Comprehensive Analysis on Social Engineering Attacks

Subhashree K[1], Satheesh Kumar D[2]

[1] Assistant Professor, Department of Computer Science and Engineering, Karpagam College of Engineering, Coimbatore, India
[2] Assistant Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, India

ABSTRACT

In online social networking platforms like facebook, twitter, instagram etc, hundreds of millions of users makes unknown persons as friends, interacts with peoples and shares huge volume of personal information without concerning about their data security. Some group of peoples attains profit with this private data received from the users and this profit will motivate the groups to lawlessly obtain private information's further. The practice of gypping people for sharing sensitive and confidential information is called social engineering. The cyber-security threat that have been evolved and broadened in scope over the decade is social engineering, which continued to be a growing attack vector for the diffusion of malicious programs with the use of online communication tools like skype, e-mail, linkedin, dropbox etc, in various business environments resulting in decrease in personal interaction between people. Regarding e-mail threat, SMS-based second factor authentication served as the mainspring for email service providers, online markets, financial institutions and over social networks. But the attackers use deceitful tricks and persuade users to share sensitive information like authentication codes using social engineering techniques, because humans easily trust each other and disclose personal information, thus making them more endangered to social engineering attacks. Due to plenty availability of sensors and services like SMS, Bluetooth etc, smartphone is the most commonly used interactive device for sharing links, files resulting in advanced persistent threat by attackers. In this paper we are going to study various techniques used to solve social engineering cyber-crime threat in different areas.

Keywords: advanced persistent threat, attack vector, confidential information, cyber-security threat, malicious programs, online communication tools, smartphone, social engineering, social networking platforms.

I. INTRODUCTION

In every day to day life over a variety of communication channels, communication is widely distributed and the largest medium of information exchange and communication is internet. In business communications, use of social networks becomes daily routine. The trend on BYOD (Bring Your Own Device) makes large volume of data available in online communication channels [4] resulting in lack of face-to-face communication. Decentralized data access enables sharing of files more comfortable across users and publishes information using third party cloud services without concerning about privacy and security. Mostly interacting partners are trusted so well leading to security vulnerability of misusing and leaking sensitive information.

In online social network such as facebook [3], hundreds of millions of users spends hundreds of billions of minutes per month. In twitter, on an average several hundreds of tweets are reached. These online social networking platforms provides more attractive way for interacting people all over the world by enabling them to share texts, photos and videos. With the existence of large amount of online users in recent days, privacy on the online user's personal information has become very sensitive. These social networks allow users to publish their profile across others and also enable privacy protection to hide user's personal information from strangers. But still the antagonist identifies user's sensitive information through social link from friend's list across the profiles. In current business environment [7], user's personal information plays the most important role and is most valuable for many companies. They lawlessly retrieve others personal information and makes profit on it. Example: after getting the privacy information, several companies can find/make their customers by sending mail/messages to users via e-mail/mobile according to their background needs and motivate them in joining groups thereby making their personal information vulnerable to the attackers. Even though privacy settings are enables, still users information are exploited, hence apart from general settings, other settings such as access control, anonymous user identification techniques are used in recent days.

To ensure the continuity of business with minimal business risk and achieve maximum profit with best business opportunities, protection of confidential information is important from wide areas

of threat and this is called information security [2]. Even though organizations identify and classify threats to information systems to defend against attackers by applying security technologies better on networks, the attackers target on the weakest link and exploit it in security. Hence with respect to information security program, the weakest link causing problems in technological implementations under consideration are humans.

The attacker makes successful attempt in controlling the user i.e making user to disclose his/her password, open malicious e-mail content, redirecting to unauthorized websites [12] on a link click, thereby bypassing the strongest protection systems technically due to human error. Hence in information security, human users are considered the weakest link. With or without the knowledge of authorized user [32], it is possible to create threat on user-computer interface. Various semantic attacks are phishing, spear phishing, malvertisement, wifi evil twin etc. Phishing tries to access sensitive information in an electronic communication by pretending as a trustworthy entity. Spear phishing targets on a specific person or system or an organization [8]. Wifi evil twin is a fraudulent wifi access point that will spoof the nearby legitimate access points. Malvertisement is an online advertisement that installs malware.

