Changing the information system's protection level from social engineering attacks, in case of reorganizing the information system's users' structure[*]

A A Azarov[1], A V Suvorova[1] and T V Tulupyeva[1]

[1]Saint-Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, Saint-Petersburg, 14-th line V.O, 39, Russia

Abstract. Paper is devoted to the development of a method for analyzing changes in information system's protection level from social engineering attacks aimed at users of such system, in the event of users of information system changing (dismissal / skills development). The approach is based on a change in the degree of the user's vulnerabilities and corresponding recalculation of the success rates of the malefactor's social engineering attack influences on the information system's user and the overall level of security of the information system. In addition, possible losses of company's productivity are also considered, in case of the user's termination. This approach allows to determine the optimal structure of the user's social graph on the basis of changing information security level and in terms of changing the productivity level of office work in the company in case of users' dismissal or skills development.

1. Introduction

In the modern world, digital technologies are being introduced everywhere. So, terms digital economy, digital industry, digital government have been appeared, even modern hospitals switch to electronic document circulation, allowing their patients to get access to their medical cards and even some types of services on-line. Such widespread introduction of digital technologies leads to a tremendous increase in the requirements for personal data of users' protection. The same trends are observed in the corporate environment. The value of corporate data, which is largely composed of personal data, is also of a great value. Such challenges pose serious tasks for experts in information security. More and more advanced methods of data protection are being developed [8–10, 12, 13]. But often users of information systems, which are a potential source of information leakage, remain without due attention [11]. Causes of leakage can be both insider attacks, and the impact on users from outside, the purpose of which is to obtain confidential data. Such impacts can be combined by the term social engineering attack of the malefactor, and the individual impact is a malefactor's social engineering attack action.

It is necessary to learn how to protect information from attacks of this kind (i.e. from socio-engineering attacks). Besides, it is necessary to find out how to estimate the degree of protection (or security level) of the personnel of information systems against socio-engineering attacks. This kind of attacks aims at users of information systems as the main way for intrusion or attack propagation. That

[*] The results were partially supported by RFBR, project No. 18-37-00340, and Governmental contract (SPIIRAS) No. 0073-2018-0001

is why it is necessary to predict and measure user's vulnerabilities, and also to build the summary, aggregated indicators of the whole personnel security.

These indicators can serve as indices for estimating the degree of user's vulnerabilities implication as the response on the malefactor's attack activities (attacking action in the elementary case; series of attack actions — in more general case; set of attacks, which the malefactor can act due to his qualification and available resources — in the most general case). It is also possible to take into account actions that are made by the user in response to the malefactor's attack actions and the probability of these responses. What is more, if we know the probability of successful attack realization and criticality level of information resource, we will be able to estimate an expected damage.

Paper is devoted to the development of a method for analyzing changes in information system’s protection level from social engineering attacks aimed at users of such system, in the event of users of information system changing (dismissal / skills development). The approach is based on a change in the degree of the user’s vulnerabilities and corresponding recalculation of the success rates of the malefactor’s social engineering attack influences on the information system’s user and the overall level of security of the information system. In addition, possible losses of company’s productivity are also considered, in case of the user’s termination. This approach allows to determine the optimal structure of the user’s social graph on the basis of changing information security level and in terms of changing the productivity level of office work in the company in case of users’ dismissal or skills development.

2. Algorithm description

Paper considers models previously proposed in [1-3]. The overall complex consists of a variety of models of the information system, including, in particular, the user’s model, the document’s model, the system’s structure model, the malefactor’s model, models of user’s social graph. In more detail, let's look at the user model, the parameters of which are user’s access to certain critical documents, the level of access to these documents, the relationships between users and user’s vulnerabilities profile. Based on the data on relationships between users, a user’s social graph with loaded bidirectional arcs and loaded vertices can be constructed. The weights of arcs are the probabilities of a user-to-user transition, based on the type of user relationships, it is obvious that the weights of user 1 to users 2 and user 2 to user 1 links are different. The weight of each vertex is the total probability of the malefactor’s social engineering attack impact on an information system’s user success, built on the strength of the severity of the user's vulnerabilities [13].

