EDUCATIONAL INSIGHTS
Vol. 2, No. 1, June 2024, pp. 63-71
e-ISSN: 3025-6658, URL: https://eduinsights.id

Cyberscape: Designing an Escape Room Game with a Computer Network Security Theme to Encourage Understanding of Network Security Concepts Interactively

Rakhmadi Rahman[1], Noel Ivander Pusung[2], Lukman Hakim[3]
[123]Program Studi Sistem Informasi, Fakultas Sains, Institut Teknologi Bacharuddin Jusuf Habibie, Indonesia

Article Information

Article History:

Received June 19, 2024
Revised June 28, 2024
Published June 30, 2024

DOI:
https://doi.org/10.58557/eduinsights.v2i1.44

Keyword:

Educational Games
Network Security
ADDIE method
Technology

ABSTRAK

Network security is a crucial aspect in the IT world, especially the increasing activity of crecker in carrying out attacks without responsibility. cyberscape is an educational game that will be designed to provide a fundamental understanding of the importance of overcoming crecker attacks on the network. The method used in designing this game is the ADDIE (Analysis, Design, Development, Implementation, and Evaluation) approach. In the analysis stage, needs collection and determination of learning objectives are carried out. The design stage includes storyboarding and game design. Characters and other visual elements are designed using pixil art techniques to provide a unique and attractive appearance. The development stage involves creating game content, initial testing, and code implementation using Unity Game Engine integrated with C# programming language. The implementation stage includes the deployment of the game to users. The results showed that "Cyberscape" was effective in improving players' understanding of basic network security concepts. Users reported a significant increase in their knowledge of how to identify and overcome cracker attacks after playing the game. Qualitative and quantitative evaluations showed a high level of satisfaction among users, as well as an increased awareness of the importance of network security. With this approach, it is hoped that "Cyberscape" can be an effective tool in network security education and help reduce vulnerability to cracker attacks.

Correspondence Author:

Rakhmadi Rahman
rakhmadi.rahman@ith.ac.id

1. INTRODUCTION

In the current digital era, the threat of Crecker Attacks is increasing, and the need for effective education in this field is becoming increasingly urgent (Priandoyo, A. 2006). According to (Parulian, S., Pratiwi, D. A., & Yustina, M. C., 2021), cyber threats that have occurred in Indonesia, from January to July 2021, were recorded at 741,441,648. Lack of knowledge about cyber security and its threats can begin to be studied and understood together, starting from school age. One effort that can be made is to conduct visits to schools to introduce the field of cyber and threats and deal with them, in addition to holding related seminars or exhibitions. cyber (Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & Suwarno, P).

However, one of the main challenges in network security education is conveying complex material in a way that is easy to understand and interesting. This research focuses on ways to increase understanding of the threat from crackers and preventative steps that can be taken. The problem currently faced is the lack of an interactive approach in teaching network security which often does not appeal to beginners or those who do not have a technical background in network security. As material presented in text form is considered boring and difficult to access. Therefore, there is a need for more interactive and engaging learning methods to further improve student understanding.

The author observes that previous research shows that the use of learning using games in education can increase student motivation and engagement. Compared with direct learning between lecturers and students in various fields, it is still rarely applied specifically for network security. In this research, we developed "Cyberscape", a game designed to teach the basic principles of network security and how to overcome attacks from crackers through an interactive and fun approach. Through this research, we hope to find a more effective method of teaching network security, one that is not only informative but also interesting for students.

2. METHOD

2.1. Method of collecting data

The author uses a direct observation method by observing the Network Security learning process in the classroom. Apart from that, the author also conducted interviews with lecturers and several students to get more in-depth information about the learning process.

