The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.44 e-ISSN: 2251-7545

Importance of Social Engineering in Community Knowledge

Bader A. Alyoubi
King Abdulaziz University
balyoubi@hotmail.com

Adel A. Alyoubi
Jeddah, Saudi Arabia

Abstract —**This report has examined the role of social engineering with reference to the computer security community.Social engineering is a method used by fraudsters to fool and cheat people into revealing their passwords and usernames and other confidential information such as server details, organisation access information and other confidential information. The hacker can then use this information to enter the computer network, steal data and carry out other attacks. Social engineering is regarded as being more dangerous since it does not require expert programming skills that hacking does. The report has examined different types of social engineering methods and techniques and the methods used to fight such social engineering attacks. A few incidents of such attacks are also presented. The main issue that has emerged is that the social engineer is now also an expert hacker who combines the skills of a fraudster with that of an expert hacker. This has increased the sophistication and skills of the attack. The paper recommends that a primary and secondary study should be undertaken to evaluate how social engineering attacks are carried out and prevented by the security community of various organisations.**

Keywords— social engineering, computer fraud, hacking, phishing, pharming ;

I. INTRODUCTION

Social engineering is "the deliberate manipulation of people to win their trust and to make then unwittingly
divulge information of confidential nature such as password or opening the doors of a highly secure area where archives and data is stored".

A. It is one of the severe threats faced by the computer and Internet security community. It requires very little technical expertise and people with good communication skills who know how to cheat people can obtain passwords and access to confidential information with relative ease. The need for computer and cyber security has increased to a high level. Billions are invested in security products, tools and fire walls that can deter even the most highly skilled hacker. A hacker attempting to hack into a bank or a large cooperation would need a high level of expertise, months of programming techniques and the help of other hackers to break into a firewall and a securely guarded computer network.

B. However, a social engineer can use fraud, deception, impersonation to fool an employee into revealingpasswords and other authentication to help a hacker gain access into a system on which millions have been spent to make it safe. Such exploits caused losses of 929 million USD in 2005 and the attacker spent very little efforts and skill in hacking the system.

C. Even the most powerful security products and security experts cannot provide protection against human foolishness, gullibility and they cannot provide security solutions against an otherwise honest employee who reveals passwords or even login a purported expert who has come to check the computer for 'malfunction'. The damage caused by such social engineers can be immense since the person who has unwittingly revealed confidential details would remain quite for fear of ridicule or censure. In the meantime, the social engineer would continue to steal information or damage the internal network, install Trojans and other spyware and his activity would not be evident until it is too late.

D. Considering all these aspects, the paper will discuss the 'role of social engineering in the security community knowledge'. The paper will also examine the subject of social engineering and asses different methods used to attack and compromise the system, present different case studies of such incidents and discuss various methods used to counter social engineering.

II. RESEARCH PROBLEM

The research problem that will be investigated is as follows. Social Engineering is a growing phenomenon
and the number of exploits and attempts are increasing. Current research only focuses on some well-known methods such as phishing. However, many other methods such as IVR

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

and phone phishing, baiting, diversion theft, pretexting, quid pro quo, tailgating and others exist that are non-technical in nature. The term 'non-technical' means that the attacker does not use malicious code or expert hacking skills to gain access. The aim of this paper is to research the most important and effective of these methods and research ways in which these methods are countered.5 Some incidents of social engineering will be assessed.

III. LITERATURE REVIEW

This chapter provides a literature review of important subjects related to social engineering. These are
discussed in the next sections.

A. Receptivity of social engineering targets

According to Barr,[6] social engineering works when people become victims for different reasons. These are
related to the psychology of the person and the factor with which he becomes a victim. These factors are authority,
kindred spirit, reciprocation, scarcity and opportunity, timing, conformity and social validation and desire to be helpful. This is similar to becoming a victim for a fraud scheme and a person becomes a victim mainly because of the gullibility. It is also possible that an attacker would assume multiple factors or a combination of factors. According to Luo,[7] in the authority factor, the social engineer would forge a level of authority that fools the victims. As an example, the hacker would attempt to pass off as a senior executive, security consultant, police officer or other people who are by nature brash and arrogant. In the kindred spirit factor, the social engineer would try to appeal and bond with the potential victim. He would claim some shared perspective, experience, and people would trust him since he would also be seen as a person of authority. In the reciprocation factors, the social engineer would provide an unsolicited favour for the target. The recipient would then try to return the favour by accepting small favours in return. In the scarcity and opportunity, the victim is often rushed into feeling that there is a good offer or discount running for a short time. The victim is then required to login to a website and enter personal details.
In the timing factor, the social engineer would make use of disasters and events such as the hurricanes and
typhoon that struck USA, earthquakes and other events. The social engineer makes use of such causes to play on the sympathies of the victims who may then login to a dedicated site and donate funds using their credit cards. In the conformity and social validation, the targets may form their decisions on how the other behaves. The desire to be helpful indicates that they not essentially be naive but that they would work under the assumption that people are good and that cheats would not take advantage of good people. However, this is not always the case since thieves are known to steal even from the Church donation box for poor people and for orphans. This last factor is often the most common factor that results in social engineering attacks. The next section examines some methods and tools used in social engineering attacks.[8]