In the user’s model that has been outlined earlier, we also add a skill module, which can be represented in the form $S = \left(\left(S_1, S_1(v)\right), ..., \left(S_n, S_n(v)\right)\right)$, where each S_i — is a user’s skill which may be useful in user’s routine, and $S_i(v)$ —the degree of user’s possession of S_i skill.

Based on the user’s vulnerabilities profile, which is a part of user’s model, the full probability of malefactor’s social engineering attack impact on the user can be constructed. Then users with minimal security ratings are selected among all users of the information system. After that, the overall information system’s protection level is assessed.

In this paper, we estimate the change in the overall information system’s protection level when following one of two strategies

- Firing an employee and replacing him with a new employee;
- Training the employee, improving his skills with a corresponding increase in his protection level.

It is obvious that replacing an employee with a new one with a comparable level of vulnerability leads to an increase in the overall level of security (at least initially): the new employee has weaker communications, so the spread of the attack through him is characterized with less probabilities. But such a decision may be unprofitable in accordance with other criteria of the organization's activities. Even assuming that 1) the level of protection of the new employee is at least not lower than that of the person whom he replaces (it can be estimated in advance, before employment, based on assessments of psychological features followed by modeling user's vulnerabilities profile); 2) the new employee has the necessary skills to work (the evaluation of the competencies and skills of the employee can be carried out through professional testing or other assessments of the new employee's professional skills), it will be necessary to take into account that the employee will need time to get acquainted with the activities of the organization and the department, which will reduce its effectiveness. Moreover, weak links with other members of the team, as numerous studies shows, affect both the work of the corporate team as a whole and the effectiveness of this particular employee [6]. In particular, the meta-analysis carried out in [7] shows that the success of the employee is interrelated with his position in the social network of the organization and the number of links.

Therefore, in order to better assess the impact of a decision, it is necessary to take into account both changes in the evaluation of security, and changes in the overall effectiveness of the corporate team.

3. Modeling

In this research a numerical experiment has been carried out as follows. Firstly, when simulating the replacement of an employee with a new one, it is necessary to make changes in the security indicators, the weight of the arcs that connect the replaced user to the rest of the user’s social graph, while the number of arcs remains unchanged. For simplicity, we choose weights for each arc randomly from a uniform distribution on the interval $\left[0, a_i\right]$, where a_i is the weight of the corresponding arc of the previous employee. In general, the algorithm for choosing weights can be based on the minimum, average or maximum weight of arcs already contained in the user’s social graph.

Secondly, we calculate the generalized skill of the corporate team on the basis of the individual skills of its members. Some studies show that it is better to use simple metrics for aggregating the team's skills - average, median, minimum (i.e. weakest score), maximum (in situations where at least one participant is able to perform the task), swing, etc. [4, 5]. However, in our research it is more reasonable to estimate the generalized skill of the corporate team, taking into account the strength of the connections between the participants [4]. We will calculate the overall skill of the corporate team as a weighted average of individual skills, where the weighed in-degree of the vertexes user’s social graph will be used as weights.

Thirdly, we assume that training an employee reduces its vulnerability by b_i %, where b_i is chosen randomly from a uniform distribution on the interval [0, 100].

Comparing the significance of changes in the overall information system’s protection level and changes in the level of the company's ability to perform its functionality, it may be decided either to replace this employee with a new one or train an employee with minimal security assessments. After the formation of such assessments and the adoption of appropriate decisions, the analysis of the graph can be continued until the analyzed employee becomes either an employee previously analyzed or a new employee, who was added to the corporate infrastructure in the previous steps of analysis. Then, a new evaluation of the security of the entire information system can be obtained with the new parameters of the employees.

