The Effectiveness of a proposed system
Based on desktop virtual reality to promote the basic concepts of
Computer security

A.F.ELGAMAL, M.ELDESOKY, N.ABDELMOHSEN, M.HUSSIEN

DEPARTMENT OF COMPUTER SCIENCE
MANSOURA UNIVERSITY

ABSTRACT

Teaching information security faces a lot of problems because, it has many abstract concepts which are difficult to understand and imagine in the traditional methods of teaching. In this paper, we have designed a proposed system based on desktop virtual reality to promote the basic concepts of computer security using animated visualization 3D objects. That helps students to understand and simulate. The study was conducted to observe the effectiveness of the proposed system. The students were randomly assigned to experimental and control groups. Computer security concepts were taught via the proposed system in the experimental, and via the traditional lecture method in the control group. The statistical analysis of the students’ results showed that the experimental group had a significantly greater increase in academic’s achievement than the control group. It was conducted that the system had been significantly beneficial on student’s learning.

Keywords: desktop virtual reality, computer security, effectiveness.

1. INTRODUCTION

Desktop Virtual Reality is a lower level of immersive VR that can be easily employed in many applications without the need for special devices. It is generally regarded as the lowest cost of all VR solutions, and it has been widely adopted in education [11]. Desktop Virtual Reality has begun to make its way in modern education because of its ability to provide real time visualization and interaction within a virtual world that closely resembles a real world [12]. Moreover, a rapid and drastic fall in prices and huge leap and improvement in the processing power of personal computer, the proliferation of World Wide Web and the prevalence of broadband connections have aggravated the use of desktop VR in schools and colleges have aggravated the use of desktop Virtual reality in schools and colleges [15]. Desktop Virtual Reality was developed in many educational systems such the virtual reality physics simulation system (VRPS). It is an educational tool using a virtual reality interface that brings together a 3D model of real apparatus and a virtual visualization of physical situations in an interactive manner. VRPS system is useful for realistic hands-on experimentation, visualization of invisible physical quantities, and replacement of dangerous, high cost, and complicated experiments at the level of high schools or college physics [2]. Another famous system is the Virtual European School (VES). The VES project is an ongoing European project with the aim to develop a comprehensive online resource of teaching material for secondary school education. The system will be fed by a group of smaller publishing houses from different European countries [16]. Additionally, VES aims to enable international social contact between pupils and teachers, providing communication tools, educational games and quizzes embedded in distributed virtual environments[2]. In addition to desktop virtual reality earth motion system (DVREMS). The SYSTEM IS implemented to assist in clarifying unclear concepts among elementary school students about astronomy education such as spatial, rotation, revolution and earth’s axis [8]. Research has shown an encouraging array of positive learning outcomes in examining desktop VR technology to support learning [12]. Findings include positive effect on students’ learning of geometric topics.
2. Computer Security

Computer security has become a critical issue that affects our everyday life. It has grown significantly in popularity in the last few years for this reason; most colleges and other departments of computer science in different institutions have devoted a consistent amount of resources to develop courses and curricula which involved security topics [5]. Educators, lecturers and instructors have a hard time teaching this subject because of the content, the lack of laboratory facilities and equipment and the need to balance theoretical knowledge with practical and hands on skills needed by the students. Different institutions adopted different approaches to teaching computer security topics.

