Evaluation of Game Resources as a Purpose of Cyber Attacks for Educational Games

Vyacheslav V. Zolotarev [1], Maria A. Lapina [2], Nikolay Y. Parotkin [1] and Elena V. Ulianova [1]

[1] *Siberian State Institute of Science and Technology named after M.F. Reshetnev, Krasnoyarsk, Russia*
[2] *North Caucasus Federal University, 2, Kulakova Str., Stavropol, 355000,*

Abstract

Game tasks are vulnerable to methods of gaining an advantage based on the results of attacks on game resources. In such conditions, it is critical to identify, monitor, and evaluate the possibility of such attacks. It is also advisable to choose methods of preventing them in advance, designing the game environment accordingly. An example of the use of training technologies that form users' awareness of information security issues for the task of predicting the choice of an attacker's attack vector is given.

The algorithm of actions of an attacker in a game environment to gain an advantage or bypass (violate) the logic of the training game is shown. Possible criteria for the selection of game resources as targets of an attack are shown. The scheme of actions for determining the target resource and the features that reduce its protection against various types of attacks are briefly described. The application of the approach is possible for multi-user games built on the simulation of various processes, including for training games of various directions.

Keywords [1]

Educational games, attacks on game resources, cyberattacks, an attacker

1. Introduction

For certain types of gaming tasks used in information security for training, there is a serious problem of countering various cyberattacks on gaming resources. These tasks include quest game tasks [1], business games [2], Capture the Flag format games [3], as well as, to some extent, MOOC-made resources of various types and university Web-resources [4, 5].

Of course, 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. For quest-type games, obtaining a key from a task by attacking game resources will mean violating the logic of the game or gaining an unfair advantage; for other types of games - solving tasks that would otherwise require the development of certain skills, and imbalance in the game.

The attacker's task in attacking the gaming environment can be twofold. On the one hand, he is interested in disrupting the gameplay. Perhaps he is not pursuing personal or team benefits. In this study, the main one is the second situation, when an attacker deliberately tries to gain an advantage or violate the logic of the game.

When solving a problem of the second type, an attacker looks for a non-standard way to bypass game tasks or obtain keys, hints, and answers by unauthorized access to them, bypassing the game environment.

[1]Proceedings of VI International Scientific and Practical Conference Distance Learning Technologies (DLT–2021), September 20-22, 2021, Yalta, Crimea

EMAIL: amida.2@yandex.ru (Vyacheslav Zolotarev); norra7@yandex.ru (Maria Lapina); nyparotkin@yandex.ru (Nikolay Parotkin); elenavladimirovnay@mail.ru (Elena Ulianova)
ORCID: 0000-0002-8054-8564 (Vyacheslav Zolotarev); 0000-0001-8117-9142 (Maria Lapina); 0000-0002-3486-0602 (Nikolay Parotkin);

Previously considered [6] targeted attacks on game resources aimed at the components of the game environment:

- the logic of the game, including the rules;
- clues, answers, and hints;
- content (for substitution and destruction);
- web interfaces;
- channels of connection;
- accounts;
- means of communication for players.

Accounts and communication tools, like web interfaces, can be used to penetrate the game environment, unauthorized access to resources, including through attacks on these components, others can be violated - for example, to influence the game logic through developer accounts or interfaces management of physical components.

In addition, it is possible to take into account the peculiarities of working with gaming technologies in a virtual environment [7] and tracking the actions (collecting a digital footprint) of players in the gaming space [8]. It may also be of interest to take into account game-theoretic modeling for certain types of relevant attacks, for example, phishing attacks [9].

The main target of an attacker can be any type of game resource including those containing game content, rules, and technology that implements it.

