Journal of Multidisciplinary Engineering Science and Technology (JMEST)
ISSN: 2458-9403
Vol. 4 Issue 6, June - 2017

# Social Engineering Attacks

**Arif KOYUN**
Department of Computer Engineering
Suleyman Demirel University
Isparta, Turkey
arifkoyun@sdu.edu.tr

**Ehssan Al Janabi**
Graduate Student
Suleyman Demirel University
Isparta, Turkey
salman.ehssan@gmail.com

***Abstract*—We are living in the Internet world, and today our (own & business) life is linked with IT systems (OS). Often these systems are exposed to the risk of a hackers or virus infection, so that we all looking for a best antivirus, anti-Spyware software and install it but still the virus and hackers attacks our system. The most powerful attack on the systems is Social Engineering Attack because of this attack deals with Psychology so that there is no hardware or software can prevent it or even can defend it and hence people need to be trained to defend against it.**

**This paper is contains a complete overview of social engineering attacks, which is structured as follows: Social Engineering taxonomy are shows in section 2 which divided to Phases, types and approaches while Section 3 contains a skills of social engineering. In Section 4, provide social engineering channels. In Section 5, describe Social Engineering attacks at Mobile applications. Before concluding the work in Section 8, Detecting / Stopping Social Engineering Attacks and Preventing Future Social Engineering Attacks Fortunately are showing in section 6 and 7.**

***Keywords—attacks, infiltration, security, social engineering***

## 1. INTRODUCTION

In our daily life we spend most of our time to looking inside or work on our mobiles (computers). Thus, we share information and data with people who do not necessarily know them, or that we've already met them.

Today some of social networks like Facebook and Twitter are become the largest and most important sources of information, data exchange, and online services by virtue of its rapid growth. The social networks give full support to find new friends in addition to the exchange of data. And thus a new source of information is added to our knowledge. Clearly, most social network sites are critical with respect to user's security and privacy due to the large amount of information available on them, as well as their very large user base.[1]

At the business, Companies expect their employees to work with their own device as well as be highly mobile and flexible concerning their workspace [2] and there is an increasing trend towards expecting employees and knowledge workers to use their own devices for work, both in the office and elsewhere. This increase in flexibility and, conversely, reduction in face-to-face communication and shared office space means that increasing amounts of data need to be made available to others through online channels[3].

This huge revolution in communications and sharing information with others made the systems more vulnerable in terms of penetration by hackers especially through social engineering attacks because of Social engineering in itself does not necessarily require a large amount of technical knowledge in order to be successful [4].

Instead, social engineering preys on common aspects of human psychology such as curiosity, courtesy, gullibility, greed, thoughtlessness, shyness and apathy [5].

Research has shown that users of online social networks tend to exhibit a higher degree of trust in friend requests and messages sent by other users. As a result, the dangerous of social engineering attacks lies in the following:

1. High degree of trusting that is established between the victim and the attacker. And the victim may not be able to know that he was penetrating and theft.
2. Ease of implementation of social engineering attacks because it doesn't need a large amount of technical knowledge in order to be successful.
3. There is no hardware or software can prevent social engineering attacks or even can defend it.
4. Most large companies and news agencies signed a victim of attacks against their information systems such as Google [6], Facebook [7], and New York Times. [8]

## 2. SOCIAL ENGINEERING TAXONOMY

PHASES IN A SOCIAL ENGINEERING ATTACK**:** Although that all social engineering attacks are different from each other and as unique as that, there are many traditional attack techniques to achieve the desired results of the attack, but the attack has some of the common patterns. These patterns consist of four stages (the collection of information, the development of the relationship, exploitation and implementation) [9] or just like some authors are divided (research, hook, play and out).[10]

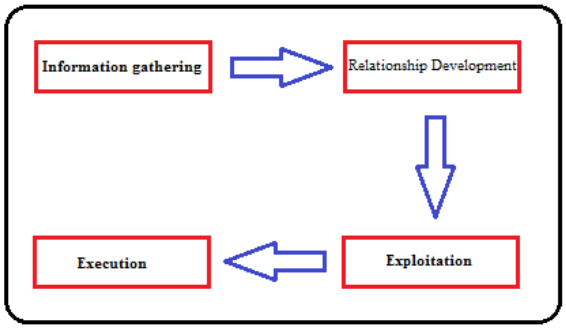


Fig. 1: *Overview of the social engineering attack phases*.

Information gathering or Research: In the information gathering phase, the attacker tries to make research about the target by gather information from various resources and means, such as dumpster diving, target website, public documents, physical interactions, and so on. Research is necessary when targeting a single user.

