Building Blocks of Social Engineering Attacks For The Organization

Shekh Abdullah-Al-Musa Ahmed, Nik Zulkarnaen Khidzir, Tan Tse Guan

Faculty of Creative Technology and Heritage, University Malaysia Kelantan, Malaysia
*Corresponding author's email: almusa.c17e002f@siswa.umk.edu.my

Abstract: In the information security domain social engineering is a methods of attacks by malicious activates . Initially it is accomplished through human interaction . Then turns the machine into mal functions . Human and machine both are similarly used in social engineering attacks. For the building block of SoE attacks article emphasize on the common relationship reference on concepts other information security issues which would be used for building blocks of SoE attacks among other security measurement . Though hundred percent information security barrier is impossible for any organization .However here discussing the various fundamental terms used in security – related topics . Showing important concepts in information classification as it forms a fundamental step toward the building blocks for SoE attacks in the organizations. Classification of business system and events was also addressed to serve as a foundation for the discussion on disaster recovery (DR) and business continuity . In this article also mentioned about an interesting technique showing the relationship among other security terms for the building blocks of SoE attacks . And discussing the methodology , that not as strong encryption but reasonably useful in some scenarios requiring protection of sensitive information.

Key words: Business Continuity , disaster recovery ,encryption , SoE, SoE attacking risk , vulnerability

1. INTRODUCTION

Social engineering is the domain of study in information security . So , it is essential for forming a right kind of background study and discussion on risk assessment of SoE attacks and analysis it , which is the cornerstone for any security management exercise in organizations (Vuorinen, 2013). Concepts development here

are important for the awareness of social engineering attacks . Showing in Figure 1.1 information security goal . These are also known as the three pillars of Info Sec.

Figure 1.1 showing information security goal . These are also known as the three pillars of Info Sec.

The reality is that security starts and stops with the human element . If that element fails , the entire system can be weakened rapidly . Social engineering attacks is a bypass attacks in the information security domain . The methods of attacks happened either by manipulation of human or manipulation of technology by spreading the malware . However , given the information overload in the present dynamic business environment , it is neither good to deal with too much information nor good to provide employee and other business entities with 'all' the data . Therefore , the organizations make data available to those concerned on a 'need' to know ' basis . For this reason this article provide the conceptual view of information classification for building block of SoE attacks in the organizations (Clay Posey, 2015). . Despite the proliferation of enterprise resource planning (ERP) systems and other integration technologies , many organizations store their related data in several disconnected systems , each of which is available to a limited number of people within specific departments . For example , an accounting system contain customer records , transactions and payment histories . Prospects or donor records may exits in a contract management system or outlook . Correspondence may exit within saved word documents on a server and email are scattered across any number of desktops in different departments (Thompson, 2010).

2. LITERATURE REVIEW

Social engineering is the context of information security area . The purpose of SoE attacks is to get confidential information from the system access . When backing to the security idea , some common term come , such as electronic security , it is like protecting the result from all measures designed to deny unauthorized persons information of value that might be derived from the interception technique or any other illegitimate means of the obtaining information . In the – repudiation by which the sender of data is provided with a proof a delivery and the recipient is

