A Comprehensive Analysis on Social Engineering based Attacks

J.K.S.Roledene
Department of Research and Postgraduate
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka.
sroledenez@gmail.com

D.S.A.Kandawala
Department of Research and Postgraduate
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka.
sachini.k@sliit.lk

Anuradha Jayakody
Department of Information Systems Engineering
Sri Lanka Institute of Information Technology
Malabe, Sri Lanka.
anuradha.i@sliit.lk

***Abstract*- This research presents a comprehensive study on social engineering attacks. An introduction of social engineering attack is given, with context to the current trends and related vulnerabilities which comprises of all aspects related to Social Engineering, thus giving a defined overview of what social engineering is and how it is affecting us all. The main reasons for the spread of social engineering attacks in the current context are discussed with the aid of an attack framework and a proposed defense in depth approaches for social engineering threats. Further, this paper presents concludes the remedies which can be taken as a safety precaution for attacks and social engineering.**

***Keywords*— attack framework model, defense approaches, social engineering.**

I. INTRODUCTION

Being human has its many strengths and flaws. And human emotion can play both strength and flaw. But when it comes to the world booming with technology human emotion which is totally unrelated to the matter is made to relate, through Social Engineering.

This relativity is not based on good intentions. But is merely a trap to play on human emotion and its vulnerability, taking advantage of the flaw. Social interaction concepts which were means of friendly gestures are used as setups to extract vital and sensitive information from a tricked victim. The technique of using people to get ones hands on their private and confidential information claiming to be trusted sources is what Social Engineering is all about [1].Many have and still are under the attack of social engineering. The victim; an individual or an organization, is made to confide personal details by means of persuasion, social interaction or requests involving a computer related body. The main reason that underlies the never ending attacks is unawareness. People make them self-prone to these attacks by not taking the subject as serious as it is. Hence many who never expected to be a victim of such a situation ends up being one and remains unaware of it. As a result, the majority of the public has had and is still facing personal, economic and social consequences and deprivation as an individual or organization [3]. The victim may always be under the impression of passing off information that is of no value to another person, nor could it be used for any improper illegal activities, and will thus be more willing to unfold them freely. But, the attacker is dedicated in exploring various techniques' and gathers information up from many sources and combines them together leading to much catastrophic consequences which the human is not aware of [3]. If only had the individual sensed the malicious activity by not living under the pretense of zero possibilities of such events, sensing one instantaneously would have been possible [3].

However, the social engineer; the attacker is a skilled human manipulator, feeding on human vulnerabilities using many psychological sparks to blind correct human judgment [3]. Many researches have proved that aspects such as personality traits, demographics and online habits of each and every individual or organization are monitored in targeting successful attacks [7].

One other main problem other than unawareness is relying on the companies running the networking sites to handle such situations and trusting them to protect their privacy from criminals and network abusers. And how famous companies like Facebook, Instagram will hold guarantee to their personal information, which is not true. Detecting an attack gets trickier while working in a stressful environment, where decisions must be made immediately [10]. As a result it is very important that the two perspectives of social engineering- the psychological perspective [3] and the computer science perspective be handled smartly and technically, as it has

become very vital to protect secured information related to any community; individual, organizations or government bodies.

Hence, avoiding the infiltration of security systems, thereby reducing many illegal activities happening online and making it a safer platform to every one being a part of it, which is almost the entire social population given the present rising fame in social networks and technology. This paper comprises of all aspects related to Social Engineering, thus giving a defined overview of what social engineering is and how it is affecting us all.

This paper is organized as follows: Section I discuss about the introduction to the area of research. Section II illustrates work related to this research area. Methodology is comprehensively elaborate in section III. Finally, the conclusion and the recommendations are stated in the final part stated as section IV.

II. LITERATURE SURVEY

A. Defense Approaches against Social Engineering Attacks

What differs social engineering attacks from other information attacks is [6] that it may target any personnel in an organization regardless of their technical knowledge, rank any other trait for that matter. This aspect of social engineering becomes very challenging to avoid as no matter how much expertise and money an organization put into its network security to prevent data theft such as firewalls, security appliances, encryption, etc [5]. The human element remains vulnerable to hackers who apply social engineering techniques [9].

