Analysis and forecasting strategies of attacks on game resources for distributed cybersecurity training games

K V Safonov, V V Zolotarev and A M Derben

Reshetnev Siberian State University of Science and Technology, 31 Krasnoyarsky Rabochny Av., Krasnoyarsk, 660037, Russia

E-mail: amida.2@yandex.ru

Abstract. Game tasks are vulnerable to methods of obtaining benefits based on the results of attacks on game resources. In such conditions, it is critical to determine, monitor and evaluate the possibility of such attacks. It is also advisable to select methods to prevent them in advance, constructing the gaming environment accordingly.

The paper describes various types of attacks on the gaming environment, its vulnerable components. Some possibilities for building gaming environment were shown. To improve the architecture of the gaming environment, identify possible channels of key information leakage, game theory methods were chosen. The analysis was performed and the possibility of predicting the attack on game resources for a certain type of gaming environment was shown.

For a distributed multiplayer security awareness game based on a real case, the estimates for the selected types of attacks are shown, the attacker's selection criteria for the attack are calculated, and countermeasures are proposed. The article presents the results of two computational experiments with minor differences in the network infrastructure and the stored amount of game key information.

The results of the modelling of the main types of threats completely coincided with the obtained empirical data. The results shown can be used to evaluate various types of information security strategies in case of limited resources. The application of the approach is possible in various gamified media, including additional restrictions.

1. Introduction

There is a serious problem of countering various cyber attacks on game resources for certain types of game tasks used in information security for training. These tasks include quest game tasks [1], serious games on critical management spheres, as early-warning systems [2], digital card games [3], games of the Capture the Flag format [4], as well as, to some extent, various types of gamified MOOC resources and Web-resources of universities [5, 6].

The main problem of the game task in this case is the presence of a key, answer or hint, integrated into the task or located on a separate game server. Also it has a problem in security dimension of bring-your-own-device (BYOD) conception, as the future of one modern challenge of serious games [7]. To obtain a key from a task by attacking game resources will mean a violation of the logic of the game or an unfair advantage if we talk about quest type games; for other types of games - the solution of tasks that would otherwise require the development of certain skills, and disturbance of the game balance.

Consider specific examples of game problems and their technical features. In the article [8], the authors give an example of a quest-type game based on an attack of social engineering aimed at imitating a company office. The logic of the game involves the consistent receipt of information elements and their comparison to form the correct conclusion (answer). Attack on game resources in...
this case is possible both by distributed cyber attacks, using viruses and phishing [9], and by violating the actions specified by the scenario. In addition, the vulnerabilities of the software can be used for bypassing the "game" protective countermeasures and gain an unfair advantage.

In the [4, 10] articles, the authors consider examples of the game based on the technical features of the protection measures, setting a specific key as an answer. The types of attacks here are also different, starting from the mentioned above advanced persistent threat (APT) and ending with identity theft (command identifier). Moreover, it is possible to substitute or steal a key value, intercepting traffic.

Figure 1 provides some insight into the types of attacks on game resources.

![Diagram of types of attacks on game resources](image)

**Figure 1.** Several types of attacks on game resources.

There is a certain set of defensive measures that can counteract several types of attacks.

2. **Model of attack on game resources**

Distributed cyberattack was chosen as the attack model adopted for analyzing and predicting attacks on game resources. This type of attack involves the consistent violation of several game resources protection boundaries using phishing or other types of social engineering, identity theft, viral technologies and Trojans.

The game, considered as an attack target, has the structure shown in figure 2.

Game logics is built in the way that forecasting of right scenario of actions for an attacker can be more valuable than directly key theft or attack on a task generator.

Technically, the essence of the game considered is as follows: a random set of key sequences is generated, located in the documentation and tasks of the gaming environment. The managing structure of the gaming environment, represented by a set of modules, distributes tasks based on the scenario and adjusts them to reflect the current game analytics. The gaming environment can be either substantially automated or fully controlled from individual accounts. The same goes for the gaming environment. Game reports and gamified environment interfaces are available to participating teams.
Distributed cyberattacks (advanced persistent threat - APT) [11] until the end of 2015 - the beginning of 2016 did not represent significant risks for information systems [12], since only 2-3 criminal groups acted on the “black market” of viruses and Trojans distributors. The situation has changed dramatically over the past year [11], [13]: several dozen criminal groups are already offering their services on the black market, methods have changed, new “tools” have emerged and the old ones have improved significantly. The traditional system of ensuring the information protection involves the preparation of a passport of vulnerabilities. At the same time, the list of current vulnerabilities can reach several hundred units [14]. Closing them means to attract limited financial and organizational resources, using various methods, such as expert assessments of various types, based on the requirements and risk analysis [15], game theory [16] and others.

