The models separation of access rights of users to critical documents of information system as factor of reduce impact of successful social engineering attacks

Anastasiia Khlobystova[a,b], Maxim Abramov[a,b]

[a] *St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, 14-th Linia, VI, № 39, St. Petersburg, 199178, Russian Federation*

[b] *St. Petersburg State University, Universitetskaya Emb., 7-9, St. Petersburg, 199034, Russian Federation*

Abstract

Problem of protection information systems from multi-step social engineering attacks is still valid for a long time. However, there are a number of unresolved issues, associated with study in this field. One of them is correctly selection configuration of access rights distribution of the organization's employees to critical documents of the information system. Namely, such a model of distribution of access rights should be chosen, which would help to reduce impact of successful social engineering attacks. To achieve this goal, two different configuration of access rights of users to critical documents of information system were considered in this study. In addition, probabilistic estimates of success multi-step social engineering attack implementation by malefactor were presented. Note that the obtained probabilistic estimates are a hybrid model of a linguistic fuzzy variable due to the parameters included in these estimates. From a theoretical standpoint, the study contributes to the development of fuzzy hybrid computing models. In addition, the results can be applied practically in the design of decision support systems in the information security field. The global applicability of the presented results is seen in the development of information systems diagnostics in terms of security against social engineering attacks.

Keywords 1

Information security, social engineering, access rights, multi-step social engineering attack, hybrid model, fuzzy hybrid computing, critical document

1. Introduction

The problem of information systems users' protection from social engineering attacks has long been relevant [1, 2, 3]. In this study, the term "social engineering attack" mean set of applied psychological and analytical methods, which attackers apply for latent motivation of users of a public or corporate network to infringements of the established rules and policies in the field of information safety [4].

Often during social engineering impact, the user is not attacked directly, but using other users associated with him. Such attacks are named multi-step social engineering attacks **Ошибка! Источник ссылки не найден.**, approaches to their analysis were presented in [6, 7].

The importance of the problem of researching multiway social engineering attacks is also emphasized in the study "Digital mess", conducted by Kaspersky Lab. Which notes that approximately every second Russian (44%) has seen confidential data of colleagues. At the same time, only 28% of users regularly check who else has access to documents and services with which they work, and make the necessary changes. Against this backdrop, it is possible to make suppose, that multi-step social engineering attacks can cause significantly more damage than direct (one-way) attacks. In addition,

Russian Advances in Fuzzy Systems and Soft Computing: selected contributions to the 8-th International Conference on Fuzzy Systems, Soft Computing and Intelligent Technologies (FSSCIT-2020), June 29 – July 1, 2020, Smolensk, Russia
EMAIL: aok@dscs.pro; mva@dscs.pro
ORCID: 0000-0002-9811-5476; 0000-0002-5476-3025
© 2020 Copyright for this paper by its authors.
Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).
CEUR Workshop Proceedings (CEUR-WS.org)

CEUR-WS.org/Vol-2782/paper_37.pdf

according to a study by the information security company InfoWatch, employees of companies who have legitimate access to personal data of users and customers often do not have basic knowledge of the rules for the safe handling of restricted information, or they deliberately ignore prohibitions and security policies [8]. That is why it is important the task of correctly selection the configuration of the distribution of access rights of users to critical documents of information system. The aim of this work is to propose various models for distribution of access rights and to calculate probabilistic estimates of the success of a multi-step social engineering attacks when a malefactor implements the most probability case for the development of the attack in the context of the proposed models.

2. Relevant works

Research about the security of information systems against technical threats has been actively developing over the years [9, 10, 11, 12, 13], but often they overlook the human factor. Nevertheless, a number of other studies [14, 15] note the importance and need for employees to comply with information security policies, and even the need for an integrated approach, namely, efficient interaction and communication between software, hardware and humans can be achieved only through an integrated manner human reliability, software failures and equipment reliability [16]**Ошибка! Источник ссылки не найден.**.

