Social Engineering is a Cyber Warfare Technique

S. Mohan
Assistant Professor of Computer Science and Engineering V.S.B. College of Engineering Technical Campus Kinathukadavu- Coimbatore -Tamil Nadu-India-642 109.

***Abstract*—Social engineering is the manipulation technique that exploit human psychology to gain unauthorize access , sensitive data or perform action that could affect the security of the system . it is a significant threat in the digital age . as it is relies a human vulnerabilities rather than system flaws . the study of social engineering involves understanding the various forms such as phishing, pretext, baiting , and tailgating psychology principles behind it . it is crucial to integrate human factors in the cyber security strategies to enhance security measure and mitigate threats. While social engineering itself is not a technical cyber attack .it is an integral part of cyber warfare because it facilitate unauthorized access , data breaches and operational disruption by exploiting human psychology . in military the nation security context understanding the defending against social engineering is as critical as protecting against malware , networks intrusion or other technical cyber threat effective defense required employee training , verification protocols and layered security measures to mitigate the human factors in cyber operation social engineering is a key components of cyber warfare as it exploit human psychology to gain unauthorized access or dispute system complementing he technical cyber attack .**

***Index Terms*—AI, API, App, digital age, data breaches.**

I. INTRODUCTION

This technique defense often take center stage as fire walls , encryption, intrusion detection system and sophisticated algorithms distributed to detect and prevent digital threats yet despite all these tools the weakest link in any security system is rarely a machine . it is human being who operate it social engineering is act of the exploiting this human vulnerability rather than breaking through fire walls , attack bypass then entirely manipulating people in ti giving up access vulnerability , understanding social engineering means understanding how human psychology can be turned in to the weapon. Social engineering is not merely a form of hacking . it is psychology manipulation techniques designed to influence behavior and decision-making . it takes adequate of trust, fear, curiosity , urgency and even employee – universal human emotion and instructs that can be subtly trained to serve malicious purpose behind every phishing E-Mail ,fraudulent phone calls or deception message like as deep understanding of how people link react and communicate.

Social engineering in the DIGITAL AGE :
As digital communication expands social engineering has adapted to new platforms traditional methods such as e-mail phishing have evolved in to wide range of digital manipulation across social methods messaging App and corporate networks . social networks often riche environments for attack to exploits , fake profile , fraudulent friends request and deceptive job offer are common tactics used might received a communication request from some are [paging a receiver are collagenous only to lather be tricked in to sharing confidential information messaging platforms have become another battle grounds attacker use WhatsApp , telegram or corporate chats tool to send malicious link disjoined as shared documents or update the informed tone of these platforms often discards user making them less cautions. Ever collaborate tool such as slack or mono soft techniques have been targeted , attacker influencer bots to extends sensitives information . the blurring of perform and causal communication in digital environments create-fertile groups of manipulation. Social engineering is built an psychological principles that have been studied and refined for decade , attacker use these principles data breaching , crafting message that tap in to subconscious drives and emotional triggers.

II. EVALUATE OF SOCIAL ENGINEERING TECHNOLOGY

Social engineering has evalued from simple scam in to complex , multi-stage operation easily attack relied or generic message send to large audience today attack and more refined , learning data analysis and automation to customize count of specific targets.

SPEAR phishing :
This is a prime example of this evaluation, instead of sending bulk message attacker outfit industrial e-mail that references real events project or collagenous this level of petrological dramatically increase success rate.

PRE TEXTING :
It is varying the fabrication scenario to satisfied information request an attacker might pose an it technician having login details for maintenance or on a bank employee verify account activation these scenario provide a logical frame work that makes the request approach legitimate .

BAITING :
This is another form of social engineering rates an curiosity or greed attacks may leave infected USB drives labelled " confidentially " in public across knowing that some one will eventually play one I similarly tactics across online where user are entirely with free download an exciters contend that hidden malwares.
The rise of AI ad automation has amplified these technique attackers how use machine learning model to generate related message , replicate writing stage and even engage in real-time converter . this function of philosophy and artificial intelligence repeat the next fraction of social engineering.

II. INTER PLAY BETWEEN SOCIAL ENGINEERING AND TECHNIQUES

Where social engineering faces an how manipulation it after interest with technique exploit many attack common psychology deception with malware or creative theft for interaction , a phishing E-mail, may contain a malicious attachments that install spyware , which a fake login page caption password for later use, Attacker use technology to enhance credibility-mail sportifies enables voice and video impressments auto method script send thousands of personalized message simultaneously increasing reactant without sacrifices believability .
Technology also facilitates persistent once an attacker gain accesses through social engineering they any install back door create hidden accounts or plants ransomware . this is the human compromise often serves as the first step in a broader technical breaches .this synergy between psychologic and technology make social engineering particularly dangerous it blur the boundaries between human and digital vulnerability ,creating multifaceted tracks that area difficulty to detect or prevents through technical means alone.

III. IN FUTIRE OF SOCIAL ENGINEERING

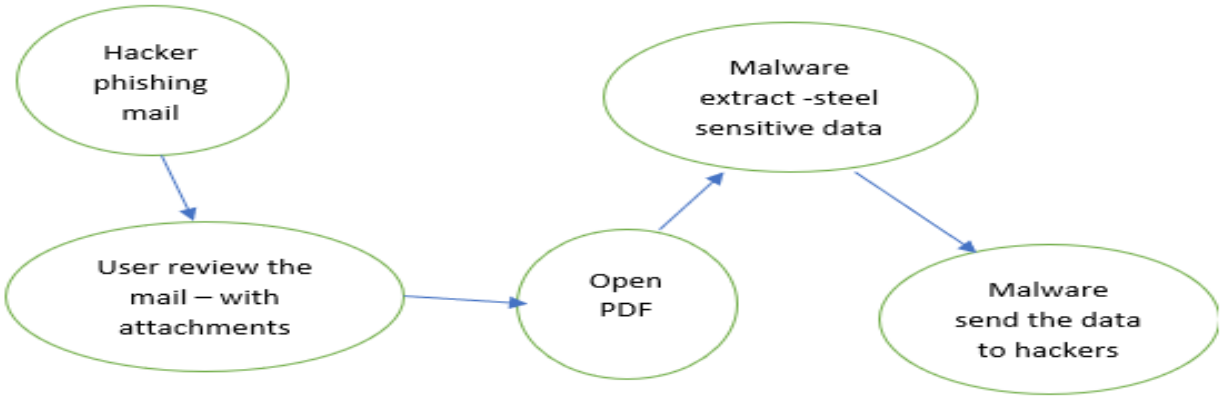
As technology events social engineering will continue to adapt , the riser of artificial intelligence , deepfakes and real-time language model will make deception unnecessary difficulties to detect , attacker may conduct live conversion using AI persons intelligence from real pagers, in the coming years augmented and virtual reality event may become new fortifier for social engineering digital avatars could impersonate collogues or headers creative immersive deception that challenges even trained professional.defesive strategies write there fore evidence and cull future secularly will depends and coquetries resins the ability to recuses manipulation at the psychology level , enhanced system workplace timing and public convenance campaign multi technologies not only technical literature bur also emotion intelligence and critical thrillings.ethical considering will also play a roll as AI become more capable if generate realisms human behavior social must comport the questions of authorized in communication lives regulation and digital verification system will need to ensure that InSite remain trustworthy in a world of synthetic interaction.

IV. REAL-LIFE

Social engineering is the indeed a form cyber warfare ,as it exploit human behavior to gain unauthorized access to system ,data, or physical location it is a manipulation technic that target the human elements

often consist the weakest link in cyber security attacker use deception percussion and psychology tactics to trick individual in to revealing sensitive information , such as password , firewall details or proprietary data with the rise of digital transformation Social engineering attack life-cycle

, social engineering attacker have become more sophisticated , leveraging technology and social media together information about targets understanding this attacker is critical for organization and individual to protect against evolving cyber threats.



