



(REVIEW ARTICLE)



Development of a 2D game application for learning networks and security

Sison Ariel Antwaun Rolando C, Centeno Criselle J, Mercado Mark Anthony S, Dapitan Louell Royce, Farparan Leonard Z * and Gonzales Ram Carlo V

College of Engineering Department, Pamantasan ng Lungsod ng Maynila, Manila, Philippines.

World Journal of Advanced Research and Reviews, 2023, 18(03), 1283–1289

Publication history: Received on 09 May 2023; revised on 21 June 2023; accepted on 23 June 2023

Article DOI: <https://doi.org/10.30574/wjarr.2023.18.3.1191>

Abstract

In adeptly learning computer networks, realizing the procedural skills needed and creating a semantic link to an abstract concept is a challenge to all learners pursuing the study as well as instructors. The problem has been more recognized during the 2020 pandemic where most of the classes are conducted online. Teaching complicated concepts without providing visualization present in a laboratory environment can be seen as ineffective to some learners – leaving them with such abstract ideas. In some scenarios, providing a nice laboratory for newcomers can be costly to most educational institutions and to said probationers.

In this paper, the research aims to develop a 2D game application with the objective of promoting an interactive way of learning advanced networking concepts while disseminating awareness on network security threats. This is to familiarize learners with the risk of such threats and to learn ways to prevent these attacks. The game application was play tested with thirty-five (35) BSIT students from Pamantasan ng Lungsod ng Maynila which shows promising feedback. It was concluded that most students find the gamification effective – delivering a more interactive way of learning networking concepts while keeping them aware of network threats.

Keywords: Procedural skills; Abstract concepts; Laboratory environment; Network security threat; Gamification

1. Introduction

It is a challenge to students as well as teachers to realize procedural skills and create a semantic link to an abstract concept especially in learning computer networks. This is the reason why it is important for students to practice such concepts in a laboratory environment. However, building real computer networks and laboratory environments can be expensive. Regardless, with the advances in computer technologies over the last decades, the use of computer-based instruction methods has become more common, delivering high end performance for education at a low cost. This serves as a virtual laboratory for students to acquire and master their practical skills with the absence of a real laboratory. A study was conducted which aims to relate the viability of using a specifically designed computer game to integrate abstract learning materials as a part of a blended learning environment in teaching routing topics in a computer network course. The method was proven to have as much effectiveness in teaching the topic as the traditional way. However, it positively influences the student's motivations towards learning the topic at hand [1]. (Halil, G. 2018)

The computer network course teaches learners the distribution arranging environment of the network topology, they often rely on network simulators to learn the structure of the study. The simulator offers an effective, interactive environment for learning networking concepts and protocols. When learning the simulator, instructors can provide lessons for the simulator while explaining the basics of the computer network course or they can apply for an online course in learning how to use the simulator while testing the user's knowledge of the system. While these can help you learn the computer networking course, learning the subject from instructors and online courses costs time and patience.

* Corresponding author: Farparan Leonard Z

It's especially very taxing for learners applying for the course due to the abstracts and complexity of the study [1]. (Halil, G. 2018)

Positive attitude towards learning is vital in achieving one's success therefore in learning abstract topics and protocols in computer networking courses, it is also important to motivate students. According to Zheng (2015), some students lose motivation in learning complicated networking concepts [2]. Having an interactive learning experience gives students the opportunity to control their own learning and a chance to have hands-on experiences with subject matter and is supportive of high-level student learning as well as mastery of practical skills.

The study aims to provide a game application that can be used as a learning tool for students, motivating them to learn the abstract concepts of the network topology and simulates in real life scenarios for when they pursue the study. The developers will create a level-based game applying the basic lessons and necessities of creating and handling the network. According to Shneiderman (2018), creation, exploration and discovery are the key factors for student motivation [3]. Sylwester (2018) claimed that engagement is critical for motivation of the students [4]. The application also aims to widen the peak of students curious enough to take the study and show how the lesson is learned and then let them simulate the stand of being a IT technician.

1.1. Statement of the problem

- Rudimentary Approach in Computer Networking Education in Online Learning

A study conducted by Hermogenes M.G. (2019) evaluates the internet security awareness and practices of students enrolled at Bulacan State University Sarmiento Campus during the 1st semester of AY 2017-2018. A total of 289 students from different departments were requested to answer a survey using Google Forms. The survey suggests that most students are still unaware of the vulnerabilities and risks that come with accessing the internet. It concluded that students are not fully aware of the existence of security threats and how to identify them, and they are, therefore, unable to execute appropriate defense mechanisms to mitigate such threats [5].

