A SURVEY ON SOCIAL ENGINEERING AND THE ART OF DECEPTION

Megha Gupta
B. Tech Student
Deptt. of Information Technology
Amity University, UP (India)

Sameer Agrawal
B. Tech Student
Deptt. of Information Technology
Amity University, UP (India)

***Abstract*—Nowadays security of data and information is the area for which and every organization is concerned about. Each and every organization is using advanced technologies for protecting its data and information from theft and fraud. But even after using best security technologies, organizations are totally vulnerable. It is because of its human resources. This paper explains how one can use human beings for capturing useful information about the organization. This technique of gathering information from human resources of the organization is known as social engineering. This art is also known as the Art of Deception. In this paper we have described various techniques used for performing social engineering attack; various qualities required for social engineer and the countermeasures for a social engineering attack.**

I. INTRODUCTION

For any organization, information security aspects are very important, as it is the information and details of the organization that can help any hacker to have a complete control over the organization. Any organization that is using the best security technologies by spending as much money as it can is still totally vulnerable. With advancements in technology, various tools and techniques have been designed to protect data and information. The organization applies those security tools and techniques like firewalls, intrusion prevention system, intrusion detection system, passwords, and registry protection, etc. The company employees follow the best security practices to make themselves and their company secure but they are the most vulnerable part in the organization. Famous security consultant Bruce Schneier said as follows, "Security is not a product, it's a process." Moreover, security is not a technology problem - it's a people and management problem. It is very well said by Bruce Schneier because it is easy for a hacker to get information by exploiting human tendency of trust by getting personalized with the employees rather than by using complicated tools and techniques.

A lot of information required for social engineering attack can be obtained from the company's website, for example company's contact numbers, authorities and other information. The main bases of social engineering attack are human beings and their tendency of trust.

The use of social engineering techniques can destroy networks, cripple identities, and result in significant monetary loss. Using social engineering techniques can defeat intrusion detection systems and bypass well-planned network security techniques. Additionally, social engineering techniques may cause individuals to leak private information which in turn can be used to acquire the victim's "identity" [5].

II. THE HUMAN PSYCHOLOGY OF TRUST

Human beings are born bad, self centred and greedy. By psychology, they think only of themselves and hold on every opportunity that give them gain. That is human nature [1]. This human nature can become the cause of the downfall of the organizational security measures. The art of deception is basically the exploitation of this human tendency of getting familiar with others very easily and very soon. An attacker tries to be familiar with the person that is an employee of an organization and who can reveal information that is of interest of the attacker and even he gets successful in getting the information that he needed. Social engineering techniques are commonly based on four qualities of human nature including the desire to be helpful, the tendency to trust people, the fear of getting into trouble, and the willingness to take "short cuts" [5].

III. MEANING OF SOCIAL ENGINEERING

According to many authors social engineering can be defined in various ways like "the art and science of getting people to comply with your wishes" [4].

Social engineering is a technique that uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not or by manipulation. As a result, social engineer is able to take advantage of people to obtain information with or without the use of technology [1].

The actual definition of social engineering can be anything but the one which actually suit is social engineering is generally a hacker's clever manipulation of the natural human tendency to trust and desire to help. The hacker's goal is to obtain important information that will allow him/her to gain unauthorized access to a valued system in an organization and the information that resides on that system. Security is all about trust. The weakest link in the security chain is the natural human willingness to help and trust someone at his or her word, which leaves the organizations vulnerable to attack. Many experienced security experts emphasize this fact.

IV. GOALS AND TARGETS OF SOCIAL ENGINEERING ATTACK

The basic goals of social engineering are : to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network [2].

Typical targets of a social engineering attack include: telephone companies and answering services, big-name corporations, financial and banking institutions, military targets and government agencies, and hospitals, etc. the organizations that have victimized the social engineering attack never admit it because to admit the security breach is very much embarrassing and moreover it also ruins the organization's reputation. Social engineering attack is never documented that is why nobody is sure of whether the social engineering attack took place or not.

V. SOCIAL ENGINEERING ATTACK TECHNIQUES

Social engineering attacks take place on two levels: the physical and the psychological [2]. Therefore social engineering techniques can be categorized into two parts:

1. Physical Techniques
2. Psychological Techniques

A. Physical Social Engineering

Physical tools of social engineering include dumpster diving and office snooping. In the event physical tools are used, discarded information may be acquired from the trash and information may be heard without any active intervention.

- **Dumpster Diving** – Dumpster diving is also known as trashing. It is one of the popular methods of social engineering. A huge amount of information can be collected through company dumpsters or company's garbage. It includes looking for information that is discarded by a company's employees. The following items can be potential security leaks in the trash: "company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware [2]. Phone books can give the names and numbers of company's employees to the attacker. Organizational charts contain information about people who are in positions of authority within the organization. System manuals, sensitive data, and other sources of technical information may give hackers the exact keys they need to unlock the network [2].