Relationship Development or Hook: In this phase the attacker tries to find or establish the relationship with victim by trying to start a conversation or another way in order to identify various ways which will excite the victim.

Exploitation or Play: The main purposes of this step are to make the relationship stronger by continue the dialog to get the desired information for completing the plan and built the software or create a new Spyware. Now everything is ready. The last step is execution.

Execution or Exit: This is the last phase of the social engineering attack, in which the attacker is execute the attack and stop the communication with the target without creating anything make the victim know what happened.

SOCIAL ENGINEERING TYPES: Basically, social engineering can be divided into two types according to the way that can perform it which is: human based and computer based.

Human-based social engineering: In this kind of social engineering attacks, the social engineering attack is conducted directly by a person. By other word the attacker interacts directly with the target to get information. Note that in human-based social engineering the number of targets is limited because of the lower capacity compared to an attack conducted by software.

Software-based social engineering: Software-based social engineering refers to attacks carried out with the help of system (such as computer, mobile) software to get the desired information. Examples include the Social Engineering Toolkit (SET), which can be used to craft spear-phishing e-mails [11].

SOCIAL ENGINEERING APPROACHES: Social engineering attacks are multifaceted and the attackers used it in different approaches which are:

Physical approaches: Physical approaches are some form of action the attacker performs it in order to gather information about the victim. An often-used method is searching through a trash (dumpster diving) [12]. A dumpster can be a valuable source of different information for attackers.

Social approaches: Social approaches are the most important aspect of successful social engineering attacks. In order to increase the chances of success of such attacks, the attackers often try to develop a relationship with their victims by rely on socio-psychological techniques [3] such as persuasion methods to manipulate their victims (e.g., use of purported authority). Or use most common social vector which is curiosity, (e.g., used in spear-phishing and baiting attacks). According to [11], the most prevalent type of social attacks is performed by phone.

Technical approaches: are mainly carried out over the Internet where social networking sites are becoming valuable sources of information. Attackers often use search engines to gather personal information about victims. There are also tools that can gather and aggregate information from different Web resources such as Maltego[1] that become one of the most popular tools of this area. Note that the Internet is especially interesting for social engineers to harvest passwords, as users often use the same (simple) passwords for different accounts.[11]

Socio-technical approaches:

Successful social engineering attacks often combine several or all of the different approaches discussed above. However, socio-technical approaches have created the most powerful weapons of social engineers. One of technical and social approaches examples is where the attackers exploit the curiosity of people by leave malware-infected storage media such as a USB drive containing a Trojan horse [13] in a location where it is likely to be found by future victims.

## 3. SOCIAL ENGINEERING SKILLS:

In this section described in detail some of the social engineering skills most commonly used which are:

Dumpster diving involves research in the trash of future victim to find sensitive information (such as passwords, filenames, or other pieces of confidential information) that can be used to compromise a system or a specific user account. This type of skill can be conducted by humans as well as by software.

Phishing is the attempt to acquire sensitive information or to make somebody act in a desired way by masquerading as a trustworthy entity in an electronic communication medium [3]. They are usually targeted at large groups of people. For example, those claiming to be from the lottery department and informing you that you have won a million dollars. They request you to click on a link in the e-mail to provide your credit card details or enter information such as your first name, address, age,

and city. Using this method the social engineer can gather social security numbers and network information. Phishing attacks can be performed over almost any channel (channel will show in next section), Attacks targeted at specific individuals or companies are referred to as spear-phishing. Spear-phishing requires the attacker to first gather information on the intended victims, but the success rate is higher than in conventional phishing. If a phishing attack is aimed at high-profile targets in enterprises, the attack is referred to as whaling.

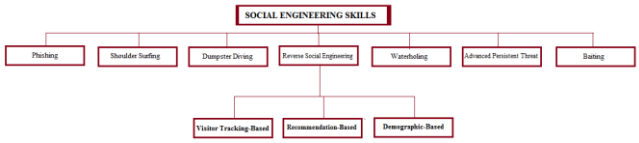


Fig. 2: *Social Engineering skills.*

Reverse Social Engineering: This type of attack is an independent technology itself is very effective, the attacker does not attempt contacting the victim directly, but makes the victim calling for her believe that attacker trustworthy entity. For example, if the attacker directly calling users on the phone and asking them for their passwords this might raise suspicion in some users. In the reverse social engineering version of the same attack, a phone number can be e-mailed to the targets a couple of days in advance by spoofing an e-mail from the system administrator. The e-mail may instruct the users to call this number in case of problems. In this example, any victim who calls the phone number would probably be less suspicious and more willing to share information as she has initiated the first contact [1].

