AN EMPIRICAL EVALUATION OF CRYPTOOL IN TEACHING COMPUTER SECURITY

Mabroka Maeref[1] and Fatma Algali[2]

[1]Department of Computer Science, Sebha University, Sebha, Libya
roka.mayouf@yahoo.com
[2]Department of Computer Science, Sebha University, Sebha, Libya
fatma.algali@yahoo.com

ABSTRACT

In the area of network security, the fundamental security principles and security practice skills are both required for students' understanding. Instructors have to emphasize both; the theoretical part and practices of security. However, this is a challenging task for instructors' teaching and students' learning. For this reason, researchers are eager to support the lecture lessons by using interactive visualization tools. The learning tool CrypTool 2 is one of these tools that mostly cover all of the above. In fact, the evaluations of the effectiveness of the tools in teaching and learning are limited. Therefore, this paper provides an overview of an empirical evaluation for assessing CrypTool 2 tool. The effectiveness of this tool was tested using an empirical evaluation method. The results show that this visualization tool was effective in meeting its learning objectives.

KEYWORDS

Computer Security, Cryptographic Protocols, Visualization and Animation, Empirical Evaluation

1. INTRODUCTION

The visualization and animation approach is increasingly being adopted in Computer Science education with the promise of enhancing student understanding of complex concepts. Using this approach, tools were developed using visualization and animation techniques to interactively help students gain knowledge and acquire skills about a subject. If these tools are exploited efficiently, they can facilitate the education process, thus minimizing the learning/teaching time for both lecturers and students.

In the area of network security, fundamental security principles and security practice skills are both required for a student to understand the subject matter. Instructors have to emphasize both the theoretical and practical aspects of security. However, this area poses a challenge for instructors to teach and for students to learn. For this reason, researchers have been eager to support lectures by offering interactive visualization and animation tools that facilitate student understanding and shorten the time consumed in long-term teaching [1-8].

Dhinaharan Nagamalai et al. (Eds) : CCSEA, DKMP, AIFU, SEA - 2015
pp. 93–100, 2015. © CS & IT-CSCP 2015 DOI : 10.5121/csit.2015.50208

In response to the rising number of security crimes and attacks, specific security courses have been developed by colleges and universities [9]. Although the Model Curricula for Computing CC-2008 [10] describes a cryptographic algorithm as an elective unit– with topics that include private and public key cryptography, key exchanges, digital signatures and security protocols– security experts, including Bishop [11], Hoglund [12] and Howard [13], emphasize the need to incorporate security into the undergraduate curriculum.

Cryptographic protocols mostly combine both theory and practice [14, 15] and as such, interactive visualization tools are essential [7, 8] to support a student's understanding of the subject matter. However, experiences with these kinds of tools are limited. A justification of these tools' effectiveness is highly required in order to declare the values of these tools. In this paper, we describe our experience with a CrypTool 2 [16] as an experimental procedure and evaluate the tool using empirical evaluation approach. The following section describes the most related works to our paper while section 3 explains the CrypTool description. Experimental procedure and results are described in section 4. A discussion of this paper is explained in section 5 and the conclusion is provided in section 6.

2. RELATED WORK

Researchers have developed various kinds of interactive visualization tools for teaching/learning cryptographic protocol behaviour and concepts. One of these tools is the Kerberos tool, which developed for visualizing one specific protocol: Kerberos protocol [17]. Another tool is the GRACE tool [3], the Game tool [18], GRASP tool [19] and crypTool [20, 21]. CrypTool is a freeware Program with graphical user interface for applying and analyzing cryptographic algorithms with extensive online help. Literature on related visualization tools, together with comparisons between them, is available in our papers [22] and [23].

