How Has AI Advanced Social Engineering?

Felipe D. Trinidad Pilier Jr.

Fordham University

CISC-3580-C01 Cybersecurity and Applications

Dr. Alhayajneh

December 6, 2023

How Has AI Advanced Social Engineering?

Social engineering is one of the most common techniques cyber criminals use to gain access to sensitive information. It is unique compared to other attacking techniques because it involves direct engagement with the victim and requires a prior investigation to be efficient. Methods such as brute force attacks and implanting malware involve the victim's device rather than the victim themself. This one, in particular, revolves around manipulating human psychology and coercing a victim into giving a hacker money or sensitive information. Social engineering can be found in several attacking methods such as phishing, scareware, and vishing.

Steps of Social Engineering

Social engineering has four stages: investigation, hook, play, and exit. All attacks of this type must begin with the investigation process. This phase involves the attacker performing due diligence to gain information on the target. The hacker gathers relevant information and plans out the fake emergency they will attempt to pressure the target. Frequently it will involve a family member, friend, or neighbor needing urgent financial help. The next phase of the attack is the hook. This is where the hacker baits the target by presenting a false emergency. This is where the attack method is implemented. A scareware attack, for example, revolves around making the victim believe their device has malware and coercing them into downloading a trojan horse. The goal of this phase is for the attacker to find a way into the system. The play is what the attacker does after infiltrating the system. Information being stolen is a typical example of what may happen. Lastly, the exit is when the actor, in this case, the hacker, exits the system without leaving a digital footprint. Over time, methods that implement social engineering have evolved

considerably fast. This is due to the use of artificial intelligence and its use in tandem with manipulation.

What is AI and How Does It Work?

Artificial Intelligence is a machine's ability to take in information given by the user and essentially learn it similar to how people do. Its job is to simulate human intelligence and make the same decisions a human would make. To quote Nicole Laskowski, the Senior News Director for techtarget.com, "In general, AI systems work by ingesting large amounts of labeled training data, analyzing the data for correlations and patterns, and using these patterns to make predictions about future states. In this way, a chatbot that is fed examples of text can learn to generate lifelike exchanges with people, or an image recognition tool can learn to identify and describe objects in images by reviewing millions of examples." (Laskowski et al, 2023) Artificial intelligence revolves around the following four techniques to simulate human intelligence: learning, reasoning, self-correction, and creativity.

Discussion

AI has now reached the forefront of discussion in the technology field. There are several factors behind the recent surge in popularity. Breakthroughs in machine learning algorithms have improved AI's ability to process data. AI chatboxes are now able to generate images after being given a prompt. It has also received investments from public and private sectors to fuel further research and produce more breakthroughs. The most significant contributor to the rise in popularity is the release of ChatGPT-3. ChatGPT is a program developed by OpenAI that focuses on understanding queries and generating a response in a conversational context. It can hold a conversation with the user very similarly to how humans interact with each other. ChatGPT,

however, has grown to be a nightmare for schools. It can understand and generate answers to homework assignments given by the user. In my Operating Systems class, my professor expressed how impressive it is that AI could produce C++ code that follows the prompts of the lab assignments. Currently, school faculty are trying to develop rules that will dissuade students from using AI to assist them on their assignments. In short, it is undeniable that artificial intelligence has become phenomenal in modern society.

Cyber criminals have found a way to implement artificial intelligence to assist them with social engineering to make their attacks appear more believable. AI is able to analyze voice samples and produce a copy. According to Subbarao Kambhampati, a Computer Science professor at Arizona State University, “In the beginning, it would require a larger amount of samples. Now there are ways in which you can do this with just three seconds of your voice. Three seconds. And with the three seconds, it can come close to how exactly you sound.” (Kambhampati 1) AI is able to capture the different factors in vocal expression such as pitch, cadence, and pauses. It can simulate thousands of different emotions just from a sample. One quick look on YouTube can show results of celebrities like former U.S. President Donald Trump and current U.S. President Joseph Biden saying phrases they have never been recorded saying. Similarly, you may be able to find fictional characters performing pop culture songs.