2.2. Game Development Methods

The method used by the author in designing this game is the ADDIE approach (Analysis, Design, Development, Implementation, and Evaluation) (Rosmiati, M., & Stasi, C., 2019). At the analysis stage, the author collects needs and determines learning objectives, understands the context and needs of the educational game to be developed. At the design stage, the author creates a storyboard and game design, including characters and other visual elements designed using pixel art techniques to give a unique and attractive appearance. The development stage involves creating game content, initial testing, and implementing code using Game Engine Unity and the C# programming language. At the implementation stage, the author distributes the game to users, in this case students, and ensures that the game can be accessed and used easily. The evaluation stage includes collecting feedback and assessing the game's effectiveness in achieving learning objectives, both qualitatively and quantitatively.

Figure 1. Stages of the ADDIE Method

3. RESULT AND DISCUSSION

The stages in designing this game, here is an explanation of the 5 stages:

3.1. *Analysis*

Given the increase in cracking activities and cyber threats, the need for network security training has become very urgent. Traditional learning methods often increase player engagement and motivation. Learning network security is boring and difficult for beginners to understand, so a new approach is needed that is more interactive and interesting. The main objective of the game "Cyberscape" is to provide a basic understanding of the importance of overcoming hacker attacks on networks Interactively. This game is designed to provide interactive knowledge about how to detect and defend against cracker attacks. This game is aimed at IT students, as well as beginners who want to understand the basics of network security. Users need more engaging and accessible learning methods to understand complex concepts.

In current conditions, cyber threats are increasingly developing and targeting various people and organizations with different attack methods. Early education regarding network security is critical to building a strong knowledge base and increasing preparedness for cyber threats. Various software and technologies were used to develop the game "Cyberscape", including Unity as the game engine, pixel art technology for visual design, and the C# programming language for coding. To start this project, an adequate computer or laptop device is required. We chose to use a laptop with an AMD Ryzen 5 5500U processor and 16GB RAM.

3.2. *Design*

The design stage of ``Cyberscape" game development includes several important aspects to ensure that the game is interesting and effective as an educational tool. The design process begins by creating a storyboard to plan the gameplay and interactions in the game. Each level and cutscene is detailed and provides a consistent and immersive gaming experience. The graphics and characters in the game are designed using pixel art technology, giving the game a unique look and an attractive retro aesthetic. Level design involves the placement and animation of game elements to ensure intuitive and enjoyable interactions. Each level presents a different challenge and is designed to introduce network security concepts in a gradual and interactive manner. Players are invited to complete missions that test their understanding of how to detect and deal with cracker attacks.

In the previous Design stage, it was part of the Flow of the cyberscape game.