Taking into account game logics and its technical basis, as well as the chosen type of attack and its features (secrecy, detection complexity), it has been suggested that the defense mechanisms do not adapt to the actions of the attacker by performing predetermined actions. Thus, the game “man against nature” is considered, where the role of “man” is assigned to the attacker (A), and by “nature” (B) is meant the state of the protected gamified environment. It is specified that player A is partially aware of the valuable intangible assets of object B, understands in general the infrastructure of the gamified environment, maximizes the benefits from using the information received, does not attack randomly.

3. Experimental evaluation
The security awareness game was chosen as an experiment to counter attacks against the resources of educational institutions. Several scenarios were selected for possible actions of the game participants. The main content of the game was the following:

1) The participants of the game can act both individually and as a team. In the first case, it is considered that the team consists of one player.
2) The game interface is a server to which it is possible to send certain information for an attack (for example, a phishing email).
3) Report of the game is data containing information about the benefit gained by the team from the attack, points earned in which the keys obtained are converted.
4) The keys were hashes of articles and personal data of "employees". It was assumed In the legend of the game that the main value are unpublished articles.

5) Keys had different value. Points were determined as follows: for one record of personal data - 0.1 points; for one article type I (on natural sciences) - 350 points; for one article of type II (in the humanities) - 150 points.

6) The game defines the periods of each key relevance. If the key is received when it is irrelevant, points are not awarded for it. The period of relevance is chosen with a certain periodicity, unknown in advance to the players.

Consequently, there are 8 scenarios in the game that a participant can play. these scenarios can be as follows: Player A can get into the interval when useful material has already been published and there is no actual content (scenario 1), there is actual content only from natural science (scenario 2), there is actual the content is only a humanitarian profile (scenario 3), there are both types of content (scenario 4).

There are also 4 scenarios for personal data case:
- Under scenario 1, player A does not have access to personal data storage.
- With scenario 2, he gets access to a smaller part of personal data storage (about 10%).
- With scenario 3 - to most of personal data (about 90%).
- Scenario 4 assumes access to 100% personal data storage.

4. Types of attacks and benefit assessment
Let us figure out the types of actions that an attacker can choose: attack on external resources (A1); attack on a server that provides access to the Internet (proxy server) (A2); attack on the messaging server (communication or mail server) (A3); APT attack (A4); phishing (A5). A ratio 5%, 3%, 1%, 0.5% of the total information cost of the natural science and humanities articles was adopted respectively to scenario 1, 2, 3, 4.

Obviously, the attacks will correspond to the action scenario in the game, if we exclude the attacks A1 and A2; in this case, the attacker's goal is to gain an unfair advantage by getting access to key information without following the game’s logic and overcoming game defenses.

The initial data is represented in tables below (tables 1-2)

| Scenario | A1 | A2 | A3 | A4 | A5 |
|----------|----|----|----|----|----|
| Scenario 1 | 0 | 0 | 245 | 0 | 3845 |
| Scenario 2 | 0 | 1568 | 66850 | 10050 | 0 |
| Scenario 3 | 1813 | 77145 | 76900 | 76900 | 76900 |
| Scenario 4 | 0 | 0 | 10050 | 66850 | 3845 |

*Here and hereafter made for the benefit for the attacker the number of points he can receive for a successful investment targeted attacks on resources. The ability to score points in parallel in a regular way is not taken into account.

The difference in the experimental data is the result of the following factors: the number of hashes articles (in first experiment - 67 humanitarian profile, 191 natural science, in the second - 92 and 337 respectively); the number and structure of PD processed (experiment 1):
- PD 13.5% (2500) entries for scenario 1
- 86.5% (16000) for scenario 2, (experiment 2):
- 5.6% (1500) for scenario 1,
- 94.4% (25000) for scenario 2.

In addition, the generated differences in the network infrastructure were considered to account the random factor. External servers are allocated to a separate subnet that does not have access to the local network of object B in experiment 1. In experiment 2, external servers also have a local network interface through which it is possible to access three articles of the natural science profile; in addition, the mail server in Experiment 2 acts as a domain controller, which allows Attacker A, to install any malware on all computers in the domain.