To assess game resources as targets of cyberattacks, the following conditions are accepted:

- game resources based on imitation of various technological or other processes are more interesting as an educational element of the game and, as a result, may be of greater interest to an attacker. The reason for this focus on imitating resources is the data that is collected for legal access to them. Such resources will collect and store lists of user accounts, be mentioned and discussed in communication systems, and serve as a point of attraction for players;
- the attacker will choose those resources to which there is access and which are more valuable to him subjectively. This behavior of an attacker can help predict his actions, evaluate the optimality of attack algorithms from his point of view [6];
- game resources, access to which is possible through access channels with the lowest level of user awareness, even if one of the conditions is not met for them, can be attacked in the first wave of an attack.

Next, consider how you can confirm the existence of these conditions in a training game.

2. Selecting Game Resources for an Attack Based on the Value for the Attacker

Earlier, in the article [6], as in some other cases [10, 11, 12]. It was shown that there are several basic attack scenarios for imitating the game process in a training game. The following criteria were used to evaluate the scenarios: "maximax", Bayes, Laplace, Wald, Savage, Hurwitz, Hodge-Lehmann. The optimal strategy for the attacker was chosen. To analyze the actions of the attacker in the above experiment, a game-theoretic model was chosen.

The criteria for selecting the target resource in the indicated experiment were:

- value of information. Information suitable for sale as a source of profit was assessed;
- the attacker's awareness of the presence or value structure of the resource;
- the attacker's awareness of the infrastructure of the target game resource;
- meaningfulness of the attacker's actions.

In the gaming environment, as a rule, these characteristics are not hidden. It is always open space for the exchange of information between players. The ability to restrict access to certain information about the gaming environment exists, but, as a rule, this concerns the infrastructure - the configuration of the environment, the location of the game resource on physical servers, the logic of assigning points for tasks, archives of digital traces, and so on. In general, collecting information about the gaming environment is not difficult for an attacker.

An attack on a game resource has a certain pattern:

- the point of entry into the game space is determined - the player's account or manager account, service interface, resource web interface;

- the authentication mechanism is analyzed;
- the communication protocol (protocols) is analyzed;
- the possibilities of the registration and accounting system are being studied;
- the capabilities of the attack response system are being studied.

Having gained a certain understanding of the protection of the gaming environment, the attacker implements one of the types of targeted attacks on the resource, taking advantage of the vulnerabilities of the studied components.

The results of an attack can be tracked both by the player's digital footprint (changing the nature of tasks, gaining an advantage, changing capabilities or information support), and by using the components of the game space - web interfaces, rarely used forms of information presentation, access to files containing certain data ...

Examples of attacking actions may even include the use of analytics of the internal chats of the game by an attacker to analyze the tasks being performed and predict the logic of access to them.

Identifying strategies can point to some security issues and recommendations for gaming environments that need to be complemented by requirements for the physical elements that implement the gaming and learning process, namely:

- to prevent attacks on gaming resources in practice, it is necessary to protect management accounts from identity theft attacks (two-factor authentication, control of connection logs, biometrics);
- ensuring the protection of physical communication interfaces of the hardware from unauthorized interception of data or the implementation of control actions, the introduction of mechanisms for monitoring the integrity and/or encryption of transmitted data;
- protection against phishing attacks on manager and game accounts is required. Tracking of keywords and frequency parameters, outgoing IP in in-game and external communications is required.

These requirements are partially offset by the use of organizational measures by the majority of participants, which is possible by increasing their level of awareness of related issues of interaction with the external one when following the instructions for using the platform.

3. The Dependence of the Attack Vector on User Awareness

To solve this problem, there are specialized systems for training and knowledge control - they help to automate such activities, in particular, the Kaspersky Automated Security Awareness Platform (ASAP) used in the study [13]. It is also possible to consider the possibility of assessing attack scenarios both at the level of theoretical modeling and at the level of related vulnerabilities [14]. For example, exploiting LMS Moodle vulnerabilities [15], such as CVE-2019-3810, CVE-2019-3848 (additional information extraction), CVE-2019-10154 (messaging analysis), CVE-2019-10186 (obtain a session key in certain XML handling situations), CVE-2019-3849 (privilege escalation), CVE-2019-3850 (comment handling) and CVE-2019-10133 (link handling).

