A Mathematical Model for Risk Assessment of Social Engineering Attacks

Andrei Șandor [1], Gabriela Tont [2], Eduard Simion [3]

[1]*Doctoral School of Engineering Sciences, Doctoral domain of Engineering and Management, University of Oradea, Oradea, Romania*
[2]*Department of Control Systems Engineering and Management, Faculty of Electrical Engineering and Information Technology, University of Oradea, Oradea, Romania*
[3]*Faculty of History, International Relations and Political Science, University of Oradea, Oradea, Romania*

***Abstract* – Social engineering is a very common type of malicious activity conducted on cyberspace that targets both individuals and companies in order to gain access to information or systems. It is part of the broader domain of cybersecurity and the first step to mitigate this type of attack is to know its attack vectors. This way, the risk of becoming a victim of this type of attack can be reduced by technical means, proper security culture and procedural solutions – if organizations are referred to.**

***Keywords* – social engineering, modelling, simulation, risk, cybersecurity.**

1. Introduction

Cybersecurity is a very complex domain that includes both technical and social aspects. One of the most human-centred types of attack is social engineering. This type of attack refers to the manipulation of individuals in order to induce them to carry out specific tasks or to give away information that can be of use by an attacker [1].

DOI: 10.18421/TEM111-42
https://doi.org/10.18421/TEM111-42

Corresponding author: Șandor Andrei,
University of Oradea, Oradea, Romania
Email: andrei.sh@protonmail.com

Received: 15 December 2021.
Revised: 06 February 2022.
Accepted: 11 February 2022.
Published: 28 February 2022.

However, not just individuals are vulnerable to social engineering attacks, but also organizations, which means that companies should be aware of this kind of attacks, as a company is only as strong as the most vulnerable individual employed there, and with some businesses containing thousands of employees, the threat is daunting and very real [2].

There are several types of social engineering, depending on the environment where it takes place and the techniques used: phishing (conducted through email), spear phishing (like phishing, but customized for the target), smishing (conducted through SMS), vishing (conducted by voice call), whaling (attack that targets high rank members of an organization), baiting (relies on victim's curiosity or greed), pretexting (conducted by pretending to be somebody else), scareware (manipulation based on shock and fear), quid pro quo (offering some help or information and then asking for something in exchange). The first step to mitigate all the mentioned types of social engineering attacks in an organization is to understand them and to make a realistic risk assessment – which is the primary objective of this research.

2. Literature Review

There are studies on social engineering that propose countermeasures for each type of social engineering attack [3] and also studies that describe procedural models [4] that might help organizations mitigate this type of attack. However, it can be noticed that there are very few studies on mathematical modelling of social engineering that could help organizations to make an assessment of the risk of such an attack. In one of these studies, phishing, which is the most common social engineering attack, is described as following [5]:

$$P \triangleq \langle a \mapsto \{D, S\} \twoheadrightarrow u, NET, \{AL\}, \{low, severe\}, PASSIVE \rangle \quad (1)$$

Equation (1) can be described in the following way: a phishing attack (P) targets data (D) that can

compromise a system (*S*) through the Internet (*NET*) at application layer (*AL*) is a *PASSIVE* attack because data and information obtained by an attacker are used for further malicious activities, and it can have low or severe consequences. This model can be used to describe a phishing attack and can be adapted for any social engineering attack, but it cannot be used to make a risk assessment because neither mitigation nor attack vectors are included.

The risk of a cyberattack was represented by Pokhrel and Tsokos using the following model [6]:

$$R^t = R^{t-1}P \quad (2)$$

This model is based on the Markovian random walk and means that the risk vector R at link t is given by the risk at link $t-1$ and the one step transition probability P. This model can be very useful when analysing risks that relate or are dependent on each other.

