iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** IX **Month of publication:** September 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Social Engineering

Abhishek Mahajan[1], AkashVerma[2]

***Abstract*— There are several techniques available to a hacker for breaching the Information Security defenses of an organization. The human approach often termed 'Social Engineering' and is probably the most difficult one to be dealt with. This paper describes Social Engineering, common techniques used and its impact to the organization. It discusses various forms of Social Engineering, and how they exploit common human behavior. The document highlights ways and means to counter these attacks, and also emphasizes on the importance of policy enforcement and user education in mitigating the risks posed by Social Engineering.**

***Index Terms*—Dumpster Driving, Phishing, Spying, Vishing.**

I. INTRODUCTION

Social engineering is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software–that will give them access to your passwords and bank information as well as giving them control over your computer.

Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password (unless the password is really weak).Security is all about knowing who and what to trust. Knowing when, and when not to, to take a person at their word; when to trust that the person you are communicating with is indeed the person you think you are communicating with; when to trust that a website is or isn't legitimate; when to trust that the person on the phone is or isn't legitimate; when providing your information is or isn't a good idea.

II. WHAT IS SOCIAL ENGINEERING?

Social Engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or a simple fraud, the term typically applies to trickery for information gathering or computer system access. In most of the cases the attacker never comes face-to-face with the victims and the latter seldom realize that they have been manipulated.

III. PERSONAL SOCIAL ENGINEERING

In the event social engineering is used on a personal level, friendship and trust may be taken advantage of to obtain information. In the above scenario, Frank uses direct persuasion by asking Susan for her user name and password since he "forgot" his. It is possible this scenario is true; Frank may have in-fact lost his account information. Let's suppose Frank is not being entirely truthful. Using Susan's account information, Frank is electronically enabled to acquire Susan's digital identity. While logged onto the organization's network as Susan, Frank decides to view prohibited content. System logs reveal that this violation occurred on Susan's account. Susan is held liable and terminated for violation of company policy.Obviously the only thing Susan did wrong was disclose her account information to Frank. It is important to keep confidential information confidential by not disclosing information to other parties. The personal level of social engineering is not a new topic; it has been around for years and continues to be a vulnerability to personal information.

IV. WHY SOCIAL ENGINEERING

Social Engineering uses human error or weakness (i.e. 'cognitive biases') to gain access to any system despite the layers of defensive security controls that may have been implemented. A hacker may have to invest a lot of time & effort in breaking an access control system, but he or she will find it much easier in persuading a person to allow admittance to a secure area or even to disclose confidential information. Despite the automation of machines and networks today, there is no computer system in the world that is not dependent on human operators at one point in time or another. Human interfaces will always be there to provide information andperform maintenance of the system.

V. KEY CHALLENGES

Despite the humungous security threat posed by Social Engineering, very little is ever highlighted about it. Primary reason for the lack of discussion about Social Engineering can be attributed to shame. Most people see Social Engineering as an attack on theirintelligence and wit, and no one wants to be considered ignorant or dumb to have been duped. This is why Social Engineering gets hidden in the closet as a "taboo" subject, whereas the fact is that no matter who a person is, he / she may be susceptible to a Social Engineering attack.

VI. CATEGORIES OF SOCIAL ENGINEERING

There are two main categories under which all socialengineering attempts could be classified – computer or technology based deception, and purely human based deception. The *technology-based approach* is to deceive the user into believing that he is interacting with a 'real' application or system and get him to provide confidential information. For instance, the user gets a popup window, informing him that the computer application has a problem, and the user will need to re-authenticate in order to proceed. Once the user provides his ID and password on that pop up window, the damage is done. The hacker who has created the popup now has access to the user's id and password and is in a position to access the network and the computer system with credentials of that user. Attacks based on *non-technicalapproach* are perpetrated purely through deception; i.e. by taking advantage of the victim's human behavior weaknesses (as described earlier). For instance, the attacker impersonates a person having a big authority; places a call to the help desk, and pretends to be a senior Manager, and says that he / she has forgotten his password and needs to get it reset right away. The help desk person resets the password and gives the new password to the person waiting at the other end of the phone. The attacker now has all the access to perform any malicious activity with the credentials of actual user.

VII. TECHNICAL ATTACK VECTORS *PHISHING*

This term applies to an email appearing to have come from a legitimate business, a bank, or credit card company requesting "verification" of information and warning of some dire consequences if it is not done. The letter usually contains a link to a fraudulent web page that looks legitimate with company logos and content and has a form that may request username, passwords, card numbers or pin details.