II. SOCIAL ENGINEERING ATTACK

The process of maintaining the availability, confidentiality and integrity of data [17] along with computer networks virtual access through internet is cyber-security. When the victims hire hackers, they are labeled as ethical or white hat and are used to discover security vulnerability and also to improve cyber-security of the victim. Ethical hacking aims to protect against hacking on violating information systems and also helps in managing organizational development.

Illegal intrusion on computer networks and systems by the hackers by making social disguises, psychological tricks and cultural ploys on computer users is social engineering [2]. In the depot of malicious code writers and hackers, the strongest weapon is social engineering, because it is quite easier for them to retrieve confidential information like login credentials from the user by applying psychological tricks rather to put effort on hack and get it.

Fig.1. depicts the social engineering attack taxonomy describing the types, mode of operation and its compliance principles, medium of channel through which the attack is made, category of social engineer and used attack vectors to attain the planned goal by gaining the confidential information from the target.

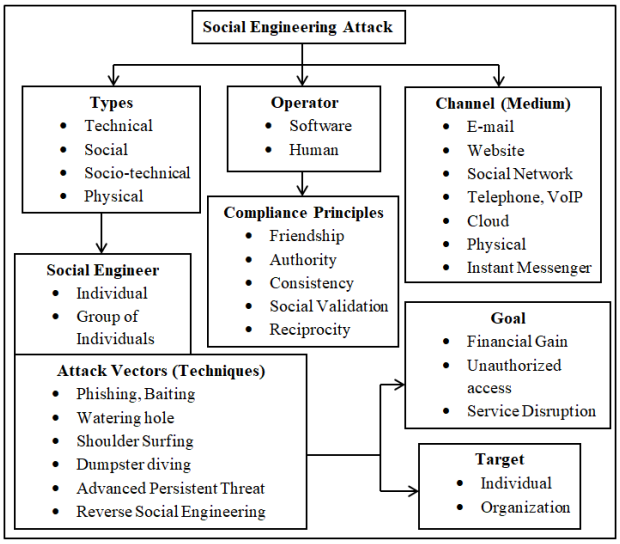

Fig.1. Social Engineering Attack Taxonomy

Social engineering targets individual or group of individuals or an organization [4]. Act of making the users to compromise their personal information is social engineering by targeting the user instead of attacking the system technically. Types of social engineering attacks [1]:

- Technology-based deceit is done through internet by using e-mails messages or through websites that façade certain communication information's of service providers at users. Example: receiving mail such as won a ticket of going to some place or won lottery and requesting to fill personal details such as bank account number, mobile number, credit card number, address etc to cover the shipping cost or like initial onetime investment.
- Social attack is done by applying psychological techniques [9] on victims and is the most commonly used attack in social engineering.
- Most of the attacks become successful by combining several techniques together. Example: in baiting attack, the attackers will leave a malware contaminated storage media (such as USB pen-drive with Torjan Horse) in victims location for him/her to find and use it so that on opening the infected media, attackers will gain the victims confidential information. Similarly

phishing through e-mail or instant messaging targets volume of people and spear-phishing attack takes place by sending messages [31] after data mining and makes the message to look like it had come from one of his/her friends.

- Human-based deceit is done by physical actions to retrieve information through telephonic calls or in person. Example: receiving calls from unknown numbers stating won cash prize being the customer in a bank based on his/her transaction and seeking for information's such as address, ATM card number, pin number, expiry date, date of birth etc. [5] This is frequently done by getting information from organizations trash namely dumpster diving. A dumpster will find the personal information of employees such as user credentials, passwords, and sensitive information on printouts which will be valuable information for the attackers [28].

The attacker's goal will be financial gain on access to unauthorized information by service disruption. Their medium of communication could be through e-mail, physical (face-to-face), SMS using instant messenger or through telephonic call [10]. The compliance principles on target will be friendship by passing friend requests, making them to commit based on position and authority of requester, social validation and favorable means of approach in communication.