4. Numerical experiment

In this paper the following user’s social graph will be consider to evaluate numerical experiment and analyze the information system’s user’s security:

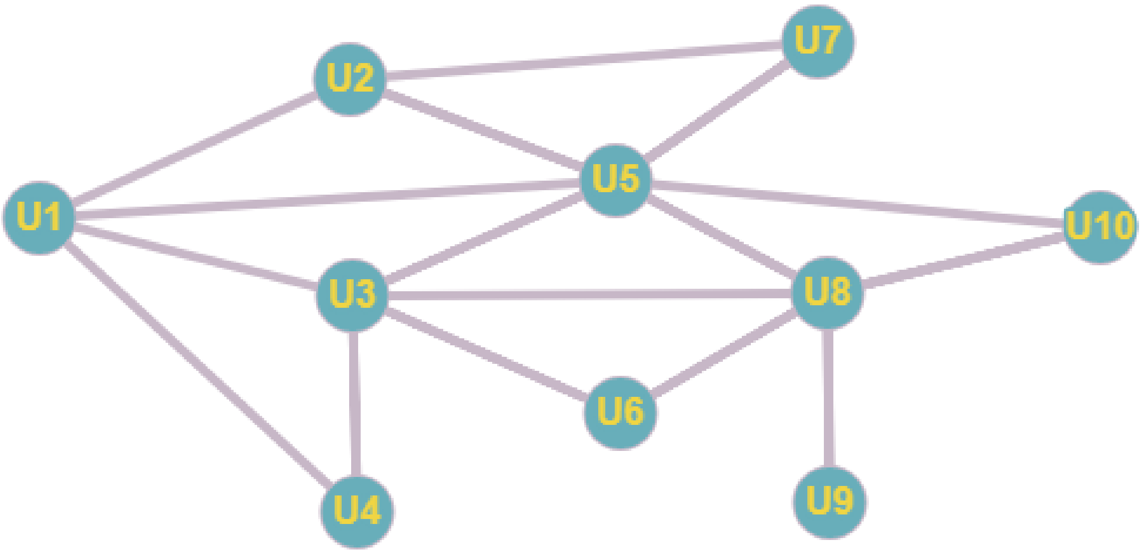

Figure 1. User's social graph.

Probabilistic estimates of the vertices and arcs weights of a given graph can be represented in the form of a matrix $\|P\|$, which can be implemented as follows:

$$\|P\| = \begin{pmatrix} 0,12 & 0,05 & 0,08 & 0,09 & 0,02 & 0 & 0 & 0 & 0 & 0 \\ 0,4 & 0,15 & 0 & 0 & 0,2 & 0 & 0,07 & 0 & 0 & 0 \\ 0,08 & 0 & 0,25 & 0,08 & 0,09 & 0,1 & 0 & 0 & 0 & 0 \\ 0,09 & 0 & 0,08 & 0,4 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0,03 & 0,19 & 0,09 & 0 & 0,09 & 0 & 0,01 & 0,02 & 0 & 0,4 \\ 0 & 0 & 0,1 & 0 & 0 & 0,7 & 0 & 0,04 & 0 & 0 \\ 0 & 0,08 & 0 & 0 & 0,04 & 0 & 0,5 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0,05 & 0,06 & 0 & 0,45 & 0,02 & 0,03 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0,04 & 0,35 & 0 \\ 0 & 0 & 0 & 0 & 0,3 & 0 & 0 & 0,04 & 0 & 0,22 \end{pmatrix}$$

On the diagonal of this matrix the probabilities of malefactor's social engineering attack actions on users of the information system are put, and on other positions of the matrix there are the probabilities of a malefactor's social engineering attack transition from user to user.

Skills evaluation vector may be represented as $(0.43,\ 0.65,\ 0.15,\ 0.60,\ 0.17,\ 0.87,\ 0.80,\ 0.01,\ 0.29,\ 0.07)$.

