Development of the strategy for selection of information-communication system security tools based on game theory

Olena Karelina[a] , Taras Lobur[a]

[a] *Ternopil Ivan Puluj National Technical University 1, Ruska, 56, Ternopil, 46001, Ukraine*

Abstract

The mathematical dual binary game of two parties one of which was PJSC “Zborivgaz” information security system and the other were intruders attacks aimed at breaking the integrity, confidentiality or accessibility of information was performed. The strategy of selection the information-communication system security tools under the conditions of the enterprise limited budget was developed.

Keywords 1

information-communication system, information security strategy, game theory.

1. Introduction

1.1. Statement of the problem in general

The exponential growth of data amounts in corporate information systems and the increase in the number of cyber attacks determine the importance of developing the strategy for the selection of information-communication system security tools.

Our investigation is carried out in order to select software and hardware security tools which specification is determined by the information security administrator, taking into account the fact that the organization defines the limitations on cybersecurity cash cover.

The stack of intruders malware for cyber attacs can not be completely predicted for individual intrusion into the integrity, confidentiality or accessibility of enterprise information. However, in general, the world cybersecurity community carries out permanent research and observation of hacking activity and publishes reports, such as, for example, [1-2]. Therefore, in our investigation, security threats to the information-communication system are considered to be known.

The task is to optimize the specification of software and hardware of information-communication system security tools under the conditions of the known attack vector and the limited organization cybersecurity cash cover. We propose to solve this problem by means of mathematical apparatus of game theory.

1.2. Review of the publications on the investigated topic

The general issues of game theory application for solving cyber security problems are discussed in papers [3-4]. The authors substantiate that the confrontation between hacker and information security administrator can be considered as the mathematical game where each player tries to maximize their interests satisfaction. Hence, a well-developed tool - game theory – can be used in order to solve new cyber security problems occurring today.

In paper [5], the algorithm for the development of information security system based on the expert evaluation methods for obtaining output data, game theory and mathematical programming was proposed. The result of solving this problem is the optimal set of security mechanisms providing maximum security level (minimum value of information security risk), under condition of restrictions. The factor of limited cyber security cash cover is important for our investigation. Therefore, we rely on

ITTAP’2021: 1nd InternationalWorkshop on Information Technologies: Theoretical and Applied Problems, November 16–18, 2021, Ternopil, Ukraine

EMAIL: karelina@tntu.edu.ua (A. 1); lobur_t@tntu.edu.ua (A. 2)
ORCID: 0000-0002-5628-9048 (A. 1); 0000-0001-8318-3815 (A. 2)

the approach proposed in paper [6], where the selection of security tools is based on the mathematical apparatus of game theory and makes it possible to make decisions in the limited enterprise budget.

2. Presentation of the main material

We carried out the investigation of relationships between the attacker of the corporate information-communication system and security administrator of PJSC “Zborivgaz” enterprise. The subject of the Company activity is: uninterrupted gas supply; execution of construction works and design of new and expansion of existing gas distribution networks. The problem of information security of strategic infrastructure objects is important for Ukraine. This is proved by a series of power plant cyber attacks in 2015, conducted using BlackEnergy malware. As a result of this effect, a large number of settlements remained without energy supply for several hours.

Let us simulate the mathematical dual binary game of two parties, one of which is the information security system of PJSC “Zborivgaz” and the other is intruders attacks.

According to the methodology developed in [6], the strategies of the security administrator are considered as the game matrix rows Si (i=1,…, n), and the intruder strategies are its columns Aj (j=1,…,m).

The intruder strategies are the types of local and network attacks that can be implemented at PJSC “Zborivgaz”. Let us determine the most probable ones based on the sources conclusions [1], [2].

The common attack is spoofing - the substitution of the traffic on the network or content on the site by that one which is beneficial to the intruder. The fraudulent offline scheme where gas consumers received payment bills containing the details of the fraudulent bank account was revealed in Kyiv. Several hundred people suffered. This one and similar schemes can also be implemented online if effective corporate information security measures are not taken.

DDOS-attacks are one of the most common attacks on corporate servers today. One of the famous DDOS attacks in Ukraine was the overloading of Ukrzaliznytsia server by requests, which resulted in the lack of access to servers during the day. Today, a large number of DDOS-attacks are performed from botnets built on the Internet of Things infrastructure. This is the Mirai botnet created by compromised routers, camcorders, DVD-players, smart TV ssets, wireless presentation systems and other devices connected to the network. Their number reaches 500,000.