Traditional lecture approach is a commonly used approach, particularly in heavy theory based topics, for example cryptography. The method used often stems from the fact that a lot of basic and fundamental concepts must be covered. More often, this emphasis on fundamental concepts may well lead to students becoming too passive [13] and not actively attempt to understand difficult material [1]. The scribe approach, on the other hand, includes elements of active learning where students are responsible for taking notes down during the lectures and will do presentations of what they understand based on their notes to fellow students and the instructor during or after a lecture session. It can be seen that a significant number of higher institutions began to implement the scribe approach [3]. The tutorial approach is often used whenever various sources of information can be obtained via online sources. An example is the use of e-learning content and online journals and papers related to the topic at hand. This type of approach gives more freedom to the students to do research and obtain information while filtering the information relevant to particular topics [13]. Attack defense laboratory approach, students are divided into offensive teams and defensive teams with the goal of the offensive teams to compromise machines managed and monitored by the defensive teams. The offensive teams are allowed to utilize any attack within a defined set of rules specific to the local environment. The goal of the defensive team is to make target machines secure to intrusion while constantly looking to detect and trace any unauthorized intrusions [3]. This approach allows students to focus on both offensive and defensive exercises [14]. Such a focus on offensive as well as defensive techniques has been purported to provide a better understanding of the material [7]. One criticism of this approach is that students are being trained to be computer criminals. These different approaches are not mutually exclusive but rather may be most effective when used in combination [3]. Reflecting on earlier analysis, our proposed system makes use of the advantages of desktop virtual reality to overcome the obstacles to teaching the abstract concepts of computer security. The effectiveness of proposed system can be evaluated by comparing the students test results before using the proposed program by conventional teaching methods and after using the proposed system.

3. Methodology

The main object of this research is to design a proposed program based on desktop virtual reality to promote the basic concepts of computer security. The interviews with students revealed that they face difficulties in learning computer security concepts due to their inability to visualize and imagine theses concepts. Visualization tools can be an effective means for teaching and reinforcing complex concepts [9]. The traditional ways of teaching did not solve this problem. To solve this problem we developed the system according to the ADDIE model proposed by (Dick et al., 2005) [6]. It is a common approach widely used in the development of instructional courses and training programs [4]. ADDIE is acronym of five phases (Analysis, Design, Development, Implementation, and Evaluation) [10]. The five development phases are summarized in figure (1) below.
The analysis phase aimed to identifying students’ characteristics and the level of educational experiences that suit them to formulate the appropriate system content to achieve the objectives of the proposed system. The study sample is chosen from among the 3rd Students in Computer Science Department, faculty of Specific Education because they have expertise in using computers and they have no previous experience in the instructional content. The process of determining educational objectives includes preparing a list of the educational objectives of the cognitive aspect of the concepts contained in the computer security subject. The number of overall objectives of the educational content amounted to 6 objectives, and there are sub-objectives formulated in the form of behavioral objectives to determine the learning outcomes expected to occur to the students after studying each concept. The number of sub-objectives amounted to 36 and the scientific content was prepared according to the procedural objectives. We denote the basic terms which the student aught to know, such as firewall, virus, antivirus, encryption as shown in the concept map figure (2). While the design phase involved designing activity plans to describe the basic elements of the proposed system such as text, image, animation, interaction and the sequence of the system screen as shown in UML activity diagram for students figure(3). The system enable the students after logging in and performing pre-test to study the first concept which involves reading the text associated with the concept, study the main concept and its related sub-concepts, interact with simulated object, practice related exercises which lead to the next concept.
Information and Network Security Concepts

Main goals involves

Confidentially

Requires

Authentication

Authorization

Achieved by

Security policies

Covers

Access control

Requires

Encryption

Achieved by

Methods

vigenere

monoalphabetic

Integrity

Safeguard

Information asset

Are targeted for

Hackers

Deploy

Malicious code

Consist of

Antivirus

Use

Detection Method

Prevented by

Virus

Include

Macro

Worm

Trojan

Packet filtering

Application fireworks

Statful inspection

Fig (2) the concept map
Fig (3) Uml activity diagram for students
During the development phase, the early step before commencing the development process is to determine the required programs used in the proposed system. The chosen programs are 3d studio max 7 to provide a visual presentation of the abstract concepts, and Macromedia Flash cs3 with action script 3 to provide interaction between the student and the system. Adobe Photoshop CS3 is used for picture editing. The text was typed using Microsoft Word 7.

In figure (4) the design of the screen allows the user to understand real time traffic view using visualization to represent package incoming and outgoing from the firewall through 3D animated objects and whether or not the traffic was rejected by the firewall. In figure (4.A) the firewall inspects the header information (source, destination IP address and ports) in each incoming packet. In figure (4.B) the firewall inspect packet against rules, based upon rules configured and regulation that have set into the firewall the packet will be allowed or rejected from entering. As shown in figure (4.c) the match is not found and the packet was rejected. Figure (4.d) show how firewall dropped outgoing packet. Based on the student's understanding of how firewall works, the student can simulate its method by interacting with the system as shown in figure (5).