B. Threats to organisations

In the previous section, some common factors that made people fall victims to social engineering attacks
were discussed. In this section, specific tools and methods used in the attack are discussed. It would appear that many of these fraud techniques were in use a long time before computers were even invented. Some of these methods are:
Pretexting: In this technique, a scenario is invented where a hoax is created that will convince the victim to
react. Some prior research is also made where details such as insurance policy number, credit card number, social security number, the last bill amount and other such details are given to the victim to indicate that the attacker has legal and valid information. The victim is then made to divulge important passwords and further confidential details or just 'confirm' details such as the date of birth, name of children and spouse, etc. This information is again used after some days to obtain more information. Many private investigators that need evidence for court cases use such method to obtain the required information. In some cases, the attacker calls up the landline number and speaks to a child or the homemaker and coaxes them into revealing sensitive information[.9]
Diversion theft: Also known as 'round the corner game' in this type of attack, the victim is made to run
around the corner to get problems and issues resolved. Invariably, confidential information is leaked out.[10]
Phishing: This is one of the most widely published methods of attack. Some level of programming and
coding skills are needed or the attackers may work in teams made up of expert hackers with programming skills and the other made up of customer facing people. The attacker sends an email that is forged with credentials of some authority such as the police, bank, income tax, the government, passport office or even the visa and immigration department. A link is also given that takes the user to an authentic looking website of a designated authority. Techniques such as email spoofing are used. Once the user reaches the site, either a malware is embedded in the user's browser or the user enters his login details and the attacker then misuses this information to steal the information. This has become a very effective and cheap way of social engineering[11]. Please refer to Appendix 'A3. Phishing Workflow' to see an illustration of how the attack is carried out. This is also called as 'Pharming'. Different types of phishing techniques are spear phishing where specific firms and individuals are targeted rather than mass phishing mails. Clone phishing involves taking over a previously delivered

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

email and attachment. This mail is then doctored to include links and attachments that are malicious in nature. Whaling is another form where high ranked officials and managers are targeted.[12] Since words and phrases are often detected by anti-virus filters, some attackers use images that are linked to the malware sites. Some attackers use images and even short movie clips of enticing and adult themed sites to fool customers. Website forgery techniques involve not only creating a cloned website but also using Java commands to change the URL address bar. When the user enters a genuine address of a bank such as Citibank, the forged URL bar will replace the original bar and the user is directed to the forged website. In some cases, 'tabnabbing' is used where a user who clicks multiple tabs in a website is directed to a forged site. 'Evil Twins' involves creating fake wireless networks that look the same as legal public network placed in coffee shops and airports. When a user logs into the system the passwords or credit card information is retrieved. In some cases, a false call from a phone-banking officer of a reputed bank where the user has an account is made. The user is then asked to authenticate by entering his login and PIN details.13 Please refer to Appendix. 'A1. Phishing Example 1' and A2. Phishing Example 2 to view
examples of phishing mails.

Phreaking: This is a case where people with experts in telecommunication and phones attempt to attack
the phone service provider or even large corporate. The term originates from the words phone and freak meaning someone who uses the phones to carry out attacks. Initially, Phreaks just wanted to use their skills to make free long distance calls. However, this changed and phreakers now use mobile networks to carry out large-scale attacks for financial benefit.[14]

IVR or phone phishing: This system makes use of forged interactive voice response system where the
caller is given a legitimate sounding version of the banks IVR system. A mail is first sent and a toll free number provided so that the user can enter the required login details. This is also called as 'vishing'. This type of attack has a much higher success rate.[15]

Baiting: This is similar to the Trojan horse attack used in ancient Greece. The attacker often provides an
infected CD Rom or USB drive either through post or by leaving it in public places such as bathrooms. When the user sees such a device, he is often curious enough to see what is in the disk. This would allow malware to be installed in the user's computer and the malicious code can spread quickly to other areas of the computer network.16