It should be noted that such means of studying user awareness can be part of the gaming environment. For example, by collecting a digital footprint during test tasks, you can analyze the potential exposure of a user (or a group of users) to phishing attacks.

Separately, we can consider conducting a test attack (penetration testing) for a gaming environment. If test attack mechanisms are integrated into the game space, the player will perceive them as an element of such space, and collecting a digital trail will give the best result.

To assess the possibility of choosing an attack vector, it is possible to designate an indicator of an increase in the level of user knowledge based on the test results before and after training. The number of test participants is 70 people. The test results for the above typical attacks for educational gaming environments are shown below (Table 1).

If we consider these vectors of attacks, we can see that the resistance of users to a direct attack on the web interface or through external resources, as well as through personal accounts in the social network, will always be higher, and the most interesting for the attacker remains in this case, as well as and in-game modeling of targeted attacks, an attack vector using email and in-game communications.

Table 1
Typical Attack Targets and User Awareness Assessment

№	Module	Number of users tested	Wed entrance test score (%) *	Wed exit test score (%) *
1	Email	20	44	92
2	Websites and internet	20	53	94
3	Social networks and messengers	20	51	91

The attacker's algorithm looks like this:

1. Determination of the module or sub-process that is the focus of attention in the interaction of players and/or organizers.
2. Define the tasks of the module or process defined in step 1.
3. Search for vectors of attacks on a module or process, defined in step 1.

3a. Assessment of “simple” metrics, such as the level of user awareness of the security issues of a component of the gaming environment.

3b. Evaluation of "complex" metrics, work with the social graph, clarification of possible ways and secondary (tertiary, etc.) goals of a phishing attack.

3c. Evaluation of the used communication protocols with the physical elements of the system to modify or intercept data.

4. Identification of additional factors for a successful attack, such as weak authentication mechanisms or lack of logging.
5. Evaluation of the results of the trial exposure.
6. Implementation of the main attack on game resources.

The general scheme of using the algorithm is shown in the figure below (Fig. 1).

