Social Engineering Attack: Analysis and Defence

Rashedul Amin Tuhin
ratuhin@kth.se
December 2012

***Abstract*— Social Engineering Attack is based on human beings' the natural tendency to trust. It is performed by manipulating the victim to act according to the attacker's desire, thereby, exploiting the victim through social means. This write-up provides insights regarding different types of Social Engineering Attack on a networked system. Several defence mechanisms against Social Engineering Attack are also discussed. Hence the write up tries to persuade the reader about the importance of addressing the issue more carefully.**

***Keywords*— social engineering, network security, defence, information security, cybercrime**

I. INTRODUCTION

Security is one of the most important factors for a systems quality. The security of a networked system depends on several technical and non-technical factors. The importance of security of a networked system is highly significant not only because of confidentiality of sensitive information but also for the sustainability of the system. Security threat on the networked system is divided into two categories: Technical Hacking and Social Engineering.

Even though vulnerabilities in the software and hardware are one of the main doors for the attackers to perform the attack, the human factor is the weakest link in the security chain [1]. It has been observed in the last few years that Social Engineering is the most successful and crucial attack vector as using this, the attacker exploits human emotions and trust to gain direct or indirect access to the networked system, which actually leads to the actual technical attack.

In section I, a well-defined model of Social Engineering (SE) attack is described. Section II discusses about the natures of different types of Social Engineering Attack performed on networked systems. Later in section III, few defence mechanisms are discussed in order to prevent the attacks. Finally, the importance addressing the issue more seriously is discussed.

II. BACKGROUND

Social Engineering is defined as the process of deceiving people into giving away access or confidential information. The adversary manipulates the victim to perform actions for the interest of the adversary by using the inherent natures and emotions of a human being or by simple deception, bribery, blackmail, threat, etc. The actions might include providing illegitimate access to an area or confidential information to the adversary to perform network intrusion, identity theft, industrial espionage, or disrupting the network [3].

The security of a networked system relies on a three-step process which includes identifying the requestor, verifying that he is not a pretender and ensuring that he has access to the resource (Identification, Authentication, and Authorization) [5]. The Social Engineering Attack attempts to bypass or defeat this process by misinterpretation and utilizing the emotion of the victim.

Even though a networked system is highly secured with most up to date security measures, it can still be vulnerable to Social Engineering Attacks. Typical SE attack exploits human trust, sympathy, willingness to help and persuasion, etc. [4]

Techniques used by the attacker includes posing as someone in authority, posing as someone requesting help, reverse social engineering, use insider lingo and terminology to gain trust [5].

The employees, who have access to plenty of confidential information, interact with many people and who are unaware of the Social Engineering Attacks are the main targets of the attackers. Secretaries, Database administrators, Call center operators, Helpdesk attendants are typically the targets.

Even though each Social Engineering Attacks are different and unique, but they have some common patterns which follow the following steps: Information gathering about the target, identifying the interest and developing a relationship, exploitation of the situation and execution of the attack [2].

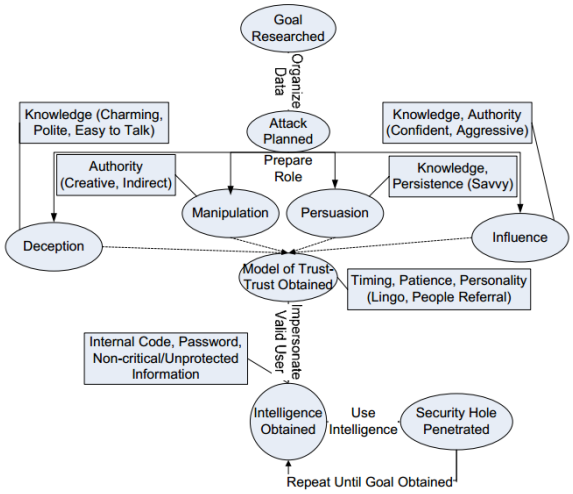

Figure 1: Social Engineering Attack Model [3]

According to the Social Engineering Attack model, the attacker collects sufficient information about the target and plans to gain the trust of the target by deception, manipulation, persuasion or influence. By using any or combinations of these techniques, the attacker gains the trust of the victim. Utilizing the trust, the attacker makes repetitive attempt to gain access to his desired information or tries to achieve his goal and finally performs the actual attack based on the exploit [3].

III. TYPES OF SOCIAL ENGINEERING ATTACK

Social Engineering is comparatively much easier to do as it involves less technical skills and more persuasion skills. Social Engineering Attack can be of two types, human based or computer based or a combination of both. Human-based attacks include shoulder surfing, impersonation, etc. where computer-based attacks commonly include phishing, scams, etc.

Theft: Theft of mobile devices or other security devices can potentially cause an attack [11]. Multifactor authentication actually fails if the stolen device is an authentication factor (e.g. USB stored certificate or mobile phone).