Reverse social engineering attacks are especially attractive for online social networks because of there is a good potential to reach a lot of registered users in online social networks and it can bypass current behavioral and filter-based detection techniques that aim to prevent wide-spread unsolicited contact. As well as if the victim contacts the attacker, less suspicion is raised, and there is a higher probability that a social engineering attack will be successful [1].

Reverse social engineering RSE can be classified according to attack into four types:


Fig. 3: *Reverse Social Engineering Attack types*.

Direct Attack: In this attack, the action of the attacker is visible to the targeted users. For example, an attacker can post a message, or publish some interesting picture on a website

Mediated Attack: It is follow a two-step approach in which the baiting is collected by an intermediate agent that is then responsible for propagating it (often in a different form) to the targeted users.

Targeted Attack: In this attack, the attacker focuses on a particular user. But in order to perform this kind of attack, the attacker has to know some previous information about the target (such as username or e-mail address).

Un-targeted Attack: In untargeted attack, the attacker is just interested in reaching as many users as possible.

RSE attacks can be divided to three different combinations according to the context of online social networks.

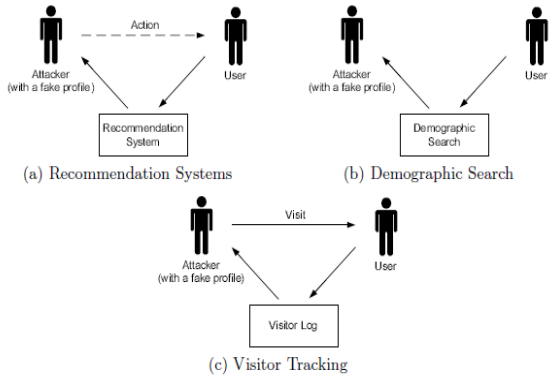


Fig.4: *Different types of Reverse Social Engineering*

Recommendation-Based RB-RSE[Targeted, Mediated] Recommendation systems in social networks propose relationships between users based on secondary knowledge on users that derives from the interactions between registered users and the friend relationships between them or background and other artifacts based on users interaction with the social network. For example, the social networking site may try to automatically identify which users know each other or might record the fact that a user has visited a certain profile in order to propose friendship recommendations. A recommendation system is an interesting target. If the attacker is able to influence the recommendation system and make the social network issue targeted recommendations, there are high ability to trick victims into contacting the attacker. Figure 4(a) demonstrates the recommendation system-based RSE attack scenario.

Demographic-Based DB-RSE [Un-targeted, Mediated] Demographic-based systems in social networks allow establishing friendships based on the information in a person's profile. Some social networks use this technique as the norm for connecting users in the same geographical location, in the same age group, or those who have expressed similar preferences. Figure 4(b) demonstrates an RSE attack that uses demographic information. In the attack, the attacker simply creates a profile (or a number of profiles) that would have a high probability of appealing to certain users, and then waits for victims to initiate contact.

Visitor Tracking-Based VTB-RSE [Targeted, Direct] Visitor tracking is a feature provided by some social

networks to allow users to track who has visited their online profiles. The attack in this case involves exploiting the user's curiosity by visiting their profile page. The notification that the page has been visited might raise interest, baiting the user to view the attacker's profile and perhaps take some action [1]. Figure 4(c) outlines this attack method.

**Table 1:** Classification of Reverse social engineering attacks according to the context of online social networks.

| RSE | RB-RSE | DB-RSE | VTB-RSE |
|---|---|---|---|
| Direct | | | ✓ |
| Mediated | ✓ | ✓ | |
| Targeted | ✓ | | ✓ |
| Un-targeted | | ✓ | |

Shoulder surfing refers to using direct observation techniques to get information, such as looking over someone's shoulder at their screen or keyboard [3].
Baiting it is a wide scale attack performed through using online adverts and websites. This includes some websites that allow the user to download, or pop-up that purport to have detected a problem with the victim's system which clicking on the pop-up will solve. Following the links provided in the bait, a user machine may automatically download malware.

Watering hole attacks are typically more sophisticated than most other social engineering techniques as they require some technical knowledge. Similar to baiting, use trusted websites to infect victim's computers where the attackers compromise a website and waiting for victim.

Advanced Persistent Threat refers to long-term, mostly Internet-based espionage attacks conducted by an attacker who has the capabilities and intent to comprise a system persistently[3].

SOCIAL ENGINEERING CHANNELS:

Attacks can be performed via the following channels:
Instant Messaging Applications (IMA) are most common channel for phishing and reverse social engineering attacks and it can also be used easily for identity theft to exploit a trustworthy relationship.
E-mail is gaining popularity among social engineers as tool for phishing and reverse social engineering attacks.