Authors of [17] raise questions to study the causes of risky behavior in the field of cybersecurity. There are also studies focusing on access behavior sensitivity, in particular, in the field of healthcare big data management [18]. One of the ways to study this behavior is to analyze user pages on social networks [19, 20]. So there is a number of works [21, 22, 23, 24] aimed at the development of automated tools for aggregate information about user from social network and drafting digital portrait of user, there are also studies aimed at analyzing the social connections of users [25]. All this is the necessary information for constructing and analyzing the social graph of the organization's employees for susceptibility to social engineering attacks. In addition, there is a study [26] aimed at security risk analysis based on concepts of partial information.

The basis for this research was the work [4, 5, 27] in which methods for analyzing the organization's information system were developed and presented in order to identify the most vulnerable places susceptible to social engineering impact. However, the questions of the influence of the access rights distribution on the level of protection against social engineering attacks were not studied in them.

3. Formulation of the problem

Let a social graph of employees of some organization *G=(U,E)* be given, where $U = \{U_i\}_{i=1}^{n}$ is set of vertices (associated with users), $E = \{(U_i, U_j, p_{i,j})\}_{1 \le i,j \le n, i \ne j}$ is set of ordered triplets with a given estimate of the probability of an attack spreading from user U_i to user U_j which is the quantified value of the linguistic fuzzy variable. Let information about critical documents available in the information system also be given: $D = \{(D_j, L_j)\}_{1 \le j \le m}$ is a set of documents of the information system with a given level of criticality. $A = \{(U_i, D_j)\}_{1 \le i \le n, 1 \le j \le m}$ is set of pairs corresponding to the users of the information system and the documents to which they have access.

Estimation of the probability of a malefactor's realization of a trajectory T in a multi-step social engineering attack according to [27] is calculated as follows:

$$p_T = \frac{1}{p_i} + \sum_{l=i}^{j-1} ln \frac{1}{p_{l,l+1}},$$

Where $T = (U_i, E_i, \dots, E_{j-1}, U_j) p_i$ is the probability of success of a social engineering attack on user *i*, and $p_{l,l+1}$ is the probability of the attack spreading from the user U_l to the user U_{l+1}.

Then the estimate of the probability that the document of the criticality level L_j will be hit when the user U_i is attacked and the trajectory T is realized will look like this:

$$H_{L_j} = 1 - \left(\frac{1}{p_i} + \sum_{l=i}^{j-1} ln \frac{1}{p_{l,l+1}} \right),$$

The objective of this study is to consider two different configurations of the distribution of access rights for employees of an organization to critical documents of an information system, as well as to calculate probabilistic estimates of the success of a multi-step social engineering attack.

4. Distribution of access rights

4.1. Users have access to documents of one level of criticality

If the distribution of access rights to documents is set in such a way that groups of users are allocated, endowed with a certain level of privileges, which allows access to critical documents of only one level of criticality and no others, then the assessment of the vulnerability of documents of the level L_j looks as follows:

$$H_{L_j} = 1 - \prod_{i \in U^{(L_j)}} \left(\frac{1}{p_i} + \sum_{l=i}^{j-1} ln \frac{1}{p_{l,l+1}} \right), \quad (1)$$

where$U^{(L_j)}$ is set of users who have access to documents of the criticality level L_j

4.2. Users have access to documents of a certain level of criticality and all levels below

When distributing access rights to documents in such a way that the user has access to documents of a certain level of criticality and all levels below, the formula for calculating the assessment of the susceptibility of level documents L_j is set recursively and looks like this:

$$H_{L_j} = 1 - (1 - H_{L_j+1}) \prod_{i \in U^{(L_j)}} \left(\frac{1}{p_i} + \sum_{l=i}^{j-1} ln \frac{1}{p_{l,l+1}} \right), \quad (2)$$

whereH_{L_j+1} is assessment of the damage rate of documents of a higher level $(L_j + 1)$ Note that with such a task, the score for documents with a higher level of criticality will be initially calculated.