Vishing

It is the practice of leveraging Voice over Internet Protocol (VoIP) technology to trick private personal and financial information from the public for the purpose of financialreward. This term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physicallocations which are known to the telephone company, and associated with a bill-payer. However, with the advent of VoIP, telephone services may now terminate in computers, which are far more susceptible to fraudulent attacks than traditional "dumb" telephony endpoints.

Spam Mails

E-mails that offer friendships, diversion, gifts and various free pictures and information take advantage of the anonymity and camaraderie of the Internet to plant malicious code. The employee opens e-mails and attachments through which Trojans, Viruses and Worms and other uninvited programs find their way into systems and networks. He or she is motivated to open the message because it appears to offer useful information, such as security notices or verification of a purchase, promises an entertaining diversion, such as jokes, gossip, cartoons or photographs, give away something for

nothing, such as music, videos or software downloads. The outcome can range in severity from nuisance to system slow-down, destruction of entire communication systems or corruption of records.

Popup Window

The attacker's rogue program generates a pop up window, saying that the application connectivity was dropped due to network problems, and now the user needs to reenter his id and password to continue with his session. The unsuspecting user promptly does as requested, because he wishes to continue working, and forgets about it. Later it is heard that there has been an attack on the system, but it never realized that that he / she was the one who opened the gate!

VIII. NON-TECHNICAL ATTACK VECTORS PRETEXTING/IMPERSONATION

This is the act of creating and using an invented scenario (the pretext) to persuade a target to release information or perform an action and is usually done over the telephone. It's

more than a simple lie as it most often involves some prior research or set up and makes use of pieces of known information (e.g. date of birth, mother's maiden name, billing address etc.) to establish legitimacy in the mind of the target.

Dumpster Diving

Seldom would someone think that throwing away junk mail or a routine company document without shredding could be a risk. However, that is exactly what it could be, if the junk mail contained personal identification information, or credit card offers that a 'dumpster diver' could use in carrying out confidential information from the hard disk of a computer as there are numerous ways to retrieve information from disks, even if the user thinks the data has been 'deleted' from the disk.

Spying and Eavesdropping

A clever spy can determine the id and password by observing a user typing it in (Shoulder Surfing). All that needs to be done is to be there behind the user and be able to see his fingers on the keyboard. If the policy is for the helpdesk to communicate the password to the user via the phone, then if the hacker can eavesdrop or listen in to the conversation, the password has been compromised. An infrequent computer user may even be in the habit of writing the id and password down, thereby providing the spy with one more avenue to get the information.

IX. DEFENDING AGAINST SOCIAL ENGINEERING ATTACKS

Tools and techniques exist to prevent social engineering attacks. Using these tools creates a lesser vulnerability to the organization or person(s) involved in a potential attack. Many of the concepts discussed pertaining to organizational security may also be used in personal security.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 (Twitchell, 2006). Educated users through training and awareness may be more reluctant to disclose personal information in turn creating less of a vulnerability to themselves or their organization. Policies should be in effect instructing users on the proper handling of company information and user data. Audits must be conducted to ensure the users of the organization are compliant with 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. Destroying the data cuts off the dumpster diver's sole method of data snooping.

identity theft. The unsuspecting 'trash thrower' could give the Dumpster Diver his break. Company phone books, organization charts and locations of employees, especially management level employees who can be impersonated to the hacker's benefit. Unshredded procedure and policy manuals can help the hacker to become knowledgeable about the company's policies and procedures, and thus be able to convince the victim about their authenticity. The hacker can use a sheet of paper with the company letterhead to create official looking correspondence. A hacker can retrieve