Social engineers may trick any person in an organization depending on the information they are after. Hence it is critical that a multilayered defense mechanism is followed. Even if an attacker manages to defeat all these defenses and get in to the fundamental layer in the system, the system should be secure enough to contain the attack at the fundamental level or eliminate it completely [2]. Information security can be divided in levels such as foundation, fortress, persistence offensive and gotcha levels.

- *Physical security*: Data can be primarily protected by ensuring confidential information stays within the organization. This ensures that outside attackers are unable to retrieve such data.

- *Foundation level:* Foundation level involves developing a security policy around social engineering [6]. These policies include password changes, accesses approval, information release, employee id, shredding confidential documents. Such policies must also be changed from time to time to ensure maximum reliability of them. It is very important that sensitive information is not released to personnel without proper authentication by the information handling party. Also keeping records on personnel who handled the information is also an effective method of providing security as it motivates people to be careful about the information that they handle. It is also important that once the usefulness of the information is expired they are properly destroyed. For hard document this can be achieved by shredding. For computer hardware, specifically designed software to corrupt data or implicating physical damage on the information storage device can be practiced. This can be useful in avoiding other information attacks such as dumpster diving.

- *Persistence and Fortress Level:* This level consists of resistance-training techniques for key personnel, Carrying out ongoing reminders and punishing staff that continuously break policy controls [6]. The aim of resistance training techniques [6] is to prepare employees to take countermeasure actions when a social engineer employs. This includes giving an awareness program often to who are specially identified as primary targets of a social engineering scheme. How they are really vulnerable to social engineering attack is demonstrated within these programs. It is necessary to inform their access level with the risk that they are exposed to the company. Give forewarning about upcoming attacks/ methods that employees may expose in near future. Inform employees not to use any unauthenticated flash drives or third party software within company network and explain how it is going to affect the entire system. Train employees to recognize psychological methods that social engineers may use. Carrying out ongoing reminders is a mandatory practice within an organization. Regular reminders should implement not to open any untrusted email/instant messages / social media sources and not to respond or not even to forward. Demonstrate the damage caused by opening suspicious of unsolicited emails, messages, etc... Conduct a recurring, unauthorized penetration test to assess the organization's vulnerabilities. Every employee has duty towards the organization. Therefore is it necessary to monitor the staff's social media outlets that have access to the most sensitive information about the organization and to prevent posting any unauthorized materials online [5].

- *Offensive level and Gotcha level:* When it comes to social engineering defense techniques, it is important to have knowledge on what actions need to be taken in the course of an attack [6]. Offensive level and gotcha level mainly describe social engineering land

mines (SELMs) and incidence response methods [6]. SELMs techniques are used to explode by surprise of an attacker's identity or to stop the attack. It is recommended to train a social security expert who can easily spot and identify an intruder within the organization and prepare emergency security mechanism plan to execute when an attack occurs. Implement a policy regarding disposal of physical documents. They should always be shredded or destroyed prior to disposal. When a party is requesting sensitive information or requesting to change passwords, use call back policy to ensure that the party is genuine. If anyone is unable to provide basic information or try to avoid the call back policy, use hold policy to stop the suspicious request and investigate further. Furthermore, incident response method can be used to implement internal awareness program with employees on regular basis to report and track incidents and implement incident-response strategy.

B. Attacking the vulnerabilities of Social Engineering

With the development of Internet of Things, social engineering attacks have been a crucial menace to the society. The main intention of social engineering is not purely based on financial benefits; it can also be to gather personal details. Basically from mind games, illusions and deception social engineering attacks are done. According to the medium and the techniques enforced to lure people and obtain valuable and confidential information, social engineering attacks can be categorized as Phishing, Tailgating, Pretexting, Quid pro quo, Baiting.

Within the above mentioned categories, two main essence of vulnerabilities are present which the attackers exploit using the tools of social engineering. These two essences can be broken down to, physical locations and psychological methods. Potential social engineering attack will be following a specific process; firstly what the attacker does is in order to build up a bond with the victim the ground information about the particular person will be gathered. This personal information is gained through following victim's social media profiles, day to day routine, friends and family members. Then on the attacker builds up a relationship with the victim using the gathered information to win over the trust. The psychological aspects of human emotions and habits will be studied by the attacker in order to gain the advantage and to present himself as a trustworthy character. After successfully completion the above step the attacker will use the relationship to his advantage to obtain confidential information of the victim such as, bank details, passwords, credit card details etc. Then the attacker will move on to the purpose of the attack which is to execute his objectives by using the gathered confidential information. The attacking process used in social engineering has a recurring manner.

