Strategies of Social Engineering Attacks on Information Resources of Gamified Online Education Projects

Vyacheslav Zolotarev[a], Anastasiya Arkhipova[b], Nikolay Parotkin[a], Anna Lvova[c]

[a] *Siberian State University of Science and Technology, Krasnoyarsk, 660037, Russia*
[b] *Novosibirsk State Technical University, Novosibirsk, 630073, Russia*
[c] *North-Caucasus Federal University, Stavropol, 355017, Russia*

Abstract

Safe collaboration in complex projects is a key way of multi-university interaction. With the development of educational strategies aiming at network implementation, safe collaboration tools have to be tested and evaluated with different empirical and analytical techniques.

The work investigates the possibility of predicting social-engineering attacks on information resources through understanding the interaction model of participants in networking educational projects. It presents results based on managing roles and tasks within a project, applying an indistinct attack readiness indicator in choosing an attack strategy.

Some experiments carried out within the framework of existing networking are shown.

The results are promising for educational environments and in the design of protective actions for information resources in networking educational projects.

Keywords [1]

education, quest, model, activity forecasting, gamification, role model, task model.

1. Introduction

The networking of universities in collaborative projects is a complex sequence of activities, including the deployment of common information resources used on a cooperative basis by all project participants. A particular challenge in terms of the emerging risks of information interoperability is the implementation of gamification in such projects.

The several approaches which are requiring a generalisation of the principles of secure information exchange between participants can be identified. For example, projects based on cooperative game tasks execution [1] or game-based learning [2] can provide interesting insights into safe collaboration. Phishing attacks [3-5] are the most studied types of social engineering attacks. Moreover, game-theoretic issues of modelling intruder actions, including using stochastic and signalling games as tools [6-9], allow us to look at the problem from the perspective of attack scenario selection. Particular attention is paid to the issues of remote access and rights differentiation between the participants, while when implementing role-based interaction (e.g., for the web or social network-based projects [10]), role-based access control models can be used within the resources and information systems of the project. The scheme of access based on roles and tasks inside a gamified networked educational project is shown in Fig. 1.

SLET-2020: International Scientific Conference on Innovative Approaches to the Application of Digital Technologies in Education, November 12-13, 2020, Stavropol, Russia

EMAIL: amida.2@yandex.ru (Vyacheslav Zolotarev); arhipova@corp.nstu.ru (Anastasiya Arkhipova); NYParotkin@yandex.ru (Nikolay Parotkin); lvova.ap@gmail.com (Anna Lvova)

ORCID: 0000-0002-8054-8564 (Vyacheslav Zolotarev); 0000-0003-0791-8087 (Anastasiya Arkhipova); 0000-0002-3486-0602 (Nikolay Parotkin); 0000-0002-9863-564X (Anna Lvova)

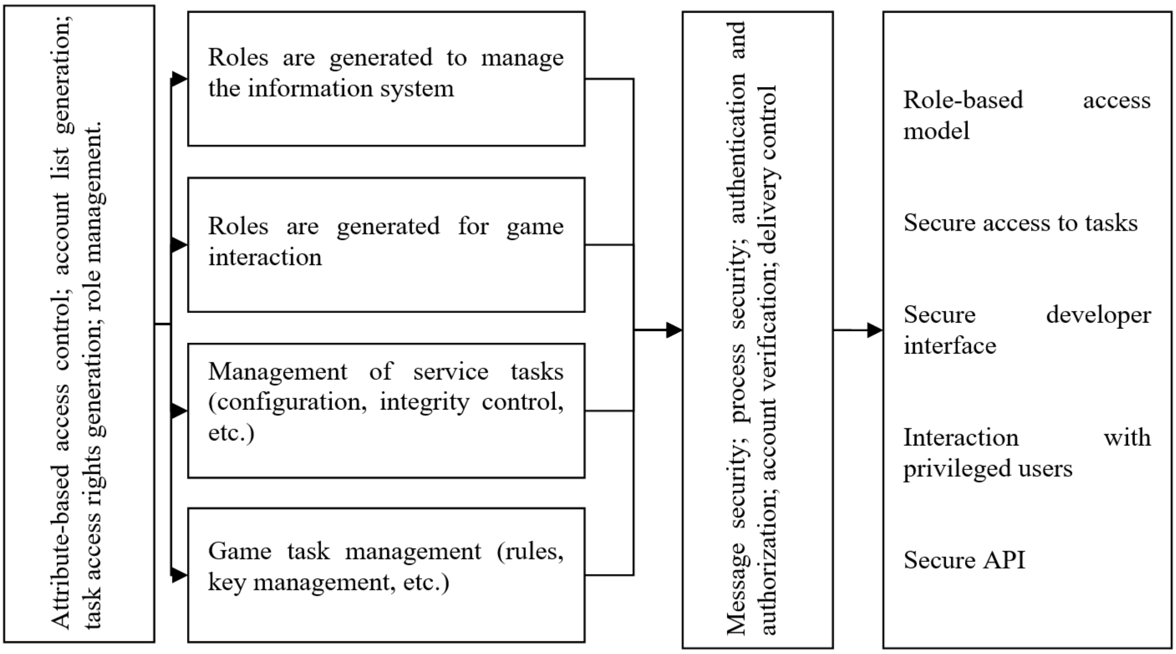
Attribute-based access control; account list generation; task access rights generation; role management.
Roles are generated to manage the information system
Roles are generated for game interaction
Management of service tasks (configuration, integrity control, etc.)
Game task management (rules, key management, etc.)
Message security; process security; authentication and authorization; account verification; delivery control
Role-based access model
Secure access to tasks
Secure developer interface
Interaction with privileged users
Secure API