assured of the sender's identity (ID), so that neither can later deny having processed the data . This concept is connected with the concept of 'electronic signature ' . The term 'electronic signature ' refers to the process and operate on a message source authenticity and integrity , and source of non-repudiation. Whereas 'encryption' refers to the modification of data for security purposes prior to their transmission so that they are not comprehensible without the decoding method. 'cipher' is the cryptographic transmission that operates on character or bits of data. 'cryptanalysis ' being able to 'break' the cipher so that the encrypted message can be read. It can be accomplished by exploiting weaknesses in the cipher or in some fashion determining the key. ' Cryptography' refers the methods for rendering the encrypted information to an intelligible form (Sumner, 2009). The word 'cryptography' comes from the Greek words kryptos meaning hidden and graphein meaning to write . 'Denial of Service' (Dos) attacks is one kind of information security attacks where to make an online service unavailable by overwhelming it with traffic from multiple sources. Targeting a wide variety of potential resources (Downing,2010). 'Timpest' is a short name that refers to investigation ,, study and control of compromising emanation from telecommunication (TC) and automated IS equipment . This term is often used in connection with military/ defense application . 'Tempsest test' is yet another term used in connection with military / defense applications . It refers to laboratory or on –site test to determine the nature of compromising emanations associated with TC or automated IS . 'TC' and automated information system security refers the protection afforded to TC and automated IS , in order to prevent exploitation through interception, unauthorized electronic access or related technical intelligence threats and ensure authenticity . 'Spoofing' is kind of interception , alteration and retransmission of a cipher signal or data , in such a way as to mislead the recipient . Spoofing refers to an attacker deliberately including a user (subject) or a device (object) into taking an incorrect action by giving its incorrect information . 'Steganography ' is the term used in information security that is a kind of art of hiding the existence of message without causing any significant change in the image. The word ' steganography' comes from the two Greek words strgano manning ' covered' and graphein meaning ' to write' . Steganography can be detect the illegal copying of digital images (Abawajy, J. 2014). Thus , it aids confidentiality and integrity of the data . Finally the most serious information security attacks is social engineering attacks. Though there are some misconception regarding SoE attacks . This work come form political science domain. According to American journal of Society in 1894 the Dutch Industrialist J.C Van Marken (de) was used that term social engineering . But now at 21th century this word is diverted- so , it refers to influence particular attitudes and social behavior on a large scale , whether by private groups , government or media in order to produce desired characteristics in a target group . But social engineering in the domain of information security is different things . It is not an influential person but it means of technique or

mechanism or way of work to attack on people , group , business by sending malware or by psychologically manipulation of people into performing action or divulging confidential information (Major, 2009) .

3. METHODOLOGY

The domain of Info Sec , the concept of ‘ confidentiality is used in building blocks for SoE attacks . As an attempts to prevent the intentional or unintentional unauthorized disclosure of message contents . Loss of confidentiality means there are no building blocks for SoE attacks , and that can occur in many ways, such as through the intentional release of private company information or through a misapplication of network rights such as social media . Another important concept in info Sec is integrity . This concepts affects in building blocks for SoE attacks . However , the concepts of integrity ensures that Modification are not made to data by unauthorized personnel. Unauthorized modification are not made to data by authorized personnel. The data are internally and externally consistent , that is internal information is consisted among all subentries and the internal information is consistent with the real world , external situation (Tham, et al., 1991).

The last of the important triad in Info Sec is availability . Which is the main components for building blocks of Soe attacks . The concepts of availability ensure the reliability and timely access to data or computer resonances by the appropriate personal (Kim, 2013) . So , availability is necessary to building block for SoE attacks. In a words availability guarantees that the systems are up and running when they are need. It means organization’s have full building blocks against any kind of SoE attacks . In a words availability guarantees that the systems are up and running when they are needed . It means organization’s have full building blocks against any kind of SoE attacks . In addition, this concepts guarantees that the security service needed by the security practitioner are in working order . The term automated information system security is synonymous with computer security . And social engineering attacks is the domain of study of information security . Social engineering attacks is a mechanism or way to attacks in the organizations . However, identification , authentication, accountability , authorization and privacy are the information security terms , that are used for the building blocks of SoE attacks in the organizations . Identification means the user claim their identities to a system. It is most commonly used for access control and is necessary for authentication and authorization. The main target to building blocks for SoE attacks is to protect the assets such as information . As a matter of fact , social engineering attacks is one kind of psychological manipulation of human . However , authentication means by which user claim their identities to a system . It is most commonly used for access control , and is necessary for authentication and authorization. So, that strong authentication is needed for the building blocks of SoE

attacks . Whereas accountability refers a system's ability to determine the action and behavior of a single individual within a system , and to identify that particular individual . Audit trials and logs support accountability . Since employee behavior can have a big impact on the organizations. So , that it is important for accountability in the system regarding the building blocks of SoE attacks . But authorization is the rights and permissions granted to an individual (or process) which enable access to a computer resource . Once a user's ID and authentication are established , authorization levels determine the extent of system rights that an operator can hold . Thus , authorization is the access rights granted to a user , program or process . Another thing is privacy which means the level of confidentiality and privacy protection that a user is given in a system . It is an important component of building blocks of SoE attacks . Privacy guarantees not only the fundamental tenet of confidentiality of a organization's data , which is being used by the operator .