In a social engineering attack, risk is strongly related to human errors. Considering this fact, Hadarics et al. described a mathematical model that shows the probability that users of the enterprise's IT infrastructure will provide sufficient facilitation for an attack to succeed, as follows [7]:

$$p_u(u,t) = \prod_{ut\ used\ by\ t} \left(1 - p_{ut}(t,ut)\right) \cdot p_{u-ut}(u,ut) \quad (3)$$

In equation (3), $p_{ut}(t,ut)$ or $p_{usertrick}(t,ut)$ is the ratio between the number of attempts of t where t used ut and the number of all attempts of t. $p_{u\text{-}ut}(u,ut)$ or $p_{user\text{-}usertrick}(u,ut)$ is the ratio between the number of successful attempts of ut on u and the number of all attempts of ut on u. All the presented equations are described in relation to all users (u) and all possible user tricks (ut) used by any malware (t). The single drawback of the model descried in equation (3) is that a social engineering risk assessment can be developed after one or a series of attacks or after conducting a penetration test.

Regardless the vulnerability that can trigger a social engineering attack, organizations need to be aware and protect their assets. Because social engineering is done by and through informational systems, organizations need to establish strategies to maintain the three basic security parameters, the CIA (Confidentiality, Integrity, and Availability) [8].

A model that includes the strategies that come to counter cybersecurity issues was developed by Strielkina and Uzun [9], as represented in the following equation:

$$\sum_{i=1}^{n} w_{ij} \cdot p(x_i) \rightarrow min \quad (4)$$

This model is based on a Game theory approach and considers that the payoff matrix is constructed on the losses w_{ij} due to successful attack and on the strategies x_i that should ensure security. In order to maintain a secure environment, the loss should be minimal.

Referring to critical infrastructure, Baig and Zeadally described the following model of risk mitigation E_i [10]:

$$E_i = \frac{number\ of\ threats\ blocked\ for\ resource\ i}{total\ number\ of\ known\ threats\ against\ resource\ i} \quad (5)$$

The model described in equation (5) can be used to show the capacity of an organization to mitigate social engineering attacks, but also resides on malicious events that are ongoing or already took place.

As it can be noticed, there are some mathematical models that describe cybersecurity aspects from different perspectives, but not very many that focus on social engineering attacks. This is why modelling social engineering is important and it might offer some insights about this type of attack and also it may increase the security of organizations through periodical risk assessments.

3. Methodology

In order to develop a mathematical model that can help organizations evaluate the risk of social engineering, there will be identified the main components or vectors of this type of attack. The before-mentioned components of social engineering will be identified based on the information available from the previous chapters and they will be chosen in a way that permits the model to be used in a very broad manner, for companies operating in various domains.

The risk model will be presented in accordance with another model, that will describe a social engineering attack. The last model will be based on the relationship between a known vulnerability and an existing threat. This will help us prepare the framework for the mathematical model of the risk associated to a social engineering attack from a probabilistic perspective.

After establishing the model, it will be simulated using Monte Carlo simulation. This method was chosen because there are multiple variables that are hard to predict and therefore their values will be estimated. The simulation will be done using a software written in Python, as it will be described in a later chapter.

Finally, there will be presented some conclusions regarding the results and most important findings that might conduct to a better understanding of social engineering and how the risk of occurrence of this type of attacks can be reduced within organizations.

4. Mathematical Model

When modelling social engineering risk, human, organizational and technological dimensions should be considered, as combining education and training with the best-of-breed technology may be the best way to mitigate social engineering risks and reduce potential damages [11].

Hackers take advantage of technical vulnerabilities and poor design of organizational processes that do not cover all possible situations or have gaps regarding responsibility attribution. In order to reduce the impact of these attack vectors, Edwards et al. identified the following most used mitigation techniques: security awareness training, revised security policies and practices, network restrictions, company website review [12].

