Social Engineering: A Partial Technical Attack

P. S. Maan and Manish Sharma

Department of Information Technology
DAV Institute of Engineering and Technology
Punjab Technical University
Jalandhar , Punjab , India

Department of Information Technology
DAV Institute of Engineering and Technology
Punjab Technical University
Jalandhar , Punjab , India

Abstract

This paper suggests the crystal clear concept behind the social engineering attack. Basically social engineering is a non technical attack. But social engineering attack is an attack on human psychology to get the information, but by using what?

Basically it is an attack on human psychology by using some technical skills or technology. Social engineering attack has many types of attacks like fake mail, telephonic cheat etc. which are impossible without any technical skills, so in this paper we suggest that, it is a partial technical attack and can be divided in human based and typical computer based social engineering attack.

General Terms: *Cyber crime, information security, hacking*

Keywords: *Social engineering, technical and non technical attack, computer-based and human-based social engineering, human psychology*

1. Introduction

Social engineering is a real problem to industries and the web security in this day and age even through the security of it is extremely downplayed.

Now if we think like an attacker because Kevin Mitnick said ‘if you want to be securing something then you have to think like an attacker first’

Social engineering is the best attack for any attacker because every attack has some needs, some tools and Every attack has its own limitations also, but social engineering is the best way to hack anything because it has no limitation. It is an attack, when attacker gets information from victim by attacking on his/her psychology and then victim is completely hacked.

Now social engineering is a non-technical attack, is it? Basically, not. We use fake mail and telephonic cheat, is there are possible without any technical knowledge, no. so in this paper we discuss all attacks by using social engineering technique. Social engineering is a technique to attack on victim in different ways like telephonic cheat. Industries with authentication process firewall, private virtual networks are still open to attack, the reason is social engineering. So it is clear that how much social engineering technique is dangerous. Social engineering target call centre employees, as they are normally underpaid, under skilled worker, whom have knowledge about the information technology infrastructure. These workers are easy to target. It is happening, because of social engineering.

In the following we describe the research on basic type to social engineering by using [2] human-based and [3]computer-based attack and then further explanation of [2.1]piggybacking, [2.2]tailgating,[2.3]telephonic cheat then [3.1]phishing,[3.2]fake mail [3.3]Pop-up windows and then this paper terminates that social engineering is a partial technical attack.

2. Human-Based Social Engineering Attack

In this type of social engineering attack attacker gathers sensitive information by interaction with victim. And use psychological handling with the help of fear, trust and get the access. In this attacker attack on victim's psychology and victim gives his/her information him/her self.

2.1 Piggybacking

Basically in this kind of attack an unauthorized person provides access to an authorized person by keeping the secured door open by using attack in sense of help like I forget my id at home, please help me so if any person doesn't know the way of get accessing in that so how can he/she can hack. So it is also attack by using technical skills, because if attacker doesn't know the about victim technical information or personal information to handle technically. So it is clear that it is a partial technical attack.

2.2 Tailgating

An attacker use all activities as an authorized person like uniform and communication and then use mind and attack on human psychology and enter in area by using technical communication skills. In this attack attacker has to know about organization details its authentication process then only he/she can go in the authorized area.

So, this is also attack in which attacker should perfect in technical communication and technical knowledge about the organization. That's why it is also a partial technical attack.

2.3 Telephonic Cheat

This is the first way and the best way to social engineering attack because in this attackers don't need anything, except a perfect technical communication on telephone and try to believe that he/she is a authorized person and get the personal information and Id's and then misuse that information and make money etc. but in this also attacker needs technical knowledge and information about victim and technology so this one also not a non-technical attack. It is also a partial technical attack.

3. Computer-Based Social Engineering Attack

This is the type of social engineering in which we use technology by using computing system or it is typically based on technology. In this we will discuss those attacks which will prove that, social engineering is not a non-technical attack. So, now we will see that how these attacks are typically based on technical computing.

3.1 Phishing

The word phishing was first used in 1996 in which an AOL account was hacked. After phishing AOL account information.

This kind of attack starts from a falsified e-mail message. Cyber criminals use the resemblance of the address and logo of a company or organization to get a user's secret information like passwords, credit card numbers etc.

Cyber criminals recognized possibilities of attacking any online payment system. Typically, phishing involves social engineering. More precisely, a phisher sends large amounts of luring e-mails that appear as if they were sent from a trusted party. These e-mails usually contain a link to a clone of the trusted websites. Fooled by the familiar look and feel of the page, the victim feels comfortable at submitting sensitive data (e.g., username and password or PIN). Unfortunately, the cloned website is controlled by the attacker whose has previously deployed a computer program that automatically collects the phishes for later use. The most valuable phishes may be passport numbers, credentials, e-mails accounts or financial information.

The consequences and the financial losses are further exacerbated by the enormous scale reached by malicious activity on the internet. In fact the cyber criminal organizations control vast amounts of computational and networking resources. Most notably by spreading malicious software that automatically infects unprotected computers, the criminals have hosts, also known as botnets.