4. INFORMATION CLASSIFICATION FOR THE PREVENTION TECHNIQUE OF SOE ATTACKS

Having discussed some security terms in this article , for building blocks of SoE attacks , now turn to another important topic from information security perspective : information classification . Generally speaking , organizations like to 'classify ' their information for suitable treatment in terms of building blocks for SoE attacks . It is not possible to protect all the information in the organizations. There are several reason why the organizations (government , private , public and defense) like to classify information. The main reason is that not all data / information have the same level of importance or same level of relevance/ criticality to an organization . Some data , such as trade secrets , formulae (used by scientific and / or research organizations) and new product information (such as the one used by marketing staff and sales force), are so valuable that . their loss could create a significant problem for the enterprise in the marketplace by creating public embarrassment or by causing a lack of credibility . Events like those could damage the company's goodwill .Thus , it is obvious that information classification provides a higher , enterprise-level benefit . The primary purpose is to enhance CIA is to building block of social engineering attacks in the organizations (Manske, 2006). It is well known that in most countries , information classification has had the longest history in the government sector . It's value has been established , and it is a required component when securing trusted systems . However , in this article discussing how information classification is primary used to prevent the unauthorized disclosure and resultant failure of confidentiality due to SoE attacks .The other reason for information classification may also be the compliance required with privacy laws and legislations , or regulatory compliance . A organizations may wish to employ classification to

maintain a competitive edge in a tough marketplace . There may also be sound legal reasons for a company to employ information classification, such as to minimize liability or to protect valuable business information. In all , classification of information and information assets helps organization to apply security policies and security procedures toward protection of information assets that are considered critical (Zhou, 2015) .

Thus , the key points is that information produced or processed by an organization must be classified according to the organizations sensitivity to its loss or disclosure . These data owners are responsible for defining the sensitivity level of the data (Alan E. et al.,2006).] . This approach enables the security controls to be properly implemented according to its classification scheme . And crating the building blocks for SoE attacks .

A convincing sample collection methods was done regarding the experience of SoE attacks in the organization , there were total 87 questionnaire were distributed in the organization and 39 returns , so 44% response rate .However the experience of SoE attacking risks , respondent response were regarding suspicious mail or unexpected called , 30% had shown such experienced and 69% had shown not this type of experience.

Regarding unexpected mail 41% had not get any this type whether 58% had this experienced.

Questionnaire were asked whether employee noticed any unauthorized person without proper id worked in organization 30% respond that had never seen any type of people but 25% had this type of experience. Even what would be the decision would they take , so the response were 15% said blocked the number, 7% were respond that cancel the call, 9% were delete the mail , 20% were respond contract with security expert and 27% were respond about block the number .So the respondent table 1 would be as below .

Table 1 : Showing the respondent response table

Experience of SoE attacks_1	***f***	***Rel f***	***cf***	***Percentile***
No	13	0.33	39	100
Yes	26	0.66	26	66
Total	39			

Experience of SoE attacks_2	***f***	***Rel f***	***cf***	***Percentile***
No	12	0.30	39	100
Yes	27	0.69	27	69
Total	39			
Experience of SoE attacks_3	***f***	***Rel f***	***cf***	***Percentile***
Block the mail	12	0.30	39	100
Contract with security expert	10	0.25	25	64
Delete the mail	6	0.15	17	43
Cancel the call	3	0.07	11	28
Block the number	8	0.20	8	20
Total	39			

5. INFORMATION CLASSIFICATION: VARIOUS ROLES IN THE ORGANIZATION

From the security perspective , the role and responsibilities of all participants in the information classification program must be clearly defined . A key element of the

classification scheme is the role the users , owners or custodians of the data play in regard to the data . The role that owner , custodian and user play in information that must be classified with their responsibility . Concepts such as these are important for project leaders and project managers in software development organizations even from configuration management and data management perspective , aspects that are emphasized by continuous improvement methods such as the International Organization for Standardization (ISO) 9001:2000 and Software Engineering Institute's (SEI) , Capability Maturity Model Integration (CMM-I). These are the methods used for security purpose (Oleksandr Korchenko , 2010). And all of these used to give concept for the building blocks of SoE attacks .

