SOCIAL ENGINEERING: THE ART OF HUMAN ATTACK

Mohammed Asad Hashmi
School of Electronics and Computer Science
University of Southampton
mah1g11@ecs.soton.ac.uk

Abstract

Due to the use of electronic media for every purpose, computer crime has been widespread. We look at a new type of hacking attack, Social Engineering. This report looks into the research on social engineering. In according we discuss its types and ways of identification, and thus discuss the ways to defend against it.

1. Introduction

In this age of computers, there is a high risk of computer crime. Be it with the use of malware, spyware or hacking mechanisms. Confidential data is stolen and exploited for personal benefit. The use of antivirus software and firewalls can help us erase out and make our systems risk free, but there is one element which no hardware or software can identify and stop. It's the human factor, the users of the system. An attacker takes advantage of this. It's a human factor to help people when they are in some need and help and trust them without any verification. A social engineer tries to exploit this factor in order to help himself with such techniques to get the information he wants [1]. A courtesy of letting someone in, because they have forgotten their ID which the scanner uses to authorize the person can undermine the organization's security.

2. What is social engineering?

"Social engineering is defined as an attack in which an attacker uses human interaction to obtain or compromise information about an organization or its computer system "[US CERT. 2009].
"Social engineering is the 'art' of utilizing human behavior to breach security without the participant (or victim) even realizing that they have been manipulated."[2].Massive dependency on digital media have forced the evolution of better spyware and malware systems which identify and block any malicious threat causing systems entering the system. In addition firewalls and security measure which are better a deal threat to the hackers. But social engineering targets the weakest components of the whole system – the human users, and thus no hardware or software can detect a software engineering attack. Social engineering attacks are a success as no formal training is employed to educate people about it.

2.1 Types of Social engineering attacks

Pretexting

Pretexting is the act of creating a situation in which the chances of the victim to divulge information or perform actions increase compared to that in a normal scenario [3]. This technique can be used to find any valuable information that would help the

attacker to exploit more into the system and gain a better access. Preparing some answers beforehand in order to validate authority and impersonate himself would make it easier for the attacker to get information from the victim.

Diversion theft

It's played as a "con" game and also known as Corner game. An example would be persuading a transport or courier company to deliver the consignment elsewhere from the original destination.

Phishing

Phishing is a technique of attempting to gain information such as passwords, usernames, credit card numbers etc. by masquerading as an authorized and trustworthy entity. An exact of replica of a website of an authorized firm is made and the user is made to enter valuable information into it which the attacker utilizes for personal benefits.

IVR or Phone Phishing (Vishing)

"Vishing is the practice of leveraging IP-based voice messaging technologies to socially engineer the victim into providing personal, financial or other confidential information for the purpose of financial reward. The term "vishing" is derived from a combination of "voice" and "phishing."[4]. Pre-recorded messages could be used instead of an IVR. The attacker could send an email to a customer of a bank that certain information has to be provided and could give a certain toll free number which would be forwarded to him. He could use prerecorded messages so that the customer would not suspect anything and ask for confidential information from the customer.

Baiting

In this attack, malware infected physical media is left at locations (bathrooms, parking lots etc) for the victim to pick up and plug into his computer. As soon as the victim uses the physical media, a Trojan is run which sends back all the password and information to the attacker. In one firm, 15 of the 20 baited Trojan USB drives were picked up by the employees from the parking lot. All had plugged the USB drive into the computer computers leading to all vulnerable information being sent to the attacker [5].

3. Impact of social engineering

Social engineer has a significant impact on the security of an organization. Many organizations have suffered due to less training given to their employees about the social engineering attacks.

For example PayPal, the online payment company experienced a social engineering attack. PayPal customers had received an email in which they were asked the account holder to re-enter and thus verify their credit card data. The e-mails looked exactly the same as those sent by Paypal , as it had the exact same Paypal logos and typefaces. When the accountholders replied to that email with their information, it was straight sent to the hacker and he was able to exploit it[6].

Such attacks can erode the good name of an organization and disgruntle the long kept relationship of the customers with the organization. Though these attacks seem to be from an outsider trying to "get in", experts seem to have found out that most violations are caused by the people working the organization and having direct or indirect access to the systems[7]. Kevin Mitnick , an infamous hacker in the 1990s said to BBC news Online 6 in an interview that the biggest threat to security of a company need not be a computer virus , a backdoor entry into the program or a bad firewall but it could be you. He said its easier to manipulate people rather than technology because most of the time the organizations overlook the human element.