III. SOCIAL ENGINEERING ATTACK PROCESS

Fig.2. shows the social engineering attack process that explains the detailed planning of attacker to gain the unauthorized confidential information.

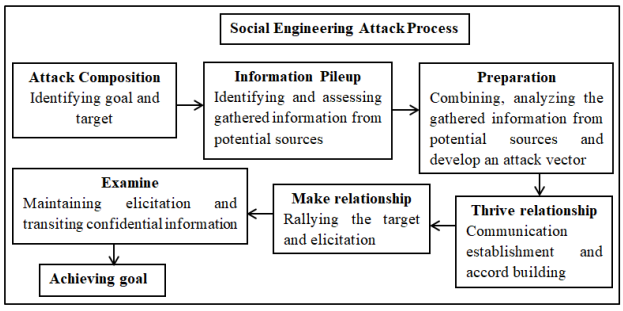

Fig.2. Social Engineering Attack Process

There are 6 phases in social engineering attack flow process [12] namely attack composition, information pileup, preparation, thrive relationship, make relationship and examine to achieve goal. Each phase will explain how the target is attacked to gain profit.

- In attack composition phase, the primary task is to identify the goal and target. First need to identify what kind of information the attacker seeks for and based on that, the target sources are identified.
- In information pileup phase, the task is to identify the potential sources among the target sources, gather required information of all the potential sources [16] and assess each of the gathered information for its correctness.
- In preparation phase, the task is to combine the information gathered of various potential sources. Analyze the information of its integrity and plan for the attack vector to be imposed on the potential users based on information gathered.
- In thrive relationship phase, the task is to establish a means of communication with the identified potential users and a kind of accord is built with them for building trust.
- In make relationship phase, the task is to make the potential sources to create rally relationship with the attacker [27], make them perform the required action and elicit the requirements as planned.
- In examine phase, the task is to maintain the trust relationship between attacker and potential user until elicitation process gets completed and once elicitation process gets over, transition of information is carried out which will confirm whether the goal is achieved.

IV. CRITICAL ATTACKING MODES

Malware:

The general term to denote viruses, trojan horses and worms that would disrupt or damage the gained unauthorized information from computer system of the user is malware. Psychological tactics are employed on users by the hackers [12] to make the social engineering malware to be successful through various communication channels. An action of malware to intrude user confidential data successfully falls into four categories [26] as follows:

- Induce the user to activate the malware by creating trust unconditionally.
- Destabilize the malware protective technologies.
- Execute the task on target.
- Disseminate required information from the targeted user.

To create threat on user computer system, various routes like websites, e-mail and social software's are used. By combining these methods, attackers apply tricks and tactics on user and make them to open an attachment in e-mail or click a malicious website link and prone themselves. On performing this action by the user with execute and activate the malicious software (malware) on their system. The malware after intruding into user system [11] will get ready and retrieve confidential information of user by making changes in security settings, download files, open backdoors etc. and these malicious actions will vary based on malware functionality.

Malware penetration channels include e-mail, websites, mobile devices, social software and portable storage devices.

- **E-mail:**

On execution of a malicious program named e-mail worm on system will escapade users e-mail capabilities and distribute the worm further. Phishing [6][2] is the most commonly used social engineering technique to thieve user's private credentials by directing users to visit fraudulent websites. Actions like resetting password, transferring funds and setting up of new user account are the ones that initiates critical authentication of the user. Phishing will make the users to believe that they are communicating with a trusted website and will make them to provide their personal information such as bank account numbers, phone number, social security numbers etc [24]. The language and padding used in e-mail messages with professional presentation will seem to have come from an authenticated source like from government or bank or any other trusted agency. Hence user will not feel suspicious about the sender of received e-mail message.

