Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2016, 3(3):64-66**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Social Engineering: An Introduction

Matthew NO Sadiku, Adebowale E Shadare, Sarhan M Musa

Roy G Perry College of Engineering, Prairie View A & M University, Texas, USA

Abstract Social engineering may be regarded as a umbrella term for computer exploitations that employ a variety of strategies to manipulate a user. It represents a real threat to individuals, companies, organizations, and governments. This paper explains the concept of social engineering and the impact it has on society.

Keywords social engineering, social attacks, social technology, phishing, information security

Introduction

Protection of sensitive information is vitally important to governments and organizations. Although the effectiveness of protecting information is increasing, people remain susceptible to manipulation and the human element is the weak link. The act of influencing and manipulating people to divulge sensitive information is known as social engineering or social attacks [1].

Social engineering consists of techniques used to manipulate people into performing actions or divulging confidential information. It is the acquisition of sensitive information by an outsider. To achieve that, a social engineer tricks someone into providing access to information or breaking normal security procedures. The process of doing that is known as social engineering attack. Social engineering can be used in face-to-face interactions, over the telephones, letters, emails, websites or through persons. It threatens not only companies, organizations, and governments, but also individuals.

While technology has made some fraudulent activities more difficult, it has created a new opportunities for adaptable fraudsters. The strongest security technology can be overcome by a smart social engineer. Social engineering is entrenched in both computer science and social psychology. Knowledge of both disciples is needed to perform research in social engineering. Elements of social engineering [2] are shown in Figure 1.

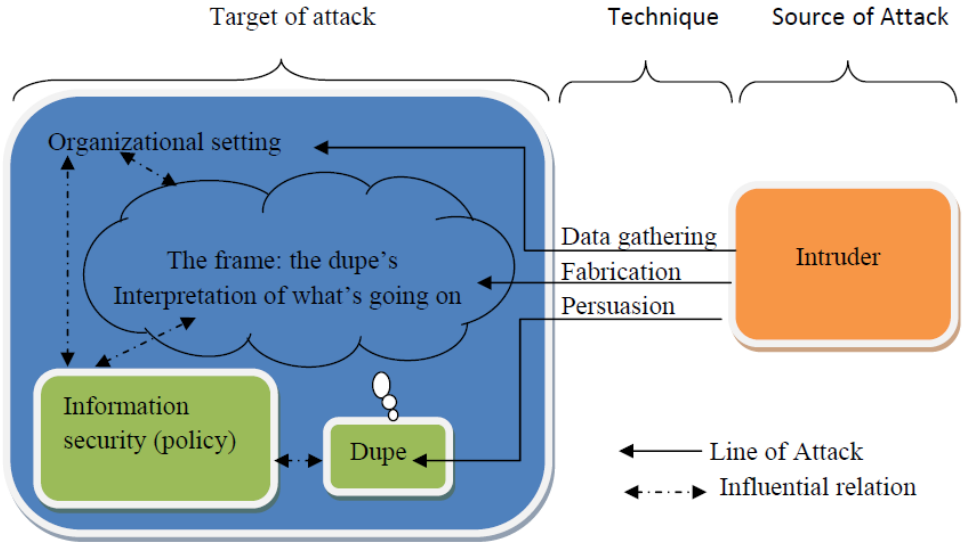

Figure 1: Elements of social engineering [2].

Types of Social Engineering

There are two types of social engineering: human-based and technology-based [3]. The human-based social engineering requires a person-to-person interaction to achieve an objective. This may mean impersonation, third-party authorization, dumpster diving, and shoulder surfing. Technology-based social engineering requires an electronic interface to achieve the desired objective. This may involve using email, email attachment, and web sites. For example, a social engineer may send false emails claiming to be from a legitimate entity. The attacker can easily deceive the victim into believing that the email originates from a legitimate source. Social engineering threats, which are human-based, are on the rise due to continued improvements in protections against technology-based threats.

Social Engineering Attackss

Social engineering attacks presume on the tendency of the human nature to desire to be helpful, to trust people, and to fear getting into trouble. A social engineer with patience and resolve will exploit this nature. The most common attack types or techniques that social engineers can use to target their victims include, but not limited to, the following: phishing, pretexting, baiting, tailgating, and scareware [4-7].