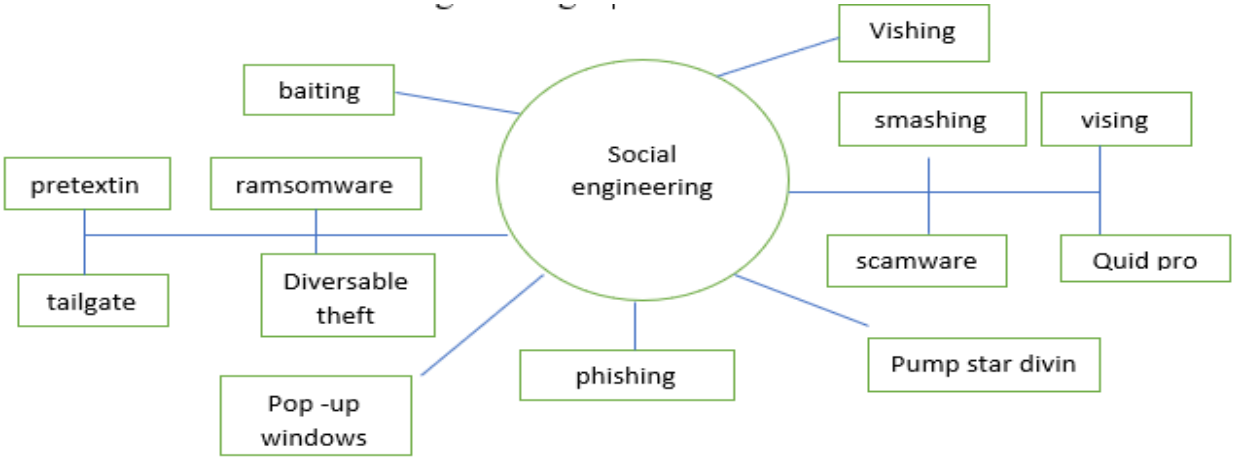
V. SOCIAL ENGINEERING RELATED TO DATA BREACHES

In the ensure-holing used of cyber security data breaches have become one of the most significant threats to organization and individual alike . these breaches which involves the unauthorized access , retrieve or expose of sensitive data can have server un sequence from fractional loss do representation damage , which most people associated data breaches with sophisticated hacking technique or technical vulnerability social engineering plays an equally vital role in enabling such individuals.

Social engineering the art of multiplication individuals in to revealing confidents information bypassing security measuring or taking action that compromise security is often the key enable in many data breaches return then exploiting software vulnerability or technical flaws social engineering targets. The human elements of an organization security which remains its most vulnerability aspects.

The several common social engineering technic an often used by attacks to facilitates the data breaches these natural typically involves giving trust , creating wagons or mimicking authority to multiple individual in to compromising security.

VI. IMPORTANT OF SOCIAL ENGINEERING ATTACK



Social engineering attack have only an important part pf the play society creation of the sense of security through threats and irrespective of the type of social engineering attacks panel provider under it act sequencing core all these become of the inclusive nature of provision . but most of the panel provide of It acts corelated with provision of IPC in these own area operation although all these provision under IT act and IPC can not be said to be pivoting nature as they only operate after attempt are commission then the government had taken various step and institution to mitigate the threats to cyber security one thing is clear from of the perusal of cyber law and institution taken by the governments toward cyber security is that all effort of the governments are directed to mitigate the threat and not to eliminate then becomes they understand the dynamic nature of the world of cyber space and new threats may arise and moments.

VII. IMPORTANTS : TYPE OF SOCIAL ENGINEERING

the both terminology “doctrine of social engineering” and “social engineering in cyber world “means poles operate and field of operation these have no common ground once can be used to create become in the society with specific means and others is create ruckus by creating . the only thing which could be cover under doctrine of social engineering is that under the head of social interest the modern technology of social engineering needs to be balanced for safe and secure transaction in the society as use of these technic shall in various laws – and order situation which will have economic often at the center and also affects other needs under the doctrine as well .

Before understanding the type of social engineering attacks and these manor of operation these are stage which follow by every one attack important of types that must be dangerous techniques of social engineering basically exploits how error by installing software in the computer which gives the access to other personal data and data such this techniques manipulate is based an the verses behaviors the instant to the device this technique required from stages .as the stage prepared the attackers gathers all the information of his targets then the work or create of trust with the targets through interaction and other means with means interact to infiltrate his personal area after creating trust and discussing the weakness attacker start to exploit the victim to progress in his contacts . once the targets does act intended by the attack the attacker disengages himself from the which transaction.

