[1]

Weaponizing Socializing: The Issue of Social Engineering in the 21st Century

Cole Cagle, Andrew Hamilton, and James Wiseman

***Abstract*--Social engineering is the art of using deceptive tactics to gain unauthorized access to data that can be translated into valuable information. The dark triad consisting of narcissism, machiavellianism, and psychopathy, was examined to understand the motivations of social engineering attacks. Defense mechanisms are discussed such as training/education programs and risk strategies to help mitigate the losses that organizations will face in the event of social engineering attacks. Organizations need multiple security layers in order to prevent attacks completely or to rebuild and regroup post-attack. The layers need to be taught and hardened when the opportunity presents itself. This is due to human error being the largest vulnerability that is exploited in these specific attacks. As the world continues to turn to technology, it is important to be aware of the deception of social engineering because it presents itself historically and contemporarily. This means that social engineering will continue to be performed in the future of our world.**

***Index Term*– Artificial Intelligence, Biometrics, IDS (Intrusion Detection System), Machiavellianism, Narcissism, Phishing, Psychopathy, Smishing, Social Engineering, Whaling**

I. Introduction

Since the dawn of humanity, people have attempted to deceive one another for various reasons. There are many historical examples that prove social engineering is an art that humans have performed and continue to evolve this art in the current world. From the Hebrew Bible, in Genesis 27, Jacob takes the birthright of his family from his older brother, Esau, by fooling their nearly blinded father, Isaac. He placed animal hair on his hands and arms to impose as Esau. A few centuries later, Julius Caesar created the infamous Caesar cipher so that enemies of the Roman Empire could not read valuable intel that was stolen from Roman messengers. Caesar created a defense mechanism to counter social engineering attempts. Many centuries later, in World War II, the United States' Marine Corps used the Navajo Indians for an "encrypted" form of communication over radio so that enemies could not obtain information on military operations.

II. The Issue: Social Engineering

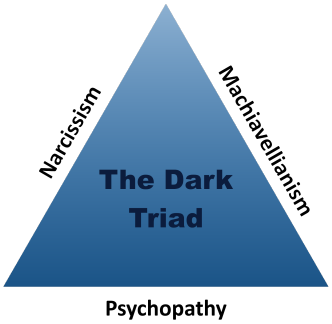
In the present time, social engineering is still a valuable skill to people with malicious intent, possibly more than it has ever been. With technology continuing to grow and evolve into every aspect of our lives, it is imperative that people are aware of this dangerous art and how it can drastically ruin businesses and lives. Social engineering attacks can be achieved in a variety of creative ways. Malicious people will try to harm devices through deceiving emails, which is known as phishing. Phishing is the most common approach taken at universities due to students being vulnerable and unaware of this tactic. Another type of attack is smishing, which involves text messaging and sending links to malicious code. The last common tactic is whaling, which is targeting a specific person with malicious intentions. These are not the only types of approaches to social engineering, however, these are the most prevalent due to technology and people becoming intertwined.

Social engineering will always continue to be a problem that people face, however, there are ways for people to defend themselves against the various attack methods. In the field of cybersecurity, there is a principle that people of this expertise abide by, and it is called the CIA triangle. The acronym stands for confidentiality, integrity, and availability. These three principles serve as the foundation for morals when it comes to protection and defense. On the contrary, researchers have studied and found three principles that malicious people build their foundation of morals on when it comes to attacking. This triangle is referred to as the dark triad, which consists of narcissism, machiavellianism, and psychopathy.[2] The authors behind this concept of the dark triad suggest methods that can help reduce social engineering attacks. The first solution is for managers in work environments to implement risk management strategies that aim to lessen the damage that could be achieved by an attack.[2]

[1] Cole Cagle is with the University of Tennessee-Chattanooga, Chattanooga, TN 37403 USA (e-mail: ygw485@mocs.utc.edu).

Andrew Hamilton is with the University of Tennessee-Chattanooga, Chattanooga, TN 37403 USA (e-mail: llg616@mocs.utc.edu).

