Literature Review of Examples of Social Engineering Techniques and Attacks

Saleem Manjoo
Department of Computer Science
University of Cape Town
Rondebosch, 7701, South Africa
+27843314861
MNJSAL001@myuct.ac.za

ABSTRACT

Information security is a fast growing discipline with the protection of personal information being of vital importance. Due to psychological vulnerabilities that humans possess, the "human element" is considered the weak element in security systems and thus are the target for attacks. These vulnerabilities give rise to various techniques that social engineers employ in their attacks. Examples of full scale social engineering attacks in literature usually lack key details of the attack which makes analysis of the attack more difficult. Through the use of the social engineering ontological model as well as the social engineering attack framework, social engineering attack templates were created in order to resolve this problem.

CCS Concepts

Social Engineering

Keywords

Social Engineering; Attack, Framework

1. INTRODUCTION

Information security is a fast growing discipline with the protection of personal information being of vital importance to governments and organizations who have a vested interest in securing such information [1]. As the technological element to security systems improve and become more difficult to exploit, the target has shifted onto the human element which can be considered the vulnerable element in the system [3].

While there are various definitions of social engineering [2], in this context, it will refer to the various techniques that are utilized to obtain information in order to bypass security systems, through the exploitation of human vulnerability [4]. It can be seen as the art of influencing people to divulge sensitive information.

This literature review will first focus on the psychological aspect of social engineering and examples of techniques used by social engineers. It will then briefly outline the social engineering ontological model and the social engineering attack framework to later demonstrate how they can be used to map out social engineering attacks for the purposes of analysis or recreation. Lastly, examples of social engineering attacks utilizing different types of communication will be presented.

The next section focuses on the psychological aspect of social engineering and demonstrates how social engineering techniques can be derived from psychological vulnerabilities that humans possess.

2. SOCIAL ENGINEERING TECHNIQUES

The definition of social engineering which states that it is the techniques used to exploit human vulnerability to bypass security systems to gather information implies that social engineering attacks involve interactions with other individuals [4]. This indicates a strong psychological aspect of social engineering [3].

There are various psychological vulnerabilities that are used by social engineers with the aim to influence an individual's emotional state and cognitive abilities in order to obtain information from them [3]. These psychological vulnerabilities can be seen as the factors which make the human element the vulnerable element in security systems, and thus the target with regards to attacks on the system. This section of the literature review will look at the seven psychological vulnerabilities that have been defined by David Gragg [5], and the ways in which social engineers can exploit these vulnerabilities in their techniques to gather information.

Strong Affect: The Strong affect is a trigger that uses a heightened emotional state to enable a social engineer to get away with more than what would be reasonable. The surge of strong emotions can work as a powerful distraction that interferes with the victim's ability to evaluate, or think logically. For example, if the victim is feeling a strong sense of surprise or anger, the victim will be less likely to think through the arguments presented by a social engineer [5]. In this state, the victim will also be less likely to verify the legitimacy of a request for information [6], thus making them more prone to divulge private information [5].

Overloading: This occurs when an individual becomes cognitively pacified or compliant through the bombardment of a series of hurried persuasive axioms [7]. This is due to that when having to deal with a lot of information quickly, a person's logical functioning can be affected and "sensory overload" can occur [5]. An example within the context of a social engineering attack would be the attacker overloading the target with too much of information that the target does not have sufficient time to scrutinize the attacker's request and properly validate it.

Reciprocation: This vulnerability plays on the notion that "One good deed deserves another". Social exchange theory states that individuals who receive a kind gesture from another feel obligated to return the favor. In the case of a social engineering attack, an attacker can create a problem for the target only to fix it again, thus making the target feel obligated to disclose information in return [7].

Deceptive Relationship: A social engineer will identify and purposefully establish a relationship with an individual with the intent of extracting information from them. This is effective as individuals tend to share information more freely within established relationships [7].