These are various type of social engineering attack but these type are not limited to phishing , baiting , diversion theft , pretexting quid pro quo seaware tailgating water holing and seams.

VIII. CONCLUSION

social engineering is the indeed a form of cyber warfare as it exploit human psychology to template individual in to revealing confidential information or performing action that covering security . it is a non-technical strategies used by cyber criminals to exploits peoples and provide unauthorized access , sensitive data or perform action that could affect the security of the system , despite advance in technical defenses , human remain the weakest link , as attacker manipulate trust urgency and authority to bypass security by tracking employees in to sharing sensitive information or granting access .

REFERENCES

[1] Dimensional Research, “The risk of social engineering on information security: A survey of IT professionals,” Dimensional Res., Tech. Rep., Sep. 2011. [Online].

[2] Ponemon Institute LLC and Accenture. (Mar. 2019). *Ninth Annual Cost of Cybercrime Study*. [Online].
Available: https://www.accenture.com/t20190305T185301Z_w_/us-en/_acnmedia/PDF-

96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf Show in ContextGoogle Scholar

[3] M. Nohlberg, "Social engineering audits using anonymous surveys: Conning the users in order to know if they can be conned," in *Proc. 4th Secur. Conf.*, Las Vegas, NV, USA, Mar. 2005. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-1714 Show in ContextGoogle Scholar

[4] Harl. (1997). *People Hacking: The Psychology of Social Engineering*. [Online]. Available: http://www.textfiles.com/russian/cyberlib.narod.ru/lib/cin/se10.html Show in ContextGoogle Scholar

[5] K. Mitnick. *My first RSA Conference*. SecurityFocus. Apr. 2001. [Online]. Available: http://www.securityfocus.com/news/199 Show in ContextGoogle Scholar

[6] T. Thornburgh, "Social engineering: The 'dark art,"' in *Proc. 1st Annu. Conf. Inf. Secur. Curriculum Develop. (InfoSecCD)*, New York, NY, USA, 2004, pp. 133–135, doi: 10.1145/1059524.1059554. Show in ContextCrossRef Google Scholar

[7] T. L. Thomas, "Cyberskepticism: The mind's Firewall," in *Spring*. IOSphere, 2008, pp. 4–8. Show in ContextGoogle Scholar

[8] I. Ghafir, V. Prenosil, A. Alhejailan, and M. Hammoudeh, "Social engineering attack strategies and defence approaches," in *Proc. IEEE 4th Int. Conf. Future Internet Things Cloud (FiCloud)*, Aug. 2016, pp. 145–149. Show in ContextView Article Google Scholar

[9] D.-J. van Mourik, "Targeted attacks and the human vulnerability," M.S. thesis, Cyber Secur. Academy, The Hague, The Netherlands, 2017. [Online]. Available: https://www.csacademy.nl/images/scripties/2017/Thesis-Van-Mourik.pdf Show in ContextGoogle Scholar

[10] R. Heartfield and G. Loukas, "A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks," *ACM Comput. Surveys*, vol. 48, no., pp. 37:1–37:39, Feb. 2016, doi: 10.1145/2835375. Show in ContextCrossRef Google Scholar

[11] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, "Social engineering attacks on the knowledge worker," in *Proc. 6th Int. Conf. Secur. Inf. Netw. (SIN)*, New York, NY, USA, 2013, pp. 28–35, doi: 10.1145/2523514.2523596. Show in ContextCrossRef Google Scholar

[12] K. Ivaturi and L. Janczewski, "A taxonomy for social engineering attacks," in *Proc. Int. Conf. Inf. Resour. Manage.*, 2011, pp. 1–12. [Online]. Available: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1015=confirm2011 Show in ContextGoogle Scholar

[13] Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York, NY, USA: Bantam, 1993. Show in ContextGoogle Scholar

[14] J. M. Hatfield, "Social engineering in cybersecurity: The evolution of a concept," *Comput. Secur.*, vol. 73, pp. 102–113, Mar. 2018. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S016740481730229 Show in ContextCrossRef Google Scholar