Figure 1: Access based on roles and tasks

It is correct to consider information interaction risks as well. When predicting the strategy of impact on information resources of a gamified collaborative project, information protection tasks can be simplified and standardized (by choosing the most suitable scenarios for the intruder for counteraction). In the following, we consider an approach that implements intruder actions evaluation for social-engineering attacks.

2. Purpose and objectives of the research

Social engineering attacks [11] have started to spread actively with the use of individual accounts of participants, both staff and learners, in online educational projects. The boundaries of privacy have shifted. A personal account can be attacked during an educational interaction and privileged within the information system of an online educational project.

Thus, the aim of the project is to identify and investigate strategies of social engineering attacks directed through participants in networked educational projects, especially gamified ones, against the shared information resources of such projects.

The choice of intruder strategy is shown through the features of role- and task-based access control model in the information system of collaborative educational project. The goals of the intruder at each levels of social-engineering attack are shown. The feature of quantitative assessment of the scenario will be the application of an indistinct attack readiness indicator when selecting a scenario of an attack. Next, the practical relevance is assessed using the example of attacks carried out on educational resources.

This will show some general steps for identifying such an attack scenario and analysing it from the intruder's perspective.

3. Main part

Based on the characteristics of social engineering and APT attacks, including those for gaming tasks [12-14], it is possible to formulate an intruder's algorithm of action:

1. Identifying a module or sub-process containing the aspect of players and/or organisers interaction which is the intruder's goal. This may be the transfer of keys to the game tasks or the formation of a solution as part of a shared resource's cooperative use.

2 Define the tasks to be undertaken by the module or process defined in step 1.

3. An empirical estimator of parameters and metrics suitable for assessing the vulnerability of participants (participants' social network accounts) in a gamified collaborative project to social engineering attacks.

3a. Estimation of "simple" metrics such as the number of friends and followers, formation of strong (relatives) and weak (living in the same city, etc.) ties, assessment of the intensity of information exchange.

3b. (if necessary). Estimation of "complex" metrics, working with the social graph, clarifying possible pathways and secondary (tertiary, etc.) targets of attack.

4. Estimate the qualitative content of the participant-resource linkages in order to estimate additional motivation.

5. (if necessary). Complementing the participant model with the means to protect against social engineering attacks that the participant or the social network itself implements.

6. Implementing the attack.

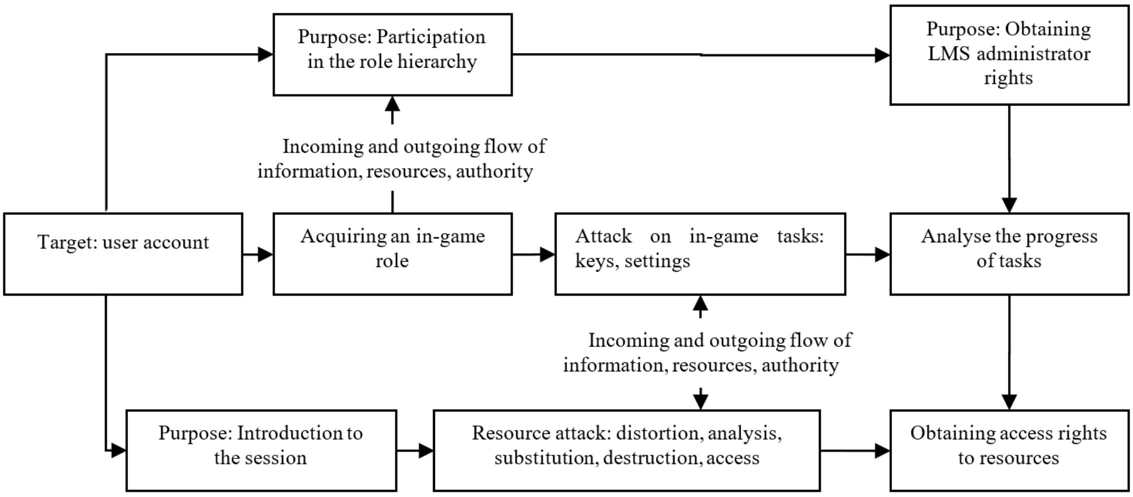
Purpose: Participation in the role hierarchy
Purpose: Obtaining LMS administrator rights
Incoming and outgoing flow of information, resources, authority
Target: user account
Acquiring an in-game role
Attack on in-game tasks: keys, settings
Analyse the progress of tasks
Incoming and outgoing flow of information, resources, authority
Purpose: Introduction to the session
Resource attack: distortion, analysis, substitution, destruction, access
Obtaining access rights to resources