So this is clear that phishing is also a partial technical attack because it has so many things which are typically technical based and now we will discuss about fake mailing.

3.2 Fake Mail

Basically this is attack by using e-mails. It is a series of useless e-mails on victim's system. Attacker uses this to get information by installing the malicious items on victim's system and get the access.

It is attack when sent e-mails to many recipients without prior permission intended for commercial purposes and get the information of victim and then victim is totally hacked. So it is now clear that it is also a partial technical attack in which we use technical things with the help of social engineering.

In fake mailing attackers send irrelevant, unwanted and unsolicited e-mails to collect financial information, social security numbers and network information. And finally hack the victim.

3.3 POP-UP Window Attack

This is the attack when victim is using any site and he get a pop-up window and web page is of enter your username and password. In this attacker send a pop-up window with the most visiting site and attack on victim. Victim just check this pop-up Because it is so attractive like free software or like you won this contest and get your money from here and enter your username and password and then attacker has done his/her work**.** And then victim is totally hacked.

Basically it is just like that attacker attracts the victim. And it is technique when victim use internet surfing and suddenly he/she got window that you are the winner of this contest or you are a lottery winner and you won money. Now login for collect your money and when victim enter his/her username and password he/she is totally hacked

In this we see that we use a pop-up window concept. So this attacks also a partial attack.

4. Conclusion

At the end, this paper suggests that social engineering is not a non technical attack. This is a partial attack and we have observed that it is a partial technical attack with the help of all its types and then we device this technique into two category which shows that it a technique form that we use different attacks and all attack are not non technical. They all are partial technical attacks and all attacks are related to technical things, it may be source code, networking, web technology etc. but each and every attack is related to technical things.

In this paper we presents social engineering attack is like a technique and all the attacks under this technique can be categorized between human-based and computer-based social engineering attack which all are not non technical attack. They all are partial technical attack. So we can suggest that social engineering is a partial technical attack.

Acknowledgment

We would like to gratefully acknowledge the support and guidance of Mr. P.S. Maan. And Editing Team of IJCSI (International Journal of Computer Science Issues)

References

[1] Alex Roney Mathew, Aayad Al Hajj, Khalil Al Ruqueshi: `` cyber crimes, threats and protection "international conference on networking and information technology, 321-21, IEEE 2010
[2] Francois Mouton, H S Venter: social engineering detection model, 321-32-10, IEEE, 2010
[3] Igor Kotenko, Mithail Stepashin: ``security analysis of information systems taking into account social engineering attacks", international conference on parallel, distributed and network – based processing, IEEE, 2010
[4] Leach J, Lingyan Fu: `` social engineering-based attacks: model and New Zealand perspective", 321-50, vol-1, IEEE, 2010
[5] Katja Walentrowitz, Daniel Biemborn : ``the social network structure of alignment", vol 3 320.21, IEEE, 2011
[6] Rae Carrington Schipke: ``the language of phishing, Pharming, other internet fraud", international conference of computer and information technology, IEEE, 2011
[7] Wei-bing Liu, Min Li: dynamic decision making in social security system, 232-12, voI-2, IEEE, 2011
[8] Federico Maggi: are the con artists back? A preliminary analysis of modern phone frauds, 10th IEEE conference on computer and information technology (CIT 2010)
[9] K D Mitnick and William L Simon, 'The Art Of deception: controlling element of security Indianapolis: Wiley publishing 2002
[10] K D Mitnick and William L Simon, ``The Art of intrusion" the real stories behind the exploits of hackers, intruders and deceivers: Wiley publishing 2005
[11] Ankit Fadia and Manu Zacharia, `` Intrusion Alert: Vikas publication 2009
[12] R J Stemberg, cognitive psychology, Thomson Watsworth, 2006
[13] CEH v6 module: EC Council 2008
[14] http://www.Insecure.in
[15] http://www.enigma.org
[16] http://alboraaq.com
[17]http://www.antiphishing.org
[18]http://www.technicalinfo.net/papers/phishing.html
[19] http://www.hk3.com
[20] http://www.computer.org/security

First Author

P. S. Maan is an Asstt. Professor in DAV institute of engineering and technology since last 5 years. He has done B.Tech. With Hons. And M.Tech. His research area is Computer Networks, Wireless Communication, Dot Net Technologies, and Cloud Computing. He has 1 International Journal, 1 International Conference, 1 National Journal, and 1 National Conference. He is Life Member of Punjab Academy of Sciences and Computer Society of India.

Second Author

Manish Sharma has done B.Tech. (IT) from DAV institute of engineering and technology in 2011 and now working as a security consultant in Appin Technology lab, Ghaziabad, India. He is member of IEEE. He is Repudiated Public Speaker and Expert Lecturer for IT security and Ethical hacking.