Quid pro quo: In this type, an attacker would call the main line and ask to be connected to random internal
numbers. He would then claim to be calling from the technical support team and ask about any problems. Eventually, someone who has a genuine problem would answer and give away internal links and passwords. He would also ask the user to enter a few commands for malware and this would launch virus and other Trojans. The term quid pro quo means giving something for something. Alternatively, the caller connects to the technical help desk and asks for the names of a few support people who go out on calls. The fact that such calls emerge from the internal lines mean that the call is genuine and about 90% of users fall a prey to this ruse.[17]

Tailgating: Also called as Piggybacking, this is a method where a person moves behind another person to
gain entry into a restricted space or to pass checkpoints at security gates. The attacker attempts to gain entry to an authorised and restricted space. Once inside the restricted space, the attacker attempts to mingle with the staff, strike up conversation and look out for a chance to compromise the security of the place. Such incidents can happen at entry and exit points that have swipe cards and where the security is lax and allows such incidents. Tailgating may be done to avoid paying ticket or entry fees and in some instances to avoid being marked late for attendance.18

Dumpster Diving: This is a very old method used to obtain confidential information from offices and from
printers who do not shred their waste. Offices generate a large number of waste paper and this is sometimes sold toscrap a merchant who collects the waste. Fraudsters try to collect this waste paper to examine it for internal information. Information about the firm, passwords, financial information, account numbers, internal phone numbers, letterheads, memo forms, login names and passwords, server IP numbers, details of mergers and so on can be obtained. This information is then used to carry out other forms of attacks.[19]

Reverse Social Engineering: This is an advanced method where an attacker creates an identity that
assumes a position of authority. Employees would then approach this person to seek help and in the process, give away important information. Some level of expertise and even 'insider' information may be needed to obtain the required information and set up the contacts.[20]

Emerging Threats: With increase in sophistication of technology, it appears that hackers have also
improved and improvised in their methods. New techniques of social engineering have appeared where mobile devices, hand held devices, smartphones, RFID equipped credit cards and tracking systems, medical devices such as pacemakers are being compromised. These are essentially 'soft targets' and attackers use a variety of means to target the vulnerable, sick and elderly people who may not be able to recognise the threats. Technologies such as Supervisory control and data acquisition - SCADA systems are used to by system administrators to make administration of large networks easy. SCADA systems are used by smart grids and other such

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

networks and hackers attempt to gain access to these systems using social engineering. Once entry is gained, then power can be switched on and off at will in the electricity network.[21]
Modern smartphones use different operating systems but these are written in languages such as JavaScript.
It is possible to obtain access to the communication between these smartphones by using phishing and other social engineering methods. These methods are combined with high skilled hacking work such as click jacking and crosssite scripting. Many medical devices such as cardioverter-defibrillators, pacemakers, bedside monitors, portable drug-delivery pumps and others have CPUs and an IP and they are remotely controlled by hospitals. It is possible for a hacker to gain access to these systems by calling up the sick and the disabled and obtaining credit card and other details. Radio frequency identification - RFID devices are used in tracking shipping containers, in monitoring the movement of murders and serial killers who are fitted with an ankle collar. Confidential information can be obtained by using social engineering. Many office machines such as printers, scanners, and fax machines are fitted with CPUs and IPs and they are placed on shared drives. Hackers find it much easier to ask someone to get a printout, monitor the path and password and gain entry to the network.[22]
III. III. Methods used to fight social engineering attacks
The previous section has highlighted a number of ways, techniques and tools that hackers use for social
engineering. While some of them are non-technical in their application, some of them need hacking skills. In this section, method used to combat and overcome these social engineering attacks is discussed. The discussion does not concern technical methods such as scripting, firewall configuration and other techniques. Given below is a figure that indicates the various areas of risk, the hacker tactic used for social engineering and the combat strategy that the security management team can use to fight the threats.
Figure 3.1. Methods used to counter social engineering[23]

C.

1- Creating a social engineering awareness program

An expert in social engineering and computer security comments "we have a ton of technology in place that
is specifically designed to stop buffer overflows (or detect them), catch malware (kind of a joke at this point), and protect our web applications. Yet our user population is still completely vulnerable and clueless on the signs of a breach. A fine balance between technology and user awareness needs to be accomplished and it'll never be 100 per cent but it'll be a lot better than an uneducated user population".[24] A few methods of creating awareness among the employees are given as below.[25],[26],[27]

Take up social engineering as a policy feature: it is important to make social engineering a matter of
organisation policy, similar to its business development and marketing policy. The policy must be featured in the strategic meeting of the board of directors. Policy management and implementation must be overseen by not only the chief security officer, but also a senior member of the board.