The probability of failure of such information system in case of malefactor's social engineering attack is 0.9872, due to the fact that the individual vulnerabilities of its users are very high (for example, a U_6 user has vulnerability 0.7). The aggregated team skill score is 0.98. Firstly, user U_6 and his influence on the informational systems' protection level should be analyzed.

4.1. User's training option

The results of the different effects of training are shown in figure 2 For example, if the degree of vulnerability is reduced by 25%, the total probability of failure of such information system in case of malefactor's social engineering attack is will be 0.9797.

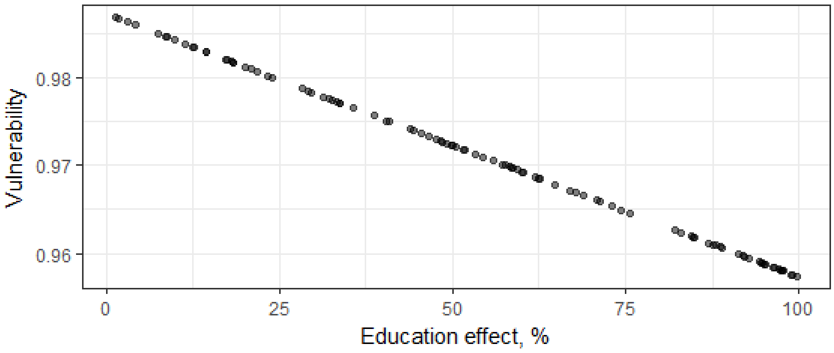

Figure 2. The results of the different effects of training

At the same time, the generalized skill of the corporate team will not change.

4.2. User's dismissal option

Let the probability of malefactor's social engineering attack impact on the new user success will be 0.3, and skill will be 0.8 (similar to the skill of the previous employee). The strength of social connections between new user and other users is determined randomly according to the algorithm described in the previous section. We will repeat the procedure with the appointment of weights, calculations of security and aggregated skill 50 times. The average indicators then will be the following: the total probability of failure of such information system in case of malefactor's social engineering attack is 0.9701, and the generalized skill of corporate team is 0.90. In figure 3 the changes in the generalized skill of corporate team with different skills of the new user is presented.

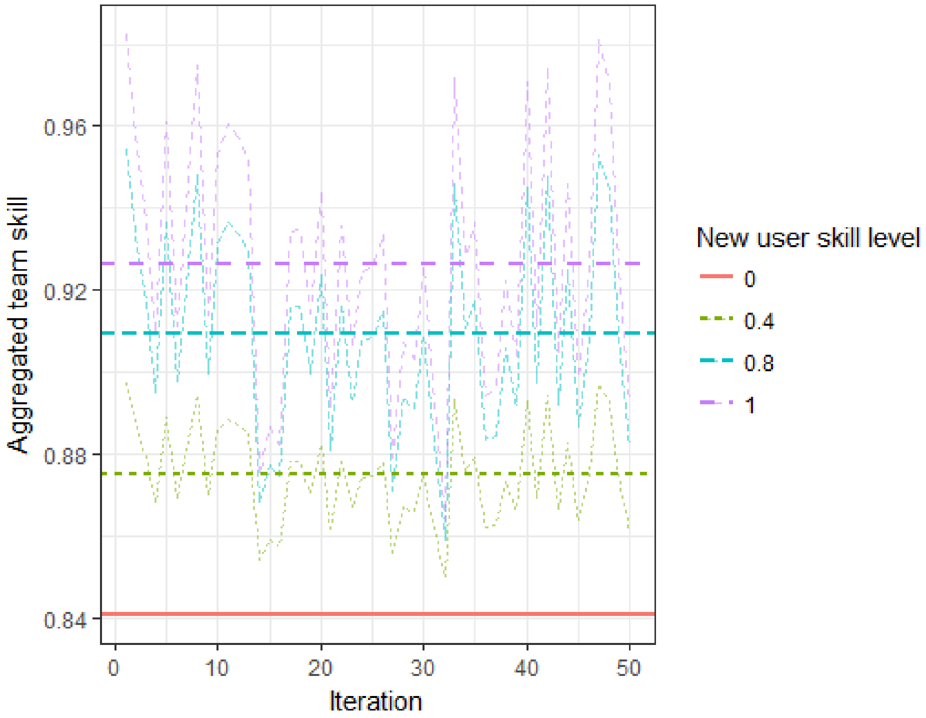

Figure 3. The results of the different effects of training.