- Limited Knowledge of Students in Mitigating Cyber Security Threats

A study by Hermogeno M.S. (2019) concluded that educational institutions should equip students, teachers, and staff with proper education on cybersecurity awareness and training programs. It was found out that students have a significant level of security awareness but are still not fully aware of the security risks and proper practices of information security [6].

- Vulnerability of Computer Networks from Cybersecurity Threats

Cybersecurity threats are estimated to cost the world \$6 trillion a year by 2021, and the number of attacks has increased five-fold after COVID-19. The purpose of cyber-attacks is to harm companies financially. In some other cases, cyber-attacks can have military or political purposes [7].(Williams et al., 2021) Some of these damages are PC viruses, knowledge breaks, data distribution service (DDS) and other assault vectors. To this end, various organizations use various solutions to prevent damage caused by cyber-attacks. Cyber security follows real-time information on the latest IT data. So far, various methods have been proposed by researchers around the world to prevent cyber-attacks or reduce the damage caused by them. Some of the methods are in the operational phase and others are in the study phase [8]. (Yuchong et al., 2021)

objectives of the study

The general objective of our study is to develop a 2D game application that will demonstrate networking concepts and spread awareness on the possible risks caused by cybersecurity threats. The specific objectives are as follows.

- To develop a 2D game application that will explore an interactive way of learning advanced networking concepts.
- To make a 2D game that will provide prevention and awareness about network security to learners of the subject.
- To create a game application that will simulate the following network security threats; Man in the Middle; Distributed Denial of Service (DDOS) and; DNS Hijacking

2. Methodology

The developers will use the spiral model which is a combination of iterative development process model and sequential linear development model. The spiral model has a repetitive approach, going forward in a circular manner where the project passes through four phases over and over in the form of a spiral, until it reaches its completion, hence allowing several rounds of refinement.

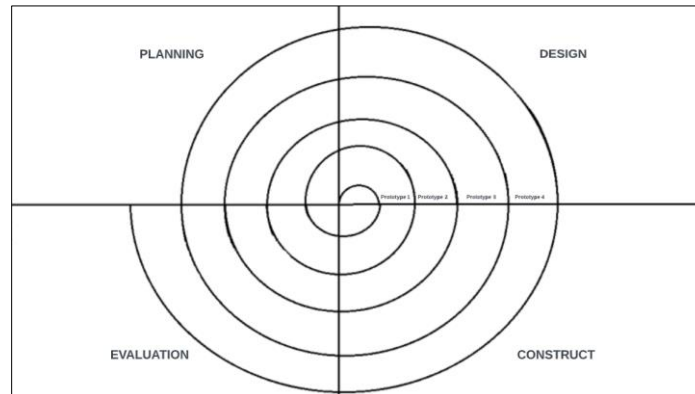


Figure 1 Spiral Model of the Game Development

The developers follow four development loops which signify 4 prototypes of the software. Each loop of the spiral is called a Phase of the software development process. The first prototype covers the title screen, main menu, map design, sprite models creation and basic functionalities such as character movements. The second prototype will feature the introduction of the game's main objectives or mechanics, tutorial stage, the first two mini-games and 1st level itself. The third prototype will feature level 2 which will introduce a new minigame and level 3 which will feature the first network security threat. The fourth prototype will feature the last two levels along with another two threats. Each iteration of the model has the following phase:

2.1. Planning

This phase of the spiral model involves the elimination of costs, scheduling, and resources for the iteration. Also, it helps to understand the requirements of the system for continuous communication between the customer and the system analyst. The discovery of system requirements, unit-level inputs, and components info occurs in this phase when the ongoing spirals act as the product evolves.

2.2. Design

After planning and identification, the next one is the design phase. It begins with an easy mind mapping within the initial spiral and including the architectural design, logical layout of modules, and therefore the product prototype within the subsequent spirals.

2.3. Construct

This refers to development of the final software product at every spiral. In the spiral, the product's thought and design is being developed. Then in the successive spirals with higher clarity on requirements and design a working model of the software called build is developed with a version number.

2.4. Evaluation

Risk analysis includes identifying, estimating, and observing technical feasibility such as schedule slippage and cost overrun. After testing the build, at the end of the first iteration, the user evaluates the software and provides the feedback. Based on the customer assessment, the development process enters the next iteration and afterwards follows the linear approach to implement the feedback provided by the user.

2.5. Project evaluation

The quality of a system is the degree to which the system satisfies the stated and implied needs of its various stakeholders, and thus provides value. Those stakeholders' needs (functionality, performance, security, maintainability,

etc.) are precisely what is represented in the quality model, which categorizes the product quality into characteristics and sub-characteristics. The product quality model defined in ISO/IEC 25010 comprises eight quality characteristics. However, the researchers will only focus on the criterion usability and its sub-characteristics as it is the most appropriate due to the nature of the system that will be tested.