In the implementation phase the proposed system was actually built and tested to ensure it performs as designed, and then we delivered a complete proposed system to the students.

The sample of the proposed system is shown in Figure (4), (5), and (6).

The students can examine the package header and evaluate port and IP address against rules and depend on this comparison, the students can accept or deny the package. If the decision is wrong, the user is redirected to send package error to give him guidance tasks that are necessary to do. A sample of training screen is shown in Figure (6) where a component of the protection system are scattered and the student can moving the objects on the screen and putting them on the right place, the system allows the student to confirm configuring the other devices. If he failed, the system gives another chance to try again in order to know the right place. Through this way, the student simulates the security lab instead of using real one, which needs a lot of expensive security devices and other expensive equipment in addition to consuming much more time.
In the evaluation phase, the system is first examined on a pilot sample, to identify the problems that students may encounter and overcome them.

**Experimental work**

To evaluate the effectiveness of the proposed system, a total of 60 students from the department of computer science, Faculty of Specific Education, Mansoura University participated in this study. The achievement tests (pre, post) were conducted for experimental and control group. These tests have multiple choices and true/false format each test contain fifty questions. All the students were first exposed to pre-test to check their knowledge baseline in computer security concepts and make sure of the group equivalence.

The experimental group was exposed to the proposed system and the control group was taught through the conventional lecture method. The study was performed over a four-week period. The post-test was then administered on all the students to check their level of cognitive achievement. The data obtained from the pre-post test of the experimental and control groups were analyzed via SPSS package software. Figure (6) illustrates the framework for the proposed system application.
6. Result and discussion

The data collected from the per-test and post-test results were statistically analyzed through t-test. The pre–test data were used to investigate the prior knowledge of students. Table (1) shows the pre-test results of experimental and control group.

<table>
<thead>
<tr>
<th>PRE–TEST</th>
<th>N</th>
<th>MEAN</th>
<th>SD</th>
<th>DF</th>
<th>T</th>
<th>P-VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experimental</td>
<td>30</td>
<td>28.57</td>
<td>4.703</td>
<td>58</td>
<td>0.175</td>
<td>0.763</td>
</tr>
<tr>
<td>group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control group</td>
<td>30</td>
<td>28.77</td>
<td>4.108</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1 pre-test results

As indicated in table (1), the students’ prior knowledge measured through the achievement tests did not differ significantly. There was no significant difference in the pre-test score between experimental group (M= 28.57, SD=4.703) and control group (M=28.77, SD=4.108, T (58) =0.175, P-value >0.05). Is not significant at the alpha level of 0.05. this indicated that both groups were equivalent.

After using the proposed system and comparing the results, independent t-test reveals a significant difference between post-test scores for the experimental group ((M= 45.43, SD=2.609) and control group (M=29.63, SD=4.319, T (58) =18.237, P-value >0.001).

Table (2) shows the post-test results for the experimental and control groups.

<table>
<thead>
<tr>
<th>POST-TEST</th>
<th>N</th>
<th>MEAN</th>
<th>SD</th>
<th>DF</th>
<th>T</th>
<th>P-VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Experimental</td>
<td>30</td>
<td>45.43</td>
<td>2.609</td>
<td>58</td>
<td>18.237</td>
<td>0.001</td>
</tr>
<tr>
<td>group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control group</td>
<td>30</td>
<td>29.63</td>
<td>4.319</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Based on the statistical finding, it can be conducted that, using desktop virtual reality can increase effectiveness in learning the abstract concepts of computer security and can improve students’ performance and motivation.

7. Conclusions

A proposed program based on desktop virtual reality was designed and implemented in this study to assist in clarifying the unclear concepts of computer security. The study revealed that there was a significant difference between the mean score of two groups in posttest in favor of the experimental one, which indicates that these differences are related to the effectiveness of the proposed system in promoting the cognitive achievement of the basic concepts of computer security. We suggested that desktop virtual reality can be an effective method for teaching and reinforcing complex concepts by allowing students to imagine and directly interact with the visualization tools, this makes the abstract concept easier to understand.
REFERENCES