James Wiseman is with the University of Tennessee-Chattanooga, Chattanooga, TN 37403 USA (e-mail: ddp552@mocs.utc.edu).



Another solution to the issue is for people in positions of leadership to be educated on the dark triad and for their institutions to offer multiple screening tests to attempt to detect these malicious behavioral traits.[2] It is also worth noting that screening tests are not capable of detecting all malicious people and that is why the risk management strategies should be in place. Security needs multiple layers in order to counter attacks because some layers will fail and others need to be installed to serve as reinforcements. However, the researchers mention that their solutions have a trade-off that can be difficult to accept. The trade-off is between protecting the organization and people and the privacy rights of the people put in place to operate the organization.[2] Each organization has its own unique priorities and objectives. It is ultimately up to each individual organization to decide the measures that should be taken into consideration and implemented in order to protect all aspects of the organization, most importantly the data that is housed in their database(s). The different aspects from a security perspective can be broken down into five layers. The first is the physical layer, which consists of the physical location of the organization and the technology their locations maintain. The second layer is the network, which serves as the connection between the various employees and client-server communications. The third layer is operating systems, which is the layer that consists of the operating system(s) an organization uses, such as Windows 10 or MacOS. The fourth layer is applications, which is the softwares and programs that the organization uses to execute productivity. The fifth and final layer is the most important and valuable in regards to what social engineering attacks target, and that is the data. The data is the priority target of attackers and should be the layer given the top priority to be protected by an organization. If an attack is successful and has severe repercussions, the reputation that took an organization decades to achieve can dissipate quickly and cause clients to look elsewhere for similar services. Fortunately, as mentioned before, there are a multitude of steps that can be taken to proactively seek solutions to combat the dark triad.

III. The Insight to the Solutions

There are several ways for combating social engineering in the workplace. These include implementing knowledge based measures such as education, training, and awareness programs. Social engineers use methods that are combated by these programs to bypass technical security tools.[3] In the education programs the employees would be taught electronically to enhance behavior towards social engineering. The employees would also be reminded about social engineering periodically, taught about common deceptive practices social engineers use, and taught how to handle an attack when it does happen. The training the staff would undergo strengthens the information they were educated on, for example, general social engineering training to identify threats, and training safe behaviors so the employees will have preventative techniques. The awareness programs are to raise awareness towards new social engineering tactics. These include program posters that notify staff of the latest tactics found, and programs to help categorize sensitive data. Another solution would be to implement new policies for employees to enhance the information security measures against social engineering. These include desk keeping, destruction, plug-in devices, and social media.[3] The desk keeping policy refers to keeping the employees desk clear of sensitive information, whether that is to store the documents in a locked drawer or to shred. Plug-in device policy disallows plug-in storage devices to prevent a backdoor of information being shared. The policy regarding social media does not allow employees to access social media on organization devices to prevent social engineering breaches.

Along with training and education, there have been some advancements to create tools that can help prevent some attacks and to control them when they do happen. These tools consist of but are not limited to network-based intrusion detection systems (NIDS), biometrics, and artificial intelligence.[3] These tools are used to prevent known attacks, potential threats, and even some successful attacks to be prevented because they create another layer of security. Because social engineering's aim is to use people to avoid different security layers, both artificial intelligence and the NIDS are put in place before attacks get in front of people. The use of these systems have become adapted now for many emails, apps to stop robo-calls, and various other communication systems. For example, spam folders in email is a form of these detection systems because it is detecting unwanted communications to the end user. Because of the advancement of artificial intelligence, many developers have adopted using it in the intrusion detection systems, and it is common practice for companies that can afford these expensive measures to use the most advanced artificial intelligence because the effectiveness of the systems depend on the accuracy of it.[4] Biometrics act as another barrier that attackers must overcome once they gain access. This barrier is beneficial if the attacker is trying to get deeper using known passwords and access because without the authorized user, the

[2] Maasberg, van Slyke, Ellis, Beebe, "The Dark Triad and Insider Threats in Cyber Security" (2020)

[3] Aldawood, Skinner, "Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal" (2019)

[4] Nagy, Hale, Strouble, "Verify Then Trust: A New Perspective on Preventing Social Engineering" (2010)

attackers can't get further. This upholds the confidentiality principle of the CIA triangle, which means that only authorized users can be granted permissions.