Financial data, personal information of PJSC “Zborivgaz” customers is stored in databases. Therefore, code injection attacks, including SQL injection, are probable. This type of attack provides a variety of opportunities for the intruder, limited only by the programming language and the access rights to the desired organization assets. For example, you can view all the database entries available for the current session of the user whose name the intruder managed to access. You can emulate fake server responses to the customers requests. This attack is particularly dangerous because anyone who has access to the organization web-site and is able to enter data into text boxes can potentially be a source of attack by SQL injections.

Functional abuse attacks require no additional tools or special knowledge, so the possibility of their occurrence is high. The essence of these attacks is that the regular program funds are used for malicious purposes. For example, chat or email can be used to send all contacts the website address with harmful exploit loading. Abuse of functionality is more characteristic for insider attacks. The insider attack in modern execution is the action of the intruder on behalf of corporate information-communication system user account.

The intruder can get unauthorized access not to the user account, as in the previous attack type, but to the operating system. Then OS-commanding attack is implemented. If accessed was done through the web server, malicious commands can be executed directly from the browser. For PJSC “Zborivgaz” there is the probability of downloading the malicious code to the compromised server and its starting, as one of the most common cyber threats in recent years is phishing, which affected many Ukrainian companies.

Administrator strategies include the use of information security tools. Firewall is the device designed to manage Internet access, encrypt data and transfer network traffic between zones of different levels of access restriction in accordance with security policies. In the work of the information-communication system of PJSC “Zborivgas” the firewall provides WAN interfaces for connection to different ISPs, LAN interface for connection to the internal network of PJSC “Zborivgas”, DMZ interface for the implementation of the zone of public servers, support for NAT technology, management of access to the LAN and zone of the shared servers and protection against attacks from the outside.

Cloud DDOS security services (such as Incapsula) ensure protection against DDOS-based attacks and reduce attack intensity within minutes.

Antivirus protects the enterprise assets from malicious software that can get onto the computers of PJSC "Zborivgaz" from the Internet or removable media.

Biometric user identification hardware makes it possible to perform authentication at PJSC "Zborivgaz" workplaces quickly and error-free according to the features difficult to fake.

The hardware-cryptographic complex protects the traffic from reviewing while intercepted because it is impossible to resume the encrypted message by the intruder attacker.

The elements of mathematical game matrix we performed in order to develop the cyber security strategy for PJSC "Zborivgaz" are the probability of successful implementation of the intruder attack, determined by the expert assessments method (Table 1).

Table 1

Dual binary game matrix of PJSC “Zborivgaz” information security administrator and threat actor

	spoofing	DDOS	code injection	abuse of functionality	OS-commanding
firewall	0,34	0,46	0,27	0,06	0,14
antivirus	0,43	0,38	0,27	0,16	0,17
cloud defense	0,36	0,23	0,24	0,19	0,14
biometry	0,63	0,38	0,38	0,27	0,21
cryptography	0,7	0,51	0,57	0,35	0,31

Assessed value (UAH) of each security tool X_i (i=1,…,5): (5800, 20000, 21000, 33000, 50000) and amount of estimated loss from the implementation of a particular attack Y_j