2.5.1. Usability

Describes the extent to which software or system products can be used to achieve specific goals with effectiveness, efficiency, and satisfaction in a specified context of use. The usability factor has a set of lower factors which include appropriateness & recognizability, learnability, operability, user error protection, user interface aesthetics and accessibility.

2.5.2. Appropriateness & recognizability

A subjective validation of data to measure the degree to which you as the user believe that the given product or system is appropriate for your needs. In other words, is it the right product for the intended use for its user or for its volunteers.

2.5.3. Learnability

Checks if the system is easy to learn by you as the user, or as it is formulated in the standard of the degree to which a product or system can be used by specified users to achieve specific goals of learning to use the product or system.

2.5.4. Operability

The degree to which a product or system has attributes that make it easy to operate and control. It sees whether the software is without problems navigating itself or not.

2.5.5. User error protection

Simply the degree to which a system protects users against making errors. The software must be aware, or the user be aware of its boundaries and limits.

2.5.6. User interface aesthetics

The degree to which a user interface enables pleasing and satisfying interaction for the user. Making the interface less convoluted and more accessible helps with the user to software experience.

2.5.7. Accessibility

The degree to which a product or system can be used by people with the widest range of characteristics and capabilities to achieve a specified goal in a specified context of use.

2.6. Data Gathering Procedures

The respondents will serve as the main source of data in the evaluation of the system. The researchers will start to playtest the game to the respondents. After completing the game, the respondents will answer the questionnaires and rate their understanding towards the topics that were discussed in the game as well as their overall experience.

2.6.1. Population and Sample

The researchers will select fifty (50) BSIT students from Pamantasan ng Lungsod of Maynila. The respondents will playtest the proposed system. After the trial, the respondents will answer a survey regarding their learning experience.

The sampling method used to gather respondents is random sampling. It is a sampling technique in which each sample has an equal probability of being chosen. A sample chosen randomly is meant to be an unbiased representation of the total population.

2.7. Research Instruments

The researchers will use survey questionnaires written in Google Forms to collect feedback from the respondents. The questions will be patterned after ISO 25010's usability sub-characteristics where each respondent will have to rate their experiences with the game application using Likert Scale.

Table 1 Likert's scale for respondent's response

Quantitative Equivalent	Ratings
1	Strongly Disagree
2	Disagree
3	Neutral
4	Agree
5	Strongly Agree

3. Results

In order to evaluate the system, a survey was conducted using Google Forms. It is to test the system under standards of the ISO/IEC 25010 specifically the Usability sub-characteristics which includes the following: (1) Appropriateness & recognizability, (2) learnability, (3) Operability, (4) User error protection, (5) User interface aesthetics and (6) Accessibility.

Table 2 Summary of Results

Criteria	Mean	Qualitative Interpretation
1. Appropriateness & recognizability	4.56	Excellent
2. Learnability	4.28	Very Good
3. Operability	4.70	Excellent
4. User Error Protection	4.02	Very Good
5. User Interface Aesthetics	4.24	Very Good
6. Accessibility	4.71	Excellent
Overall Mean	4.42	Very Good

Table 3 Numerical Scale

Numerical Scale	Descriptive Rating
4.51 - 5.00	Excellent
3.51 - 4.50	Very Good
2.51 - 3.50	Good
1.51 - 2.50	Fair
1.00 - 1.51	Poor

4. Discussion

The 2D game application was successfully developed using Unity Game Engine which runs on computers with Windows 7, 8, 10 & 11 Operating System.

The evaluation was carried out successfully, surveying 50 BSIT students from Pamantasan ng Lungsod ng Maynila using Google Forms. The researchers patterned the survey questions after the standards of ISO/IEC 25010 specifically the Usability sub-characteristics; (1) Appropriateness & recognizability, (2) learnability, (3) Operability, (4) User error protection, (5) User interface aesthetics and (6) Accessibility.

The survey was successfully conducted as an evaluation procedure for the research “Development of a 2D Game Application for Learning Networks and Security”. The following findings were as follows.

The total mean result of the system based on the appropriateness & recognizability criteria was 4.56 with the descriptive rating of “Excellent” which means that the game software is recognized as a system that is appropriate to the user’s needs and demands.

The total mean result of the system based on the learnability criteria was 4.28 with the descriptive rating of “Very Good” which means that the game software achieved its goal as an effective mode of learning computer network related topics.

The total mean result of the system based on the operability criteria was 4.70 with the descriptive rating of “Excellent” which means that the users. Find their experience with the software exceptional in terms of controls and operations of the game software.

The total mean result of the system based on the user error protection criteria was 4.02 with the descriptive rating of “Very Good” which means that users experience little to no system bugs and errors.