6. EVENT CLASSIFICATION IN THE ORGANIZATION

The concept of disaster recovery and business continuity is important for building block of social engineering attacks . Basically disaster is an event that causes permanent and substantial damage or destruction to the property equipment , information, staff or services of the business . However , crisis is an abnormal situation that presents some extraordinary high risks to s business and that will develop into a 'disaster' unless carefully managed . Whereas catastrophe is the major disruption resulting from the destruction of critical equipment in processing . Figure 6.1 showing the relationship among the building blocks of SoE attacks with various security – related terms .

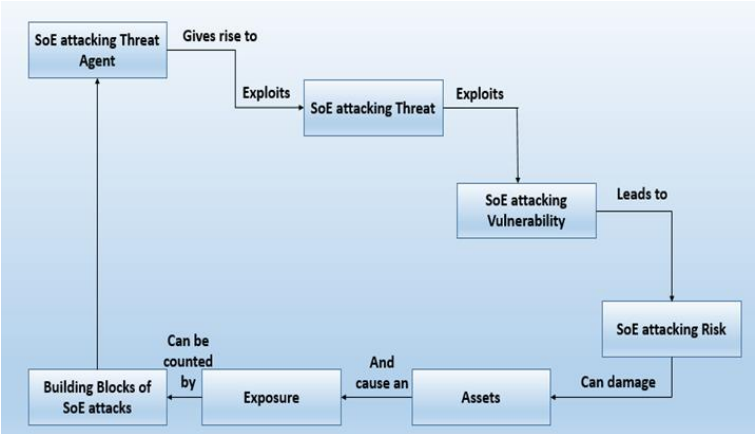

Figure 6.1 : Relationship of building blocks of SoE attacks among different security concepts

7. CONCLUSION

Information in an organizations will continue to face threats that is given global paradigm in today's digital economy . Building block of SoE attacks is one kind of management to address the security issues by forming appropriate security . The matter of security implementation is complex and all organizations must be involved to understand and commit to the relationship among other security issues for building blocks of SoE attacks . Strong encryption is best way to protect the information . But social engineering is one kind of bypass attacks happening in the information security domain . It will be an smart idea for all organization to make blocks for the social engineering attacks . In the global context for the building blocks of SoE attacks threats to the information , it is clear that many business processes do not work without reliable IT systems , so confidentiality and thus integrity and availability of information are of high importance in today's business life . So , in this article showing the concepts about how the building block of SoE attacks helps organizations to save the assets such as information.

Acknowledgments
Thanks to University Malaysia Kelantan , as done the survey for collecting data.

REFERENCES

Abdullah Algarni, Y. X. T. C. (2017). An empirical study on the susceptibility to social engineering in social networking sites: the case of Facebook. European Journal of Information Systems, Volume 26(Issue 6), Pages 661-687.

Alan E. Brill , M. P. C. M. W. (2006). The Evolution of Computer Forensic Best Practices: An Update on Programs and Publications. Journal of Digital Forensic Practice, Volume 1(Issue 1), 3-11.

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, Volume 33(Issue 3), 237-248.

Buang, M. F. M. E. A., Daud, S.M. (2012). A web-based KM system for digital forensics - Knowledge sharing capability. Proceedings of 2012 International Conference on Multimedia Computing and Systems, ICMCS 2012, Pages 528-533.

CISA, T. W. S. P. D. A. J. S. C. (2008). The Potential for a Synergistic Relationship Between Information Security and a Financial Audit. Information Security Journal: A Global Perspective, Volume 17(Issue 2), Pages 80-86.

Clay Posey, T. L. R. P. B. L. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. Journal of Management Information Systems, Volume 32(Issue 4), Pages 179-214.