Piggybacking: The attacker simply walks in just after another employee without having proper authentication. The employee often allows this out of sympathy to the attacker assuming him as a colleague. In some cases, the victim is unaware of the incident that somebody walked in just after him. In both cases, the organization couldn't detect the infiltration of the adversary into their office [9].

Tailgating: Attacker puts on a uniform or shows fake IDs to gain physical access to the company office [9].

Impersonation: The adversary presents himself as someone else and manipulates the victim to act according to his wish. Telephonic cheat is a very common attack nowadays, which is actually a variant of impersonation attack or fraud. The adversary makes a telephone call to the victim and persuades him to disclose confidential information by impersonating himself as someone having authority or by gaining the sympathy of the victim. An example of this kind of attack is fake calls as customer care employee and asking for passwords, ATM pins, credit card numbers, etc.

Eavesdropping: The attacker having physical access to the network or the organization can overhear the conversations at the office between two employees or in a meeting. Having the trust is already earned by the attacker, the victim or the target organization is often unaware of the information being leaked or unaware of the imminent attack.

Shoulder Surfing: The attacker collects information by looking at the open window of the victim's computer or the papers which the victim is working on without the notifying the victim. This is a very common technique employed by the attacker to gain access to confidential information on which the victim has access and which can lead to theft of password or disclosure of confidential information to the attacker [11].

Dumpster Diving: Trash cans at different organizations often contain sensitive information such as Company phone books, System manuals, Printouts of sensitive data or login names and passwords, Printouts of source code, Disks and tapes, etc. The attacker collects his desired information by going through the dumpster of the organization [2].

Reverse Social Engineering: The adversary presents himself as a trustworthy person who has the ability to solve a problem and creates a situation that the victim himself asks for help to the adversary and hands in confidential information to the attacker. The beauty of this attack is that the adversary never asks for the information directly to the victim, rather makes the victim himself provide the information to the attacker without letting the victim know that he is being social engineered.

Spam: Up to December 30, 2013, among the total number of exchanged emails, 77.4% of them were spam emails [7]. Spam emails usually contain malicious links, emails which are seemingly from illegitimate addresses or containing malicious scripts, attachments, advertisements which might cause security risks at different levels.

Phishing: Impersonation attack via online media is called phishing. The adversary manipulates the victim to click on the malicious link or to provide his information to a seemingly trusted website or sender. In the case of phishing, the website or the sender address might look more or less legitimate to the victim, and the victim falls for it. The financial sector is the most targeted sector for phishing attacks [10].

419 attacks or Scam: In this attack, the adversary sends some interesting offer (such as: click here to win a free DVD player, or you have won 50000 dollars, click here to claim, etc.) as bait to the victim. The victim often falls for it and complies with the wish of the adversary in order to have financial or any other gain.

Pop-up windows: Unsecured browsers often show pop-up windows containing malicious links or advertisements which can often lead to a high threat to the security of the networked system. Most of the browsers have pop-up blockers built in nowadays, so this is rarely a problem unless the victim is not very much aware of the importance of it.

Through Social Networks: Social networks are often used to manipulate the victim or collect information about the target. The attacker often lures the victim to click on a malicious link to direct him toward a malicious website. People often victimize themselves out of curiosity about a current trend or a seemingly interesting content shared by the attacker on the social networks.

IV. DEFENCE MECHANISMS

Each Social Engineering Attack is unique and powerful as no hardware or software can defend it fully till now. Analyzing the patterns and nature of the attacks, the only defensive measure which could be taken in order to prevent Social Engineering Attacks is to "maintain a security aware culture", which includes attack recognition, auditing and penetration testing, employee education and training, information classification, etc.

Recognition of Social Engineering Attack: Recognizing a Social Engineering Attack is very difficult as the targets are generally less aware of it. Yet some of the recurring characteristics include refusal to give a callback number (in the case of telephone calls), making an out-of-ordinary request, showing discomfort when questioned, name dropping, stressing urgency, etc. Sometimes the attacker might threaten the employee or claims fake authority while performing the attack. If these cases apply, it is more likely to be a Social Engineering Attack [5][8].

Preventing Physical Access: If the attacker can't have physical access to the organization or to the network, the risk of having many kinds of Social Engineering Attacks can be eliminated. Blocking physical access (specially piggybacking and tailgating) for unauthorized persons under any circumstances greatly minimize the risk of attack.

Multiple Security Level: Deploying multiple levels of security can also significantly reduce the security risk for a networked system. The probability of the attacker getting through multiple layers of security is actually lower than a single layer. Even if the attacker manages to get through a layer, he might not be able to get through the next layer.

Information Classification: To ensure better confidentiality, integrity and availability, it should be strictly defined that which system or employee should have access to which information or area. Employees should have access only to the needed information under his authority. This particular preventive measure can also minimize the damage in case of an actual attack.