Figure 2: Initial attack scenario selection based on access control features

Having decided on a primary attack scenario, the intruder uses the idea of the greatest benefit to refine the scenario. The model below describes how it is possible to predict an intruder's actions when using a particular scenario or a combination of scenarios.

At the same time, within the framework of the task of implementing a social engineering attack, several basic scenarios can be identified for common information resources of gamified network projects.

Such scenarios could be:

1. Exposure to rules and content. Pretexting. Implementation of reverse social engineering.

2. Attack to the web interface. Introducing elements to facilitate a phishing attack.

3. Account theft and spoofing. Identify a participant's place in a role- and task-based access control model and use their account to execute an attack.

4. Attack to the communications, including interception or spoofing for social media, forums or email messages.

5. Infrastructure integrity attack, i.e. the substitution or distortion of a common resource to implement a social engineering attack.

Working within the specified algorithm, an intruder chooses one or more scenarios for an attack. The choice of scenario will primarily be based on the access control features of the project, depending on the purpose of the attack (Fig. 2).

From the intruder's perspective, (given the constraints of the security policy framework in which the attacked entity operates), the following sequence of indistinct evaluations can be constructed.

Let an information system X have a security policy that involves the following components:

O is the set of system objects;

S is the set of subjects ($S \rightarrow O$);

T is a set of types;

X = {r (read), w (write), x (execution)} is the set of access types.

U is the set of user competences.

Then the owner of object *O* can be defined for any *X* as $T \rightarrow U$, and the access of subjects to certain objects of the system is *T*×*R* → *{allow, deny}*. The intruder considers the attack context and possible targets for the attack, formed as an enumeration of objects with specified owners.

An affiliation matrix can be formed like this:

Table 1

Membership matrix

	O_1	…	O_N
O_1	<X, U>	…	<X, U>
…	…	<X_i, U_j>	…
O_N	<X, U>	…	<X, U>

Let us denote the set of attacks on information system *X* as $A = \{A_1, \ldots, A_Z\}$. Then the set of attack scenarios on the information system is a Cartesian product of the form:

$$<C_{A^1} \times C_{A^2} \times \ldots \times C_{A^Z}>,$$

where $C_{A^Z} = \{C^1_{A^Z}, \ldots, C^l_{A^Z}\}$ is the set of possibilities to implement *l* attack scenarios A^Z.

Next, forming the coefficients of importance for the implementation of scenarios based on expert estimation of the capabilities of the managerial staff of the organization (the intruder, applying methods of targeting, select a specific target - LMS administrator, the owner of the in-game process, in-game role and the person who assigns it) and adjust from their position set C_{A^k} (*k* = [1, *Z*]).

As a result of expert qualitative estimation of the set of system objects *O* in the form of a set of indistinct *CE* evaluations, it is possible to propose a definition of the attack readiness indicator in the form of an indistinct number $\underset{\sim}{LS_j}$:

$$\underset{\sim}{LS} = \sum\nolimits_{\sim}{}_{t=1}^{Z} C_{A^t} \times \underset{\sim}{CE}\,.$$

where $\sum_{\sim}$ – indistinct addition performed using one of the methods of implementing indistinct arithmetic operations.

From this position in the simulation, an attack scenario can be identified that provides information on both the possible depth of attack (see Fig. 2) and the attack target that the intruder will choose based on the analysis of potential targets.

4. Relevant vulnerabilities

Within the framework of the considered scenarios of attack implementation in network learning and gamification it is necessary to consider a possible set of office applications, social networks and networking environments of communication and interaction between users. The use of which is convenient and commonplace both within the interaction of the educational project and the everyday activities of the participants. As such, let us consider the following representatives of the mentioned classes:

1. Discord messaging system (discord. com/);
2. Adobe Acrobat Reader is a reading and editing tool;
3. The social network VKontakte (vk. com);
4. LMS Moodle.