As mentioned before the main two essence of a social engineering attack is physical locations and psychological methods. Physical location denotes where or the medium which the attacker executes his procedure. Few examples can be servers, working place, personal area networks and telephone. By tapping into servers which has restricted access authorization through deception, malevolent programs can be injected into the network and create carnage that can harm the whole performance of the system. Work place critical data acquisition can be done through impersonation of a third party such as maintenance staff, security and drivers. After accessing the desired location, through shoulder surfing and eavesdropping required information is gathered. Depending upon the attacker's convenience the process can be continued remotely as well.

Psychological methods mostly exploit the human tendencies using the weakness of the human emotions and trust. For psychological methods potential examples can be, deception which the attackers used to gain trust in a person and create an illusion of closeness and compassion towards the victim which will emotionally make him feel comfortable. By manipulating new recruitments can get the access to the inside information which the new recruits are not aware of the value which the information possess. And also capitalizing on emotionally disturbed situations of individuals to use their vulnerability in order to get benefit out of the situation and them, here the psychological state of the individual is capitalized with respect to the time. Humans exchange thoughts with people who have similar concepts, so by knowing his likes and dislikes the attacker can make casual conversation and drive the conversation towards his target topics at which point the victim will share the information without any hesitance. These opportunities will be taken to grant by the attacker depending upon the situation, the type of the person and the necessity of the information needed.

III. RESEARCH METHODOLOGY

The technique of influencing people to disclose sensitive information is called social engineering and the process of doing so is known as a social engineering attack [5]. When a user appears to trust a hacker or the intruder, the attacker tends to exploits the trust to miss use and draw out information from the target. There are various definitions of social engineering attacks and a number of different models [8] which are explored and analyzed. The attack cycle proposed by Kevin Mitnick in 2002 is frequently used framework by security professionals and academics when explaining social engineering attacks.

In this model first stage information gathering is done by the attacker extensively on the target before the attack

initiation. Second stage is the development of trustworthy relationship with the target. User is more likely to disclose requested information to an attacker if he trusts him too much [8]. According to Mitnick when a target appears to trust an attacker, the attacker tends to abuse the trust to elicit information from the user as pre planned. Final stage deals with the outcome of the previous stage to reach the ultimate goal of the attack [4].

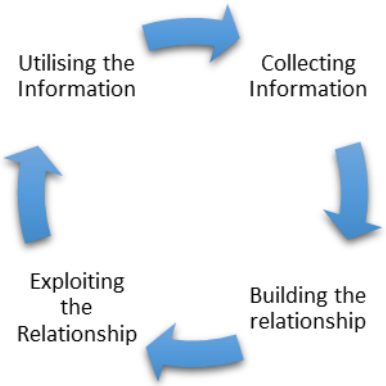

Fig 1: Main Steps of Attack Cycle

Studying users' behavior and perception on social engineering attacks is vital to understand the weak points in users' ability to detect and defeat social engineering attacks [7]. This section proposes a user-centric framework to realize and build a coherent understanding of user vulnerability to social engineering attacks in the network security context. Following framework has been developed to give a full overview on user centric characteristics that may affect the user's threat detection capability factors that may influence the user's judgment on social engineering attacks [7].

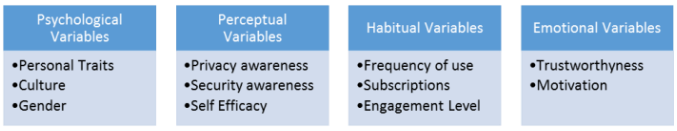

Fig 2: User Centric Framework

Designing a strong defense against social engineering is a must. Defense approach must start with determining what the vulnerabilities and threats are and then to defend against those risks. The defense cycle describes the general options available to the defender.

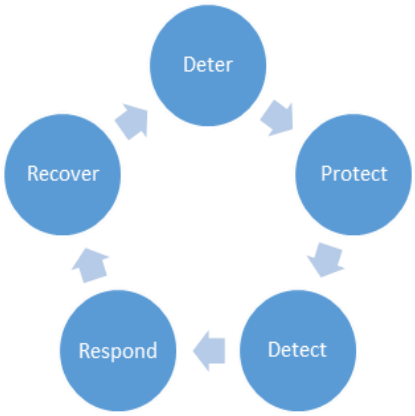

Fig 3: Main Steps of Defense Cycle

The defender might in some cases be the victim or it might be security professionals in an organization. Above mentioned defense cycle (Fig.3) is based on the description of defenses given by Kowalski in 2002. According to his model knowing the value of our data, having attacks reported with a well-designed security policy these attacks can be avoided.