Table 2

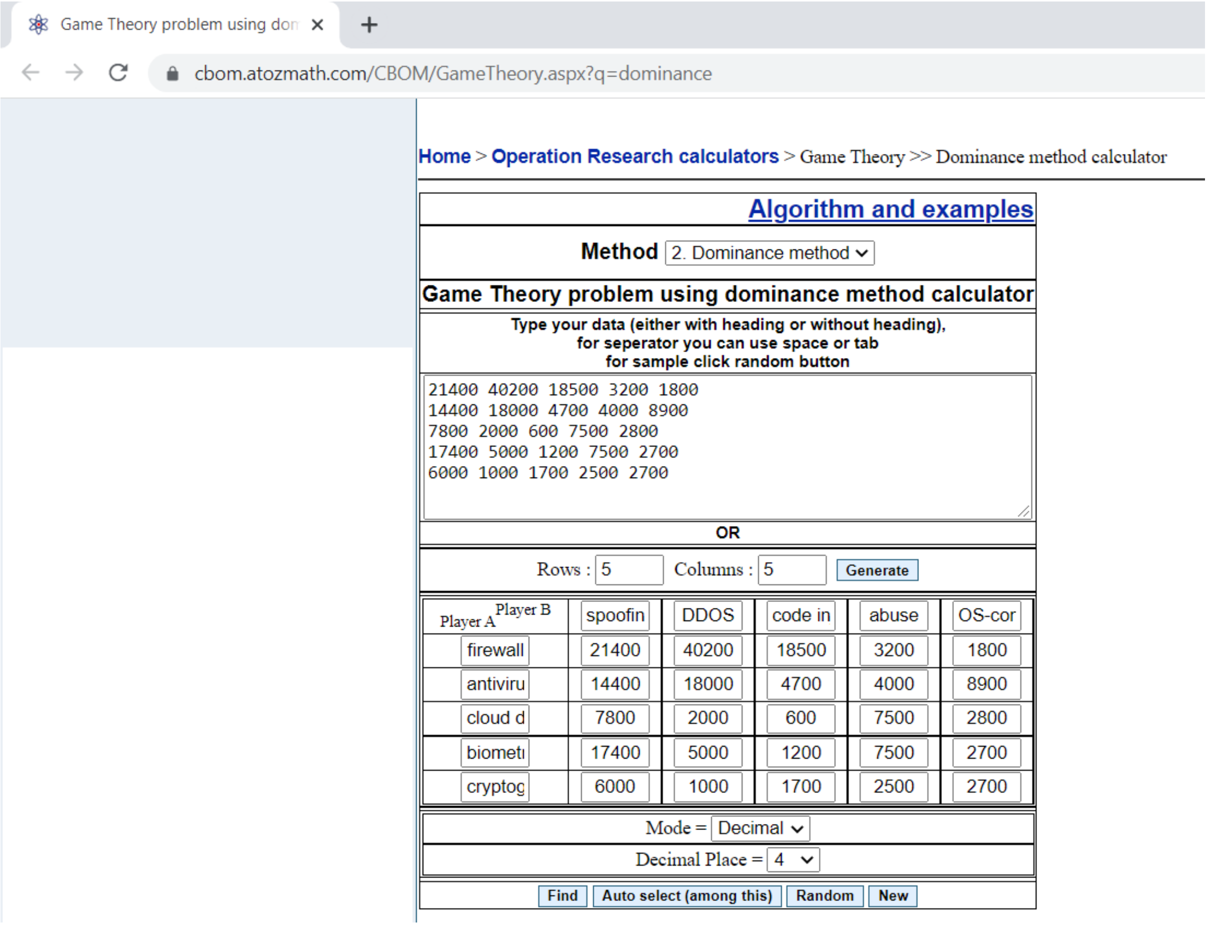
Game matrix of PJSC “Zborivgaz” information security administrator and information interloper after ROI calculation

	spoofing	DDOS	code injection	abuse of functionality	OS-commanding
Firewall	21400	40200	18500	3200	18000
antivirus	14400	18000	4300	4000	8900
cloud defense	7800	2000	600	7500	2800
biometry	17400	5000	1200	7500	2700
cryptography	6000	1000	1300	2500	2700

We used the online service https://math.semestr.ru/games/index.php to solve the obtained game matrix using Brown-Robinson method. The window for data entry and selection of the problem–solving method is shown in Fig. 1.

We check if the payment matrix has a saddle point. If this is a case, then we write out the game solution in pure strategies. The pure strategy of the security administrator is to select one of the gains matrix lines, and the pure strategy of the intruder is to select one of the columns of this matrix. We believe that the security administrator selects his strategy in such a way as to obtain the full maximum gain, and the intruder chooses his strategy in a way that minimizes the administrator gain.

The minimum cost values and maximum cost savings are defined in Table 3.


Game Theory problem using don
cbom.atozmath.com/CBOM/GameTheory.aspx?q=dominance

Home > Operation Research calculators > Game Theory >> Dominance method calculator

Algorithm and examples

Method 2. Dominance method

Game Theory problem using dominance method calculator

Type your data (either with heading or without heading),
for seperator you can use space or tab
for sample click random button

```
21400 40200 18500 3200 1800
14400 18000 4700 4000 8900
7800 2000 600 7500 2800
17400 5000 1200 7500 2700
6000 1000 1700 2500 2700
```

OR

Rows : 5 Columns : 5 Generate

Player B Player A	spoofin	DDOS	code in	abuse	OS-cor
firewall	21400	40200	18500	3200	1800
antiviru	14400	18000	4700	4000	8900
cloud d	7800	2000	600	7500	2800
biometi	17400	5000	1200	7500	2700
cryptog	6000	1000	1700	2500	2700