The total mean result of the system based on the user interface aesthetics criteria was 4.24 with the descriptive rating of “Very Good” which means that the users find the aesthetics satisfactory, enabling a pleasant and satisfying interaction with the system.

The total mean result of the system based on the accessibility criteria was 4.71 with the descriptive rating of “Excellent” which means that the users experienced no complication in executing the game application on their respective devices.

Overall, after a thorough evaluation, the total mean for the ISO 25010’s characteristic, Usability was 4.42 which has a descriptive rating of “Very Good”. This implies that the game software satisfies within the parameters of usability sub-characteristics.

5. Conclusions

In line with the study’s objectives, result of the testing and evaluation, the following were the conclusions that were drawn.

- Based on the results of the study, it was concluded by the researchers that using interactive approach and materials, specifically the gamification of the networking concepts to be used in learning was found effective and highly accepted by its respondents.
- The researchers also concluded that using the game application as a learning tool had effectively raised awareness on the risk of cyber security threats and provided insights on how to mitigate such risks.
- In order for the users to visualize the following threats, the game application had successfully implemented the following security threats as a part of the mechanics of the game.

Man in the Middle. In the game application, a minigame was added where the player needs to detect and protect the packets from anonymous eavesdroppers.

Distributed Denial of Service (DDOS). A mechanic implemented in the game application as multiple packets that were sent at the same time causing data traffic.

DNS Hijacking. Implemented as DNS records that were modified to confuse the players.

Recommendations

The game system “Cyber Dash” is recommended to learners who undergo computer centric courses to teach them about how networks are presented in the modern world and be aware of the risks presented by different cybersecurity threats. Lastly, for the future researchers and developers who are interested and wish to pursue topics that are related to the study, recommendations will be listed:

- Broaden the scope of topics about networking and cybersecurity threats.
- Implement a scoring system or a sort of evaluation inside the game that can assess the player’s understanding on the existing topics that are covered in the game.

- Introduce a game mechanic that further simulates the processes that take place in each layer of the ISO model.

Compliance with ethical standards

Acknowledgments

The researchers would like to extend their sincere gratitude to Pamantasan ng Lungsod ng Maynila for granting permission to conduct the playtest of the game. The researchers would also like to thank Kenneth Usares for his contribution in the development of the game and to our fellow BSIT students who willingly became the participants of the study. Lastly, we would also like to thank our panels, Mr. Joseph Darwin Co, Mr. Jefferson D. De Leon and Mr. Domingo V. Tanael for providing insightful feedback during the research development.

Disclosure of conflict of interest

The Authors proclaim no conflict of interest.

Statement of informed consent

Informed consent was obtained from all individual participants included in the study to ensure compliance with the relevant statutory requirement, including the Data Privacy Act of 2012, RA 10173.

References

- [1] Gullu, H., & Delialioglu, O. (2018, June 25). Research paper the effect of computer network simulators on students' Motivation and Learning. Retrieved August 13, 2022, from <https://dergipark.org.tr/en/download/article-file/1175637>
- [2] Zheng, D. (2015) Future Communication, Information and Computer Science. CRC Press.
- [3] Shneiderman, B. (1993, June) Education by engagement and construction: Experiences in the AT&T teaching theater. Keynote for ED-MEDIA meeting, Orlando, FL.
- [4] Sylwester, R. (1995). A celebration of neurons. Alexandria, VA: ACSD Books
- [5] Hermogenes M.G (2019). Evaluating Internet Security Awareness and Practices of BulSU-SC Students. Retrieved September 2022 from https://www.researchgate.net/publication/333524930_Evaluating_Internet_Security_Awareness_and_Practices_of_BulSU-SC_Students
- [6] Hermogeno M.S. (2019). Assessment on the Cybersecurity Awareness in Academic. Retrieved August 2022 from [https://ijesc.org/upload/cc84eddb2d8dc6f3e70575bf91a7e63f.Assessment%20on%20the%20Cyber%20security%20Awareness%20in%20Academic%20Institutions%20\(1\).pdf](https://ijesc.org/upload/cc84eddb2d8dc6f3e70575bf91a7e63f.Assessment%20on%20the%20Cyber%20security%20Awareness%20in%20Academic%20Institutions%20(1).pdf)
- [7] Williams, C., Chaturvedi, R., Chakravarthy, K., & Chaturvedi, C. A. R. (2020, September 17). Cybersecurity risks in a pandemic. Journal of Medical Internet Research. Retrieved September 2022, from <https://www.jmir.org/2020/9/e23692>
- [8] Yuchong et al., (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Retrieved September 2022 from https://www.researchgate.net/publication/354346903_A_comprehensive_review_study_of_cyber-attacks_and_cyber_security_Emerging_trends_and_recent_developments