4.3. All users replacements/training

Let's consider consistent replacement of all users, aggregated team skills change and the total probability of failure of such information system in case of malefactor's social engineering attack. For modeling, we assume that the new user has the same skill level as the one he replaces. Users will be replaced in order of decreasing initial vulnerability indicators, i.e. $U_6 \to U_7 \to U_8 \to U_4 \to U_9 \to U_3 \to U_{10} \to \mathrm{U}_2 \to \mathrm{U}_1 \to U_5$.

The averages of 50 iterations are shown in figure 4. As we can see on this figure, when the user U_{10} is replaced, the common skill of corporate team falls sharply, even considering that we assume that the individual skills do not change during the replacement, while the total probability of failure of such information system in case of malefactor's social engineering attack decreases more slowly.

Changes in aggregated team skills and the total probability of failure of such information system in case of malefactor's social engineering attack while modeling training of all users are shown in figure 5. The common skill of corporate team stays at the same level, while total probability of failure of such information system in case of malefactor's social engineering attack decreases slowly.

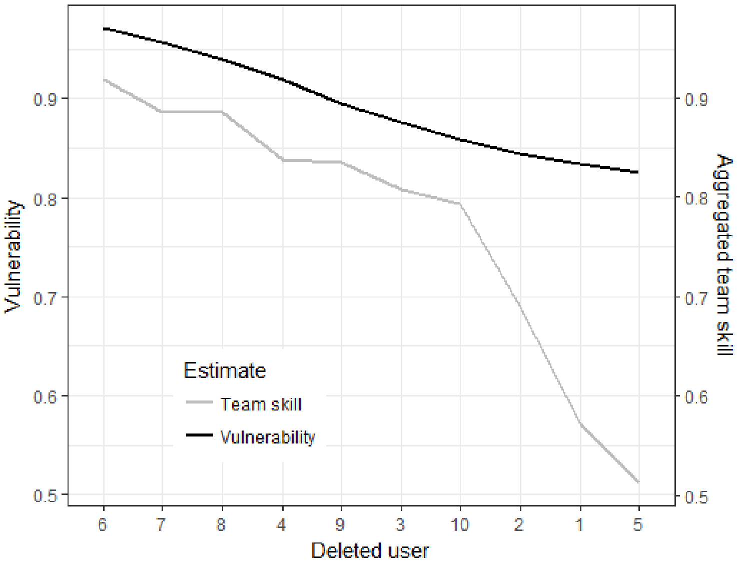

Figure 4. Replacement of all users.

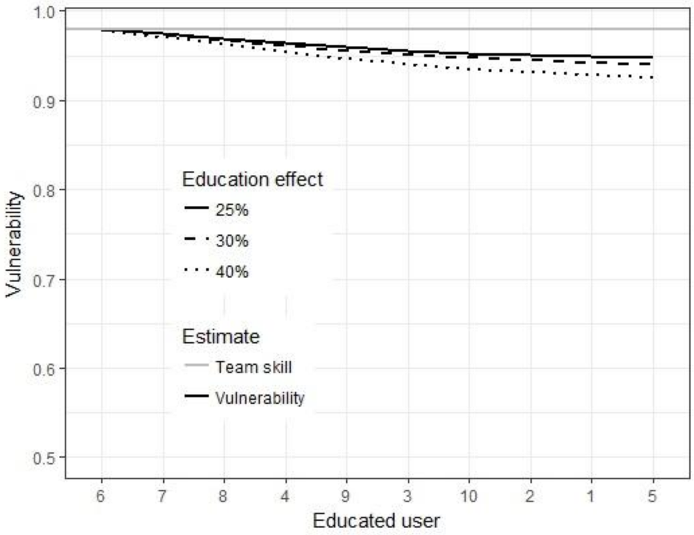

Figure 5. Education of all users.