- **Websites:**

Hackers install malicious code on the most vulnerable websites. This will redirect the visitors to fraudulent websites and make them seem like legitimate websites to the visitors. Those fraudulent websites will attract the users by their appearance, images and content [23] which will create temptation on users to perform actions like clicking a link available or opening an image on that page. Vulnerable search engines also redirect the users to fraudulent webpages. The strategy involved is manipulation of words (flipping characters in words) in the web addresses. Example: replacing character 'o' with integer '0', adding or removing a character in a word of web address. Due to the frequent usage of internet in recent days, users are more aware of fraudulent e-mails and attachments. To promote malware, cyber criminals use fake anti-virus software and perform manipulation of optimization results of search engine [13]. Example: drive-by-pharming attack makes the users to view malicious attacker's code placed on an e-mail or web page and infects the user machines and this malicious code will provide the attacker full control on user's internet connection by altering the address settings. Thus by redirecting the users to fake web pages, attackers retrieve credit card information and personally identifiable information.

- **Social Software:**

Communication between individuals through a loosely connected application tracking discussions across web is the action of social software. Social network websites, wikipedia, instant messenger, blogs etc. are most commonly used social software's by enormous number of users creating opportunities for people to socialize and transfer knowledge. These volumes of users are considered as target users by the malware authors in social networks since they share personal information across each other thereby becoming the rich sources of information. Example: denial-of-service attack [14] disrupts or slows down the services. On clicking a tweet in twitter may download a malware by redirecting the user to a good-for-nothing web page. People in social networking sites make their personal information available to public thus making them more vulnerable to attacks like phishing. Also file sharing websites enables users to share files like images and videos among family and friends more frequently [22]. Here, the malware authors will place the malware-infected files in the form of images or videos or as music files and will induce user to download as well as to install the malware in their system. The worm opens backdoors and spreads even further once the user clicks on malware-infected files.

- **Portable Storage Devices:**

USB flash drives induce social engineering malware on end-user systems. Example: a malware that spreads through portable flash drive is conficker.

V. SOCIAL ENGINEERING ATTACK DETECTION TECHNIQUES

To stop the social engineering attack on individuals or a group of individuals, researchers found various detection techniques [18] and they are as follows:

- **Detection based on Machine Learning methods:**

A problem solving technique in big data [19] which is more effective in price is machine learning (ML). In business, medical and biological studies machine learning methods are expanded since these methods perform the process of extraction and obtain knowledge out of experience. For detecting malicious accounts in social media, machine learning plays a major role.

The three important categories of ML methods are as follows:

- **Detection based on Supervised learning technique:**

The goal of most commonly used supervised learning detection technique is to build a model in terms of predictor characteristics. The model will depict the class label distribution. Once the values for predictor attributes are given, the class labels for unlabeled instances will be predicted by the classifier i.e the classifier will be trained with a set of labeled accounts and based on the known characteristics, the classifier will learn to spot the real accounts and fake accounts [20]. To train the model, extracted attributes of labeled instances dataset is required resulting in construction of the classifier. The trained dataset features and efficiency will determine the performance of the model. The textual content will not be analyzed deeply when using behavioral features to train the model and it will determine user's metadata, their interactions, text counting, timestamp's and action [21]. Whereas textual content will be analyzed when using content features to differentiate fake users from real users.

- **Detection based on Unsupervised learning technique:**

The unsupervised learning detection technique works on the basis of clustering the input data without the need for labeled data to find the fake accounts. Also it does not require any feature extraction for classifying each user accounts. The unsupervised learning technique [25] will just observe the common attributes between the groups of user accounts and cluster them on the basis of resemblance between accounts. The user accounts with similar attributes are grouped into a single cluster [30]. Based on their activities grouping will be performed and the user accounts that perform any kind of suspicious activities will be considered the fake accounts.

- **Detection based on Semi-supervised learning technique:**

An intermediate between supervised and unsupervised learning technique plunge the semi-supervised learning detection technique [29]. Because, to construct the classifier, semi-supervised learning technique uses a certain volume of labeled data and a large volume of unlabeled data in order to increase the data classification accuracy as well as to reduce the collection of labeled instances cost. Based on the user interactions, the model will detect the fake accounts.