Diffusion of responsibility and moral duty: This occurs when an individual is made to believe that their actions, such as disclosing information, will have greater benefits and important beneficial consequences and that they will not be held solely responsible for their actions [7]. A social engineer could make a target feel that he or she is making decisions that will be the difference between the success or failure of the company in order to make the target feel more compliant to divulge information [5].

Authority: The likelihood of an individual to comply with the request to disclose information is greater if the request is from an authority figure as they almost implicitly elicit a conditioned response to adhere to their wishes. This combined with a fear of punishment for the individual makes it less likely for the verification of the authority figure [7]. By taking this into account, a social engineer could portray an authority figure to obtain information from an employee.

The literature regarding the psychological vulnerabilities of humans shows how social engineering techniques can be derived from the psychological vulnerabilities that humans possess. Social engineers may try to exploit one or more of these vulnerabilities during their attacks in order to achieve their goal. Some the of vulnerabilities listed here are also present in the compliance principles found in the ontological model for social engineering in the next section.

3. Social Engineering Attacks

This section briefly outlines the social engineering ontological model as well as the social engineering attack framework to demonstrate how through the use of these tools, every aspect of a full scale social engineering attack can effectively be mapped out.

3.1 Ontological Model

There are various models and taxonomies for social engineering attacks. According to the ontological model described in [2], a social engineering attack consists of a social engineer, a target, a goal, a medium, one or more compliance principles and one or more techniques. An attack can be split into one or more attack phases with each of the phases being considered a new attack according to the model [2]. Figure 1 depicts this model.

With regards to communication in this model, there are two main types.

Direct communication: where two or more people are communicating directly with each other. This category can further be divided up into bidirectional communication, where the attacker and the target are in conversation with each other, and unidirectional communication where the conversation is only one way: from the attacker to the target [1].

Indirect Communication: Indirect communication occurs when there is no actual interaction between the target and the attacker and communication occurs through some third party medium. For example, an infected flash drive that is found by some random target who then inserts it into their computer and thus compromises it [2].

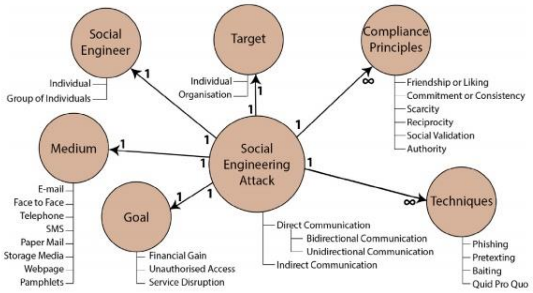

Figure 1. Social Engineering Ontological Model [2]

3.2 Social Engineering Attack Framework

The social engineering attack framework depicted in figure 2 shows the planning and flow of a full scale social engineering attack. It can be seen as the method in which social engineering attacks are carried out. There are 6 core phases in this attack framework [1].

1. Attack Formulation: The goal and the target of the specific attack is identified.
2. Information Gathering: All sources of information on both the goal and the target are identified.
3. Preparation: All information gathered is combined and an attack vector is developed. All elements of the ontological model above can be identified in this phase.
4. Develop Relationship: The attacker establishes communication with the target and a trust relationship is built.
5. Exploit Relationship: The relationship between the target and the social engineer is exploited and the target is elicited to perform the request or action that the social engineer desires.
6. Debrief: This phase tests whether the goal has been satisfied. If it is, the attack is a success. If not, the attack can return to the preparation phase where a new attack vector can be developed for another attempt.