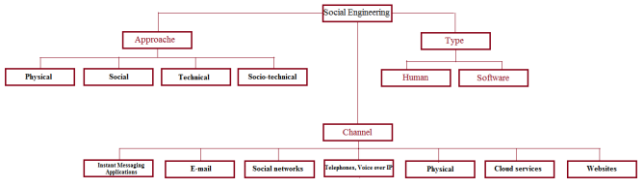


Fig. 5: *The classification of social engineering and attack channels.*

Social networks offer a various opportunities for social engineering attacks because of its ability to create fake identities and make it easy for attackers to hide their identity and harvest sensitive information.

Physical as showed some form of action the attacker performs it in order to gather information about the victim using (dumpster diving) method. Cloud services can be used from attackers to place a file or software in a shared directory to make the victim hand information over. Telephones, Voice over IP are attack channels to make the victim deliver sensitive information for attackers. Websites are most commonly used to perform watering hole and baiting attacks. Furthermore, it can be used with e-mails to perform phishing attacks. Table 2 outlines the relationship between the social engineering types, approaches, channels and attack skills. Note that many types social engineering attacks exclusively depend on a physical attack channel, such as dumpster diving, phishing, Reverse social engineering, shoulder surfing, baiting. To protect against this class of attacks, physical security needs to be improved.

**Table 2:** Classification of social engineering attacks according to our taxonomy

| | | Dumpster Diving | Phishing | Reverse Social Engineering | Shoulder Surfing | Baiting | Watering hole | Advanced Persistent Threat |
|---|---|---|---|---|---|---|---|---|
| Type | Human | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| | Software | ✓ | ✓ | ✓ | | | ✓ | ✓ |
| Approach | Physical | ✓ | | | ✓ | ✓ | | |
| | Technical | | | | | | ✓ | ✓ |
| | Social | | | ✓ | | | | |
| | Socio-technical | | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Channel | IMA | | ✓ | ✓ | | | | |
| | E-mail | | ✓ | ✓ | | | | ✓ |
| | Social Network | | ✓ | ✓ | | | | |
| | Physical | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| | Cloud services | | ✓ | | | | | |
| | Telephone, VoIP | | ✓ | ✓ | | | | |
| | Website | | ✓ | | | | ✓ | ✓ |

SOCIAL ENGINEERING ATTACKS AT MOILE APPLICATIONS:

The increase in using the mobile applications in business and a private context make the Mobile applications are an increasingly popular channel for social engineering attacks where the mobile messaging and e-mail applications are a high interest to social engineers.

The employees of companies are often tends to use their personal devices, which are computers, Mobile phones, and tablets or all of it. And it's become a policy established by companies since a close time. Therefor more employees use their smartphones to do their jobs or to check their company e-mails or to share documents with the cloud. However, many smartphone applications (such as WhatsApp [14]) can be misused to conduct social engineering attacks.

Considering that many smartphone applications are highly vulnerable and can leak sensitive information, we can conclude that such mobile devices offer a variety of attack vectors for social engineering and other attacks on user privacy. Moreover, when we setup some smartphone applications it request permissions to access sensitive data on the device. If attackers were to create such an application, they would obtain the information and could use it as a starting point for a social engineering attack.

One of authors [15] shows two different scenarios of attack can serve as a starting point for mobile applications attacks. And the other [16] discussed how inter-application information exchange can be sniffed on smartphones and then be misused to violate application policies and permissions. While in some cases, the attacker simply plagiarizes a popular smartphone application and deploys it in order to perform an attack. [17]

DETECTING / STOPING SOCIAL ENGINEERING ATTACKS:

As we stated previously there are no specific and clear way for the implementation of social engineering attacks, but we can say that use common sense is the simplest way to defend against it. If something seems suspicious it may be an attack. Following some common indicators of a social engineering attack: [18]

- Someone creating a tremendous sense of urgency to make you take a very quick decision, be suspicious.
- Someone asking for information they should not have access to or should already know.
- Something too good to be true. Such as if you are notified that you won the lottery, even though you never even entered it. Basically, for stopping Social Engineering attacks there are some steps that must dealing with it carefully:
- If you suspect someone is trying to make you the victim of a social engineering attack, do not communicate with him any more.
- If it is someone you don't know him calling you on the phone, hang up.
- If it is someone you don't know him chatting with you online, terminate the connection.
- If it is an email you do not trust, delete it.
- If the attack is work-related, be sure to report it to your help desk or information security team right away.