Incident Response: If unfortunately, a networked system of an organization experiences security

breach even though it employed every possible security measures, it should have an Incident Response Team (IRT) immediately detecting and taking care of the situation before further damage happens. The IRT should also learn and take necessary steps to prevent similar kind of attack for the future.

Auditing and Penetration Tests: To prevent Social Engineering Attacks, an organization should perform a regular penetration test and auditing in order to understand the systems and employees to find the vulnerabilities and taking preventive measures about them. Besides, auditing is important to find out the most important points to raise security awareness among the employees in order to train them efficiently. For example, if the employees are very much aware of phishing attacks, but with auditing, it could be found out that they provide too much information on the telephone calls or they are not at all aware of shoulder surfing. Auditing and penetration tests help to set the correct security policies.

Training and Retraining: Training the employees, again and again, is the key to prevent Social Engineering Attacks. The training should be done efficiently in accordance with the audit report. According to the example in the previous paragraph, a training session about shoulder surfing would be much more helpful than a session about phishing. This training should be done on a regular basis to ensure the security of the networked system of the organization [8].

Strict Security Policy: Having a strict security policy is one of the key factors of a secure system. An organization should have a clear and strict policy about every possible circumstance. For example, whenever an employee is fired, he should be escorted outside immediately and kept an eye upon until he leaves the office. Security policy might also include penalties for non-compliance with the policy [12].

Realistic Prevention: Security policy makers should also keep that in mind that the security policy should be strict but not unrealistic or too harsh that they lose customers or their revenue generation is hampered. A trade off should be present while setting the policy.

Updating Software: Updating software is a cumbersome task for a large network. But outdated software often suffers from unpublished or published (or even just published) exploits which could be utilized by the attackers. Recent events reflect that, this kind of attack could be performed by outdated PDF reader software as well. So, a centralized system could be employed in order to avoid the hassle of updating software from every single node individually.

V. IMPORTANCE

Identifying the factors of failure can strengthen the security of a system. Among all the successful attacks in recent years, most of them involved some form of Social Engineering Attack as human being is the most vulnerable point in terms of security. Attacks involving social engineering might waste millions of dollar spent on modern security gadgets and software, in the worst case, the attack might even go unnoticed. Studies show that the presented preventive measures provide valuable contributions against the attack making the networked system robust. Another important aspect is that many of the organizations are already considering Social Engineering Attacks seriously as it is the basis of Advance Persistent Threat (APT) targeted specifically towards them. Preparing against the attack would at least provide them a head-start among other competitors at the play ensuring that they will not be the first to be attacked.

VI. CONCLUSION

This study provided the types of Social Engineering Attacks and brief discussion about several prevention mechanisms against it.Even though Social Engineering Attack is a partial technical attack [9], its consequences can be deadly as it often facilitates the actual attack on the networked system. Preventive measures can't rely on hardware or software only; rather the prevention includes establishing and maintaining a security aware culture inside the organization in order to protect the networked system. Without securing a networked system against Social Engineering Attacks, a system can't be considered as a fully secure system and suffers from the risk of being attacked.

REFERENCES

1. Gulati, R, "*The threat of social engineering and your defence against it*", SANS InfoSec reading room, SANS Institute, 2003.
2. Hasan, M,"*Case study on social engineering techniques for persuasion*", International Journal on Application of Graph Theory in Wireless ad hoc Networks and Sensor Networks, Vol 2, No 2, June 2010.
3. Laribee, L.; Barnes, D.S.; Rowe C.N.; Martell, C. H.; , "*Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems*" , Proceedings of the 2006 IEEE Workshop on Information Assurance, United States Military Academy, 2006.
4. Laribee, L; "*Development of methodical social engineering taxonomy*" Master's Thesis, Christian Brothers University, 2001.
5. Thornburgh, T.; "*Social Engineering: The "Dark Art""*, Proceeding InfoSecCD '04 Proceedings of the 1st annual conference on Information security curriculum development, 2004.
6. Sarah Granger, *Social Engineering Fundamentals, Part I: Hacker Tactics* <http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>
7. Trustwave, *Spam Statistics*, December 30,2012, <https://www.trustwave.com/support/labs/spam_statistics.asp>
8. Bezuidenhout, M. ; Social engineering attack detection model: SEADM; Information Security for South Africa (ISSA), 2010;
9. Maan, P. S.; Sharma, M.; "*Social Engineering: A Partial Technical Attack*", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012.
10. Anti-Phishing Working Group, *Phishing Activity Trends Report*, September 2012.
11. Nyamsuren, E.; Choi, H; "*Preventing Social Engineering in Ubiquitous Environment*", Proceeding FGCN '07 Proceedings of the Future Generation Communication and Networking - Volume 02, 2007.
12. Orgill, G, "*The urgency for effective user privacy education to counter social engineering attacks on secure computer systems*", ProceedingCITC5 '04 Proceedings of the 5th conference on Information technology education, 2004.