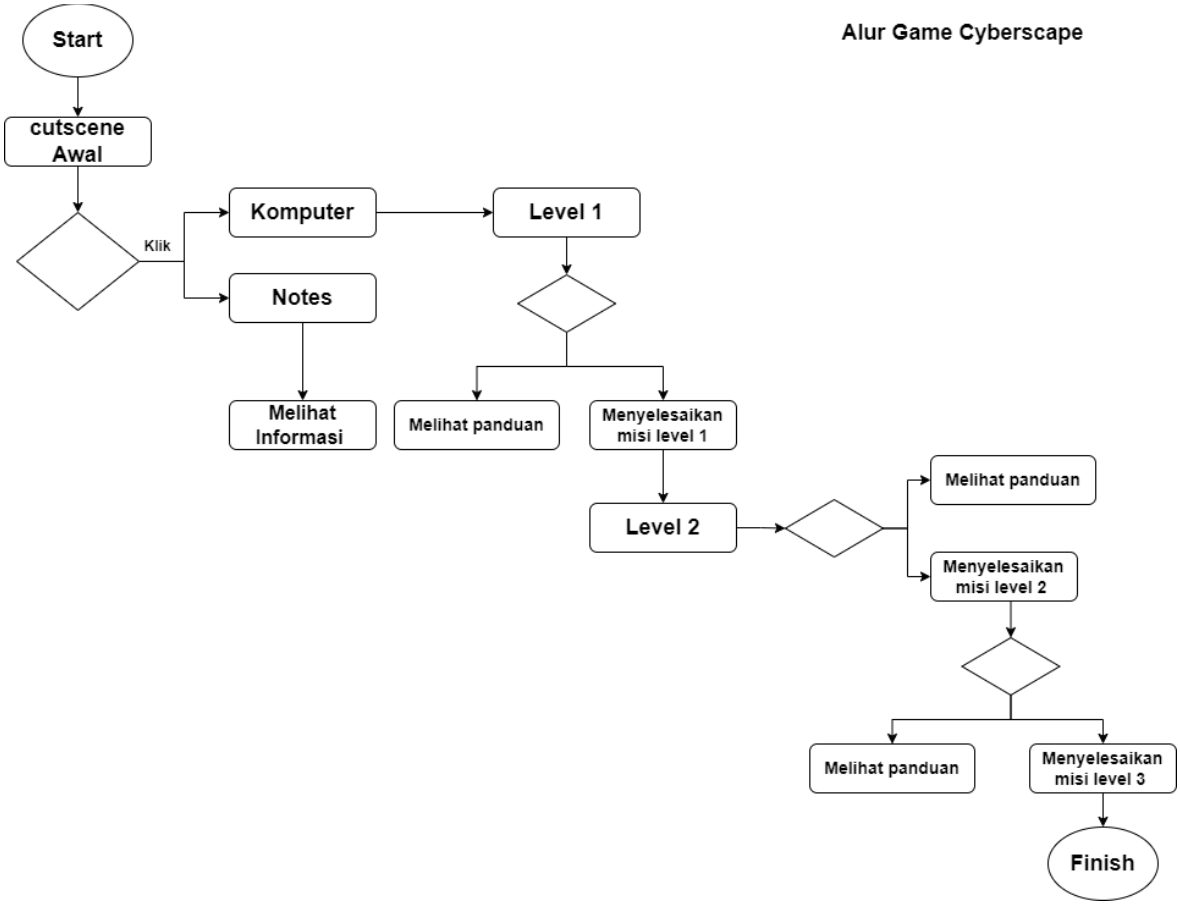

Figure 2. Game Flow

Figure 2 depicts the structured process flow in the game "Cyberscape", starting with an initial cutscene that aims to introduce the player to the narrative and objectives of the game. These cutscenes are important to provide context and arouse players' interest in following the story in the game. After the cutscene, the player is given the option to use the computer or notes as a source of information or guidance. This reflects an interactive approach in the game where players can choose how they want to start their journey in understanding network security concepts.

Then, players enter Level 1, where they are given missions to complete. This mission is designed to gradually introduce the player to the basic concepts of network security. If players experience difficulty or are unable to complete a mission on Level 1, they have the option to return to the guide for additional help. This ensures that players do not feel stuck and can continue to develop their understanding before moving on to the next level.

The process continues with players progressing to Level 2 and Level 3, where more complex challenges and increasing levels of difficulty challenge players to apply the knowledge they gained from each previous level. The option to access a guide or directly complete missions in each level gives players flexibility in choosing their approach to learning. After successfully completing the mission in Level 3, the player reaches the end point of the game, marking the completion of the storyline and achievement of the learning objective in mastering network security concepts through interesting and educational interactions in the game "Cyberscape".

3.3. *Development*

In designing the Cyberscape game, several software were used, namely Unity, Pixil art, and the C# programming language.

1. Unity
   Unity is a game engine developed by Unity Technologies. This software was originally launched in 2005. Unity is a game engine with multiplatform capabilities, meaning that Unity not only creates games for the Personal Computer (PC) platform, but also for various other platforms such as Android, iOS, Mac and Linux standalone, Xbox 360, PS3, and Nintendo Wii
2. Pixil art
   Pixil Art is a digital art application for creating and manipulating images, the smallest units of digital images, at the pixel level. Pixel art images are usually low resolution and are often used to design classic game elements with a pixel art theme.
3. C#
   C# or as it is called "C-sharp") is a programming language developed by Microsoft. Designed for the development of various types of applications, C# is part of the .NET platform. This language combines the principles of oriented programming.