- The policy for security should be amended to cover all aspects of social engineering, possible threats and the manner in which employees can be fooled.
- Training and policy implementation: It is important that training should be given to all levels of employees, more so for lower level employees who enter data or carry out clerical tasks. These people often fall prey to social engineering not because they are foolish but because they do not know how to react when a person claiming to be from the managing director's office calls up.

Empower the victims: If an employee has fallen prey to a suspected social engineering incident, then he should be encouraged to report the matter immediately to the security office. Immunity from persecution and official action can be promised in case the employee was genuinely subjected to deception. Such promises help to embolden the victim and prevent major harm if the exploit was not reported.

There is a need to carry out risk assessment and a risk management plan to spot potential points of danger. Such an activity can help to reduce the dangers. The method recommended by European Network and Information Security Agency - ENISA should be adopted. The agency provides a checklist to evaluate information requests and four factors are considered. These are legitimacy, importance, source and timing. In the legitimacy factor, the employee should ask if the request appears as usual and legitimate. They should also ask themselves about the value of the information and the manner in which
it can be misused. The source factor involves the employees asking themselves about the authenticity of the source that asks for the password and confidential access. Timing is the last factor and it is important to see how much time is given to comply with the request.[28] If it means immediate access then there can be some doubts.

2- Social Engineering Kit

The above sections have provided some useful insight on the manner in which social engineering can be
stopped. However, a network administrator must know the vulnerabilities that can arise when a hacker uses social engineering to obtain access to the network. The Social Engineering Toolkit – SET helps to carry out such penetration testing. In this method, ethical hackers or hackers who hack a website with the permission of the subject organisation are

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

called in to conduct penetration testing of their website. The friendly hacker then uses SET to hack into a system and asses the strength of the system, its ability to resist such attacks, find points of vulnerability and he then submits a report that is then used by the security team to strengthen their system. The SET is written in Python.

As seen from the above screen, the tool can be used to launch a number of attacks against the site derby.com. In a similar manner, a number of hacking tools and backdoor entry tools are available. These require different levels of expertise and they can be used to improve the security of a system.

3- Incidents of social engineering attacks

Incidents of social engineering attacks are often eclipsed by large scale hacking attacks that take place once the security passwords and other details are revealed. In the resulting the confusion, the social engineering root cause is often hidden. However, many security services agencies often commit social engineering attacks to test the security of an organisation. Once such incident took place at Wall-mart store. A security consultant called up a Wal- Mart manager, managed to convince him that he was from the central corporate office, and wanted some urgent information. The unsuspecting manager fell a victim to the sweet talk and gave out important information.31 Granger[32] reports about an incident where a security team walked into a corporate office, in full suit and with a limousine and driver. They claimed they were from the government security audit department and that they were tasked with evaluating the security of the network. Demanding passwords and full access, they were able to make copies of confidential data, they managed to access the personal computer of the chief financial officer and made away with important data. The while organisation and the security industry was shaken by this brazen act. A number of incidents have been reported by Software Engineering Institute of Carnegie Mellon University. The archive presents many reports of how the security system of many organisations was compromised by using social engineering methods (CERT, 2002)

4- MAIN ISSUE

From the above discussions and analysis, it can be seen that social engineering has now evolved to a fine art where the social engineer also has access to high skills of a hacker. This would mean that the hacker who was earlier presumed to be social outcastes who worked alone and anonymously is now a social creature who makes direct contact with his targets, who visits offices and gains access using fraud methods. Therefore, methods to handle such socially aware hackers become more complex. The main issue and problem is "to identify the new face of the modern social engineer who not only knows about customer and human psychology but who would also have expert hacking skills".

5- IMPORTANT FINDINGS

The above sections have provided an extensive discussion on social engineering and the many issues associated with this problem. The thesis question was "role of social engineering in the security community knowledge". This is discussed as follows. Social engineering techniques can be used by even non-technical persons to gain passwords and to obtain other confidential information about a computer network. There is no need to learn complex coding and other techniques of hacking. Advances in Internet computing have unfortunately been used by hackers to attack networks with even more sophistication. The security community has implemented a large number of security measures that help to fight all types of hacking attempts using scripts and codes. However, the security community can do very little to stop a gullible employee from giving up his password and other confidential details. The solution for social engineering seems to be more oriented towards modifying behaviour, understanding psychology and the manner in which fraudsters attack. However, this does not mean that the security community can remain aloof from this behavioural problem. On the other hand, the community needs to be more alert and devise methods to beat such social engineering attackers. Thus, the role of social engineering becomes a matter of top priority for the security community.