- **Detection based on Graph methodology:**

A set of points in a space is a mathematical graph with set of line segments of curve where each of which joins with itself or by two points. Pairwise relations are modeled between objects using these structures to detect threats in social media thereby representing the social networking structure. Social graph properties are used to differentiate between fake users and real users [15]. To differentiate fake users from real users, ranking based technique is followed where the fake users are ranked lower. High weight is given for real user nodes and low weight is given for fake user nodes. Supervised learning technique is used for classification of victims and graph technique is used to build network structure. Starting from the trusted user, random short walk is performed to assign low ranking to the users connected with victims.

VI. CONCLUSION

With better software development and testing, computer systems become more secure, but still the hackers creates threat and penetrate into users system and retrieve user's confidential information. The technologies as well as various security policies alone will not be enough to protect assets of various organizations from the cyber-attack. Malware is pervasive and persistent. Cyber criminals perform their attack through channels like e-mail, electronic portable storage devices, social software and websites. Fake blogs and websites are most common in recent days. Hence detection techniques on machine learning and graph based are used to detect the fraudulent accounts from the real ones and overcome from social engineering attack.

REFERENCES

[1] Richard Power and Dario Forte, Social engineering: attacks have evolved, but countermeasures have not, Computer Fraud & Security, October 2006.
[2] Sherly Abraham and InduShobha Chengalur-Smith, An overview of social engineering malware: Trends, tactics,and implications, Technology in Society 32 (2010), 183–196.
[3] Mingzhen Mo, Irwin King, and Kwong-Sak Leung, Empirical Comparisons of Attack and Protection Algorithms for Online Social Networks, The 8th International Conference on Mobile Web Information Systems (MobiWIS 2011), 1877–0509 .
[4] Katharina Krombholz, Heidelinde Hobel, Markus Huber and Edgar Weippl, Advanced social engineering attacks, journal of information security and applications 22 (2015), 113-122.
[5] Oinas-Kukkonen H and Siponen M. A review of information security issues and respective research Contributions. Database for Advances in Information Systems 2007; 38:60–81.
[6] Hossein Siadati, Toan Nguyen, Payas Gupta, Markus Jakobsson and Nasir Memon, Mind your SMSes: Mitigating social engineering in second factor authentication, computers & security 65 (2017), 14–28.
[7] Brownlow M. E-mail and website statistics. E-mail Marketing Reports; May 3, 2008.
[8] K. LeFevre and L. Fang, Privacy wizards for social networking sites, in: Proc. of WWW, ACM, 2010, pp. 351–360.
[9] P. Fong, M. Anwar and Z. Zhao, A privacy preservation model for Facebook-style social network systems, Computer Security–ESORICS 2009 (2010), 303–320.
[10] Granger S. Social engineering fundamentals, Part I: hacker tactics. SecurityFocus. 2001.
[11] Gragg D. A multi-level defense against social engineering. SANS Reading Room. March, 13, 2003.
[12] Ryan Heartfield and George Loukas, Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework, computers & security 76 (2018), 101–127.
[13] Elovici Y, Fire M, Herzberg A and Shulman H. Ethical considerations when employing fake identities in online social networks for research. Sci Eng Ethics 2014; 20(4):1027–43.
[14] Hatfield JM. Social engineering in cybersecurity: The evolution of a concept. Computers Security 2018; 73:102–13.
[15] Mouton F, Malan MM, Kimppa KK and Venter H. Necessity for ethics in social engineering research. Comput Secur 2015; 55: 114–127.
[16] Nicho M and Khan S. Identifying vulnerabilities of advanced persistent threats: an organizational perspective. Int J Inf Secur Priv 2014; 8(1):1–14.
[17] Joseph M. Hatfield, Virtuous human hacking: The ethics of social engineering in penetration-testing, computers & security 83 (2019) 354–366.
[18] Mariam Orabi, Djedjiga Mouheb, Zaher Al Aghbari and Ibrahim Kamel, Detection of Bots in Social Media: A Systematic Review, Information Processing and Management 57 (2020), 102250.
[19] Abu-El-Rub N, and Mueen A (2019). Botcamp: Bot-driven interactions in social campaigns. The world wide web conference. ACM2529–2535.
[20] Ahmed F, and Abulaish M (2013). A generic statistical approach for spam detection in online social networks. Computer Communications, 36(10-11), 1120–1129.
[21] Alothali E, Zaki N, Mohamed E.A, and Alashwal, H (2018). Detecting social bots on Twitter: A litekure review. 2018 International conference on innovations in information technology (IIT). IEEE 175–180.
[22] Andriotis P, and Takasu A (2018). Emotional bots: Content-based spammer detection on social media. 2018 IEEE international workshop on information forensics and security (WIFS). IEEE 1–8.
[23] Bara I.A, Fung C.J, and Dinh T (2015). Enhancing Twitter spam accounts discovery using cross-account pattern mining. 2015 IFIP/IEEE international symposium on integrated network management (IM). IEEE 491–496.
[24] Cai C, Li L, and Zengi D (2017). Behavior enhanced deep bot detection in social media. 2017 IEEE international conference on intelligence and security informatics (ISI). IEEE 128–130.
[25] Chen Z, and Subramanian D (2018). An unsupervised approach to detect spam campaigns that use botnets on Twitter. arXiv: 1804.05232.
[26] Chen Z, Tanash R.S, Stoll R, and Subramanian D (2017). Hunting malicious bots on Twitter: An unsupervised approach. International conference on social informatics. Springer 501–510.
[27] Kartaltepe E.J, Morales J.A, Xu S, and Sandhu R (2010). Social network-based botnet command-and-control: Emerging threats and countermeasures. International conference on