5. Results

Let us compare the estimates obtained. Note that the calculation by formula (2) includes the calculation (1), since it calculates the assessment of documents with the highest level of criticality. Thus, a model with a differentiation of the level of access to documents of only one level of criticality is preferable from the point of view of information security of the system.

6. Conclusions

Thus, the article considered two different models of distribution access rights and calculated probabilistic estimates of the success of the multi-step social engineering attack when a malefactor implements the most probability scenario of an attack, depending on the distribution of rights between users of the information system. From a theoretical standpoint, the study contributes to the development

of fuzzy hybrid computing models. In addition, the results can be applied practically in the design of decision support systems in the information security field. The global applicability of the presented results is seen in the development of information systems diagnostics in terms of security against social engineering attacks.

7. Acknowledgements

The work was carried out as part of the project according to the RF Government Assignment SPIIRAS No. 0073-2019-0003, with financial support RFBR, projects No.18-01-00626 and No.20-07-00839.

8. References

[1] Dangers of digitalization or digitalization at risk, 2019. URL: https://spb.plus.rbc.ru/news/5cb448c57a8aa90a3814c68e/.
[2] Sberbank named three trends in the field of cybercrime, 2019. URL: https://ria.ru/20190427/1553112124.html/.
[3] In the Russian Federation, an increase in theft through social networks has been recorded. How not to become another victim? 2019. URL: https://rskrf.ru/news/v-rf-zafiksirovan-rost-khishcheniy-cherez-sotsseti-kak-ne-stat-ocherednoy-zhertvoy/.
[4] A. A. Azarov, T. V. Tulupyeva, A. V. Suvorova, A. L. Tulupyev, M. V. Abramov, R. M. Usupov, Social Engineering Attacks: The problems of analysis, Nauka, St. Petersburg, 2016.
[5] M. V. Abramov, T. V. Tulupyeva, A. L. Tulupyev, Social Engineering Attacks: social networks and user security estimates, SUAI, St. Petersburg, 2018.
[6] A. O. Khlobystova, M. V. Abramov, A. L. Tulupyev, A. A. Zolotin, Identifying the most critical trajectory of the spread of a social engineering attack between two users. Information and Control Systems, 6 (2018) 74-81. doi:10.31799/1684-8853-2018-6-74-81.
[7] A. O. Khlobystova, M. V. Abramov, A. L. Tulupyev, Soft Estimates for Social Engineering Attack Propagation Probabilities Depending on Interaction Rates Among Instagram Users, in: Kotenko I., Badica C., Desnitsky V., El Baz D., Ivanovic M. (eds) Intelligent Distributed Computing XIII, IDC 2019, Studies in Computational Intelligence, Springer, Cham, 868 (2019) 272-277. doi:10.1007/978-3-030-32258-8_32
[8] Data leaks. Russia. 2018 year. InfoWatch. Resources. Analytical reports, 2019. URL: https://www.infowatch.ru/analytics/reports/russia2018/.
[9] A. V. Fedotova, A. V. Volkov, V. B. Tarasov, From classic to multi-agent systems for protecting corporate information, Regional informatics and information security, 2015, 316-319.
[10] M. Mohammadpourfard, Y. Weng, M. Pechenizkiy, M. Tajdinian, B. Mohammadi-Ivatloo, Ensuring cybersecurity of smart grid against data integrity attacks under concept drift. International Journal of Electrical Power & Energy Systems, 119 (2020). doi:10.1016/j.ijepes.2020.105947.
[11] J. Roldán, J. Boubeta-Puig, J. L. Martínez, G. Ortiz, Integrating complex event processing and machine learning: An intelligent architecture for detecting IoT security attacks. Expert Systems with Applications, 149 (2020). doi: 10.1016/j.eswa.2020.113251.
[12] A. Yazdinejad, R. Parizi, A. Dehghantanha, G. Srivastava, S. Mohan, A. Rababah, Cost optimization of secure routing with untrusted devices in software defined networking. Journal of Parallel and Distributed Computing, 143 (2020) 36-46. doi:10.1016/j.jpdc.2020.03.021.
[13] Y. Wang, Y. Guo, Z. Guo, T. Baker, W. Liu, CLOSURE: A cloud scientific workflow scheduling algorithm based on attack–defense game model. Future Generation Computer Systems, 111 (2019) 460-474. doi:10.1016/j.future.2019.11.003.
[14] C. Liu, N. Wang, H. Liang, Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment. International Journal of Information Management, 54 (2020). doi: 10.1016/j.ijinfomgt.2020.102152.
[15] F. G. Alotaibi, N. Clarke, S. M. Furnell, A novel approach for improving information security management and awareness for home environments. Information & Computer Security, 2020. doi: 10.1108/ICS-05-2020-0073.