5. **Analysis and prediction of attack scenario**

Initial data were assessed using the following criteria: Maximax, Bayes, Laplace, Wald, Savage, Hurwitz, Hodge-Lehmann. According to the results, the optimal strategy was chosen (table 3).

| Experiment | Criteria |
|------------|----------|
|            | Maximax | Bayes | Laplace | Wald | Savage | Hurwitz | Hodge-Lehmann |
| 1          | A3      | A3    | A3      | A3   | A5     | A3       | A3             |
| 2          | A3      | A3    | A3      | A3   | A3     | A4       | A3             |

As can be seen (table 3), the A3 attack is optimal for player A, the A5 attack for Experiment 1 and the A4 attack for Experiment 2 are in the second place. Therefore, it is necessary to protect management accounts from “identity theft” attacks to prevent attacks on game resources in practice, (two-factor authentication, control of connection logs, biometrics).

In addition, the key problems are phishing messages sent on management and game accounts, tracking of keywords and frequency parameters, outgoing IP is required. The use of targeted attacks on individual accounts and game resources is possible from the attacker point of view as can be seen from the modeling results.

6. **Future research and conclusion**

Taking into account the dynamics of gaming environments development, further research may focus on the development of attack models that involve role-playing interaction in gaming environments; the possibility of increasing or decreasing authorities. It is also interesting to investigate a variant of the gamified environment, built with account of group interaction in solving individual problems.

However, the final goal is to create a series of models that show the development of attacks on game resources of various types of gamified environments.

The results of the research allow ranking the threat model according to the following criteria: “most probable” predicted by most methods, “probable” – the prediction of which appeared at least once, and all others – threats with a “low probability”. The methodology proposed in the paper provides a mechanism for the allocation of resources for the organization of information protection in multi-user distributed gaming environments.

This method can be successfully implemented in managing information security risks, as well as in distributing the responsibilities of security personnel according to various schemes and models.

**Acknowledgement**

This work was supported by the Russian Foundation for Basic Research project No 19-013-00711 a.

**References**

[1] Kaivola T, Salomaki T and Taina J 2012 In quest for better understanding of student learning experiences *Procedia - Social and Behavioral Sciences* 46 8-12
[2] Roblek V, Kresal F, Pejic B and Meško M 2018 Early warning systems as a paradigm for understanding organizational behaviour in extreme environment 5th International Symposium: Cocreating responsible futures in the digital age

[3] Kordaki M and Gousiou A 2017 Digital card games in education: A ten year systematic review Computers & Education 109 122–161

[4] Tricker E, Disperati F and Gustafson E 2017 Shell We Play A Game? CTF-as-a-service for Security Education USENIX Workshop on Advances in Security Education (ASE)

[5] Klemke R, Eradze M and Antonaci A 2018 The Flipped MOOC: Using Gamification and Learning Analytics in MOOC Design – A Conceptual Approach Education Sciences 8(1) 25

[6] Tikhomirov V, Dneprovskaya N and Yankovskaya E 2015 Development of University’s Web-Services Smart Education and Smart e-Learning, Smart Innovation, Systems and Technologies 41 265-271

[7] Fernández-Manjón B, Moreno Ger P, Martinez-Ortiz I and Freire M 2015 Challenges of serious games EAI Endorsed Transactions on Game-Based Learning 2 150611

[8] Zolotarev V, Maro E and Kulikova S 2018 New approach to activity evaluation for social network based student collaboration 12th IEEE International Conference on Application of Information and Communication Technologies (AICT 2018) 374-380

[9] Chiew K L, Yong K S and Tan C L 2018 A survey of phishing attacks: Their types, vectors and technical approaches Expert Systems with Applications 106 1–20

[10] Pham C, Tang D, Chinen K and Beuran R 2016 CyRIS: a cyber range instantiation system for facilitating security training International Symposium on Information and Communication Technology 251-258

[11] Kaspersky Laboratory: Report on targeted attacks and complex cyber threats for the second quarter of 2017, available at: https://www.kaspersky.ru/about/press-releases/2017_how-targeted-attacks-developed-in-q2-of-2017

[12] InfoWatch: Global survey of confidential information leaks in 2016, available at: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2016_year.pdf?rel=1

[13] Vault 7: Projects, Wikileaks, available at: https://wikileaks.org/vault7/

[14] Cisco 2017 Midyear Cybersecurity Report, MCR, available at: https://www.cisco.com/c/en/us/about/press/press-releases/2017/07-21.html

[15] Zolotareva G, Zolotarev V and Filko S 2019 New approach to risk controlling in information security IOP Conference Series – Materials Science and Engineering in press

[16] Rass S, König S, and Schauer S 2017 Defending Against Advanced Persistent Threats Using Game-Theory PLOS ONE 12(1) e0168675