Using simulation in network security learning

E P Nugroho*, R Yuliana*, E Junaeti, J Kusnendar, H W Prabawa and Munir
Department of Computer Science Education, Universitas Pendidikan Indonesia

*Corresponding author’s email: eddypn@upi.edu

Abstract. Widespread use of computer networks, opening up opportunities for the emergence of crimes involving computer technology itself. If crime or attacks have occurred, reliable handling is needed to overcome crimes in the internet. In general, simulation can be understood as a representation of imitation of the functionality of a system or process. Preliminary studies related to the development of simulation tools in network security learning show information that simulation in general can increase student involvement. In its development, the simulation media utilizes Fungus 3.7.0 software. Fungus is a package available for engine unity. The feasibility of using simulation media in learning is judged on the basis of an instrument that generally evaluates several important components in learning media, including the availability of information for students, content-structure and navigation, interactivity, and assistance and accessibility technology. The development of network security simulation devices has not been able to ascertain whether the involvement of simulations in the learning process improves students’ cognitive abilities.

1. Introduction

Computer networks (computer networks) can be defined as a set of interconnections of a number of autonomous computers [1]. With the existence of a computer network one can communicate without having to be limited in space and time, because computers are connected to each other. At first the internet or computer network was only used for needs and defense, along with the development of technology, the internet can be used to connect millions of people from various sectors, whether military or civil, the internet accommodates all varied services [2].

Widespread use of computer networks, opening up opportunities for the emergence of crimes involving computer technology itself. If crime or attacks have occurred, reliable handling is needed to overcome crimes in the internet. Handling and preventing crime in a computer network is usually called network security. Network security is one of the vocational subjects that contains 2 categories, namely theory and practice. Unfortunately, learning related to network security is still struggling with theoretical matters, whereas in its implementation, when a digital crime is committed, data security measures need to be carried out immediately. Usually, the main problem of learning network security is the limited infrastructure and media that can represent the attack situation and at the same time safeguard / defense. In other words, there needs to be a real environment that triggers a security attack so that real action can be taken immediately.

In general the simulation can be understood as a representation of imitation of the functionality of a system or process (http://www.merriam-webster.com/). Robinson [3] defines simulation as an
experimentation by performing simple imitations using a computer on a particular system (and for a certain period of time), with the aim of providing a better understanding of how the system works.

Preliminary studies related to the development of simulation tools in network security learning [4-7] show information that simulations in general can increase student involvement [4-5]. Nevertheless, research conducted regarding the development of network security simulation devices has not been able to ascertain whether the involvement of simulations in the learning process improves students' cognitive abilities [5].

The concept of the simulation device (Visual Interactive Simulation - VIS) was first introduced by Hurrion (1976) as a computer model that presents a visual appearance in the form of animated moving objects [3]. The use of simulation devices in presenting information at least promises several benefits, including [3]: a) a better understanding of object patterns, this is because the device allows users to track events that occur and identify potential deficiencies of objects; b) the ease of verification and validation of the effectiveness of the system; c) allows for an interactive experimentation process, especially in order to try out new ideas to develop problems or test a possibility; d) increasing understanding of possible outcomes, this condition relates to the process of observing an event that can be carried out continuously; e) allows to be used as a media for data collection and communication aids in presenting information to a wider party; f) has the potential to be used as a problem-solving media in groups. The simulation itself is an important part (of many other important aspects) in computer science learning. This is because he is able to reach understanding at the lowest level (only for the fulfillment of certain tasks) to the highest understanding (eg system analysis) [5]. There are many studies regarding key processes in simulation studies. One of them is as stated by Robinson [3] based on the simulation study framework proposed by Landry [3].

1.1. Conceptual Modeling
The basis of a simulation study is the process of recognition of a problem that occurs in the real world. This problem can come from an existing system or just an alleged problem that might arise from a particular system. Robinson [3] reveals that there are 4 main requirements of Conceptual Modeling, including: Validity (ideally a conceptual model can be used as a fairly accurate reference in developing computer models); Credibility (meaning is almost the same as validity, the difference is the validity of the model maker while the credibility of the user review); Utilities (understanding that a conceptual model can be useful as an aid to decision-making processes in a particular context); and accessibility (ideally a conceptual model is possible to be developed into a computer model). The task of Conceptual Modeling is to provide a description of the nature of the problem and propose the right model to deal with the problem. Therefore, at least there are several activities that occur at this stage [3].