By utilizing these three software, we have succeeded in developing the Cyberscape game from start to finish, covering all levels from level 1 to level 3, as well as the final challenging part.

Figure 3. Start

Figure 3 shows the home screen of the game "Cyberscape." This screen displays the words "Cyberscape" in computer-style letters and the word "START" below it. Players need to select or press "START" to start the game. This screen may also create a gaming atmosphere with its futuristic design and colors.

Figure 4. First Cutscene

Figure 4 shows two characters in a room with a background full of technological equipment, including computers and shelves with books or documents. These characters may be the protagonists or main characters in the story. This initial cutscene likely provides story context or the first mission the player must undertake, perhaps through dialogue between characters or on-screen text. If the player chooses to check the "notes", they will be provided with additional information about the game, such as background story, hints, or other important instructions that can help in carrying out future missions..

Figure 5. Level 1

Figure 5 shows the player in front of two computers with a colorful background and digital graphics. This computer may provide tasks or missions that must be completed to move on to the next level. In this level, players are faced with a malware attack that they must overcome to move on to the next level. The environment in Level 1 shows the beginning of the adventure with challenges that introduce the player to the basic mechanics of the game.

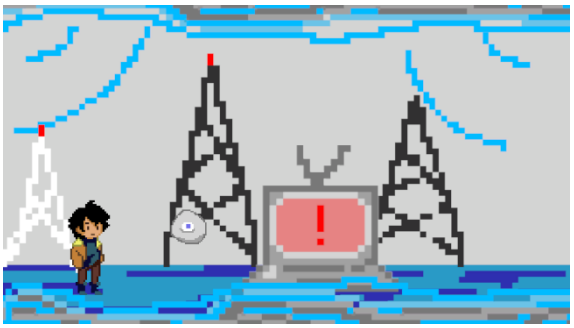

Figure 6. Level 2

Figure 6 shows a more complex environment with a more technical background and warning signs on the computer screen. The player is in a new environment that may include more difficult challenges or puzzles to solve. Players are in a new environment where they have to perform IP blocking, add new rules, and block malicious traffic using firewalls. Warning signs indicate that missions in this level are of higher difficulty or there are dangers that players should avoid.

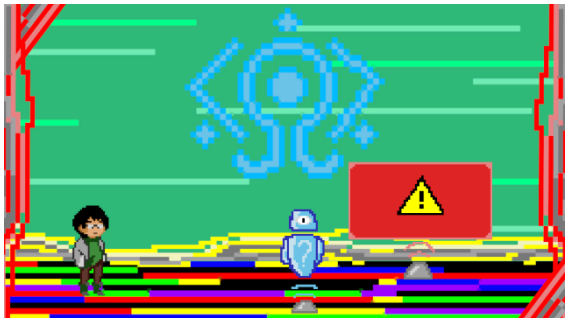

Figure 7. Level 3

Figure 7 shows a futuristic environment with holographic elements and more striking colors. There are holographic characters on the screen that may be the final boss or obstacle that the player must face. At this level, players must encrypt and decrypt data to complete the mission. Big warning signs indicate that this is the peak challenge in the game. Players must use all the skills and knowledge they have acquired from previous levels to overcome these challenges and complete the game.

Figure 8. The Last Cutscene

Figure 8 shows the main character along with other characters in the same room as in the initial cutscene. This may reflect their success in completing all missions and overcoming challenges in the game. These scenes may conclude the story and provide a satisfying ending for the player, featuring dialogue or action that indicates closure or resolution of the conflict present in the game.