4. Defending against social engineering attacks

A multi-faceted approach must be employed to secure an organization against successful SE attacks using policy, procedures, training, awareness programs, and incident response plans. Well-defined policy should establish an information classification

system that clearly defines not only what information can be disclosed but also to whom and by whom. The previous implies that the organization also assign a security clearance level to individuals both inside and outside of the institution. Policy takes decision-making out of the hands of the employee and gives them justification for not "helping out."Education on what information a social engineer can use, how he gains it, and how it can be used is very important, especially for the non-technical (read "most") employees of an organization[8]. Kevin Mitnick gives some tips on how to identify a SE attack [9].

- Refusal to give a callback number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of noncompliance
- Show discomfort when questioned
- Name dropping

Victor, Julian and Christian in their paper have employed the ontological semantic technology to detect insider threat and social engineering. They have maintained repositories with which they compare a human speech in order to identify the point of interest of a person with conflicting contradictions in the speech [10]. Similar checking standards of talking time and speech study are suggested by T Qi [11]. Accordingly use of neural networks is also employed to identify social engineering attacks [12].

5. Summary

Social engineering attacks are widespread as people have no knowledge about the attacks. Though some people feel that as it involves human factor there is no easy way to identify an attack and defend against it, new ways are being found out on how they can be identified and defended against.

References

1. An Attack Vector for Deception Through Persuasion Used by Hackers and Crakers. Hasan, M.I.; Prajapati, N.B. Networks and Communications, 2009. NETCOM '09. First International Conference on Issue. IEEE Xplore

2.The Threat of Social Engineering and Your Defense Against It. R Gulati - SANS Reading Room, 2003

3. "HP Pretexting Scandal by Faraz Davani".Scribd, Retrieved 2011-8-15

4. The vishing guide ,G Ollmann - IBM Global Technology Services, May 2007 - infosec.co.uk

5.National Security Institute's (www.nsi.org) online 'Employee Information Awareness Service' URL: http://nsi.org/SSWebSite/TheService.html

6. Rosencrance, Linda. "Online Payment Service PayPal hit by scam". Computerworld, September 27, 2002.

7. R Gulati - SANS Reading Room, 2003 - course.ccert.edu.cn

8.Social Engineering: The "Dark Art" Tim Thornburgh. InfoSecCD '04 Proceedings of the 1st annual conference on Information security curriculum development.

9. Mitnick, K. & Simon, W. (2002) *The art of deception:Controlling the human element of security*. Indianapolis,Indiana: Wiley Publishing, Inc. p. 333.

10. Victor Raskin , Julia M.Taylor and Christian F. Hempelmann. Purdue University . Ontological Semantic Technology for Detecting Insider Threat and Social Engineering . NSPW '10 Proceedings of the 2010 workshop on New security paradigms .

11. "An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering" T Qi - Intelligence and Security Informatics, 2007 IEEE, 2007 - ieeexplore.ieee.org

12. Social Engineering Detection Using Neural Networks Sandouka, H.Cullen, A.J. Mann, I.CyberWorlds, 2009. CW '09. International Conference on Issue Date: 7-11 Sept. 2009 .

Bibliography

1.Social Engineering Fundamentals Part I: Hacker tactics Granger - Security Focus. Disponible, 2009 - knowyourenemy.eu

2. Social engineering: Concepts and solutionsfrom cpecourses.comTR Peltier - Information Systems Security, 2006 - cpecourses.com

3. Social Engineering: The Art of Human Hacking by Paul Wilson and Christopher Hadnagy , Wiley Publications ISBN: 978-0-470-63953-5.

4. Hacking the Human: Social Engineering Techniques and Security Countermeasures ISBN-13: 978-0566087738

5. G Conti, T Babbitt… - Security & Privacy, IEEE, May- June 2011

6. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems .Gregory L. Orgill, Gordon W. Romney, Michael G. Bailey, Paul M. Orgill . CITC5 '04 : Proceedings of the 5th conference on Information technology education.

7.Two methodologies for physical penetration testing using social engineering .Trajce Dimkov, André van Cleeff, Wolter Pieters, Pieter Hartel. ACSAC'10:Proceedings of the 26th Annual Computer Security Applications Conference.

8.Social engineering: a serious underestimated problem.Guido Rößling, Marius Müller.ITiCSE '09:Proceedings of the 14th annual ACM SIGCSE conference on Innovation and technology in computer science education.

9. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers by Kevin D. Mitnick and William L. Simon . ISBN: 978-0764569593.

10. The use of formal social engineering techniques to identify weaknesses during a computer vulnerability competition. Derek Kvedar, Michael Nettis, Steven P. Fulton. Journal of Computing Sciences in Colleges, Volume 26 Issue 2

11. Social engineering: Concepts and solutionsfrom cpecourses.com TR Peltier - Information Systems Security, 2006 - cpecourses.com