016). This gap in understanding could be an exploitable vulnerability.

There was also an interview with an expert, explaining that attackers build profiles on potential victims (Lohrmann, 2016). Like preparing for a job interview, attackers learn about their target: their leaders, their motives, and their goals. After understanding this, attackers learn about the technology used by their target and the people involved with it. By doing so, attackers can make themselves seem legitimate (Lohrmann, 2016). Attackers must be adaptive to constantly adjust to different interactions with different people. To be effective, cybersecurity experts must understand the system to the same level as the attackers, they must be able to imagine what the attacker will be after and how to stop them (Lohrmann, 2016). Corporations like Duo sell tools that combat attacks (Duo Trusted Access, 2019). Two-factor authentication

prevents attackers from accessing data without a second confirmation from the victim, making the attacker's task harder, though not impossible as social engineering attacks can get the user to give access, often through annoyance. These corporations try to strike a balance between security and convenience to optimize security. If users feel too inconvenienced by security, they may ignore or disable it, but if security is too lax, an attacker could easily get past it. The FBI keeps track of attacks, their effects, and ways to resist them (FBI, 2023). The FBI has interests beyond most other participants, primarily national security. Matters concerning national security mean dealing with threats from entire countries, instead of small groups of criminals. This presents a larger threat and so needs better understanding of how rival nations can take advantage of social engineering to steal critical information. These participants look for ways to understand how attackers work and to resist them. By delving deeper into these sources, it may be possible to understand how attackers exploit psychology for social engineering attacks.

References

Aiyer, B., Caso, J., Russell, P., & Sorel, M. (2022, October 27). *New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers | McKinsey*. www.mckinsey.com. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188–194. Web of Science

Dash, A., Sarmah, D., Behera, B. K., & Panigrahi, P. K. (2018). Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer. Arxiv.org.

Duo Trusted Access. (2019). Duo Security. https://duo.com/product

FBI, Internet Crime Complaint Center Releases 2022 Statistics. (2023, March 22). Federal Bureau of Investigation. https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics

Goltz, S. (2021). The Intern That Fell for the Phishing Scam | Usherwood Office Technology. www.usherwood.com. https://www.usherwood.com/blog/intern-fell-phishing-scam

Huddleston, T. (2019, March 27). How this scammer used phishing emails to steal over $100 million from Google and Facebook. CNBC; CNBC. https://www.cnbc.com/2019/03/27/phishing-email-scam-stole-100-million-from-facebook-and-google.html

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses. *Science, Technology, & Human Values*, *46*(6), 1316-1339. Web of Science

Lohrmann, D (2016). How to Respond to Social Engineering Incidents: An Expert Interview. www.govtech.com. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/how-to-respond-to-social-engineering-incidents-an-expert-interview.html

Montañez, R., Golob, E., & Xu, S. (2020). Human Cognition Through the Lens of Social Engineering Cyberattacks. Frontiers in Psychology, 11. https://doi.org/10.3389/fpsyg.2020.01755

NIST. (2022). NIST Announces First Four Quantum-Resistant Cryptographic Algorithms. NIST. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Salahdine, F., & Kaabouch, N. (2019). Social Engineering Attacks: A Survey. *Future Internet*, *11*(4), 89. Web of Science

Shor, P.W. (1994), "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th Annual Symposium on Foundations of Computer Science, 124-134. Web of Science

University of North Georgia. (2023). *Cybersecurity: A Global Priority and Career Opportunity*. University of North Georgia. https://ung.edu/continuing-education/news-and-media/cybersecurity.php