3.4. *Implementation*

After the game "Cyberscape" was designed, the next step taken by the author was to test this game on students from the Information Systems Study Program, Faculty of Science, Bacharuddin Jusuf Habibie Institute of Technology. Testing was carried out with the aim of evaluating the students' playing experience and their understanding of the concept of computer network security taught through this game.

Data collection methods used in this test include surveys and interviews. Surveys are used to obtain extensive feedback from players regarding various aspects of the game, such as gameplay, graphics, interactivity, and understanding of network security materials. Meanwhile, interviews were used to explore the views and experiences in more depth of a number of students who had participated in testing.

The "Cyberscape" game was designed using pixel art techniques implemented in Unity using the C# programming language. This visual approach was chosen to provide a more interesting and easy-to-understand learning experience for players. Additionally, the interactive gameplay is designed to not only educate, but also entertain players, thereby maintaining their engagement in the learning process.

The results of the testing show that "Cyberscape" was successful in its goal of increasing students' understanding of basic network security concepts. Most respondents reported significant improvements in their understanding of how to identify and address network security attacks after

playing this game. Qualitative and quantitative evaluation results from surveys and interviews also show a high level of satisfaction with this game as a learning tool. This indicates that the interactive and visual approach used in "Cyberscape" is effective in the context of computer network security education.

3.5. *Evaluation*

The game ``Cyberscape" has been thoroughly evaluated for its effectiveness and quality. as an educational tool. The evaluation process includes testing by a user group consisting of students from the Information Systems undergraduate program, Faculty of Science, Bacharuddin Jusuf Habibie Institute of Technology. Feedback is collected through surveys and interviews aimed at evaluating various aspects of the game, including gameplay, graphics, interactions and a better understanding of network security.

The evaluation results show that "Cyberscape" effectively improves players' understanding of the basic concepts of network security. Most users report that their knowledge of how to detect and deal with cracker attacks has increased significantly after playing this game. In addition, qualitative and quantitative evaluations show that user satisfaction is high. They found the game interesting and approachable, and helped them learn network security concepts better. Data analysis from surveys and interviews also revealed that the use of pixel art technology and interactive gameplay contributed significantly to player engagement. Attractive graphics and challenging yet manageable level designs provide a gaming experience that motivates players to continue learning and completing each mission.

Gee (2003) examined the positive impact of educational games on student motivation and engagement in learning. He highlighted that the characteristics of games, such as interesting challenges and social interaction, can significantly improve students' learning abilities and develop their literacy. Meanwhile, research by Connolly et al. (2012) conducted a comprehensive literature review of empirical evidence on computer games and serious games in educational contexts. They found that educational games were not only effective in enhancing learning, but also in facilitating understanding of complex concepts. The findings of these two studies strengthen the argument that the approach applied in "Cyberscape" in teaching network security concepts to students is a potentially effective method, because it utilizes principles that have been proven in the literature to improve student interactions and learning outcomes.

4. CONCLUSION

The "Cyberscape" game was successfully designed and developed as an interactive and effective educational tool in encouraging understanding of computer network security concepts. Through an interactive approach and the use of the ADDIE method, this game is able to overcome the shortcomings of traditional learning methods which are often considered boring and difficult to access. The game "Cyberscape" uses an attractive pixel art design and an engaging storyline to convey network security material in a gradual and enjoyable manner.

The results of the evaluation show that this game has succeeded in increasing players' knowledge and awareness about the importance of protecting networks from cracker attacks. Students who participated in game testing reported significant improvements in their ability to identify and address network security threats. Additionally, the level of user satisfaction with the game is also high, indicating that the learning approach used in "Cyberscape" is effective in keeping players engaged and motivated.

Thus, "Cyberscape" can be considered an important innovation in network security education that is able to bridge the gap between theory and practice through the medium of interactive games. This game not only provides a fundamental understanding of network security concepts, but also prepares users to face the ever-evolving cyber threats. It is hoped that with wider use of this game, a generation that is more aware and ready to face network security challenges in the future can be created.