1.2. Coding Model
In the Coding Model, the conceptual model is converted into a Computer Model. Here coding is defined in the sense that it is more general and does not necessarily mean computer programming or can be said to be more likely to refer to the process of developing a computer simulation model [3]. Compared to developing a complete code to then be tested and documented, the best recommended step is to develop the code in the small step. This process is to ensure that the model has gone through a more rigorous testing process and can avoid deeper errors.

1.3. Experimentation
After being developed, the experimentation process is carried out by using simulation media on subjects that have been defined beforehand to get a better understanding of certain situations or can even obtain actual solutions that can be implemented in the real world.
1.4. Implementation

The implementation process can be understood as an activity of applying the findings from a simulation study into real-world problems. In its development, experiments carried out with simulation media aim to gain a better understanding of the real world and/or to find solutions to real-world problems [3]. This is a "how-if" analysis process, which is making changes to the input media simulation, running simulation media, checking results, learning from the results of running simulation media, making changes to inputs and so on (Figure 1).

For example, determining defense/security in handling an attack on a computer network, this can be classified into input. The simulation will run certain defense/security scenarios, the hope is that the simulation results presented can give a picture of the final results that correspond to a reality condition. Based on the results, defense/security will be adjusted (can change conditions or not) this is included in the result process. This process will continue until it is felt that enough has been learned about the influence of the defense/security against the attack that occurred.

The results of the experimental process are described as solutions and/or understandings. Because simulation media are not always developed with the aim of getting concrete solutions, users of simulation media can also develop a better understanding by learning from the results of running simulation media this is included in the learning process. And in adjusting you can adjust the input in the simulation media.

2. Methods

The basis of a simulation study is the process of recognition of a problem that occurs in the real world. This problem can come from an existing system or just an alleged problem that might arise from a particular system. The task of Conceptual Modeling is to provide a description of the nature of the problem and propose the right model to deal with the problem. There are at least some activities carried out at this stage, including [3] development of understanding of the problems to be modeled, determine the purpose of the modeling process, create a conceptual model design (Figure 1), and collect and analyze the data used in the development of the model.

In developing the simulation media (coding model), the Fungus 3.7.0 software was used. Fungus is a package available for engine unity. This fungus is used as a framework, where the event or function in this learning simulation media uses the majority of events provided by Fungus.

Testing of simulation media (experimentation) was carried out by involving vocational school students with scientific background in Computer and Informatics Engineering who had studied several subjects which were the prerequisites for understanding network security material. The selection of users is based on teaching materials related to the use of computers on the network, more specifically this network simulation media can be used by Computer Network Engineering students as an initial understanding in studying Network Security subjects.

The feasibility of using simulation media in learning is assessed based on an instrument that generally evaluates several important components in learning media, including the availability of information for students, content-structure and navigation, interactivity, and assistance and
accessibility technology. In terms of students, an instrument was adopted based on Multimedia Mania's multimedia assessment instrument [8].

3. Results and Discussion
To simplify the concept of attack and defence in a simulation, the first thing to do is to look for information on attacks that occurred in Indonesia. What often happens in Indonesia is DOS attacks, one of which has been experienced by the bnn.go.id site, which is paralyzed without access [9], a fishing attack that targets the Bank's account [10] with spoofing or sniffing techniques in one network and several cases others with the same attack pattern. From the literature study, 3 simplified attacks were formulated in the simulation and 3 security defences. The first DOS attack, is the most common attack from frequent, many types of DOS, but in the same concept that distinguishes only the target is being attacked. Then spoofing and finally sniffing. Defence/security consists of a firewall, IDS and SSL that functions as encryption.