The main goal of this paper is to evaluate quantitatively the effectiveness of CrypTool. For the purpose of this paper, effectiveness refers to the ability of this tool in enhancing student's understanding. This goal is evaluated using an empirical evaluation approach (without animation vs. animation with CrypTool tool). We have chosen this tool because it covers the most aspects of computer security. With respect to this chosen tool, the question is, "*Is teaching using CrypTool more effective than traditional teaching medium?"*

Various studies have been carried out for evaluating interactive mediums. From the literature, a study conducted by Kehoe et al. [24] used an interactive animation to teach algorithm animation and data structure. Their results showed in scores on a post-test used to evaluate the understanding with 12 students divided into two groups. The results showed that the animation group significantly outperformed the non animation group. Moreover, Yuan et al. [8] used Kerberos as an interactive animation tool to teach Kerberos protocol. His results showed in scores on pre-post tests used to evaluate the understanding with 16 students. The *t*-test results show that the improvement from pre-test to post-test is statistically significant. Hundhausen et al. [25] also considered 24 experiments used different concept of animation to teach algorithm animation and data structures. Twenty two of the experiments used post-test or pre-post tests to evaluate the understanding. Their results are various according to the interactivity of animation.

3. CRYPTOOL DESCRIPTION

Cryptool is a freeware Program with graphical user interface for applying and analysing cryptographic algorithms with extensive online help. It can be understandable without deep crypto knowledge. It contains nearly all state of the art crypto algorithms with "playful"

introduction to modern and classical cryptography. Learning through CrypTool is almost can be done by everyone either through the internet or by download and install the tool from the website (www.cryptool.org). The features of CrypTool include cryptography and cryptanalysis. Both of them constitute the science of cryptology. Figure 1 shows the main menu of the tool.

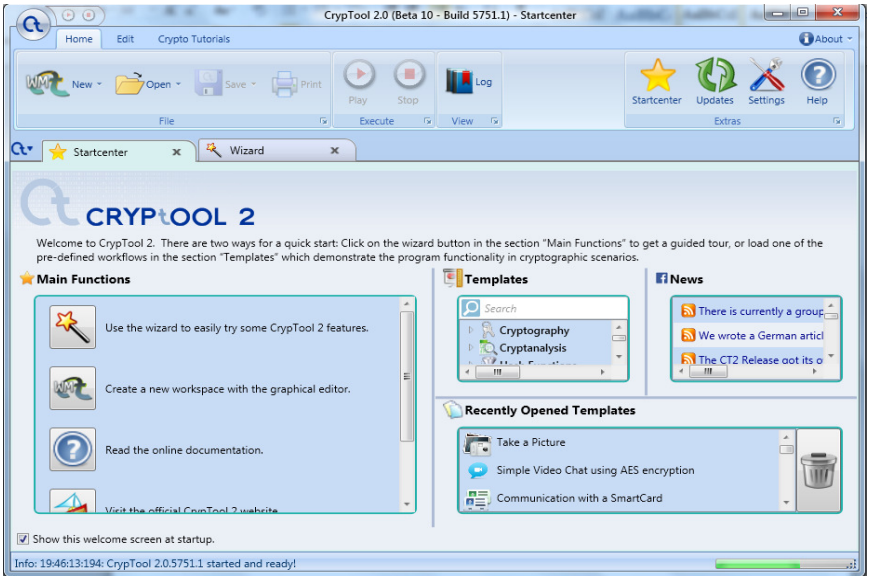

Figure 1. CrypTool main menu

4. CRYPTOOL EVALUATION

We carried out an experiment consists of one group of the same lesson taught to the undergraduate Computer Science students of the Network Security course at Sebha University of Libya during the semester II of 2013-2014 year. The experiment was conducted in two stages where each stage uses a different learning medium approach; the first stage uses only text-based materials (no animation), the second stage uses CrypTool in the final part of the lesson. The student will be given a same test throughout the two stages. They are allowed to improve their answer after each stage. The results of the tests after each stage of the medium approach are compared.

The same topics of the lessons are given during all of the two stages. These topics are: symmetric-key and Asymmetric-key cryptographic protocol, Diffie-Hellman protocol with respect to the possible attack to Diffie-Hellman protocol, the concept of hash function, digital signature and digital certificate.

In this experiment, the tool SPSS [26] is used to statistically evaluate the effectiveness of CrypTool using t-test and p-value.