  Dumpster diving can be explained through an example as follows: Maryam is an employee of XYZ organization. While she is cleaning out her file cabinet containing her bills from the past year; she discards past credit card bills, utility bills, and bank statements into the garbage collector or the dustbin. The night before garbage day, Maryam hauls all of her garbage to the curb, including the past bills. After that Maryam sleeps soundly as she thought that her bills from the past year have been discarded. But at the same time an identity attacker is going through Maryam's garbage looking for information that is of his own interest. He discovers the discarded billing information. From the credit card statements he acquires Maryam's credit card numbers. From the bank statements he acquires bank account information including balances, Maryam's social security number and account numbers. The attacker uses this information to start electrical service with Maryam's name at his home. This act is known as dumpster diving or identity theft. Dumpster divers are also known as thrawlers or garbologists who find sensitive information in garbage cans and dumpsters [5].

- **Shoulder Surfing –** It includes simply looking over someone's shoulder while they are using a computer. This can be done in close range as well as long range using a pair of binoculars [8]. The attacker or the shoulder surfer look's over someone's shoulder to gain information such as passwords and pin numbers. A news report from several years ago showed the significance of protecting personal information from shoulder surfers. In their report, a reporter was given a phone card and

told to use it in Grand Central Station in New York. While the reporter was making the call, police counted at least five people "shoulder surfing" the reporter's pin number [6].

B. Personal or Psychological Social Engineering

Social engineering is accomplished through many techniques including persuasion. Some of the techniques are:

i. Telephone
ii. Online
iii. Persuasion
iv. Impersonation
v. Reverse Social Engineering

- **Social Engineering on Phone -** The most prevalent type of social engineering attack is conducted on phone.

  An attacker will call up on the company's contact number and pretends to be someone in a position of authority or relevance and gradually pull information out of the user. Help desks' employees are particularly prone to this type of attack. Hackers are able to pretend they are calling from inside the corporation or organization by playing tricks on the PBX or the company operator. Help desks are particularly vulnerable because they are in place specifically to *help*, a fact that may be exploited by the attackers who are trying to gain useful information that they needed to hack the organization. Generally the help desk employees are trained to be friendly and give out information as they are in the organization to help. So this is a gold mine for social engineering attack. Most help desk employees are minimally educated in the area of security, so they tend to just answer questions and go on to the next phone call [2]. This tendency of human beings can create a huge security hole in any organizations security measures.

- **Online Social Engineering** – Persuading or gathering information through the use of an online chat session, emails, or any other method that your company may use to interact online with the public.

  Hackers may obtain information on-line is by pretending to be the network administrator, sending e-mail through the network and asking for a user's password. This type of social engineering attack doesn't generally work, because users are generally more aware of hackers when online [8].

- **Persuasion –** Persuading someone to give you confidential information either by convincing them you are someone who can be trusted or by simply just asking for it. , the main objective is to convince the person disclosing the information that the social engineer is in fact a person that they can trust with that sensitive information. The other important key is to never ask for too much information at a time, but to ask for a little from each person in order to maintain the appearance of a comfortable relationship. Impersonation generally means creating some sort of character and playing out the role. Some common roles that may be played in impersonation attacks include: a repairman, IT support, a manager, a trusted third party, or a fellow employee. The best way to obtain information in a social engineering attack is just to be friendly [2].

  Common alternative routes of persuasion encompass two routes: direct and secondary. Direct routes involve specifically asking an individual for information. For instance, "Susan, I need to log into the company Web site to check stock information and I forgot my password. What is your login information?" [6].

  In the indirect method of persuasion, a social engineer will increase the susceptibility of the victim by influencing an emotional response. Social engineers may spend significant amounts of time learning their victims and developing a situation that plays on the background of a victim. The targeted person must feel compelled to disclose the requested information. Additionally, the attacker must create a strong enough emotional attachment that the victim is willing to ignore policies and procedures of their personal beliefs or organizational policies [7]. The victim makes the decision to disclose the information to the other party since they feel the reason has been justified. Many factors are used to cause these strong emotions. Most commonly, authority and empathy are the leading cause of disclosure by this method [7].

  With social engineering, you are not working with hardware or software, but wetware. Wetware is the human element of computing. People are naturally trusting of others, and social engineers exploit this to their advantage.

  Social engineering is essentially the art of persuasion.

- **Impersonation** – Impersonation is a technique of social engineering in which the attacker pretends to be someone he is not. For example attacker pretends to be someone in authority. Some of the impersonation attack techniques include acting like network administrator, service provider, IT support or help desk employee.