This has especially become a problem for voice actors in the entertainment industry. Artificial intelligence can now forge an identical voice and can be used maliciously to turn actors’ talents into something undesirable in the eyes of agencies. In July 2023, Erica Lindbeck, renowned for her performances in the video game industry, was made aware of her voice being used by an AI to perform the song “Welcome to the Internet,” by comedian Bo Burnham. To her,

the video was a violation on a personal level as it was impersonating her own voice. Several voice actors stood with her against this and brought to question the ethics of AI as a whole.

With AI being shown to seemingly perfectly sound like someone after being given a sample of their voice, it was only a matter of time before hackers joined in. Unfortunately, it can be very easy to retrieve a voice sample. Some ways include intercepting communication over the internet, eavesdropping in-person conversations, and finding a video of the target or someone close to them on social media. Artificial intelligence combined with simple due diligence can produce effective bait. In an April 2023 article by Susan Campbell, Jennifer DeStefano in Arizona answered a phone call from an unfamiliar number. Upon picking up, a voice resembling her daughter's was urgently seeking assistance. She said “Mom, I messed up,” and continued crying. Afterward, a man took the phone and asserted, "Listen closely. I have your daughter," and insisted on a fifty-thousand-dollar ransom. According to DeStephano herself, “It was never a question of who is this? It was completely her voice. It was her inflection. It was the way she would have cried… I never doubted for one second it was her. That’s the freaky part that really got me to my core.” (Campbell 1) In reality, DeStefano's daughter was in her room unaware of what was transpiring. AI was used to mimic her voice and present it with distressed emotion to convince Ms. Destefano to send ransom money.

Conclusion

There are no permanent solutions to social engineering as hackers will simply develop a workaround to our current measures. One method being looked into by families is to come up with a safe word to use in emergencies. The philosophy behind this course of action is similar to passwords we use in online accounts. Raising awareness and educating users on the dangers of social engineering may also prove helpful to avoid getting caught by the bait. Lastly, AI

desperately needs a form of regulation and measures to ensure that it is not being misused. As artificial intelligence continues to drive the digital era we are in, we must adapt to it and research implementations that will help us live alongside it.

References

What is Social Engineering: Attack Techniques & Prevention Methods: Imperva. Learning Center. (2023, March 14). https://www.imperva.com/learn/application-security/social-engineering-attack/

Raza, M. (2023, February 14). *Social engineering attacks: The 4 Stage Lifecycle & Common Techniques*. Splunk. https://www.splunk.com/en_us/blog/learn/social-engineering-attacks.html

Laskowski, N., & Tucci, L. (2023, November 13). *What is artificial intelligence and how does ai work?: Definition from TechTarget*. Enterprise AI. https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence

Irwin, P., Jones, D., & Fealy, S. (2023, May 30). *What is chatgpt and what do we do with it? implications of the age of AI for nursing and midwifery practice and education: An Editorial*. Nurse Education Today. https://www.sciencedirect.com/science/article/pii/S0260691723001296

Broadwell, J. (2023, July 10). *Persona 5 voice actor leaves Twitter after harassment over ai*. USA Today. https://ftw.usatoday.com/2023/07/persona-5-voice-actor-erica-lindbeck-ai-harassment

Campbell, S., & Harper, G. (2023, April 10). *"I've got your daughter": Scottsdale mom warns of close call with Ai Voice Cloning Scam*. https://www.azfamily.com.

https://www.azfamily.com/2023/04/10/ive-got-your-daughter-scottsdale-mom-warns-close-encounter-with-ai-voice-cloning-scam/

Woman falls prey to AI voice scam, loses Rs 1.4 lakh by mistaking caller for nephew; The woman transferred the money immediately into the man's account only to realise that she had been scammed using AI voice scam. (2023, November 20). The Financial Express (New Delhi, India).