4.1. Experimental Procedure

A total of 20 students participated in the experiment. The students are final year of Computer Science students (undergraduate students) at Sebha University of Libya. We follow the pre-test to post-test accuracy [8, 25, 27] in order to evaluate the effectiveness of CrypTool. The same students were given the same lesson but using different medium each time. The experiment was

conducted using the learning medium approach (no animation vs. animation with CrypTool). The students were given the lesson using only text-based materials followed by a pre-test, then, the same students were introduced to CrypTool followed by a post-test.

The experiment was controlled by delivering the same lesson to all of the students by the same teacher during the two consecutive sessions. The topics were: symmetric-key and Asymmetric-key cryptographic protocol, Diffie-Hellman protocol with respect to the possible attack to Diffie-Hellman protocol and the concept of hash function, digital signature and digital certificate.

In the first session of the three hours, only text-based materials were used during the lesson time with the help of electronic slides. At the end of the session, the students were given a pre-test of ten multiple choice questions with a time limit of 30 minutes to answer them.

In the second session, after the pre-test, students were introduced to CrypTool and to its visual interface. They were asked to experiment with simple symmetric and asymmetric-key cryptographic protocols and to recreate Diffie-Hellman protocol. They were also asked to experiment with the concepts of hash function, digital signature, digital certificate and their usages of avoiding possible attack. At the end of the session, the students were given a post-test of the same questions as in the first session with a time limit of 30 minutes to answer them.

Again, to control the tasks performance, the same test of ten multiple questions were given to all students with a specific time. During the test, the students were not allowed to consult books or use any materials. Then the results of pre-test and post-tests were compared. The following points describe the details of the ten multiple questions:

- The first question dealt with the communication components of asymmetric-key cryptographic protocol.
- The second question dealt with the differences between symmetric-key and asymmetric-key cryptography.
- The third question dealt with Diffie-Hellman protocol steps.
- The fourth question dealt with the communication components of Diffie-Hellman protocols.
- The fifth question dealt with digital signature.
- The sixth question dealt with digital certificate.
- The seventh question dealt with Diffie-Hellman possible attack.
- The eighth question dealt with a hash function.
- The ninth question dealt with avoiding Diffie-Hellman protocol attack.
- The last question dealt with a hybrid system (using of both symmetric and asymmetric-key cryptography).

4.2. Experimental Results

To determine the effectiveness of CrypTool, a pre-test and post-test accuracy is used. Table 1 describes the students' scores for the pre-test and post-tests. Notice that the maximum score for each student is 10. In the other side, the Table 2 describes the mean of the group tested and Figure 2 explains the idea.

Table 1. The students' scores of pre-test and post-test

No.	Pre-test scores No animation	Post-test scores Using CrypTool
1	4	6
2	4	6
3	5	5
4	4	6
5	4	4
6	5	5
7	5	5
8	5	7
9	4	7
10	4	5
11	4	6
12	5	7
13	4	6
14	4	4
15	4	4
16	5	5
17	5	5
18	5	7
19	4	7
20	5	7

Table 2. The students' scores means of pre-test and post-test

Time	Treatment	No.	Mean
Sebha University	No animation	20	4.45
	CrypTool	20	5.70

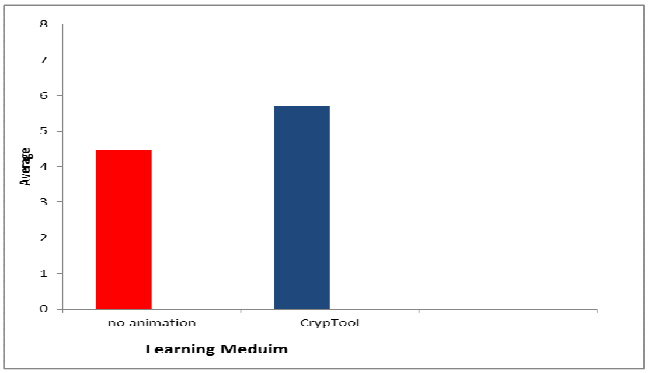

Figure 2. The means of the students' scores

The adopted statistical analysis of this experiment is that:

- Null Hypothesis (H_0): the conducted hypothesis is that there is no difference in the mean of pre-test and post-tests scores. In other words, the pre-test and post-tests scores will have equal means.
- Alternative hypothesis (H_1): the alternative hypothesis is that there is at least one difference in the mean of the pre-test and post-test scores in the group tested.

