A Survey on Social Engineering: Techniques and Countermeasures

Tejasvini A. Kher[1] Swati L. Kariya[2]
[1,2]Department of Computer Engineering & Information Technology
[1,2]Shri S'ad Vidya Mandal Institute of Technology Bharuch, India

Abstract— Social engineering is untruthful to people to get information." It targets emotional parts of human to gain access to controlled area or achieve sensitive information for various purposes. This survey presents framework of social engineering attacks and different types of social engineering approaches. Social engineering attacks are classified into three different categories: Type, Operator and Channel. Psychological attacks and physical attacks are two types of social engineering attacks. In this attacks attacker gather sensitive information of a victim and misuse the sensitive information such as, damage public reputation, financial loss, disruption of services. To protect sensitive information from social engineering attacks mitigation steps and techniques are presented in this survey.

Key words: Social Engineering, Framework, Techniques, Countermeasure

I. INTRODUCTION

"Social engineering is the art of operating people into performing actions or divulging confidential information." It is unique of the best creative and active means of achievement access to secure systems and gaining sensitive information up till now wants negligible technical knowledge. Social engineering in itself does not certainly want a big amount of official information in instruction to be successful. As a substitute, social engineering kills on mutual characteristics of human psychology such as interest, courteousness, unwariness, greed, inattentiveness, wariness and indifference. Social engineering is the most powerful tool for an attacker to access this knowledge. However, people freely publish information in online communication and collaboration tools, such as cloud services and on social networks with very little thought of security and privacy [2]. A social engineering attack targets this weakness by using various manipulation techniques in order to cause sensitive information. The field of social engineering is still in its infancy stages with regards to formal definitions and attack frameworks [5]. Section-II describes Social engineering Framework. Section-III describes types of social engineering approaches. Section IV describes various techniques for social engineering Attack. Section V describes the countermeasure of social engineering. Section VI describes the conclusion of the paper.

II. SOCIAL ENGINEERING ATTACK FRAMEWORK

The first phase, the research phase, when executing a social engineering attack one needs to get the most possible information about the target. The additional step before gathering the information which is meant for determining what the goal of the attack is the best possible target to assist with reaching the goal. Once the goal and target is known, the actual information gathering can start. This process is also described one needs to identify sources of information before anything can be gathered and it is beneficial to assess the gathered information to ensure that there is sufficient information to execute the attack [5]. The next phase, development of rapport and trust, is very similar in the proposed framework but the starting point is modelled as a separate step. Establishment of communication is a requirement for any relationship to be built with the target. The gathered information is used to assist in establishing communication [5]. The third phase is the exploitation phase. Exploiting a relationship is done with different manipulation techniques and in order for these techniques to work the target has to be in an emotional state where the exploitation is possible [5]. Finally a fourth phase is utilising the information which is not part of the actual social engineering attack. The social engineering attack focuses on attacking the human aspect with the intention to achieve a specified goal, in this case to gain privileged information.

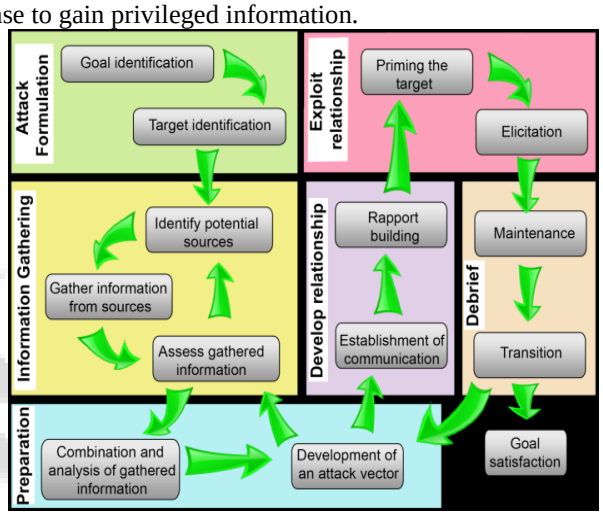

Fig. 1: Social Engineering Attack Framework [5].

III. TYPES OF SOCIAL ENGINEERING APPROACHES

Social engineering attacks are complicated and contain: physical, social, and technical features which are used in different platforms of the real attack. This section describes different approaches attacker can used.