6- CONCLUSION AND FUTURE WORK

The paper has examined the role of social engineering and its importance to the security community. From the discussions, it is clear that social engineers use deception and fraud to trick people into giving up confidential information, passwords, internal security set up, server details and so on. It was also seen that the modern social engineer also uses hacking skills and combines 'effective communication' along with hacking skills. Thus, the security community needs to be more aware and think ahead of how the system can be compromised and secured. Accordingly, some suggestions for future work are presented.

- There is a need to develop a full risk identification and management plan. All risks for social engineering should be identified for an organisation and a plan put in place to mitigate the risks.
- Studies should be done of how large organisations such as Microsoft and others control social engineering 32 Ibid Granger 2002
- Interviews and surveys should be administered to security professionals of different firms to understand how they counter such threats.

REFERENCES

The International Journal of Soft Computing and Software Engineering [JSCSE], Vol. 3, No. 3, Special Issue:
The Proceeding of International Conference on Soft Computing and Software Engineering 2013 [SCSE'13],
San Francisco State University, CA, U.S.A., March 2013
Doi: 10.7321/jscse.v3.n3.42 e-ISSN: 2251-7545

[1] Casciaro, T. and Lobo, M. (2005) Competent jerks, lovable fools, and the formation of social networks. Harvard Business Review, 83, pp. 92-98.

CERT. (2002) Social Engineering Attacks via IRC and Instant Messaging. http://www.cert.org/incident_notes/IN- 2002-03.html (accessed 23 December 2012)

[1] Granger, S., (2002) Social Engineering Fundamentals, Part II: Combat Strategies.

[2] http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies (accessed 23 December 2012).

[3] Green, J., (2011) Social Networking Threats. Faulkner Information Services. www.faulkner.com (accessed 23 December 2012).

[4] Hadnagy, C., (2011) Social Engineering: The Art of Human Hacking. NY: Wiley Publications.

[5] Howarth, F., (2010) Emerging Hacker Attacks. http://www.faulkner.com/ (accessed 23 December 2012).

[6] Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., (2011) Reverse Social Engineering Attacks in Online Social

[7] Networks. Detection of Intrusions and Malware, and Vulnerability Assessment, Lecture Notes in Computer Science, 6739, pp 55-74

[8] Josang, A., Al Fayyadh, B and Grandison. T., (2007) Security Usability Principles for Vulnerability Analysis and Risk Assessment. Proceedings of the Annual Computer Security Applications Conference - ACSAC'07, Miami Beach, USA.

[9] Karthik, R. (2011) Social Engineering Toolkit. http://www.social-engineer.org (accessed 23 December 2012).

[10] Kennedy, D., (May 2011) There is something 'Human' to Social Engineering: The Hacker News Magazine.

[11] http://magazine.thehackernews.com/article-1.html (accessed 23 December 2012)

[12] Long, J., (2008) No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing. NY: Syngress Publishing Inc.

[13] Luo, W., Liu, J., and Fan, C., (2009) An Analysis of Security in Social Networks. Dependable, Autonomic and Secure Computing, 2009. DASC '09. Eighth IEEE International Conference on 12-14 Dec. 2009, China, pp. 648- 651.

[14] Luo, X., (2011) Social Engineering: The Neglected Human Factor for Information Security Management.

[15] Information Resources Management Journal, 24(3), pp. 3-8.

[16] Mann, I., (2008) Hacking the Human: Social Engineering Techniques and Security Counter measures. London: Gower Publishing Ltd.

[17] Mitnick, K., (2004) CSEPS Course Workbook. NY: Mitnick Security Publishing

[18] Papadaki, M., Furnell, S., and Dodge. R.C., (2008) Social Engineering: Exploiting the Weakest Links: European Network and Information Security Agency (ENISA). http://www.enisa.europa.eu/activities/cert/securitymonth/deliverables/2008/social engineering?searchterm=social+engineering (accessed 23 December 2012).

[19] s260f, (2010) Phishing, anti-phishing, and social engineering. http://s260f.weebly.com/index.html (accessed 23 December 2012).

[20] Vaas, L., (August 2012) How social engineering tricked Wal-Mart into handing over sensitive information.

[21] http://nakedsecurity.sophos.com/2012/08/10/social-engineer-walmart/ (accessed 23 December 2012).

[22] Workman, M., (2008) Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, 59(4), pp. 662-674.

[1K] Justino E., Oliveira L.S., Freitas C. Reconstructing shredded documents through feature matching. Forensic Science International Volume 1I0, Issues F-G, F00I.