The scenario of an intruder gaining access to the system of any participant in the same messenger communication channel can be illustrated by the use of the closed 2020 Discord vulnerability CVE-2020-15174 [15] for cross-site scripting in iframe. The latter is an attack using social engineering techniques, as with this technology an intruder can get participants of a conversation interested in unusual content (a video, 3d model, interactive module), with content that can be tailored to a specific person or be interesting to all, followed by connection filtering.

The use of PDF documents containing interactive elements with JavaScript code to distribute tasks, receiving responses from participants via interactive forms, could lead to a similar situation. If we consider the number of vulnerabilities that Adobe addresses in this product and the relatively infrequent updates by the end user, the level of risk will be quite high.

As an example, here is a list of vulnerabilities resolved at the end of 2020 from CVE-2020-9693 to CVE-2020-9723. These allow access outside of the user's memory area and execution of arbitrary code [15].

LMS Moodle as a basis for educational projects also has a set of vulnerabilities [15]. Some relevant ones can be highlighted**.** For example, CVE-2019-3810, CVE-2019-3848 were used for additional information extraction.

CVE-2019-10154 was used for messaging analysis. CVE-2019-10186 was used to obtain a session key in certain XML handling situations, and CVE-2019-3849 was used for privilege escalation. Within the resource interaction, CVE-2019-3850 (comment handling) and CVE-2019-10133 (link handling) should also be noted.

5. Conclusion

The approach shown for estimating an intruder's actions in a social engineering attack on information resources is not only suitable for networked educational projects. In any distributed work with databases or other shared resources, this approach is acceptable.

In addition, it should be noted that the approach takes into account some peculiarities of the development of network education projects, which have not been considered much before. For example, the issue of mixing personal and corporate accounts is touched upon. The idea of vulnerability of particular representatives of project administration to targeted social-engineering attack is also taken into account. Working with project resources from the intruder's point of view is also possible, taking into account the peculiarities of the access control model.

Assessing the potential for targeted attacks on the information resources of online education projects will be shown in future research, but given existing publications [7,8], this seems to be a promising avenue.

6. Acknowledgement

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

7. References

[1] Grandhi S.R., Galimotu N.C. Understanding social engineering threats in massively multiplayer online role-playing games: an issue review / GAP Indian Journal of Forensics and Behavioural Sciences, 2020. Vol. 1, Issue 1, pp. 66-71.

[2] Rugelj J., Lapina M. Game Design Based Learning of Programming: CEUR Workshop Proceedings SLET-2019 – Proceedings of the International Scientific Conference Innovative Approaches to the Application of Digital Technologies in Education and Research, 2019. Pp. 29-42

[3] Kang L., Chek K., Choon L. A survey of phishing attacks: Their types, vectors and technical approaches / Expert Systems with Applications, 2018. Vol. 106, pp. 1-20.

[4] Chaudhry J.A., Chaudhry S. A., Rittenhouse R. G. Phishing Attacks and Defenses / International Journal of Security and Its Applications, 2016. Vol. 10, No. 1(2016), pp.247-256.

[5] Sahu K.R., Dubey J. A Survey on Phishing Attacks / International Journal of Computer Applications, 2014. Vol. 88(10), pp. 42-45.

[6] Figueroa N., L’Huillier G., Weber R. Adversarial classification using signaling games with an application to phishing detection / Data Min Knowl Disc, 2017. Vol. 31, pp. 92–133.

[7] Zhu Q., Rass, S. On Multi-Phase and Multi-Stage Game-Theoretic Modeling of Advanced Persistent Threats / IEEE Access, 2018. pp. 1-1.

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

[9] Ge J., Manghui T., Tae-Hoon K., Justin H., Jonathan W. Game based Cybersecurity Training for High School Students / SIGCSE '18 Proceedings of the 49th ACM Technical Symposium on Computer Science Education, 2018, pp. 68-73.

[10] Zolotarev V., Zhukova M. Role model features in educational serious games / 2019 International conference «quality management, transport and information security, information technologies» (IT&QM&IS–2019), 2019, pp. 583-586.

[11] Salahdine F., Kaabouch N. Social Engineering Attacks: A Survey / Future Internet. 2019, p. 11.

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

[13] Safonov K., Zolotarev V., Derben A. Analysis and forecasting strategies of attacks on game resources for distributed cybersecurity training games / IOP Conf. Ser.: Mater. Sci. Eng., 2020. Vol. 822, paper No. 012027.

[14] Khlobystova A., Abramov M. The models separation of access rights of users to critical documents of information system as factor of reduce impact of successful social engineering attacks / CEUR Workshop Proceedings, 2020. Vol. 2782, pp. 264-268.

[15] CVE® Program https://cve.mitre.org/

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