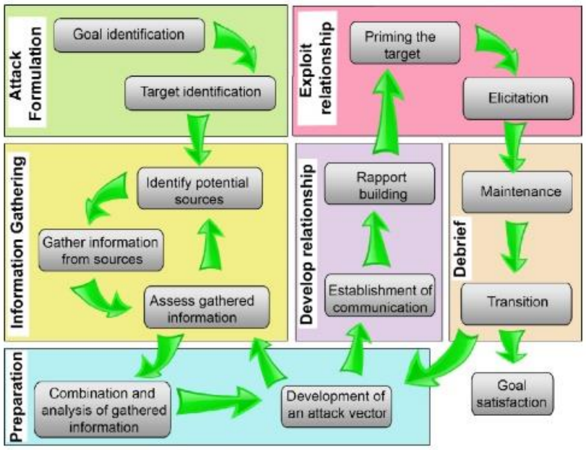

Figure 2. Social Engineer Attack Framework

Thus, by identifying the elements of the ontological model, shown in figure 1, as well as following the attack framework in figure 2, a social engineering attack can be generated. The use of these two tools aids in the creating and the analysis of social engineering attack scenarios.

4. ATTACK EXAMPLES

There are many examples of well-known social engineering attacks in literature and examples that have been documented in news articles. However, a common issue with the examples found in these is that not all pieces of information about the attacks are included. The “goal identification” and “target identification” steps are usually not included. Little information about the “information gathering phase is given. Also usually not detailed in literature are the “exploit relationship” and “debrief” phases. This “preparation phase” and the “develop relationship phase” are usually included, but the lack of detail in or the exclusion of the other phases means that information on real world attacks typically only focuses on how the attack affected the specific target [1].

The authors of [1] have proposed social engineering attack templates to address the above issue by detailing every phase of an attack by using the social engineering attack framework and the ontological model. The templates were created using elements of real world examples of social engineering attacks, but due to the issue of missing details mentioned above, some of the details of some of the missing phases had to be inferred.

The social engineering attack examples in this literature review will be presented in the format of a brief description of the attack, followed by the outlining each element of the ontological model shown in figure 1. The following attack examples are outlined in greater detail in [1], where each step of the social engineering framework is also provided for each example. The attack examples were derived from real world examples and found in the following literature: [10], [11], [12], [13], [14], [15].

For the purpose of this literature review only 3 of the examples will be presented: One example using direct bidirectional communication, another using direct unidirectional communication, and lastly one using indirect communication. This is to illustrate that through the use of the ontological model, a social engineering attack can easily be generated, analyzed, or recreated regardless of the type of communication.

Example 1: Bidirectional communication

An attacker attempts to gain physical access to a computerized terminal at the premises of an organization. Once the attacker has gained access to the computerized terminal, he/she is deemed to be successful and installs a backdoor onto the terminal for future further access from the outside.

Communication – The SEA is using bidirectional communication.

Social Engineer – The Social Engineer (SE) is an individual.

Target – The target is an organization.

Medium – The communication medium is face-to-face.

Goal – The goal of the attack is to gain unauthorized access to a computerized terminal within the organization.

Compliance Principles – The compliance principles that are used are authority, commitment and consistency.

Techniques – The technique that is used is pretexting.

Example 2: Unidirectional communication

An attacker attempts to obtain financial gain by sending out emails that request a group of individuals to make a small deposit into a bank account owned by the attacker. Once the deposit has been received the attack is deemed successful.

Communication – The SEA is using unidirectional communication.

Social Engineer – The SE is an individual.

Target – The target is a group of individuals.

Medium – The communication medium is e-mail.

Goal – The goal of the attack is financial gain, as the targets are requested to make a deposit into a bank account owned by the attacker.

Compliance Principles – The compliance principle that is used is scarcity.

Techniques – The technique that is used is phishing.

Example 3: Indirect communication

An attacker attempts to gain unauthorized access to a workstation by using an infected storage device. The storage device is planted so that a target picks it up. Once the target has plugged the storage device into the workstation the attack is deemed successful as the attacker is now able to install a backdoor onto the workstation. The workstation can then be used as a pivot point for any further attacks on the organization.

Communication – The SEA is using indirect communication.

Social Engineer – The SE is an individual.

Target – The target is an organisation.