The making of conceptual model design from simulation media begins with paper prototyping activities. The basic idea of simulation is translated into a low fidelity prototype (in the form of a sketch) which generally aims to determine the scope of work of the simulation media. This step is needed so that if the simulation media design is not in accordance with the material, the design flow is not appropriate or it is impossible to continue its development using unity / game engine, then the design is replaced and repaired.

Media-flow in this simulation medium was developed using Fungus Unity software as a framework. The workings of fungus unity use programming flowcharts and code blocks that are easily accessible and applied. Using fungus makes it easy to translate simulation storyboards. Because the program code used in the fungus is not as complex as using ordinary unity. In making the media-flow, it is made based on the respective scene. In media-flow, there are 5 flowcharts which are divided into 5 scenes. Each scene only requires 1 flowchart.

In general, the main flow of the developed simulation media is presented in Figure 2.

![Figure 2. Simulation media’s flowchart.](image-url)
In main menu-flow or main menu flowchart there are only code blocks to call scene instructions, material simulation, and evaluation (Figure 3). In this main flow menu it blocks using the clicked object feature. If the object is clicked it will load to the scene to be targeted. This is the second main flowchart after opening, because this flow connects with all scenes. In this flow each code block has an action to call objects that are affected by the condition. Although the plot does not look, but in each block it has connectivity as a mapping for attack and defense simulation.

Figure 4 shows the flow of material. Flow is used sequentially, because each block correlates using the call feature. Each block uses more text or uses the Say feature. Say is a feature to make text available in Fungus Unity, which functions to write material text.

The interface design concept used in this simulation media is 2D animation. So at this stage begins with the 2D asset collection process by modifying or creating it yourself with the help of CorelDRAW X7 and equipped with other interfaces that are obtained for free from freepik.com and flaticon.com.

The initial step is to choose an attack (Figure 5). To choose an attack, the user drags the attack to the object, for example in the following example the user tries a DOS attack (Spoofing and Sniffing).

Figure 6 shows a popup when clients 1 and 2 do not get services from the server, and are marked with a cross mark indicating that clients 1 and 2 are having problems.
After choosing an attack, then try what defense (‘Pertahanan’) corresponds to the attack. Suppose the first choice of firewall is dragged to the server. If the chosen security solution is right and can solve the problem, there will be a pop-up indicating the success or failure of the defense installation. If it is green, it indicates that defense can handle the attack, but if it is red indicates that you have to try another defense.

Likewise for a combination of attacks and other defenses, if the defense is appropriate, aside from pop-up the green firewall will disappear from the defense list will disappear because it is installed. To install a firewall, it still needs another defense so that the attack cannot enter again. But the client can access again, because the firewall is filtering. The sign (x) in the client will disappear.

The scenario of installing spoofing on a server cannot be done; this is because the server has good security so it is difficult to penetrate with spoofing attacks, unlike DOS, because DOS is the purpose of spending bandwidth that makes a loss either server or client. Spoofing initially tries to fool the client with links that are forged or track IP depending on the type of spoofing used, but in general the process is the same. So that developers create scenarios in general.

Before going to the implementation stage, researchers experienced 4 students to test the feasibility and material development before being tested on students as the main subject in this study. The results of the experience test, the first student argues for the simulation concept can be understood in a plot, but there is a deficiency in the description of each element in the simulation. So that the added suggestion is to add information, so that students can understand more without having to explain it again.

For the second and third students, the test is the same time. Their opinions for the design and flow of the simulation media are good and understandable. Then, they also give the same advice that is to add information to each element simulated, because at the time of testing in the second and third students there has been no improvement. There is also an addition from the third student to increase the viewing time on the instructions for use and marking the instructions for changing the color. Before having experience with the last student, researchers consider the advice of the three previous students. So that changes are made according to suggestions, because suggestions are acceptable and do not change the main content of the media.

Assessment by experts and users is done to ascertain the advantages and disadvantages of the simulation media, so that it can be an adjustment and depiction if further development is carried out. Evaluation of simulation media by experts is summarized in Table 1 (scale 1-3).