[16] M. A. Ramos, C. A. Thieme, I. B. Utne, A. Mosleh, A generic approach to analysing failures in human–System interaction in autonomy. Safety Science, 129 (2020). doi: 10.1016/j.ssci.2020.104808.
[17] A. R. Gillam, W. T. Foster, Factors affecting risky cybersecurity behaviors by US workers: An exploratory study. Computers in Human Behavior, 2020. doi:10.1016/j.chb.2020.106319.
[18] M. Shi, R. Jiang, X. Hu, J. Shang, A privacy protection method for health care big data management based on risk access control. Health care management science, 23(3) (2020) 427-442. doi:10.1007/s10729-019-09490-4.
[19] M. V. Abramov, Automation of the social networks websites content analysis in the problems of forecasting the protection of the information systems users from social engineering attacks. Automation of management processes, 1 (2018) 34-40.
[20] X. Song, W. Jiang, X. Liu, H. Lu, Z. Tian, X. Du, A survey of game theory as applied to social networks. Tsinghua Science and Technology, 25, 6 (2020) 734-742. doi: 10.26599/TST.2020.9010005.
[21] J. Roponen, D. Insua, A. Salo, Adversarial Risk Analysis under Partial Information. European Journal of Operational Research, 287(1) (2020) 306-316. doi:10.1016/j.ejor.2020.04.037.
[22] A. A. Korepanova, T. V. Tulupyeva, User identification across different social networks through social circles, in: Proceedings of XI St. Petersburg interregional conference Information Security of Russian regions, ISRR-2019, SPOISY, St. Petersburg, 2019, 442-443.
[23] A. A. Korepanova, V. D. Oliseenko, M. V. Abramov, A. L. Tulupyev, Application of machine learning methods to the user accounts identification in two social networks. Computer tools in education, 3 (2019) 29-43.
[24] A. M. Namestnikov, A. A. Filippov, V. S. Moshkin, N. G. Yarushkina, The social portrait model of social network user based on the semantic analysis of a semi-structured content profile, in: Proceedings of the 8th international conference on systems analysis and information technologies, SAIT-2019, 2019, 336-341.
[25] E. D. Pavlygin, A. G. Podloboshnikov, R. A. Savinov, N. G. Yarushkina, A. M. Namestnikov, A. A. Filippov, A. A. Romanov, V. S. Moshkin, G. I. Guskov, M. S. Grigoricheva, Development of a software package for data mining of social media, Automation of management processes, 2 (2019) 23-36.
[26] M. V. Abramov, T. V. Tulupyeva, A. L. Tulupyev, Social Engineering Attacks: social networks and user security estimates, SUAI, St. Petersburg, 2018.
[27] A. O. Khlobystova, M. V. Abramov, A. L. Tulupyev, A. A. Zolotin, Identifying the most critical trajectory of the spread of a social engineering attack between two users. Information and Control Systems, 6 (2018) 74-81. doi:10.31799/1684-8853-2018-6-74-81.