IV. CONCLUSION & RECOMMENDATIONS FOR SOCIAL ENGINEERING ATTACKS

Basically social engineering principle is not about using complex technology to breach security, it's totally about manipulating people through their emotions and taking advantage from critical situations which they face. So generally it is advisable to be aware of what social engineering is and the effects and impacts on the social life of people due to it. By following few techniques can secure yourself or your company against social engineering attackers, such as:

- Knowledge is a precious component in life to move forward and face the challenges in life. Educating yourself is not just about following a curriculum but rather gaining and observing the social conundrums and being vigilant about the surroundings and life style. By educating yourself, can mitigate social engineering attacks by a vast range. Mostly social engineering attacks occur due to the uneducated or lack of knowledge regarding such matters. Therefore it's better to gain some basic knowledge so that such attacks can be avoided in the future [5].

- People go to great heights to protect their information, spending huge amounts of money, resources and also man power. This show the importance which information possess. Therefore when sharing the information which an individual possess, he or she should take precautionary measures to protect their valuables. Many algorithms have been developed to provide security for data during transmission so that attackers can't gain the information through tapping into transmission channels. With the development of the smart phone even with the touch of your

finger a person can gain such algorithms which encrypts messages and information which is transferred through internet and radio or mobile transmission. Therefore securing your information is not such a difficult matter with the development of technology. It is just a matter of effort that should be put in to protect your information.

- Attackers of social engineering come up with malicious programs which can impact protective software used to safeguard their information. Therefore software manufacturers who produce such programs monitor these activities and counter attack these threats by upgrading their software and by introducing new algorithms to the market. So as users it is the responsible of them to update their software to the latest versions so that compromised versions will not be in use which will reduce the integrity of information

The securing of information from the continuous onslaughts of cyber-attacks proved to be critically important after the realization of this advanced technique opted by the attackers; of manipulating human. No matter how strongly the security systems have been designed to overcome the malicious events; using up to date techniques and technology, human will always be the weakest connection to collapse the entire security system. The paper has provided a complete research analysis of social engineering, starting from pointing out the factors leading to this social engineering crisis and how human vulnerability of emotions and other psychological aspects play an important role in the process. And how the situation is been handled with the various outcomes of many experiments in regard to the situation.

ACKNOWLEDGMENT

This work has been supported by the Sri Lanka Institute of Information Technology, Malabe, Sri Lanka.

REFERENCES

[1] M. I. Mann, Hacking the human: social engineering techniques and security countermeasures. Gower Publishing, Ltd., 2012.

[2] CPNI, “Social engineering: Understanding the threat, "Available [Online]:http://www.cpni.gov.uk/documents/publications/2013/201306 5-social-engineering.pdf?epslanguage=en-gb, accessed: 25-32016.

[3] M. Bezuidenhout, et-al, “Social engineering attack detection model: Seadm,” in Information Security for South Africa (ISSA), 2010. IEEE, 2010, pp. 1–8.

[4] A. Algarni, et-al, “Social engineering in social networking sites: Affect-based model,” in Internet Technology & Secured Transactions, 2013 8th International Conference for. IEEE, 2013, pp. 508–515.

[5] F. Mouton, L. Leenen, and H. Venter, “Social engineering attack examples, templates and scenarios,” Computers & Security, 2016.

[6] G. Ibrahim, et-al"Social Engineering Attack Strategies and Defence Approaches" , 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016

[7] S. Albladi, G. Weir. "Vulnerability to social engineering in social networks: a proposed user-centric framework" , 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF), 2016

[8] Mouton, Francois, M. Malan, L. Leenen, and H.S. Venter. "Social engineering 5 1% 6 1% 7 1% 8

[9] The Investigators, “Government Licensed Private & Fraud Investigators,” Available [Online]: https://www.theinvestigators.co.nz/

[10] F.Mouton, L. Leenen, H.S. Venter. "Social Engineering Attack Detection Model: SEADMv2" , 2015 International Conference on Cyberworlds (CW), 2015