- **Reverse Social Engineering -** This is a more advanced method of social engineering and is almost always successful. An attacker will have had to already done reconnaissance as well as already have some amount of luck with previous attacks

whether through hacking or social engineering. Reverse social engineering is a method where an attacker can get their victims to call them back pertaining to something an attacker may have previously. Since a victim is calling the attacker, the victim is already at the attacker's mercy, and it is almost impossible for the victim to tell that they are being attacked if they have already legitimately made the call back to the attacker. A social engineer can use a combination of all of these methods to accomplish his final goal. In fact, most successful ploys will incorporate at least 2 of these methods [8].

VI. COMPARISION OF PHYSICAL AND PSYCHOLOGICAL TECHNIQUES

TABLE I. COMPARISION OF PHYSICAL AND PSYCHOLOGICAL TECHNIQUES OF SOCIAL ENGINEERING.

Parameters	Techniques	
	Physical Techniques	***Psychological Techniques***
Physical Theft	Yes	No
Need of persuasive power	Not essential	Required
Good Communication skills	Not necessary	Required
Planning	Required	Required
Knowledge of company's details	Not required	Required
Knowledge of company's location	Required	Not Required
Exploitation of human tendency of trust	No	Yes
Use of telephone and internet	No	Yes

VII. QUALITIES OF A SOCIAL ENGINEER

To be successful at social engineering, we need the following four qualities:

- **Patience**- Patience is by far the most important trait to have as a social engineer. Many fail because they ask for information before they build up trust with someone.
- **Confidence**- If we appear confident, people will believe us.
- **Trust**- Besides patience and confidence, we also must build trust with our target person. Reciprocation and similarity techniques help to build trust with others.
- **Inside knowledge**- The last ingredient to successful social engineering is to possess inside knowledge of the company. We must do your research if we want to appear authentic.

VIII. DEFENDING AGAINST SOCIAL ENGINEERING ATTACK

Tools and techniques have been designed to prevent social engineering attack. Using these tools make the organizations less vulnerable. According to Douglas Twitchell, there are currently three ways commonly suggested to defend against social engineering attacks: education, training and awareness; policies; and enforcement through auditing.

- Organization's employees can be educated through training and awareness which can make them more reluctant to disclose personal information. In depth security training of the employees should be conducted. This reduces the risk of social engineering attack and makes the organization less vulnerable.
- Policies should be made which provides instructions to the employees on proper handling of company's information and user data.
- Audits must be conducted in order to ensure that the employees of the organization are following the policies and procedures.

- Hard copies of organizational data, records, or personal information must be destroyed before being discarded. Common effective methods for destroying hard copy information include shredders and incinerators.
- Employees should be trained to question the credentials of the person who is calling himself to be in authoritive position in that organization.
- Organizations should be careful about what they are posting on their company's website. Company's details like names of people on authority and contact numbers should be avoided.

IX. CONCLUSION

On conducting a survey on the social engineering techniques and the art of deception, we can conclude that even after using the best and even the most expensive security technologies, an organization or a company is completely vulnerable. It means it is very easy for a good attacker to gather information about that organization just by gaining trust and being friendly with the user.

Social engineering technique of capturing information is being used since lone time but it came into notice just some time before. Before people and organizations were not much aware of these security breach practices and techniques for securing information but nowadays information security is the main concern of the corporate world.

Social engineering techniques can be physical or psychological. Physical techniques do not require any type of persuasive power or good communication skills. These basically include checking out dumps and trashes in organizations. Psychological techniques include persuasion and impersonation. That is to imitate as someone in authority. These techniques require a lot of confidence and very good communication skills.

REFERENCES

[1] Kevin D. Mitnick, William L. Simon, "The art of Deception, controlling the human element of security" pg 12-13, Publisher: Wiley, John & Sons, 2003

[2] Sarah Granger, "The Social Engineering Fundamentals: Part 1 Hacker tactics" Endpoint protection, Security focus, December 2001.

[3] Jonathan J. Rusch, "The Social Engineering of Internet Fraud", United States Department of Justice, 2009.

[4] http://packetstorm.decepticons.org/docs/social-engineering/socialen.txt

[5] David Wheeler, "Running Head: Social Engineering", Purdue University Calumet, ITS 350, Section 1, April 2008.

[6] Peltier, T., "Social Engineering: Concepts and Solutions" Information Systems Security, publish 2006.

[7] Thornburgh, T., "Social Engineering: The Dark Art", Information security curriculum development, pg 133-135, publish 2004.

[8] Jared Kee, "Social Engineering: Manipulating the source", GCIA Gold Certification, October 2008.

[9] Malcom Allen, "Social Engineering –A means to violate a Computer System", June 2006.