Ding-Long Huang , P.-L. P. R. G. S. Perception of information security. Behavior & Information Technology, Volume 29(Issue 3), 221-232.

Downing, G. W. M. E. (2010). What Security Professionals Need to Know About Digital Evidence. Information Security Journal: A Global Perspective, Volume 19(Issue 3), 124-131.

Hinson, G. (2008). Social Engineering Techniques, Risks, and Controls. The EDP Audit, Control, and Security Newsletter, Volume 37(Issue 4-5), Pages 32-46.

Icon, V. R. K. O. I. H. S. V. O. (2018). Novel digital forensic readiness technique in the cloud environment. Australian Journal of Forensic Sciences, Volume 50(Issue 5), 552-591.

Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. Information Security Journal: A Global Perspective, Volume 22(Issue 4), 171-179.

Mohamed, N. a., Nawawi, A.a, Ismail, I.S.b, Ahmad, S.A.b, Azmi, N.A.b, Zakaria, N.B.b (2013). Cyber fraud challenges and the analysts competency: Evidence from digital forensic department of cyber security Malaysia. Recent Trends in Social and Behaviour Sciences - Proceedings of the 2nd International Congress on Interdisciplinary Behavior and Social Sciences, 581-583.

Major, S. D. A. (2009). Social Engineering: Hacking the Wetware! Information Security Journal: A Global Perspective, Volume 18(1), 40-46.

Manske, K. (2006). An Introduction to Social Engineering. Information Systems Security, Volume 9(Issue 5), 1-7.

Oleksandr Korchenko , Y. V. S. G. (2010). Modern quantum technologies of information security against cyber-terrorist attacks. Aviation, Volume 14(Issue 2), Pages 58-69.

Peltier, T. R. (2006). Social Engineering: Concepts and Solutions. The EDP Audit, Control, and Security Newsletter, Volume 33(Issue 8), 1-13.

Peltier, T. R. (2006). Social Engineering: Concepts and Solutions. The EDP Audit, Control, and Security Newsletter, Volume 33(Issue 8), 1-13.

Pieters, W. (2011). The (Social) Construction of Information Security. The Information Society, Volume 27(Issue 5).

Raman, K., Baumes, S., Beets, K., & Ness, C. (2014). Social-Engineering and Low-Tech Attacks. Computer Security Handbook Computer Security Handbook, Sixth Edition, 345-347.

Radhakrishna, G. (2012). Digital evidence in Malaysia. Digital Evidence and Electronic Signature Law Review, Volume 9, 31-41.

Sommer, P. (2004). Emerging Problems in Digital Evidence. Criminal Justice Matters, Volume 58(Issue 1), 24-25.

Sumner, M. (2009). Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. Information Systems Management, Volume 26(Issue 1), 2-12.

Thompson, S. T. C. (2010). Policies to Protect Information Systems Building Barriers to Intrusion from Social Engineering Attacks. Library & Archival Security, Volume 19, 2004 - Issue 1, Pages 3-14.

Vuorinen, P. T. J. (2013). Dissecting social engineering. Journal Behavior & Information Technology 32(10), Pages 1014-1023.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Publication cover image Volume59, Issue4, 551-564.

Tham, M. T., Vagi, F., Morris, A. J., & Wood, R. K. (1991). On-line multivariable adaptive control of a binary distillation column. Volume 69(Issue 4), 997-1009.

Taylor, R. G. (2015). Potential Problems with Information Security Risk Assessments. Information Security Journal: A Global Perspective, Volume 24(Issue 4-6), Pages 177-184.

Gaining Access with Social Engineering: An Empirical Study of the Threat. Information Systems Security, Volume 16(Issue 6), Pages 315-331.

Yusof, N. S. M. E. A., Hashim, R.Email Author, Rashim, S.N.A. . (2012). Assessment of educational divide and computer literacy among primary school students in Selangor Malaysia. ISBEIA 2012 - IEEE Symposium on Business, Engineering and Industrial Applications, 437-442.

Zhou, S. (2015). A Survey on Fast-flux Attacks. Information Security Journal: A Global Perspective, 24(4-6), Pages 79-97.