PREVENTING FUTURE SOCIAL ENGINEERING ATTACKS:

There are precautions you can take to help prevent exposing yourself to future social engineering attacks:
Make a strong passwords for your accounts and never share its. There are no organization will ever contact you and ask for your password. If someone does that, it is an attack.
Don't Share Too Much. Everything you shared it with others increases the chance of exposure to attack and make the attacker able to know more about you. Even sharing small details about yourself over time can be put together to create a complete picture of you. Thus it is easy to the attackers to find and mislead you into doing exactly what they want from you
Verify Contacts. At times, you may be called by some organizations for legitimate reasons such as bank, Credit Card Company, mobile service provider or other to get some information or problem. If you have any doubt about the calling whether a request for information is legitimate, don't give any Sensitive information and suggest going to an organization as well as asking the person for their name and extension number. This way although it seems like a hassle, safeguarding your identity and personal information is well worth the additional step.

## 4. CONCLUSIONS:

In this paper, we described a complete overview for social engineering attacks. And to facilitate this, we introduced a comprehensive taxonomy of attacks, classifying them by attack phases and different types of social engineering attacks and shows that attackers perform social engineering attacks over a variety of different channels. They are mostly conducted by humans as well as by software and furthermore by a different approaches as physical, technical, social or socio-technical. The boundaries of the individual types of attack are highly expandable and have, in most cases, not yet been technically exhausted as well as a detailed understanding of social engineering skills and social engineering attacks at Mobile applications.
We furthermore highlights that the majority of today's social engineering attacks rely on a combination of social and technical methods. Hence, to Detecting, Stopping and effectively protect against socio-technical attacks, user awareness for social engineering attacks needs to be improved and their devices protected on a technical level.

## 5. REFERENCES:

[1] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, and C. Pu. Reverse social engineering attacks in online social networks. Detection of Intrusions and Malware, and Vulnerability Assessment, 2011.

[2] R. Ballagas, M. Rohs, J. G. Sheridan, and J. Borchers. Byod: Bring your own device. In 'In Proceedings of the Workshop on Ubiquitous Display Environments', Ubicomp, 2004.

[3] K. Krombholz, H. Hobel, M. Huber, and E. Weippl. Advanced Social Engineering Attacks. SBA Research, Favoritenstrabe 16, AT-1040 Vienna, Austria, 2014.

[4] A CERT-UK PUBLICATION An introduction to social engineering www.cert.gov.uk, 2015.

[5]How hackers exploit 'the seven deadly sins', *BBC News* http://www.bbc.co.uk/news/technology-20717773.

[6] Google hack attack was ultra-sophisticated available online: http://www.wired.com/threatlevel/2010/01/operation-aurora/, last accessed on 2013-07-17.

[7] Microsoft hacked: Joins apple, Facebook, twitter - InformationWeek. available online: http://www.informationweek.com/security/\Attackacks/microsoft-hacked-joins-apple-facebook-tw/240149323, last accessed on 2013-07-10.

[8] N. Perlroth. Chinese hackers infiltrate New York Times computers, Jan. 2013. available at https://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html, last accessed on: 2013-07-01.

[9] M. Hasan, N. Prajapati, S. Vohara, ‘‘Case Study on Social Engineering Techniques for Persuasion’’ International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.2, No.2, June 2010.

[10] Patel, Rahul Singh, “KALI LINUX SOCAIL ENDINEERING”, UK, 2013.

[11] TrustedSec. Social-engineer toolkit, 2013. Available online at: https://www.trustedsec.com/downloads/social-engineer-toolkit/, last accessed 03/12/2013.

[12] S. Granger. Social Engineering Fundamentals, Part I: Hacker Tactics. Security Focus, 2001.

[13] S. Stasiukonis. Social Engineering, the USB Way. 2006. available at http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634, last accessed on: 2013-07-02.

[14] Whatsapp. available online: http://www.whatsapp.com/, last accessed on 2013-07-18.

[15] S. Schrittwieser, P. Fruehwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. Weippl. Guess Who Is Texting You? Evaluating the Security of Smartphone Messaging Applications. In Network and Distributed System Security Symposium (NDSS 2012), 2 2012.

[16] E. Chin, A. P. Felt, K. Greenwood, and D. Wagner. Analyzing inter-application communication in android. In Proceedings of the 9th international conference on Mobile systems, applications, and services, MobiSys '11, pages 239-252, New York,NY, USA, 2011. ACM.

[17] R. Potharaju, A. Newell, C. Nita-Rotaru, and X. Zhang. Plagiarizing smartphone applications: attack strategies and defense techniques. In Proceedings of the 4th international conference on Engineering Secure Software and Systems, ESSoS'12, pages 106-120, Berlin, Heidelberg, 2012. Springer-Verlag.