5. Conclusion

Paper considers method for analyzing changes in information system's protection level from social engineering attacks aimed at users of such system, in the event of users of information system changing (dismissal / skills development). The approach is based on a change in the degree of the user's vulnerabilities and corresponding recalculation of the success rates of the malefactor's social engineering attack influences on the information system's user and the overall level of security of the information system. In addition, possible losses of company's productivity are also considered, in case of the user's termination. This approach allows to determine the optimal structure of the user's social graph on the basis of changing information security level and in terms of changing the productivity level of office work in the company in case of users' dismissal or skills development. Paper also presents a numerical experiment.

Further development of this research is assumed as the calculation of not only changes in the level of common skill of corporate team, but also an assessment of the economic effects that will be received by the company in case of training new employees and additional training of old employees.

6. References

[1] Abramov M and Azarov A 2017 Identifying user's of social networks psychological features on the basis of their musical preferences *Soft Computing and Measurements (SCM)* pp 90–92

[2] Azarov A, Abramov M, Tulupyev A and Tulupyeva T 2016 Models and algorithms for the information system's users' protection level probabilistic estimation *Proceedings of the First International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'16)* **2** pp 39-46

[3] Azarov A, Tulupyeva T, Suvorova A, Tulupyev A, Abramov M and Yusupov R 2016 *Social Engineering Attacks: the Problems of Analysis* (St. Petersburg: Nauka) p 349

[4] Barrick M, Stewart G, Neubert M and Mount M 1998 Relating member ability and personality to work-team processes and team effectiveness *Journal of applied psychology* **83(3)** p 377

[5] Cooke N, Salas E, Cannon-Bowers J and Stout R 2000 Measuring team knowledge *HUMAN FACTORS* **42** pp 151-173

[6] D'Innocenzo L, Mathieu J and Kukenberger M 2016 A meta-analysis of different forms of shared leadership–team performance relations *Journal of Management* **42(7)** pp 1964-1991

[7] Fang R, Landis B, Zhang Z, Anderson M, Shaw J and Kilduff M 2015 Integrating personality and social networks: A meta-analysis of personality, network position, and work outcomes in organizations *Organization Science* **26(4)** pp 1243-1260

[8] Gupta B, Tewari A, Jain A and Agrawal D 2017 Fighting against phishing attacks: state of the art and future challenges *Neural Computing and Applications* **28** pp 3629–3654

[9] Huda A and Živanović R 2017 Accelerated distribution systems reliability evaluation by multilevel Monte Carlo simulation: implementation of two discretisation schemes *IET Generation, Transmission & Distribution* **11** pp 3397–3405

[10] Liu J, Lyu Q, Wang Q and Yu X 2017 A digital memories based user authentication scheme with privacy preservation *PloS ONE* **12** 0186925

[11] Schaik P, Jeske D, Onibokun J, Coventry L, Jansen J and Kusev P 2017 Risk perceptions of cyber-security and precautionary behavior *Computers in Human Behavior* **62** pp 5678–5693

[12] Struharik R and Vukobratović B 2018 A system for hardware aided decision tree ensemble evolution *Journal of Parallel and Distributed Computing* **112** pp 67–83

[13] Terlizzi M, Meirelles F and Viegas Cortez da Cunha M 2017 Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance *Journal of Applied Security Research* **12** pp 224–252

Acknowledgments

Authors wishing to acknowledge assistance of A.L. Tulupyev, the Head of the Laboratory of interdisciplinary problems of informatics in SPIIRAS. The results were partially supported by RFBR, project No. 18-37-00340, and Governmental contract (SPIIRAS) No. 0073-2018-0001.