Based on the assessment results presented in Table 1, the simulation media gets an average value of 2.33. An ideal score that is acceptable and shows the media is good and can be received or tested, that is if the score is equal to 2. So, with an average score of 2.33 it is interpreted that the simulation media represents a good model.
Table 1. Media Simulation assessment by experts.

| Assessment Aspect                              | Score |
|-----------------------------------------------|-------|
| Availability of Information for students      | 2.25  |
| Flow, Structure, Content and Navigation       | 2.3   |
| Interaction and Assessment                    | 2.1   |
| Technology, Help and Accessibility            | 2.67  |
| Mean Score                                    | 2.33  |

Evaluation media simulation by students involves 29 students as users who have interacted with the simulation media. In the evaluation activity, students were given a test before and after learning each of 10 different questions. The achievement indicators that were measured are students able to explain network security, describes threats and attacks on Network Security, distinguish types of threats and attacks on network security, explain Network Security needed for threats and attacks on Network Security, classify threats and attacks from the cases presented, and classify the suitability of the Network Security System with threats and attacks from the cases presented.

Table 2 presents the results of student assessment. From Table 2, it can be seen aspects related to mechanical media to get a value of 87.3, multimedia elements of 86.6, then information structure of 88.4 and quality of content 87.9. Overall this simulation media gets a score of 87.6. If an interpretation is done, the simulation media can be categorized very well. So, it can be concluded that the simulation media gets a very good response by students as users.

Table 2. Media simulation assessment by students

| Assessment Aspect | Criteria                   | Score | Mean Aspect Score |
|-------------------|----------------------------|-------|-------------------|
| Mechanical        | Technical                  | 82    |                   |
|                   | Navigation                 | 91.4  |                   |
|                   | Spelling and Grammar       | 87.1  | 87.3              |
|                   | Termination                | 88.8  |                   |
| Multimedia Element| Design                    | 85.3  |                   |
|                   | Enhancements               | 87.9  | 86.6              |
| Information Structure| Organization          | 88.8  |                   |
|                   | Branching                  | 87.9  | 88.4              |
| Content Quality   | Indications of achieving goals | 87.9  | 87.9              |
|                   | Total Mean Score           |       | 87.6              |

4. Conclusions
In conclusion, respondents' assessment of the simulation media including good and very good. The advantages of this simulation media can improve understanding from the lower classes to the upper classes, created using engine applications that are familiar to respondents because respondents often play games developed by the unity engine. And the drawback of this simulation media is that it is less able to adapt to a PC whose specifications are below standard and the design composition in this simulation media will change if the user chooses a size that is not in accordance with what was instructed by the developer. Despite these shortcomings, users can still use this simulation media properly and there are no specific application requirements to run this simulation media.

5. References
[1] Marsic I 2013 Computer Network: Performance and Quality of Services (Piscataway, New Jersey: Rutgers University).
[2] Tanenbaum A S and Wetherall D. J. 2011 Computer Networks, 5 ed. (Massachusetts: Pearson Education)
[3] Robinson S. 2004 *Simulation : The Practice of Model Development and Use* (Chichester, West Sussex England: John Wiley & Sons Ltd).

[4] Crellin J. and Karatzouni S. 2009 Simulation in Digital Forensic Education 3rd International Conference on Cybercrime Forensic Education adn Training (CFET3)

[5] Crellin J, Adda M and Duke-Williams E 2010 The Use of Simulation in Digital Forensics Teaching 11th Annual Conference of the Higher Education Academy, Information and Computer Science Group

[6] Årnes A, Haas P, Vigna G and Kemmerer R A 2007 Using a virtual security testbed for digital forensic reconstruction. *Journal in Computer Virology* 2 4 275-289.

[7] Carrier B and Spafford E H 2004 An event-based digital forensic investigation framework. In Digital forensic research workshop (pp. 11-13).

[8] ISTE Hypersig, "hypersig - multimedia mania," 2005. [Online]. Available: https://projects.ncsu.edu/mmania/index.html.

[9] A. Nouval, "merdeka.com," 2011 https://www.merdeka.com/teknologi/diduga-kena-serangan-hacker-situs-bnn-tidak-bisa-diakses.html.

[10] Arifah D. A. 2011 Kasus Cybercrime di Indonesia *Jurnal Bisnis dan Ekonomi JBE* 185 – 195.