Medium – The communication medium is a storage device. In this case, the storage device to be used is a USB flash drive.

Goal – The goal of the attack is to gain unauthorised access to a workstation within the organisation.

Compliance Principles – The compliance principle that is used is social validation.

Techniques – The technique that is used is baiting.

With the three above examples, it can be seen that through the use of the social engineering ontological model, as well as taking into account the full attack templates presented in [1], social engineering attacks, irrespective of the type communication, can easily be mapped out for analysis as well as for the purposes of recreation.

5. CONCLUSIONS

With regards to social engineering techniques, it can be seen that due to the strong psychological aspect of social engineering, social engineering techniques can be created out of documented psychological vulnerabilities that humans possess. The literature indicates that due to the many vulnerabilities humans possess and the social compliances that humans often adhere to, the “human element” of a security system is often the weakest element and therefore the target for attackers [3].

The social engineering ontological model as well as the social engineering attack framework can be used as tools to effectively map out social engineering attacks for the purposes of analysis or recreation. They are particularly useful as they detail each aspect of an attack from the conception of the attack as well detailing all the steps taken by the social engineer to carry out the attack. They can be used to map an attacks irrespective of its details such as the type of communication [1].

Although there are many examples of social engineering attacks provided in literature as well as in news articles, a common issue with the examples is the lack of detailing of particular phases of the attacks [1]. This creates a gap of information in the literature as the lack of details of these phases makes analysis of the attacks more difficult. To address this, social engineering attack templates were created using real world examples and detailing every element of the ontological model as well each step of the social engineering attack framework [1].

6. REFERENCES

[1] Mouton, F., Leenen, L. & Venter, H. 2016. Social engineering attack examples, templates and scenarios. *Computers & Security.* 59:186-209.

[2] Mouton, F., Leenen, L., Malan, M.M. & Venter, H. 2014. Towards an ontological model defining the social engineering domain. In *ICT and Society.* Springer. 266-279.

[3] Bezuidenhout, M., Mouton, F. & Venter, H.S.2010. Social engineering attack detection model: SEADM. *Information Security for South Africa (ISSA), 2010.* IEEE. 1.

[4] Mitnick, K.D. & Simon, W.L. 2011. *The art of deception: Controlling the human element of security.* John Wiley & Sons.

[5] Gragg, D. 2002. A multi-layer defense against social engineering. *SANS Insitute Reading Room.*

[6] Dong, X., Clark, J.A. & Jacob, J.L.2008. User behaviour based phishing websites detection. *Computer Science and Information Technology, 2008. IMCSIT 2008. International Multiconference on.* IEEE. 783.

[7] Chantler, A.N. & Broadhurst, R. 2006. Social engineering and crime prevention in cyberspace.

[8] Mitnick, K.D. & Simon, W.L. 2009. *The Art of Intrusion: The real stories behind the exploits of hackers, intruders and deceivers.* John Wiley & Sons.

[9] Workman, M. 2008. A test of interventions for security threats from social engineering. *Information Management & Computer Security.* 16(5):463-483.

[10] Janczewski, L.J. & Fu, L.2010. Social engineering-based attacks: Model and new zealand perspective. *Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on.* IEEE. 847.

[11] Thornburgh, T.2004. Social engineering: the dark art. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development.* ACM. 133.

[12] Rao, U.H. & Nayak, U. 2014. Social Engineering. In *The InfoSec Handbook.* Springer. 307-323.

[13] Team, C.I.T. 2014. Unintentional Insider Threats: Social Engineering. *Software Engineering Institute.*

[14] Jahankhani, H. 2012. The behaviour and perceptions of on-line consumers: Risk, risk perception and trust. *International Journal of Information Science and Management (IJISM).* 7(1):79-90.

[15] Salem, O., Hossain, A. & Kamala, M.2010. Awareness program and ai based tool to reduce risk of phishing attacks. *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on.* IEEE. 1418.