Mode = Decimal

Decimal Place = 4

Figure 1: Online-service window of the game matrix solution by Brown-Robinson method

Table 3

Game matrix taking into account minimum expences on information security tools and maximum economy of their use

	spoofing	DDOS	code injection	abuse of functionality	OS-commanding	a = min(Ai)
firewall	21400	40200	18500	3200	18000	3200
antivirus	14400	18000	4700	4000	8900	4000
cloud defense	7800	2000	600	7500	2800	600
biometry	17400	5000	1200	7500	2700	1200
cryptography	6000	1000	1700	2500	2700	1000
b = max(Bi)	21400	40200	18500	7500	18000	

Let us find the guaranteed gain, which is determined by the lower game price a = max(a_i) = 4000 indicating the maximum pure strategy for antivirus use. The upper game price is b = min(b_j) = 7500. This indicates the absence of saddle point, since $a \neq b$, then the game price ranges within $4000 \leq y \leq 7500$.

We find the game solution in mixed strategies. This is explained by the fact that security administrator and intruder cannot report the opponent their pure strategies, they should hide their actions.

Let's check the payment matrix for dominant lines and dominant columns. Sometimes, based on a simple consideration of the game matrix, it can be said that some pure strategies can enter the optimal mixed strategy with zero probability.

The i-th strategy of the 1st player dominates his k-th strategy if $a_{ij} \geq a_{kj}$ for all j ∋ N and at least for one j $a_{ij} > a_{kj}$. In this case, they also say that the i-th strategy (or line) is dominanting, k-th is dominant. It is said that the j-th strategy of the 2nd player is dominating his l-th if for all j ∋ M $a_{ij} \leq a_{il}$ and at least for one i $a_{ij} < a_{il}$. In this case, the j-th strategy (column) is called dominating, the l-y is dominated.

The use of firewall security strategy dominates the use of cryptosystem strategy (all elements of line 1 are greater than or equal to the values of line 5), thus we remove the 5th line of the matrix (Table 4). The probability is $p_5 = 0$.

Table 4

Game matrix after dominated line removal

	spoofing	DDOS	code injection	abuse of functionality	OS-commanding
firewall	21400	40200	18500	3200	18000
antivirus	14400	18000	4300	4000	8900
cloud defense	7800	2000	600	7500	2800
biometry	17400	5000	1200	7500	2700

From the intruder loss position, the code injection strategy dominates the spoofing strategy (all column 3 elements are smaller than column 1 elements), so we remove the first column of the matrix (Table 5). Probability is $q_1 = 0$. From the intruder loss position, the code injection strategy dominates the DDOS attack strategy (all column 3 elements are smaller than column 2), and we remove the second column of the matrix (Table 5). The probability is $q_2 = 0$.

Table 5

Game matrix after dominated columns removal

	code injection	abuse of functionality	OS-commanding
firewall	18500	3200	18000
antivirus	4300	4000	8900
cloud defense	600	7500	2800
biometry	1200	7500	2700

We reduced the game 5x5 to the game 4x3. The players select their pure strategies at random, so the gain of the information security administrator is random value. The administrator must select his strategies in such a way as to maximize the average gain. The intruder must choose his strategies in such a way as to minimize the mathematical expectation of the administrator.

Every playing off in pure strategies is called the game. The Brown-Robinson method is an iterative procedure for constructing the sequence of pairs of players mixed strategies that converges to the matrix game solution.

Let us select the strategy of firewall use at the first step. Iteration # 1: the minimum element is 3200 and is numbered j=2, hence the intruder selects the strategy for functionality abuse. The maximum element equals 7500 and is j=3, so the administrator chooses the cloud security strategy.

Iteration # 1: the minimum element is 10700 and is j=2, hence the intruder selects the strategy for functionality abuse. The maximum element is 15000 and is numbered j=3, so the administrator chooses the cloud security strategy.

The iterations results are summarized in Tables 6-7.