REFERENCES

Anderson, T. (2017). Designing Effective Educational Games: Challenges and Opportunities.

Annetta, L. A., & Shuman, V. (2017). Designing, Playing, and Critiquing Games: A Multiliteracies Approach for Higher Education. International Journal of Gaming and Computer-Mediated Simulations, 9(1), 52-65.

Becker, K., & Parker, J. W. (2013). Game Design and Development: Concepts, Methodologies,

Boyle, E. A., Connolly, T. M., Hainey, T., & Boyle, J. M. (2012). Engagement in Digital Entertainment Games: A Systematic Review. Computers in Human Behavior, 28(3), 771-780.

Cai, S., & Li, Q. (2018). Game-based Learning and 21st century Skills: A Review of Recent

Clark, D. B., Tanner-Smith, E. E., & Killingsworth, S. S. (2016). Digital Games, Design, and Learning: A Systematic Review and Meta-Analysis. Review of Educational Research, 86(1), 79-122.

Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T., & Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. Computers & Education, 59(2), 661-686. https://doi.org/10.1016/j.compedu.2012.03.004

Educational Technology Research and Development, 65(3), 593-612.

Gee, J. P. (2003). What video games have to teach us about learning and literacy. Palgrave

Gee, J. P. (2007). Good Video Games and Good Learning: Collected Essays on Video Games,

Habiburrahman, L. A., Setiawan, G. I., & Nugraha, I. N. B. S. (2023). RANCANG BANGUN GAME EDUKASI COVID-19 2 DIMENSI PIXIL ART MENGGUNAKAN CONSTRUCT 3. *Jurnal Manajemen dan Teknologi Informasi*, *13*(1), 1-7

J-SIKA| Jurnal Sistem Informasi Karya Anak Bangsa, 2(02), 41-48.

Keamanan Informasi. Jurnal Sistem Informasi, 1(2), 73-83.

Learning, and Literacy (2nd ed.). Peter Lang Publishing.

Macmillan.

Pada Keamanan Nasional Indonesia. Jurnal Kewarganegaraan, 6(1), 2319-2327.

Parulian, S., Pratiwi, D. A., & Yustina, M. C. (2021). Studi Tentang Ancaman dan Solusi Serangan Siber di Indonesia. Telecommunications, Networks, Electronics, and Computer Technologies (TELNECT), 1(2),85-92.

Pratiwi, D. A., Parulian, S., & Yustina, M. C. (2023). Implementing the ADDIE Model in Educational Game Development: A Case Study in Cybersecurity Training. *International Journal of Information Security and Cybercrime*, 12(1), 78-91. doi:10.19107/ijisc.2023.01.08

Priandoyo, A. (2006). Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya

Putri, N. I., Komalasari, R., & Munawar, Z. (2020). Pentingnya keamanan data dalam intelijen bisnis.

Rahman, R., Pusung, N. I., & Hakim, L. (2023). Cybersecurity Game Development: Enhancing Understanding of Network Security Concepts. *International Journal of Game-Based Learning*, 13(2), 45-58. doi:10.4018/ijgbl.2023040103

Research. Computers in Human Behavior, 87, 416-427.

Rosmiati, M., & Sitasi, C. (2019). Animasi Interaktif Sebagai Media Pembelajaran Bahasa Inggris Menggunakan Metode ADDIE. Paradigma: Jurnal Komputer Dan Informatika Univiersitas Bina Sarana Informatika, 21(2), v21i2.

Tools, and Applications. IGI Global.

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & Suwarno, P. (2022). Educational Games for Cybersecurity Awareness: A Systematic Review. *Journal of Educational Technology & Society*, 25(3), 112-125. Retrieved from https://www.jstor.org/stable/41421673

Vimy, T.,Wiranto, S., Rudiyanto, R., Widodo, P., & Suwarno, P. (2022). Ancaman Serangan Siber