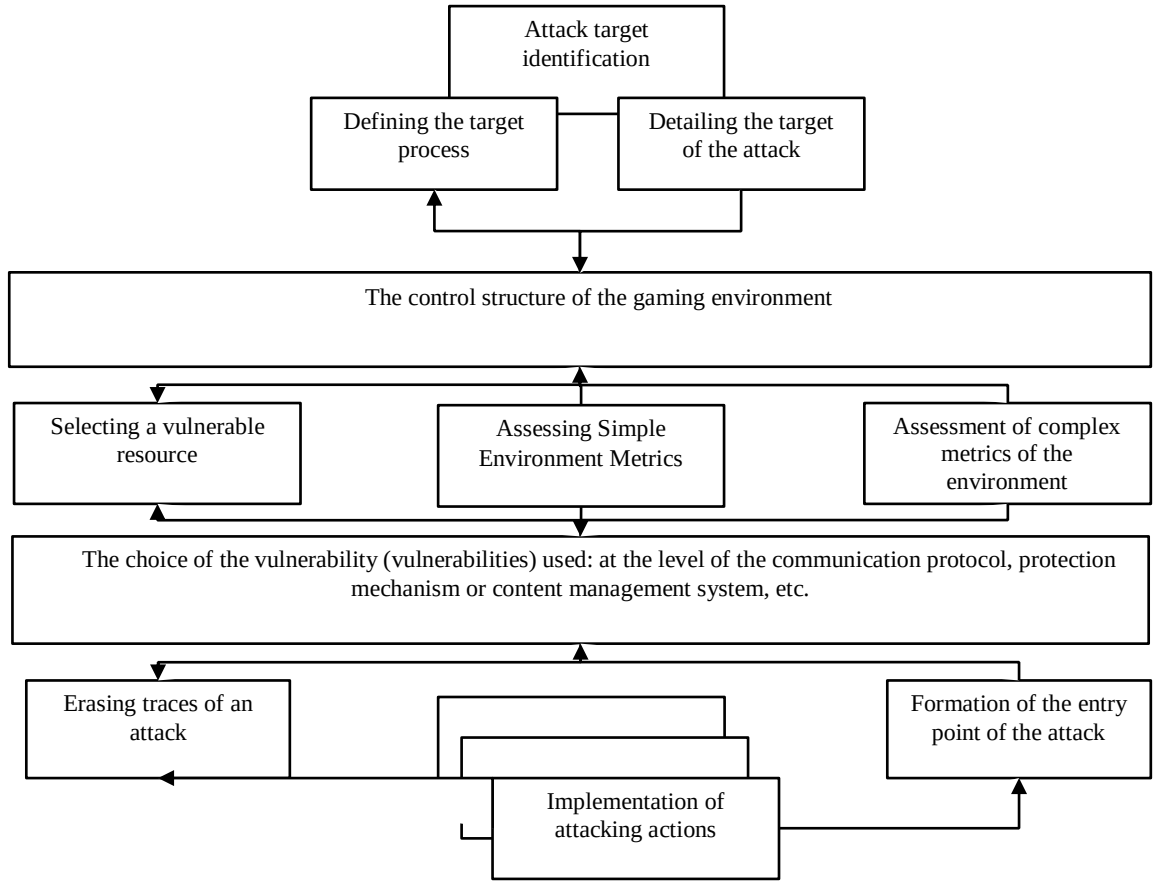

Figure 1: Diagram of using the algorithm

It should be noted that when forming an attacking toolkit, an attacker must adhere to the results of a previously obtained study of the system, but only if a targeted attack is being implemented. In the case of a mass attack, for example, phishing or using viruses, the attacker analyzes the initial response of the system and reacts to it.

It is also possible to note situations of using fuzzing as an element of an attack when the studied web interfaces or applications are tested by an attacker using random data sets, but such an attack is more of theoretical interest since it is easily detected and blocked. The only dangerous situation here is when the open web interfaces of the game space (or software services with open access) are not controlled by the security subsystem and their response is not investigated, at least in retrospect, but even a banal selection of authentication data such as logins and passwords for manager accounts.

As a rule, a certain minimum level of implementation of protective measures is assumed, which guarantees the successful existence of the game space in the aggressive virtual environment of the open network by default.

In addition to the attack itself, as indicated in the diagram, the attacker will be interested both in assessing vulnerable resources (including through predicting user awareness) and in eliminating traces of the attack. The work of an attacker with the protective mechanisms of the gaming environment can consist in both destroying and substituting data for registering security events, distorting or destroying a digital footprint, changing or distorting game analytics.

An attacker, evaluating complex attack metrics, can also target user vulnerabilities outside the gaming environment. For example, the theoretical assessment of the resistance of users of the gaming environment to a phishing attack necessarily includes the work of the target user with social networks.

The attacker will aim to identify the focus of users' attention, to select an attack vector using system components for which there is low user awareness of security issues.

4. Future Research and Perspectives

Previous studies allow us to focus on developing attack models and assessing how an attacker can influence the gaming environment or its physical components that do not have secure interaction interfaces. Possible attacks on certain information protection mechanisms, such as authentication, may also be of interest for further research. It is planned to study various gaming environments for various areas of study.

The following areas of research are of particular interest: multimodal authentication systems and their vulnerabilities when implemented in educational gaming environments; the possibility of implementing targeted attacks on game resources and statistics of this type of attacks; study of incidents related to game resources in educational games; changing attack vectors taking into account the massive transition to distance learning.