Based on the before-mentioned aspects and on the existing models on cybersecurity issues, there will be developed a mathematical model for risk assessment of social engineering attacks, starting from the basic representation of risk:

$$R = \sum_{i=1}^{n} p(a_i) \cdot L_i \quad (6)$$

In equation (6), the risk R is the sum of all types of social engineering attack that have a_i probability to occur, with the expected loss L_i. In order to estimate a_i, the following model will be used:

$$SE = (v - v_m) \cdot T \quad (7)$$

In equation (7), a social engineering attack SE occurs when a threat T makes use of a vulnerability v that cannot be fully mitigated by v_m means. For sophisticated social engineering attacks, when a threat T takes advantage of several vulnerabilities v_i, the model can be described as in equation (8):

$$SE = T \sum_{i=1}^{n} (v_i - v_{mi}) \quad (8)$$

Using the model presented in equation (7), for a social engineering attack that makes use of a single vulnerability, the probability of a social engineering attack of type i to be successful against an organization – $p(a_i)$ can be estimated as the average mean between the probability of the implemented security measures to reduce the vulnerabilities (v-v_m) and the probability of a threat to target the organization (T):

$$p(a_i) = \frac{p(v - v_m) + p(T)}{2} \quad (9)$$

The other parameter that is part of the risk model - L_i, the expected loss in case of a social engineering attack i, can be described in terms of confidentiality (C), integrity (I) and availability (A) of data and information affected by the attack:

$$L_i = C + I + A \quad (10)$$

When estimating loss, there will be considered just the dimensions that are affected by a certain attack. For example, in case of a phishing attack, the loss L_i will be expressed just in terms of C - data confidentiality. Loss can be expressed as a financial asset, time of interrupted services, amount of data or number of compromised systems.

Using all the presented data in this chapter, there can be presented the following risk model of a social engineering attack:

$$R = \frac{[p(v - v_m) + p(T)](C + I + A)}{2} \quad (11)$$

This model can be used in case of a single type of social engineering attack that targets an organization. In case of a complex social engineering campaign that is directed against an organization, the following model can be used:

$$R = \sum_{i=1}^{n} \frac{[p(v_i - v_{mi}) + p(T_i)](C_i + I_i + A_i)}{2} \quad (12)$$

In the following chapter, the model will be simulated according to a scenario that is often encountered by organizations.

5. Risk Assessment Simulation

To simulate a risk assessment of a social engineering attack, there will be used a Monte Carlo simulation. For this purpose, the code of a Python-based software written by Francois St-Amant [13] will be customized according to the model presented in the previous chapter. The variables that will be used in our simulation will be the probability that a security measure to counter a vulnerability – $p(v_i\text{-}v_{mi})$ and the probability that a known threat targets an organization – T_i. To express loss, there will be used estimates to quantify the effects of the social engineering attacks in terms of confidentiality, integrity and availability.

For the first simulation, there will be considered the following scenario: a phishing campaign already started targeting companies operating in the same domain like company A and company B (which means that a threat is probable to happen, estimating a probability of 0.8). The two organizations have the same number of employees, around 5000, that work on their own workstation (the number of possible devices that could be infected with malware). The employees working in company A are unaware of

phishing attacks and are likely to click any link or attachment they receive through email, SMS or social apps, while the employees working in company B are more aware and they are usually paying attention to details like sender address or bad language. So, employees working in company A are likely (with a probability larger than 0.5) to get tricked by hackers, while this is less likely for company B (the probability is under 0.5).

After adding the data into the Python software and running the Monte Carlo simulation with 100000 iterations, the following graph is generated:

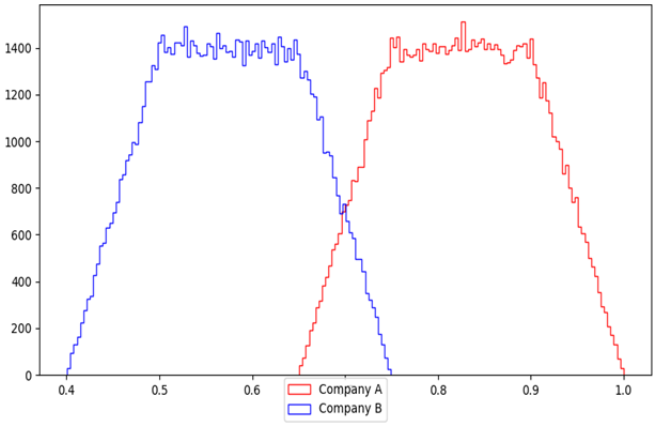

Figure 1. Monte Carlo simulation for phishing attack occurrence probability

The graph presented in Figure 1. is plotted in accordance with the probability of a successful phishing attack on x axis and density on y axis. Density refers to the probability that an event is to occur, so that the higher the density, the much probable the event to occur.

The most probable values for the event to occur in company A are between 0.75 and 0.9, which means that the risk of a phishing attack is malware infection of a number between 3750 and 4500 workstations. For company B, the values of a probable event to occur are between 0.5 and 0.65, which means that the risk is malware infection of a number between 2500 and 3250 workstations.

It can be noticed that the risk has high values due to the chosen values: high probability of the threat and high intervals for the probability that users get tricked by hackers to open links or attachments containing malware. Also, there must be noticed that the risk assessment is done for one specific situation.

In order to have more accurate results on a longer period of time for a specific threat, there should be identified all the vulnerabilities and mitigation techniques, offering each pair a score that reflects the probability to happen. This can be done as presented in the following table:

Table 1. Probability values for phishing attacks to occur, according to vulnerabilities and mitigation techniques

T_i - Phishing attacks		
v_i	**v_{mi}**	**$p(v_i\text{-}v_{mi})$**
employees click links/attachments received on email/SMS	security awareness training	0.1
	use of security products	0.1
employees provide sensitive data	security awareness training	0.05
	classification of data	0.05
	access based on "need-to-know" principle	0.05
	well-established roles and responsibilities	0.05
employees get tricked by impersonation techniques	policies regarding information flow	0.1
	use of a security check system	0.1
employees provide data after receiving threatening messages	security awareness training	0.1
	use of a security check system	0.1
employees connect unknown devices to organization's network	policies regarding use of devices	0.1
	network protected by security policies	0.1

Using values as presented in Table 1., organizations can evaluate the risk of a threat with higher accuracy. To show how this type of risk assessment can be done, let us consider the following scenario: organization A wants to evaluate the number of employees that might be victims of phishing attacks this year, considering that there are employed all technical security measures and procedural measures, except the security culture of the employees. The company has 5000 members and the probability to become victims of phishing attack is 0.3.

First, there will be counted the probabilities for the phishing attack to succeed based on lack of mitigation measures, which consists in this example in the lack of security awareness training. So, based on Table 1., the estimated value for $p(v_i\text{-}v_{mi})$ for this scenario is 0.25. Considering the values from Table 1., there is accepted a deviation error of 0.05, which means that $p(v_i\text{-}v_{mi})$ will be simulated considering values between 0.20 and 0.30. There will be considered the same deviation error for T_i, which means that it has values between 0.25 and 0.35. After changing data in the Python code and running the simulation using 100000 iterations, the following graph is plotted:

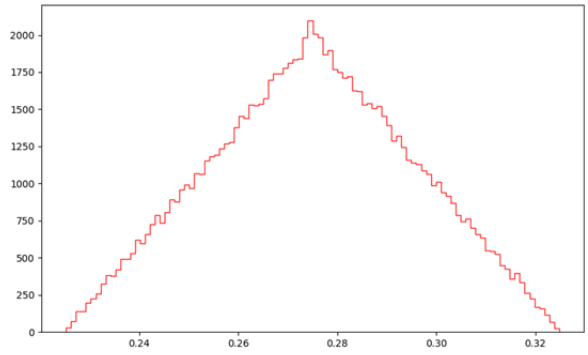

Figure 2. Monte Carlo simulation for phishing attack occurrence probability

Figure 2. shows that the most probable value for a phishing attack to occur against employees working in company A is around 0.27. This means the risk is that approximately 1350 employees might be victims of phishing attacks this year.