applied cryptography and network security. Springer 511–528.
[28] Libbrecht M.W, and Noble W.S (2015). Machine learning applications in genetics and genomics. Nature Reviews Genetics, 16(6), 321.
[29] Mitter S, Wagner C, and Strohmaier M (2014). A categorization scheme for socialbot attacks in online social networks. arXiv: 1402.6288.
[30] Ping H, and Qin S (2018). A social bots detection model based on deep learning algorithm. 2018 IEEE 18th international conference on communication technology (icct).IEEE 1435–1439.
[31] Varol O, Ferrara E, Davis C.A, Menczer F, and Flammini A (2017). Online human-bot interactions: Detection, estimation, and characterization. Eleventh international AAAI conference on web and social media 280289.
[32] Wang Y, Wu C, Zheng K, and Wang X (2018). Social bot detection using tweets similarity. International conference on security and privacy in communication systems. Springer 63–78.
[33] Venkateswaran N, Satheesh Kumar D (2015) Clustering based effective and ensures data dissemination in wireless sensor network" in International Journal of Modern Communication Technologies & Research (IJMCTR), Volume-3, Issue-1, January 2015 ISSN: 2321-0850.
[34] Muthu Ayyanar.v, D Satheesh Kumar, Dr.P.Ezhilarasu (2016) Energy Effective Data Collection in Problematic Disseminated Sensor Network" in International Journal on Applications in Information and Communication Engineering, Volume 2:Issue 1: January 2016.ISSN 2394 6237.
[35] K Sudhakar, D Satheesh Kumar, B Rajesh Kumar (2015) Automatic Renal Neoplasm Volumetry on Prior Shape Level Set Segmentation Method in international journal of applied Engineering Research, Volume 10 Issue: 6

AUTHORS

First Author – Subhashree K, M.E. Assistant Professor, Department of CSE, Karpagam College of Engineering, shreecourses18@gmail.com

Second Author – Satheesh Kumar D, M.E., (Ph.D), Assistant Professor, Department of CSE, Hindusthan College of Engineering and Technology, dsatheeshkumar.cse@hindusthan.net

Correspondence Author – SUBHASHREE K, shreecourses18@gmail.com, subhashree.k@kce.ac.in