The authors suggest that the study of the vulnerabilities of communication protocols of video conferencing systems that implement communication channels in gaming environments, as well as analysis of the possibilities and methods of preventing phishing attacks, is also of significant interest.

5. Conclusions

The conclusions made allow us to concisely formulate the order of actions of the attacker, allocate key resources and entry points to the system that need to be protected. It is of interest to evaluate the choice of an attack vector based on the prior knowledge of the attacker about the technologies used. This assessment predicts an attacker's actions and vulnerabilities in existing gaming environments.

The study of user awareness as an element of predicting the targets of an attack has also practical application as a study of the dynamics of changes in the landscape of security threats. Using these approaches, the security service can tune and adjust both the configuration of the environment and the registration and accounting system, including such protective technologies as a honeypot and/or honeynet.

In general, it should be noted that the study of attacks on educational games is necessary since at the moment there is a tendency to increase the danger of their use due to the opening of interfaces, access

points to the game space when transferring games to a virtual environment, and this, in turn, can be dangerous and for the basic infrastructure of the educational institution on which the game is deployed.

6. Acknowledgments

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

7. References

[1] E. Ishchukova, E. Maro and G. Veselov, Development of information security quest based on the use of information and communication technologies. ACM International Conference Proceeding Series, No 3357632. 2019

[2] V. Roblek, F. Kresal, B. Pejic, and M. Meško, Early warning systems as a paradigm for understanding organizational behavior. In extreme environments 5th International Symposium: Co-creating responsible futures in the digital age. 2018

[3] E. Trickel, F. Disperati and E. Gustafson, Shall We Play a Game? CTF-as-a-service for Security Education USENIX Workshop on Advances in Security Education (ASE). 2017

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

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

[6] K. Safonov, V. Zolotarev, and A. Derben, Analysis of attack strategies on game resources for technological processes training games. IOP Conference Series: Materials Science and Engineering 822 (1) 012027. 2020

[7] S. Karagiannis, E. Magkos, Adapting CTF challenges into virtual cybersecurity learning environments. Information and Computer Security, 2020. DOI: 10.1108/ICS-04-2019-0050.

[8] B. Krylov, M. Abramov, A. Khlobystova, Automated Player Activity Analysis for a Serious Game About Social Engineering. Studies in Systems, Decision and Control, 2021. V. 337, PP. 587-599.

[9] F. Tchakounte, V. Nyassi, E. Duplex, K. Udagepola, M.Atemkeng, A Game Theoretical Model for Anticipating Email Spear-Phishing Strategies. ICST Transactions on Scalable Information Systems, 2020. pp. 1-24.

[10] S. Hart, A. Margheri, F. Paci and V. Sassone, Riskio: A Serious Game for Cyber Security Awareness and Education Computers & Security 95 101827. 2020

[11] A. Ali Zani, A. Norman, and N. Ghani, A review of security awareness approach: Towards achieving communal awareness. In Cyber Influence and Cognitive Threats Academic Press 97-127. 2020

[12] S. Sherbakov, M. Lapina, V. Lapin, & J. Rugelj, Methodological support of game modeling in the educational process. Paper presented at the CEUR Workshop Proceedings SLET-2019. Proceedings of the International Scientific Conference Innovative Approaches to the Application of Digital Technologies in Education, 2861, 2020, PP. 351-361. http://ceur-ws.org/Vol-2861/

[13] Kaspersky Automated Security Awareness Platform URL: https://k-asap.com/ru/

[14] V.V. Zolotarev, A.B. Arkhipova, N.Y. Parotkin, A.P. Lvova, Strategies of social engineering attacks on information resources of gamified online education projects. CEUR Workshop Proceedings. 2021. Vol. 2861: International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education (SLET–2020), Stavropol, 12–13 Nov. 2020. PP. 386-391.

[15] Moodle: CVE security vulnerabilities, version, and detailed reports. https://www.cvedetails.com/product/3590/Moodle-Moodle.html?vendor_id=2105