- p-value: the return value of the statistical test which indicates the probability of getting a mean difference between the groups as high as what is observed by chance. The lower the P-value, the more significant difference between the groups. The typical significance level that has been chosen in this experiment is 0.05.
- t-test: this test was run on the pre-test and post-test scores. In this experiment, the result t-test shows that there is a difference between the pre-test and post-test according to the p-value which is 0.0 and less than the significance level 0.05. table 3 shows the result of t-test.

Table 3. The results of t-test

Treatment	No. of student	Mean	p-value	t- test
CrypTool	20	5.7	0.0	CrypTool > No animation
No animation	20	4.45		

The test shows that there is a difference between no animation and CrypTool based on the p-value which equal to 0.0. The p-value is less than the significance level (0.05) and that means the improvement from pre-test to post-test is statistically significant.

5. DISCUSSION

The results in this experiment indicate that CrypTool is more effective and efficient than traditional learning medium. According to our hypothesis testing, there is a significant difference between using CrypTool as a teaching/learning medium and text-only material. It shows that CrypTool (interactive visualization and animation tool) significantly outperformed text-only material (no animation). The overall improvement of enhancing the students' ability for understanding the cryptographic protocols and computer security concepts using CrypTool is demonstrated and achieved.

6. CONCLUSION

Regardless of the advancement in the area of educational techniques, the area needs to be further tested with more empirical evaluation, especially of using the teaching/learning interactive visualization and animation tools. Currently, a few researches dealt with the problem of the lack of using these kinds of tools. The missing of a clear and complete principle design for interactive tools is seldom discussed and yet plays a crucial role in the tool development. The principle design is important because a tool without a base is inadequate even if it is supplied with good structures. Furthermore, studies have shown that visualization and animation educationally enhanced students' understanding if they were supported by active learning. This paper was motivated by these observations. In particular, this paper suggested more experiments of other interactive visualization tools through empirical evaluation in order to improve their effectiveness and teaching/learning support.

REFERENCES

[1] Asseisah, M. S., Bahig, H. M., & Daoud, S. S., (2010) Interactive Visualization System for DES. Berlin Heidelberg: Springer-Verlag

[2] Catrambone, R. & Seay, A. F., (2002) "Using Animation to Help Students Learn Computer Algorithms," The Journal of the Human Factors and Ergonomics Society, vol. 44, pp. 495-511.

[3] Cattaneo, G., Santis, A. D., & Petrillo, U. F., (2008) "Visualization of cryptographic protocols with GRACE," Journal of Visual Languages and Computing, vol. 19 pp. 258-290.

[4] Holliday, M. A., (2003) "Animation of computer networking concepts," ACM Journal on Educational Resources in Computing (JERIC), vol. 3, pp. 1-26.