A. Physical Approaches

The attacker performs some form of physical action in order to gather information on a future victim, which can range from personal information (such as e.g. social security number, date of birth) to valid credentials for a computer system. A common technique is searching through the trash of an organization, which is also known as dumpster diving [2].

B. Social Approaches

The most prevalent type of these social attacks is conducted by phone. To increase the chances of these attacks, the perpetrators try to develop a relationship with their future victims beforehand [2].

C. Reverse Social Engineering

Instead of contacting the victim, attackers can try to make the victims ask for help from them. This indirect approach is

known as reverse social engineering. The attackers then advertise that they can fix the problem. Finally when the victim asks for help the social engineers resolve the problem they created earlier and while doing so ask the victims to comply with their requests [2].

D. Technical Approaches

The users often use the same passwords for different accounts. Furthermore, most people are not aware that they give away a lot of personal information for free, which is useful to the attackers. So web search-engines are used by attackers to gather personal information about future victims. There are also tools available to gather and aggregate information from different web resources with Maltego being one of the most popular of such tools. [2].

E. Socio-Technical Approaches

Successful social engineering attacks often conglomerate several or all of the different approaches discussed above. However, socio-technical approaches have created the most powerful ordnances of social engineers. One example is the so-called baiting attack: Attackers approval malware infected storage media in a location where it is likely to be found by future victims [4]. Social engineering, in contrast, is classically directed at individuals or small groups of people. Scammers hope that by sending messages to a huge number of users, they will fool sufficient people to make their phishing attack profitable. Hence, spear phishing is measured a grouping of technological approaches and social engineering [4].

IV. Various Techniques Used for Social Engineering Attack

A. Psychological Attacks

Social engineering works by manipulating emotions such as fear, curiosity, excitement, empathy, and greed or through the exploitation of cognitive biases [1].

1) Phishing

Phishing is defined as a technical method of gathering information via frauds, or typically, the act of sending an e-mail to a target seemly from a legitimate organization in an attempt to grift the victim to reveal the private information, which can be used for identity theft. The e-mail generally has a link to direct the victim to access a fraudulent web page where he or she is requested to update or change something of the account in a legitimate organization such as bank, but it needs to log in first. But the web site, in fact, is set up to steal the target's information, such as passwords or credit card number. Phishing as a social engineering attack occurs in the form of an email or other online mechanism [6].

2) Spear Phishing

Spear phishing is any highly targeted email or telephone scam, usually employed in a business environment. Spear phishing targets at particular group. So instead of casting out thousands of e-mails randomly spear phishers target selected groups of people with something in common [8].

3) Watering Holes

This is a type of social engineering attack in which cybercriminals will identify important web sites that are frequented by individuals or groups they would like to attack, such as mobile app developers. These targeted Web sites are then infected with malware. An example of one such attack was an iOS mobile developers' medium that hosted malware targeted against Apple and Facebook [7].

4) Spoofing

"A spoofing attack is when a malicious party satirizes another device or user on a network in order to launch attacks against network hosts, steal data, and spread malware or bypasses access controls".

5) Trojan Horse

Some social engineers exploit people's curiosity or greed to deliver "malware". The criminal sends an email with attachment posing as something free or urgent. The attachment could be labeled: tracking number for a courier parcel or a winning prize. Opening the attachment loads Trojan onto one's computer. The Trojan could be designed to track keystrokes, upload address book, or look for financial software files to modify [7].

B. Physical Attacks

1) Dumpster Diving

The thieves take the benefit of this law and try to figure out any confidential information that can help them identify any personal information about the victim. The attacker tries to search for the victim's phone number, credit card evidence, and other personal data. However, in the case of an organization, the dumpster diver will search for the organization's phone books, policy, charts or even calendars of meeting [6].

2) Shoulder Surfing

When attackers try to observe over a victim's shoulder to get the password, PIN number or any other sensitive information [6]. In most crowded places this kind of attack works effectively while the attacker can sit behind the victim and observe as they are entering their PIN in an ATM, entering the password for a system or even when he fills forms that needs sensitive information to provide [6].