Table 6

Iterations of the game matrix solution by Brown-Robinson method

k	i	B1	B2	B3
1	1	18500	3200	18000
2	3	19100	10700	20800
3	3	19700	18200	23600
4	3	20300	25700	26400
5	1	38800	28900	44400
6	1	57300	32100	62400
7	4	58500	39600	65100
8	4	59700	47100	67800
9	4	60900	54600	70500
10	4	62100	62100	73200

Table 7

Iterations of the game matrix solution by Browm-Robinson method for elements j

k	j	A1	A2	A3	A4	V_{min}	V_{max}	V_{avg}
1	2	3200	4000	7500	7500	3200	7500	5350
2	2	6400	8000	15000	15000	5350	7500	6425
3	2	9600	12000	22500	22500	18200/3	7500	20350/3
4	1	28100	16700	23100	23700	5075	7025	6050
5	2	31300	20700	30600	31200	5780	6260	6020
6	2	34500	24700	38100	38700	5350	6450	5900
7	2	37700	28700	45600	46200	39600/7	6600	42900/7
8	2	40900	32700	53100	53700	11775/2	13425/2	6300
9	2	44100	36700	60600	61200	18200/3	6800	19300/3
10	1	62600	41400	61200	62400	6210	6260	6235

where: k is the game number; i is the strategy number selected by the administrator; j - the number of the strategy selected by the intruder; B_i – gain accumulated by the administrator for k games, provided that in this game the intruder chooses B_i strategy; A_j - loss accumulated by the intruder for k games, provided that in this game the administrator chooses A_j strategy.

V_{min} - lower game score = min (accumulated gain)/k.

V^{max} - top game score = max (accumulated loss)/k.

It is proved that: W=(V_{min}+V^{max})/2, if k → ∞ and $p_i = N_i/k$ $q_j = N_j/k$, N_i – how many times Ai strategy is selected.N_j – how many times Bj strategy is chosen.

$N_{A1} = 3$

$P(A_1) = 3/10 = {}^3/_{10}$

$N_{A2} = 0$

$P(A_2) = 0/10 = 0$

$N_{A3} = 3$

$P(A_3) = 3/10 = {}^3/_{10}$

$N_{A4} = 4$

$P(A_4) = 4/10 = {}^2/_5$

$N_{B1} = 2$

$P(B_5) = 2/10 = {}^1/_5$

$N_{B2} = 8$

$P(B_5) = 8/10 = {}^4/_5$

$N_{B3} = 0$

$P(B_5) = 0/10 = 0$

Game price, W = 6235

Information security administrator strategy:

$p = (^3/_{10}, 0, ^3/_{10}, ^2/_5)$,

that is firewall, cloud security and biometric identification use for protection in determined proportions.

The intruder strategy:

$q = (^1/_5, ^4/_5, 0)$,

that is code injection use and functionality abuse in determined proportions.

Thus, the investigation task is performed: it is determined what means of protection of integrity, confidentiality and accessibility of information are reasonable to use at PJSC “Zborivgaz” for cyber attacks protection under conditions of limited financial support.

3. Conclusions and prospects of further research

The interests of the information security administrator and the hacker regarding the computer assets of the enterprise are the same: to use them for their own activities. Therefore, to solve the problem of choosing a protection system, methods of game theory are proposed. The study confirmed the feasibility of using game theory to solve cybersecurity problems. Based on the proposed method, it is possible to choose a system of information security for the enterprise, taking into account the current landscape of threats and the available budget.

We are going to carry out investigations in the field of the development of corporate information security system having certain security level. There are many international methods and standards for determination of the information systems security reflecting the scientists and experts interest to this problem. However, there is no generally accepted method of security evaluation. We believe this is due to the rapid growth of cybersecurity as a new field of information technologies. Our further investigations will be aimed at generalization of methods for determination of the information-communication system security level and universal methodology formation.

4. References

[1] WASC Threet Classification v. 2.0, 2010. http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

[2] 2019 Cyberthreets Defense Report, Group CyberEdge, 2019 https://go.illusivenetworks.com/2019-cyberthreat-defense-report

[3] S Shiva, S Roy, D Dasgupta. “Game theory for cyber security”, CSIIRW '10: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, 2010, Article No.: 34, Pages 1–4.

[4] C. T. Do, N. H. Tran, C. Hong, C. A. Camhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, S. S. Iyengar “Game Theory for Cyber Security and Privacy”, ACM Computing Surveys (CSUR), 2017, Article No.: 30/

[5] V. Glushak, O. Novikov “Synthesys of defence system`s structure using positional game of defender and threat actor”. System investigation and information technologies, 2013, vol. II, p. 89-100 (in Ukrainian).

[6] I. Dobrynin, M. Borova “Optimization of information defense system building in the circumstances of antagonistic game”. Weapons systems and military equipment, 2018, vol. II, p. 89-93 (in Ukrainian).