The two examples presented loss as number of compromised login credentials and number of employees that might become social engineering victims, but it can be also expressed as loss in financial, credibility or prestige terms.

6. Conclusions

The risk assessment model can be used both for assessments in high uncertainty situations and assessments with known facts. The biggest difference will be the accuracy of the assessment, but however it may help decision makers choose the best solutions to mitigate the vulnerabilities and reduce risks.

The proposed model and simulation technique in this paper can be very useful if the vulnerabilities and mitigation measures are estimated in a realistic way. Also, if already having data about malicious events that happened in the past or against other organizations, there can be created very accurate risk assessments.

For increased accuracy of an assessment, there can be created a scoring table for each mitigation technique against a vulnerability, where a maximum value means that all known security measures for that vulnerability had been implemented by the organization. This way, the value of the probability that a threat makes use of a certain vulnerability will have a very low deviation error, which implies a higher accuracy when expressing the risk.

Because social engineering attacks heavily relate on social aspects, it is very hard to make predictions or risk assessments. For this purpose, models like the presented one in this paper can be valuable tools for both awareness and decision making through simulation.

References

[1]. Lohani, S. (2019). Social engineering: Hacking into humans. *International Journal of Advanced Studies of Scientific Research*, *4*(1).

[2]. Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, *4*, 100126.

[3]. Alsufyani A.A., Alhathally L.A., Al-Amri B.O., Alzahrani S.M., (2020), Social Engineering, New Era of Stealth and Fraud. Common Attack Techniques and How to Prevent Against, *International Journal of Scientific & Technology Research, 9*(10), 371-376.

[4]. Mouton, F., Nottingham, A., Leenen, L., & Venter, H. S. (2018). Finite state machine for the social engineering attack detection model: SEADM. *SAIEE Africa Research Journal*, *109*(2), 133-148.

[5]. Chowdhury F., Ferdous S., (2017), Modelling Cyber Attacks, *International Journal of Network Security & Its Applications (IJNSA), 9*(4), 13-32.

[6]. Pokhrel, N. R., & Tsokos, C. P. (2017). Cybersecurity: A stochastic predictive model to determine overall network security risk using markovian process. *Journal of Information Security*, *8*(2), 91-105.

[7]. Hadarics, K., Györffy, K., Nagy, B., Bognár, L., Arrott, A., & Leitold, F. (2017). Mathematical Model of Distributed Vulnerability Assessment. In *Jaroslav Dockal, Milan Jirsa, Josef Kaderka, Proceedings of Conference SPI* (pp. 45-57).

[8]. Fray, I. E., Kurkowski, M., Pejaś, J., & Maćków, W. (2012). A new mathematical model for analytical risk assessment and prediction in IT systems. *Control and Cybernetics*, *41*(1), 241-268.

[9]. Strielkina A., Uzun D., (2017), Researching the Aplicability of Mathematical Approaches for Modelling Cyber Security Processes, *The 13th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer, Kyiv, Ukraine, May 15-18.*

[10]. Baig, Z., & Zeadally, S. (2019). Cyber-security risk assessment framework for critical infrastructures. *Intelligent automation and soft computing*, *25*(1), 121-129.

[11]. Tayouri, D. (2015). The human factor in the social media security–combining education and technology to reduce social engineering risks and damages. *Procedia Manufacturing*, *3*, 1096-1100.

[12]. Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2017). Panning for gold: Automatically analysing online social engineering attack surfaces. *computers & security*, *69*, 18-34.

[13]. St-Amant F., (2021). How to use Monte Carlo simulation to help decision making, Retrieved from: https://towardsdatascience.com/how-to-use-monte-carlo-simulation-to-help-decision-making-a0a164bc8619. [accessed: 02 December 2021].