3) Road Apples

Refers to situations whereby the cybercriminal drops a physical media such as CD or USB Flash memory that is labeled to draw curiosity ("Executive Salary Survey", "HR Staff Reduction Plan", "Confidential Organizational Changes"). Once a staff preferences the media and slots into a PC to view, the "auto run" feature will load Trojan or virus to track keystrokes and harvest IDs and passwords [7].

4) Staff Impersonation

The idea of this attack is that an attacker persuades any IT staff member by phone that he is an authorized person and he forgot his password and wants IT staff to help him to regenerate a new one. While most IT staff will ask the caller (who they think is an authorized person) the basic information like his full name or birthday, the attacker can easily answer especially if he gathered all the information about the authorized person [6].

V. Countermeasures of Social Engineering

A. Anti-Phishing Tools

The use of Anti Phishing Tools that connect to a database of blacklisted phishing websites is recommended. Some of the examples include: Web sense, McAfee's anti–phishing filter, Netcraft anti-phishing system and Microsoft Phishing Filter. This cannot provide 100% security since phishing sites are cheap, easy to build and their average lifetime is only a few days [7].

B. Increase of the Population of Cyber Security Professionals

There is shortage of Cyber security specialists in many developing countries, the ever-changing threat landscape and the need for 24/6 monitoring and response; demands the training of more professionals in this area [7].

C. Use of appropriate Internet Security Technologies

Businesses with online presence should ensure their Secure Sockets Layer (SSL) or the more robust version of the technology, Extended Validation (EV) SSL certificates are updated and are from well-known reputable providers; this is the only effective way to help protect customers and the company, from phishing attacks [7].

These are two critical security measures that can help customers tell the difference between legitimate sites and fake sites designed to steal their information [7].

D. Social Network Vulnerabilities

For self-protection, individuals should not add unknown persons to their network and also they should choose Privacy Settings on Social Networking sites that provide the greatest security and limit information shared with the social networking community [7].

E. Strong Passwords

Individuals should help themselves, by having a strong password and changing it regularly. Organizations should ensure compliance on office networks [7].

It is advisable not to have the same passwords for all accounts. Many people store vital information on phones, to avoid identity theft such phones should be password [7].

F. Education and Training

This involves evolving security alertness and training programs to train employees in techniques to resist social engineering. It must also include regular remainder about the necessity of security consciousness [3].

G. Policy and Management

This involves developing clear and concise security protocols that are enforced consistently throughout the organization as well as developing simple rules defining what information is sensitive. This also requires the requestor's identity when restricted actions are requested and develops a data classification policy [3].

H. Auditing and Testing

This includes testing employees' vulnerability to social engineering attacks. The aim of this countermeasure is to make sure that employees are aware of the threat and to discover what vulnerabilities exist [3].

VI. Conclusion

The defense of information is very important in a contemporary culture and even yet the security about information is constantly improving, the one weak point is still the human being who is vulnerable to use techniques. The social engineering attacks concentrations on attacking the human aspect with the purpose to accomplish a specified goal, in this case to gain privileged information. Social engineering used different approaches for performed security attack. Psychological attack and physical attack are type social engineering attack technique. This paper presented the survey of most prevailing social engineering attacks and mentioned general countermeasures for social engineering and further more mitigation schemes can be in focus.

References

[1] Sherly Abraham, InduShobha Chengalur-Smith, "An overview of social engineering malware: Trends, tactics, and implications", Elsevier/2010.
[2] Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, "Social engineering Attacks on the Knowledge Worker", Springer/2013.
[3] Abdullah Algarni, Yue Xu, Taizan Chan, Yu-Chu Tian," Social Engineering in Social Networking Sites: Affected based model", IEEE/2014.
[4] Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl, "Advanced social engineering attacks", Elsevier/2014.
[5] Francois Mouton, Mercia M. Malany, Louise Leenen and H.S. Venterz, "Social Engineering Attack Framework", IEEE/2014.
[6] Aisha Suliaman Alazri, "The Awareness of Social engineering in Information Revolution: Techniques and Challenges", IEEE/2015.
[7] Osuagwu E. U. and Chukwudebe G. A, Salihu T., Chukwudebe V. N., "Mitigating Social Engineering for Improved Cyber security", IEEE/2015.
[8] M. Nazreen Banu et al, "A Comprehensive Study of Phishing Attacks"/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6), 2013, 783-786.