Each of the solutions aforementioned have an intended use and result but have limitations. For the various educational measures the limitations fall under human error. The limitations of the training measures is the amount of funding. All of the policies also fall under the human error category. Each of these solutions should be evaluated based on the capability of compliance of the employees.[3] These measures and policies would be the most appropriate solution without introducing role based access controls. Each evaluation of the different tools depends on the funding, quality of the machine learning, and the development of the tool, so the successfulness of these tools is measured in precision[3]. Grant precision of detecting attacks is not without faults currently, but as more advancements are found and developed, precision will increase.

IV. Comparison of Solutions From the Past to Now

The common theme of all the security practices is to reduce human error, but despite all efforts human error will persist which could also come from unclear policies.[2] Although emphasis of company policies will be to create consistency and prevent errors, humans will always need to interact with information to perform their duties. Even in implementing role based access, separation of duties, and hierarchical access, which are things that help reduce attacks from penetrating deep, there is still possibility for an error of assigning the wrong role, sharing sensitive information, etc. Because social engineering has to deal with people, everywhere that someone touches infrastructure, information, or any other protected area there is risk for a breach, so the only way to prevent it would be to take human access away. This inturn would violate the Accessibility policy of C.I.A. and make productivity plummet.

Compared to other security practices, there have been only small changes made to best practices against social engineering. Twelve years ago, the best practices were almost identical to what is being recommended to do now, which includes training and educating employees, manager, and IT departments.[3] Despite awareness and training being the emphasized security practice, there have been some advancements that have been made to help eliminate human error, such as artificial intelligence, biometrics, and network-based intrusion detection systems (IDS). The strength of these small technological advances is small, but these tools keep repetitive attacks from getting to people which prevents even a small possibility of someone falling to the attack. Seeing these tools implemented more and more in companies and email systems will help push the profitability of social engineering down which would lessen attacks. The advancement of machine learning and better hardware continues to advance, these tools will only continue to become more efficient.

V. Hardening Database Security

Database security concepts revolve around creating layers of security that protect data, and countering social engineering attacks is just another way of upholding these layers. The major issue with social engineering is that the attacker wants to bypass having to break other layers of the security layer by having someone else do it for them. Like in the earliest example of this attack, The Trojan Horse, the Trojans didn't even realize that this was an avenue that they could be attacked by.[3] By getting past the walls, moats, and guards, the Greeks were able to get right to what they wanted, and today attackers can get past all the other protective layers to get straight to the data that they are after. By implementing these proposed practices, employees will be more aware of the dangers and possibilities of attacks, which would make them think about where they type passwords, what they share, what they plug-in, etc. Once the likelihood of these mistakes are reduced, other security layers also become more effective because attacks are not able to jump around them to get to their intended destination. If the security layers, practices, and protocols are able to do the duties they were put in place for, if something breaches, security experts can go back through their systems to amend and improve their designs.

VI. References

[2] M. Maasberg, C. van Sklyke, S. Ellis, N. Beebe (2020) The Dark Triad and Insider Threats in Cyber Security [Online] https://dl.acm.org/doi/10.1145/3408864

[3] H. Aldawood, G. Skinner (2019) Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal [Online] https://f.hubspotusercontent30.net/hubfs/8156085/WhitePaper%20-%20IJS%20-%20Contemporary%20Cyber%20Security%20Social%20Engineering%20Solutions%5B1%5D.pdf

[4] Kristopher Nagy, Brian Hale, & Dennis Strouble. (2010). Verify Then Trust: A New Perspective on Preventing Social Engineering. International Conference on Information Warfare and Security, 259–. https://www.proquest.com/docview/869617328?parentSessionId=s7domaQN75AhFdy%2FuwaK6xXlrCuFmaiPYFr9N0ekqYU%3D&pq-origsite=primo&accountid=14767