Phishing

Phishing seems to be the most common type of social engineering attack. It is associated with fake emails and websites. Phishing occurs when a malicious party sends a fraudulent email. The email is meant to trick the recipient into sharing personal information such as credit cards, passwords, or social security numbers. It may also involve enticing a victim to download an attachment or click a hyperlink. People sometimes will divulge sensitive or private information to those they feel obligated. Phishing has been around for a long time, but it has become more numerous and sophisticated.

Pretexting

Pretexting occurs when one party lies to another in order to gain access to privileged information. An impostor creates a setting designed to influence the victim to release sensitive information. While phishing emails use fear and urgency to their advantage, pretexting attacks rely on building a false sense of trust with the victim. For example, the attacker may pretend the need some personal information in order to confirm the identity of the target.

Baiting

Baiting involves the hacker promising an item or good to entice victims. It is similar to phishing attacks. For example, baiters may offer users free music if they surrender their personal information to a certain site.

Tailgating

This attack is also known as "piggybacking." This type of attack involves someone who lacks the proper authentication following an employee into a restricted area. This attacker tailgates the employee who has legitimate access to the area.

Scareware

This is a malicious computer program that is meant to convince the victim that their system is infected, pressuring the victim to buy and download fake antivirus software. The protection software regularly displays warnings for infections and demands payment for removing them.

Defense against Social Engineering

Attempt made by the security professionals to prevent social engineering are bound to fail. Social engineering attacks are inevitable, but their impact can be minimized. The following are some of the good practices against social engineering [3,7]:

- Implement an information security awareness program.
- Require proper identification for everyone who performs a service.
- Establish a standard that passwords are never given over phone.
- Require that passwords are kept confidential.
- Create a security alert system.
- Minimize access to information.
- Implement caller ID technology for help desk and other support functions.
- Have shredders on every floor.

In order for policies, procedures, and standards to be effective, they must be communicated, taught, and reinforced to the employees. The employees must be educated to identify an attack, minimize the impact of the attack, and create barriers for the attacker. Everyone from top to bottom must understand security principles and act accordingly.

Conclusions

Protection of sensitive information is important in our modern society. Despite the increasing awareness of the threats to information security, there continues to be information security violations. Social engineering is becoming perceived as an attack methodology. This paper has presented social engineering as a domain and social engineering attacks as a process in the domain. Social engineering remains a real threat to individuals, companies, organizations, and governments. The field of social engineering is still in its infancy.

References

[1]. F. Mouton et al., "Social engineering attack framework*," Proc. of Information Security for South Africa* (ISSA), 2014, pp. 1-9.
[2]. P. Tetri and J. Vuorinen, "Dissecting social engineering," *Behavior and Information Technology*, vol. 32, no. 10, 2013, pp. 1014-1023.
[3]. T. R. Peltier, "Social engineering: concepts and solutions," *Information Security and Risk Management*, Nov. 2006, pp. 13-21.
[4]. M. Rouse, "Social engineering," http://searchsecurity.techtarget.com/definition/social-engineering (accessed April 7, 2016)
[5]. D. Bisson, "5 Social Engineering Attacks to Watch Out For," March 2015,
[6]. http://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/ (accessed April 7, 2016)
[7]. S. D. Applegate, "Social engineering: hacking the wetware!" *Information Security Journal: a Global Perspective*, vol. 18, 2009, pp. 40-46.
[8]. K. Manske, "An introduction to social engineering," *Security Management Practices*, November/December 2000, pp. 53-59.

About the authors

Matthew N.O. Sadiku is a professor at Prairie View A&M University, Texas. He is the author of several books and papers. He is a fellow of IEEE.
Adebowale Shadare is a doctoral student at Prairie View A&M University, Texas. He is the author of several papers.
Sarhan M. Musa is an associate professor in the Department of Engineering Technology at Prairie View A&M University, Texas. He has been the director of Prairie View Networking Academy, Texas, since 2004. He is an LTD Spring and Boeing Welliver Fellow.