[5] Kazemi, N. & Azadegan, S., "IPsecLite: a tool for teaching security concepts," in SIGCSE '10 Proceedings of the 41st ACM technical symposium on Computer science education NY, USA, 2010.
[6] Kerren, A. & Stasko, J. T., (2002) "Algorithm animation," Software Visualization, LNCS 2269, pp. 1-15.
[7] Schweitzer, D. & Brown, W., (2009) "Using Visualization to Teach Security," JCSC, vol. 24, pp. 143-150.
[8] Yuan, X., Vega, P., Qadah, Y., Archer, R., Yu, H., & Xu, J., (2010) "Visualization Tools for Teaching Computer Security," ACM Transactions on Computing Education, vol. 9, pp. 147-155.
[9] Taylor, B. & Azadegan, S., "Moving Beyond Security Tracks: Integrating Security in CS0 and CS1," in SIGCSE '08: Proceedings of the 39th SIGCSE technical symposium on Computer science education, 2008, pp. 320-324.
[10] CC2008, "Computer Science 2008, An Interim Revision of CS 2001."
[11] Bishop, M. & Frincke, D., (2005) "Teaching Secure Programming," IEEE Security and Privacy, vol. 3, pp. 54-56.
[12] Hoglund, G. & McGraw, G., (2004) Exploiting Software:How to Break Code. Boston: Addison-Wesley.
[13] Howard, M. & LeBlanc, D., (2003) Writing Secure Code. Redmund, WA: Microsoft Press.
[14] Stallings, W., (2006) Cryptography and Network Security: Principles and Practices, 4 ed. Upper Saddle River, NJ: Prentice Hall.
[15] Forouzan, B. A., (2008) Cryptography and Network Security, 1 ed. New York, NY: McGraw-Hill Higher Education.
[16] Deutsche, A., "CrypTool," 2009.
[17] Yuan, X., Qadah, Y., Xu, J., Yu, H., Archer, R., & Chu, B., (2007) "An animated learning tool for Kerberos authentication architecture," Journal of Computing Sciences in Colleges, the twelfth annual CCSC Northeastern Conference, vol. 22, pp. 147 – 155.
[18] Hamey, L. G. C., "Teaching Secure Communication Protocols Using a Game Representation," in Australasian Computing Education Conference (ACE2003), Adelaide, Australia, 2002.
[19] Schweitzer, D., Baird, L., Collins, M., Brown, W., & Sherman, M., "GRASP: a visualization tool for teaching security protocols," in the Tenth Colloquium for Information Systems Security Education, Adelphi, MD, 2006, pp. 1-7.
[20] Eckert, C., Clausius, T., Esslinger, B., Schneider, J., & Koy, H., "CrypTool," 2003.
[21] Esslinger, B., "The CrypTool Script: Cryptography, Mathematics, and More," 10 ed: Frankfurt am Main, Germany, 2010.
[22] Mayouf, M. A. & Shukur, Z., (2008) "Animation of Natural Language Specifications of Authentication Protocol," Journal of Computer Science, vol. 4, pp. 503-508
[23] Mayouf, M. A. & Shukur, Z., (2009) "Using Animation in Active Learning Tool to Detect Possible Attacks in Cryptographic Protocols," LNCS 5857, pp. 510-520.
[24] Kehoe, C., Stasko, J., & Taylor, A., (2001) "Rethinking the evaluation of algorithm animations as learning aids: an observational study," International Journal of Human Computer Studies, vol. 54, pp. 265-284.
[25] Hundhausen, C. D., Douglas, S. A., & Stasko, A. T., (2002) "A meta-study of algorithm visualization effectiveness," Journal of Visual Languages and Computing, vol. 13, pp. 259-290.
[26] Pallant, J., (2010) SPSS Survival Manual: A step by step guide to data analysis using SPSS. Berkshire UK: McGraw-Hill Education.
[27] Hansen, S. R., Narayanan, N. H., & Douglas, S., (2000) "Helping Learners Visualize and Comprehend Algorithms Interactive Multimedia Electronic " Interactive Multimedia Electronic Journal of Computer-Enhanced Learning, vol. 2,

AUTHORS

Mabroka Maeref: received her BSc degree in Computer Science from University of Sebha, Libya, MSc in Computer Science from Universiti Sains Malaysia, and PhD in Software Engineering from Universiti Kebangsaan Malaysia. Her interests span a wide range of topics in the area of Software Engineering, Networking, Computer Security, Visual Informatic and Computer Education. she is currently working as a lecturer at the departement of computer science, Faculty of Sciences in Sebha University of Libya.

Fatma Abdullah Alghali received a Ph.D. in Computer Science (Software Engineering) from University of AL-Neelain SUDAN 2006, Master of Computer Science from Warsaw University of Technology, Poland , 1997,BSc of Computer Science from Sebha University, Libya, 1991,Her research interest includes Software Engineering, Human Computer Interactive (HCI) , E-Learning, Cloud Computing, She is working as Assistant Professor. In Computer Science Department of Sebha University LIBYA