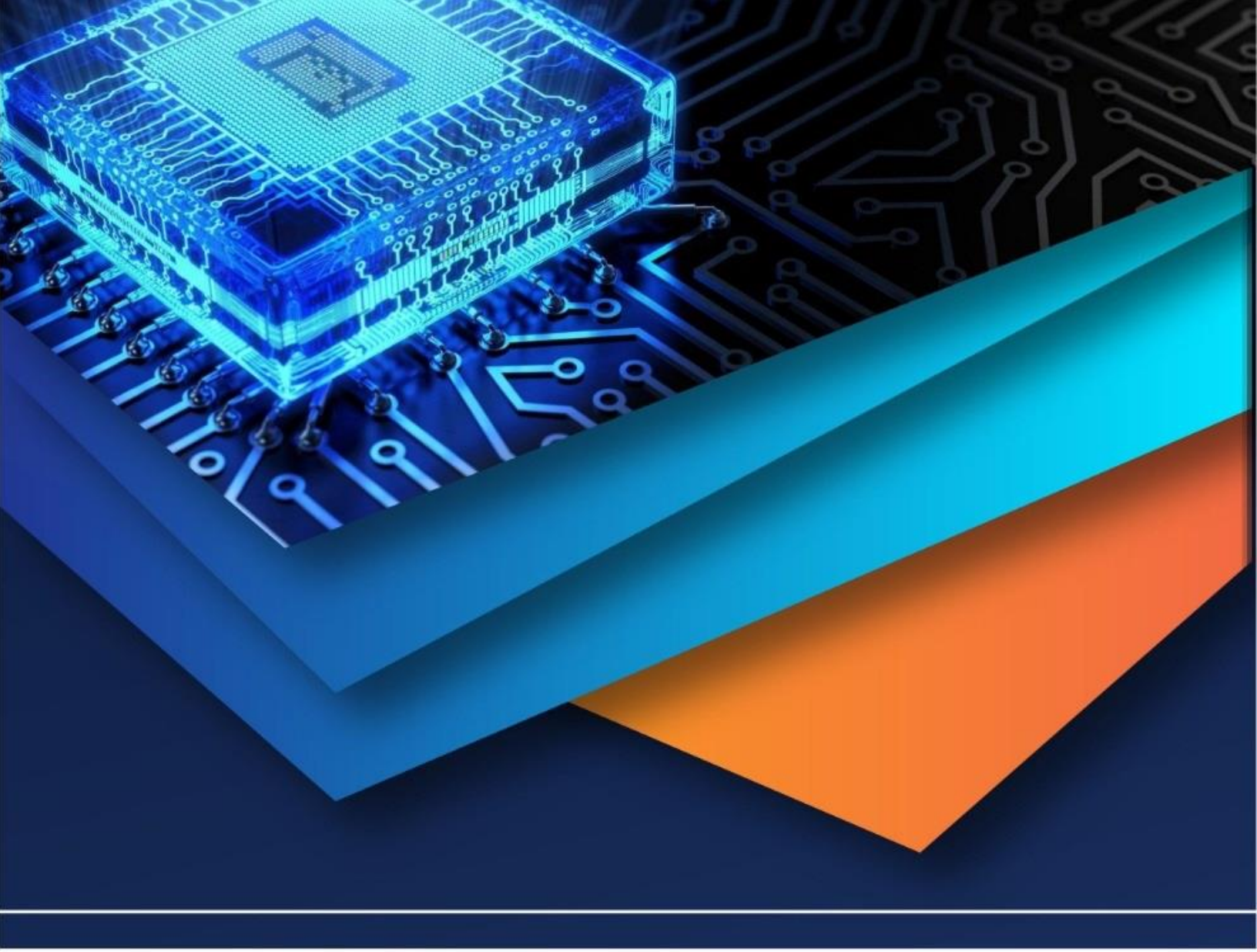
X. CONCLUSION

Social engineering is not a new technique of acquiring data; it has been around for years. Social engineering may take place on a physical, social, and electronic level. Common social engineering attack techniques include dumpster diving, the physical act of acquiring data from personal or organizational garbage; shoulder surfing, the act of acquiring data by looking at the information as it is being used by the owner; phishing, the act of sending a fictitious email or hosting a fictitious Web site constructed to mimic a legitimate site with the sole purpose of acquiring personal information; and spear phishing, a more specific, broad-area phishing attack. Tools and techniques exist which, if used and enforced, will prevent most of these social engineering attack techniques. The main concept to consider when actively protecting confidential information is the art of "using common sense." If something seems too good to be true, it probably is. Do not release any information to anyone unless you are sure they are legitimate. If there is any doubt of the legitimacy of a situation, do not disclose any information. Once your information is disclosed, you or your organization may have been put at risk for identity theft.

REFERENCES

[1] http://www.microsoft.com/technet/security/midsizebusiness/topics/complianceandpolicies/socialengineeringthreats.mspx
[2] http://en.wikipedia.org/wiki/Social_engineering_%28security%29
[3] http://en.wikipedia.org/wiki/Dumpster_diving

[4] http://www.cisco.com/web/about/security/intelligence/mysdn-social-engineering.html
[5] http://www.windowsecurity.com/articles/Social_Engineers.html
[6] http://www.gartner.com/gc/webletter/security/issue1/article1.html
[7] www.cert-in.org.in



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY