The Impact of Learning Style Adaptivity in Teaching Computer Security

Mohammad Alshammari[1], Rachid Anane[2], Robert J. Hendley[1]
[1]School of Computer Science, University of Birmingham, UK
{m.t.m.alshammari, r.j.hendley}@cs.bham.ac.uk
[2]Faculty of Engineering and Computing, Coventry University, UK
r.anane@coventry.ac.uk

ABSTRACT
Teaching computer security is one of the most challenging tasks in computer science, because of the need to successfully integrate abstract concepts and practical applications. Several e-learning systems have been developed to address this issue. However, they usually provide the same material in the same sequence irrespective of the characteristics of the students, such as their knowledge level and learning style. In this paper, an approach to learning style adaptivity is proposed for the teaching of computer security. An e-learning system was developed to provide more personalised and adaptive learning, based on the information perception style of the Felder-Silverman model. This is the dimension of learning style, which has received the least attention in published research. In the approach, a personalised sequence of learning material is generated based on an individual learning style. The approach is evaluated in order to determine its effectiveness in learning provision. An experiment conducted with sixty subjects produced significant results. They indicate that matching computer security learning material, according to the learning style of the students, yields significantly better learning gain and student satisfaction than without matching.

Categories and Subject Descriptors
K.3.1 and K.3.2 [**Computers and Education**]: Computer Uses in Education- *Computer-assisted Instruction (CAI)*; Computer and Information Science Education- *Computer Science Education*

General Terms
Experimentation, Human Factors

Keywords
Computer Security Education, Adaptivity, E-learning Systems, Learning Style

1. INTRODUCTION
Computer security is often considered one of the most relevant and challenging topics in computer science. Teaching computer security is a complex task. In a traditional setting, the complexity of teaching computer science courses in general, and computer security courses in particular, arises from the requirement of combining theoretical concepts with applications and examples, all within the constraints of lecture schedules and laboratory resources [19,20]. Another source of difficulty stems from the requirement to meet the needs of all the students in classroom learning. Some students may also find the classroom setting distracting or too rigid.

ITICSE '15, July 04 - 08, 2015, Vilnius, Lithuania.
Copyright 2015 ACM 978-1-4503-3440-2/15/07…$15.00
http://dx.doi.org/10.1145/2729094.2742614

E-learning systems can, to some extent, alleviate this complexity by offering learning opportunities anytime and anywhere. These systems are expected to support better, more student-centric instruction and enable more self-paced and self-directed learning. They provide learning material and content in several forms such as hypermedia, animation and virtual laboratories. For example, Hu and Wang have introduced a virtual laboratory environment for computer security education; it allows students to perform different hands-on exercises [15]. Tele-Lab IT Security is a tutoring system that provides different security exercises and tasks augmented with background concepts [16]. More innovative tools have been also proposed, such as the CyberCIEGE game; it supports the teaching of computer security in an engaging process [11].

Although traditional e-learning systems offer useful learning environments, they are not flexible enough [20]. They provide the same material and tasks in the same sequence irrespective of the characteristics of students - such as their knowledge, abilities and learning style. Moreover, the learning process can be time consuming, inefficient and less effective. An independent approach to studying taken by students may lead to poor decisions on what and how to study. In addition, pedagogical aspects need to be carefully considered so that systems do not focus exclusively on technical issues but also on well-defined instructional design models [19].

Several instructional approaches have been proposed in computer science in order to make the educational process more effective and to meet the needs of students. Adaptation of learning material based on knowledge and learning style has been the subject of intensive research [7]. For example, the SQL-Tutor is an intelligent e-learning system that customises the sequence of SQL lessons based on the knowledge level of students [21]. An approach that takes into account the learning style in order to provide instructional recommendations to students has also been represented by the eTeacher system for teaching artificial intelligence [23]. The Protus system combines knowledge level and learning style to personalise learning material for teaching Java programming [18].

The deployment of these systems, among others, has produced promising results in enhancing the learning and the satisfaction of students for different computer science topics [1]. However, few attempts have been made in the domain of computer security [1,19]. Furthermore, learning style adaptivity is still a controversial issue; it is not always evident how to provide adaptation based on learning style [6]. These issues need to be addressed in order to make computer security education more effective.

This paper presents an initial investigation into the impact of learning style adaptivity in teaching computer security using e-learning systems. An adaptive approach based on learning style is proposed. It customises the sequence of learning objects for each student based on their learning style.

An evaluation of the approach's effectiveness in terms of learning gain and student satisfaction is also provided. All students go through the same learning objects with the same allocated time. However, the system generates different sequences of the learning objects to match the learning style of each student. By varying the order of the learning objects, it is possible to undertake a more controlled set of experiments.

The next section reviews existing work on learning styles, and puts it into the context of computer security. Section 3 gives an outline of the proposed approach of learning style adaptivity. Section 4 describes the evaluation method. Section 5 presents the results. Section 6 offers a critical discussion of the work, and Section 7 summarises the work and draws some conclusions.

2. LEARNING STYLE

Learning style is defined as "characteristic cognitive, affective, and psychological behaviours that serve as relatively stable indicators of how learners perceive, interact with, and respond to the learning environment" [17]. Several studies have emphasised the importance of learning style in order to improve learning [13,17]. More importantly, it is argued that computer science education should support many different learning styles [22]. Several approaches have been proposed to support the teaching of topics in computer science, such as programming and databases, by adapting learning material according to different learning style models [1,18,21,23]. However, the lack of studies in learning style adaptivity that are based on well-designed experimental evaluation calls for more research [1].

Although a large number of learning style models and frameworks have been introduced [10], the Felder-Silverman model is the most widely used and preferred model in science and engineering education [1,2]. It provides comprehensive details on its components and identifies a teaching style for each component [13]. It also comes with a reliable and validated learning style assessment instrument [14].

The information perception style (sensory-intuitive) is an important component of the Felder-Silverman model [13]. It is argued by some researchers that it is the most important learning style [12]. Conversely, it has received the least attention in published research [1,9]. An investigation of how to provide adaptation based on this style is highly desirable; in addition, its effectiveness in e-learning systems, particularly the teaching of computer security, needs to be evaluated.

The information perception dimension of learning style is concerned with the type of learning material (abstract/concrete) with which an individual student will learn best and also with the best order in which to present material. Students are classified into two categories: sensory and intuitive. Sensory students prefer facts, problem solving by standard methods and real-world examples; intuitive students prefer principles, theories and mathematical models [13]. Sensory students may benefit more from concrete information; intuitive students may learn better with abstract concepts. Felder and Silverman define sensing and intuition as follows: "Sensing involves observing, gathering data through the senses; intuition involves indirect perception by way of the unconscious—speculation, imagination, hunches. Everyone uses both faculties, but most people tend to favour one over the other." [13].

In the linkage between the information perception style and computer security education, students should grasp scientific concepts besides their applications through hands-on activities and concrete examples [19]. In addition, students find the hybrid approach of theory and practice in a computer security course more appealing and exciting [24]. The information perception style is appropriate for dealing with this issue in providing appropriate learning material when taking into account abstract conceptualisation and concrete experience. Furthermore, the incorporation of this approach offers a solution to the debate over how to offer instruction: from abstract concepts to concrete examples, or from examples to concepts.

The next section presents the proposed approach. It personalises the sequences of learning material for each student based on their information perception style.

3. LEARNING STYLE ADAPTIVITY

A specific adaptivity approach based on the information perception style is proposed for computer security education. Personalised learning paths through learning material are generated in an e-learning system [3]. Learning material is represented at two levels. Level one contains a number of learning units. A learning unit focuses entirely on one topic of the course. Each learning unit contains a set of interrelated learning objects in level two [5]. The learning objects are annotated to support adaptation to match the information perception learning style - following the Felder-Silverman model [13]. The main aim is to provide an appropriate combination and ordering of concrete and abstract learning objects.

Figure 1 depicts an example of the course, and how learning paths are generated for sensory and intuitive students. Sensory students study concrete learning objects first and then interact with abstract learning objects (i.e., concrete-to-abstract). It implies that examples and practical activities will be presented first and then followed by concepts and mathematical models when teaching each learning unit. In contrast, intuitive students interact with abstract learning objects first, and then study concrete learning objects (i.e., abstract-to-concrete). Concepts and mathematical models are presented first; followed by examples and practical activities.

A basic computer security course is built and represented in the adaptive e-learning system. It contains two learning units: symmetric key encryption and key-exchange protocols. The symmetric key encryption unit contains four learning objects (concept, example, mathematical notation and interactive tool).

The key-exchange protocols unit has two learning objects (concept and example).

Each learning unit incorporates concrete and abstract learning objects, which will ensure that sensory and intuitive learning styles are equally supported when generating learning paths. Concrete learning objects provide direct practical experience by performing a new task or by presenting a real-world example. A screenshot of a concrete learning object as provided by the system is presented in Figure 2. Abstract learning objects present the mathematical models, principles and concepts of a specific subject of computer security.

It should be noted that this approach is, to some extent, generic; it can be adapted to many application domains by providing personalised sequence of learning material. It is not limited to the computer security domain only.

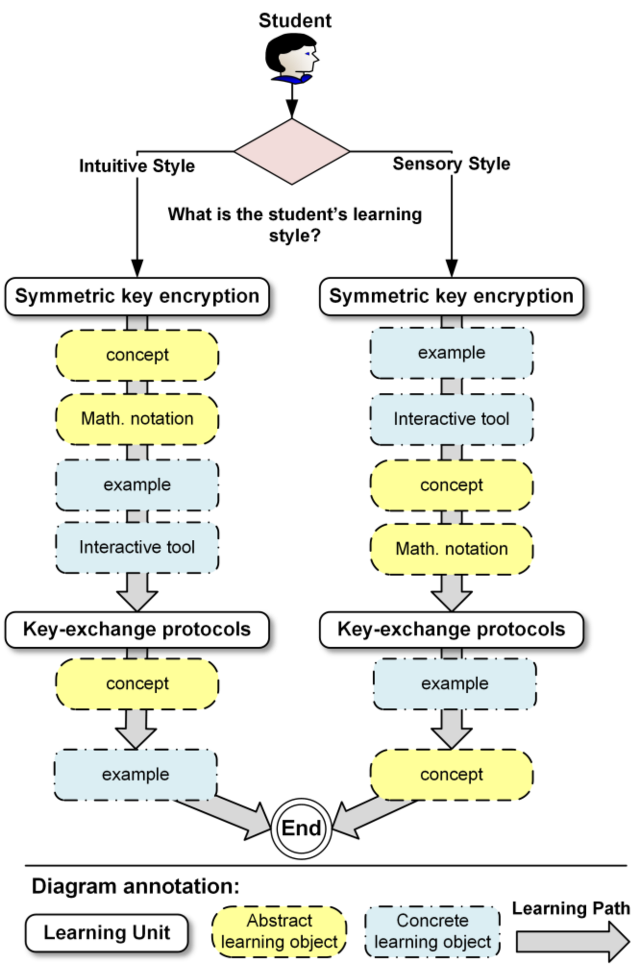

Figure 1. Generation of learning paths for sensory and intuitive students.

4. EXPERIMENTAL EVALUATION

A controlled experiment in a higher education learning environment was conducted in a computer laboratory in order to evaluate the proposed approach. Eight experimental sessions were conducted; each session lasted for about 75 minutes. An important point is that computer security was not part of the subjects' curriculum; the students were encouraged to take part in the experiment to learn a new topic.

A between subjects design, in which each subject experiences only one condition, was used to avoid the problems of carryover and learning effect from one condition to another.

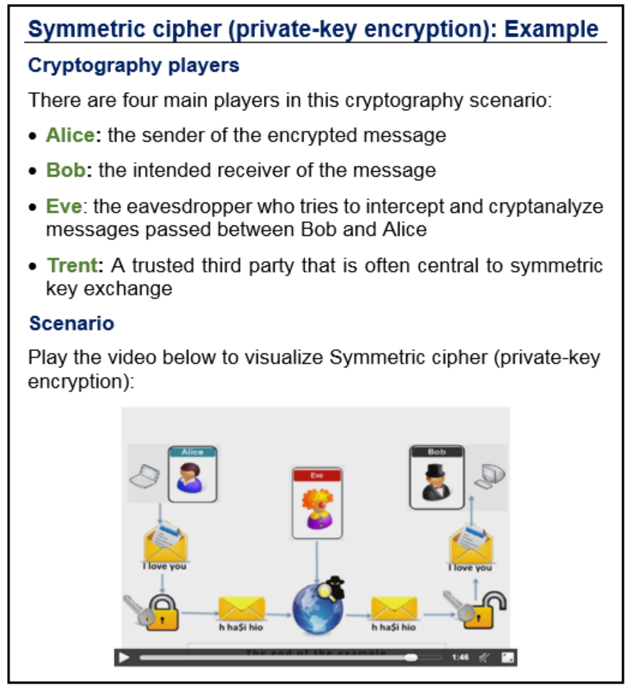

Figure 2. A concrete learning object example as provided by the adaptive e-learning system.

The next sections provide the research hypotheses, data collection tools and experimental procedure. They are prerequisites for any well-conducted and controlled experiment.

4.1 Hypotheses

Two hypotheses were put forward for this study based on the information perception style. The hypotheses are formulated as follows:

Hypothesis 1. Matching computer security learning material and the information perception style of students yields significantly better learning gain than without matching.

Hypothesis 2. Matching computer security learning material and the information perception style of students yields significantly better student satisfaction than without matching.

According to these hypotheses, the variables were classified into two types: independent and dependent variables. Two independent variables were manipulated to test the dependent variable: (1) an experimental group who interacted with an e-learning system that matched learning material and the information perception style (matched group), and (2) a control group who interacted with an e-learning system that mismatched learning material and the information perception style (mismatched group).

Learning gain and student satisfaction (i.e., the dependent variables) were measured to provide insight into the effectiveness of adaptivity based on the information perception style in computer security education.

4.2 Data Collection

Three data collection tools are used. A subset of the Index of Learning Style (ILS[1]) questionnaire, based on the Felder-Silverman model, containing 11 questions was used to identify the information perception style [13]. The tool is considered reliable and valid for identifying the learning style of students [14].

Pre and post-tests were developed and subjectively evaluated by three computer security experts to measure the learning gain (post-test – pre-test). Recalling, understanding and applying learning factors were taken into account when developing the questions of the tests. Both tests were similar except for the formulation of some questions, their order and the answer options. They were multiple-choice questions with four options for each question. Incorrect answers were penalised in order to discourage random guessing following the strategy developed for standardised tests (such as the SAT[2] test). The strategy is to deduct 100/(n-1) percent of the value of the question, where n is the number of answer options. There were 10 multiple-choice questions in each test, and the value of each question is 10.

Student satisfaction was measured by the e-learner satisfaction questionnaire tool (ELS) which can be found in [25]. The tool is a questionnaire that measures satisfaction in terms of four components including the system interface, learning community, learning content and system personalisation. Three components (i.e., interface, content and personalisation) were taken into account; their related 13 questions were used with 7-point Likert scale with anchors ranging from "strongly disagree" to "strongly agree". An example related to satisfaction with the learning content in the ELS tool is: '*the content provided by the e-learning system is easy to understand*' [25].

4.3 Experimental Procedure

The subjects were first introduced to the main objectives of the experiment and informed of the procedure. They were asked to access the e-learning system via an Internet browser. They completed a demographic data form and the ILS questionnaire using the system. Then, the system randomly assigned subjects to experimental (matched) or control (mismatched) groups, and then they completed a pre-test. The pre-test involved answering a set of questions related to computer security.

The subjects then started the process of learning and completed all the learning objects related to symmetric key encryption and key-exchange protocols, but in a different sequence according to their matched or mismatched learning style. At the end of the learning session, they completed a post-test, followed by the e-learner satisfaction questionnaire tool (ELS) [25]. This ended the procedure.

5. RESULTS

The experiment was completed successfully by 60 male subjects. There were 29 subjects in the matched group and 31 subjects in the mismatched group. The subjects were undergraduate computer science students. The mean age of the subjects was 25. In the experiment, there were more sensory students (72%) than intuitive students (28%). Few subjects had strong characteristics of the information perception style for both categories: sensory and intuitive. However, the majority of the subjects had mild to moderate characteristics. The distribution of sensory and intuitive students somewhat matches other studies according to their samples [14]; there are often more sensory students than intuitive students.

5.1 Learning Gain

The learning gain (i.e., post-test score – pre-test score) and the post-test results of the matched group were higher than those of the mismatched group as presented in Figure 3. The maximum learning gain score was 66, which is the same for both groups.

In order to test the significance of the learning gain, a null hypothesis was put forward indicating that the matched and the mismatched groups are different in terms of the pre-test (prior knowledge). An independent sample t-test at the alpha level .05 was calculated to test the null hypothesis. It indicates that there was no significant difference between the two groups in terms of the pre-test, $p>.05$. It should be also noted that computer security was a new topic to 95% of the experimental subjects, based on their self-assessment. Therefore, the null hypothesis is rejected; differences between the study groups can be neglected and the significance of the learning gain can be conducted.

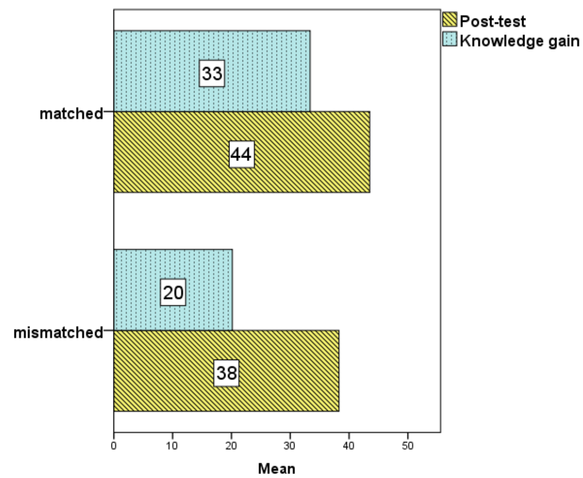

Figure 3. Learning gain and post-test results for the matched and mismatched groups.

An independent sample t-test was conducted to compare the learning gain for the matched group and the mismatched group. There was a significant difference in the learning gain scores for the matched group and the mismatched group, $p<.05$. Hypothesis 1 is therefore confirmed, and it can be concluded that matching learning material to the information perception style yields significantly better learning gain than without matching, with medium to large effect ($d=.57$).

A further analysis was conducted to test the difference between sensory and intuitive students in terms of learning gain. Figure 4 shows that in general the matched group had greater learning gain for both sensory and intuitive students than the mismatched group. Therefore, matching learning material and the information perception style is beneficial for both sensory and intuitive students.

Concerning affinity with learning style, the learning gain scores of the students who have mild sensory and intuitive characteristics in both the matched and mismatched groups were relatively the same. Balanced treatments for students who have mild preferences may be more suitable than either matching or mismatching learning style and learning material. As the affinity with learning

[1] http://www.engr.ncsu.edu/learningstyles/ilsweb.html

[2] https://sat.collegeboard.org/home

style increases, the learning gain for the matched group was higher than the mismatched group. For example, moderate sensory and intuitive students in the matched group had better learning gain than moderate sensory and intuitive students in the mismatched group. However, a comparison between students who had a strong affinity with their learning style could not be made; very few subjects had strong sensory and intuitive characteristics in the experimental sample.

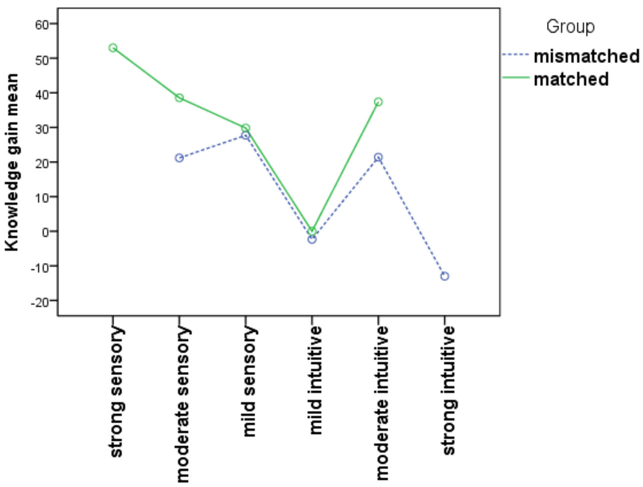

Figure 4. Learning gain of sensory and intuitive students.

5.2 Student Satisfaction

General student satisfaction was evaluated using the e-learner satisfaction questionnaire tool (ELS) [25]. Three components of the ELS tool were taken into account including the system interface, the learning content and the system personalisation; satisfaction for each component was also calculated. An independent sample *t*-test was conducted; it indicates that the matched group ($M=6.17$) had significantly higher general student satisfaction scores than the mismatched group ($M=5.35$), $p<.05$. Hypothesis 2 is also confirmed.

Table 1 indicates that the matched group had higher student satisfaction mean scores in terms of the system interface, the learning content and the system personalisation than the mismatched group. It may imply that the satisfaction of students even for elements that are not directly related to learning such as the interface is higher when matching the information perception style and learning material.

Table 1. Students' satisfaction scores.

Component	Matched group	Mismatched group
System interface	5.93	5.12
Learning content	6.14	5.41
System personalisation	6.10	5.45

5.3 Additional Findings

The correlation between learning gain and student satisfaction variables was tested. It was found that the relationship between the two variables was non-monotonic. Hence, it can be suggested that there is no clear correlation between the learning gain and student satisfaction. A Pearson correlation coefficient test was computed to assess the relationship between learning gain and time spent on learning. There was a weak, positive correlation which was not statistically significant, $r(58)=.23$, $p> .05$.

A Spearman rank correlation coefficient test was also computed to investigate the relationship between age and learning gain as well as the relationship between age and time spent on learning. There was a weak, negative correlation between age and learning gain variables, which was statistically significant, $r_s(58)=-.27$, $p< .05$. There was also a very weak, negative correlation between age and time spent on learning, which was not statistically significant, $r_s(58)= - .07$, $p> .05$.

6. DISCUSSION

In contrast with some published studies [8,10], the findings of this work confirm the view that the adaptation of learning material based on learning style does have an effect on learning gain. These results are in line with the outcome of many related research programmes [18,23]. More specifically, it was demonstrated that matching computer security learning material with the students' information perception style yields significantly better learning gain. It should be noted that the learning gain is related to the short-term learning effect where students completed the post-test immediately after the experiment. This finding cannot however be generalised to cover the long-term learning effect. A study with a wider scope is currently being carried out, which will incorporate the students' existing knowledge level into the adaptation model.

In this study, other relevant factors were also investigated. It was found that there was a positive correlation between the learning gain and the time spent on learning. Although it may be the case that the more students spend their time on learning, the higher their learning gain, the correlation between learning gain and time spent was weak and was not significant. In addition, a negative but significant correlation between learning gain and age was found. This might imply that the older the student the lower the learning gain. Furthermore, the time spent on learning decreased with age. These particular results may be specific to the experimental sample. With respect to student satisfaction, the results reveal that student satisfaction is higher when the computer security material is matched with student information perception style. However, there was no correlation between learning gain and student satisfaction. This may point to the potential use of learning style as a motivational factor in enhancing the experience of the students [1].

It is expected that the results can, to some extent, be generalised to other topics in computer security, such as Data Encryption Standards (DES) [4] and Kerberos protocols. Furthermore, since the proposed approach effectively enhances learning and contributes to better computer security education, its application could be beneficial in other computer science topics such as programming and databases. This potential generalisation could provide an opportunity for exploring further the range of the characteristics of the information perception dimension: mild, moderate and strong. This could also encourage a more refined and creative approach to the design, implementation and deployment of learning objects. The research would also benefit from a more heterogeneous sample of subjects, who would be exposed to a larger set of learning objects.

Although the information perception dimension of learning style might be considered the most important [12], other learning style dimensions should also be integrated into the proposed approach in order to enhance the learning process. Moreover, the cognitive and meta-cognitive skills of the students can be enriched by encouraging more collaborative work, and by enabling students to monitor their learning performance and learning style profiles.

This paper reports on one of the few studies where the information perception style is explicitly applied in the domain of computer security education. This work has also the merit of offering a resolution to the on-going debate, in teaching, between the exclusive application of an abstract-to-concrete approach or a concrete-to-abstract approach. It provides a compromise by adopting an appropriate approach according to the learning style of each student.

7. CONCLUSION

In this paper, an approach of learning style adaptivity was proposed for computer security education. In the approach, a personalised sequence of learning material was generated for each student based on the information perception dimension of learning style. This involved providing a concrete-to-abstract sequence of learning material to sensory learners, and the generation of the sequence of abstract-to-concrete material for intuitive students.

The approach was evaluated by a controlled experiment with sixty subjects. There were positive findings in terms of learning gain and student satisfaction when matching learning material to the learning style of students. It indicates that this approach can contribute to better computer security education. It may be also useful in other computer science topics such as programming and databases. Moreover, it is suggested that the fixed teaching approach such as abstract-to-concrete or concrete-to-abstract will not always be beneficial for all students. The findings have however revealed that the teaching approach should match the students' preferences.

The main limitations of the experiment were that it was based on a short-term study with a limited number of computer security learning objects and with a relatively small group of subjects. Future research will extend the proposed approach to incorporate other learning factors such as cognitive and meta-cognitive skills and the abilities of students. It will also involve a long-term evaluation.

8. REFERENCES

1. Akbulut, Y. and Cardak, C.S.Adaptive educational hypermedia accommodating learning styles: A content analysis of publications from 2000 to 2011. *Computers & Education 58*, 2 (2012), 835–842.
2. Alshammari, M., Anane, R., and Hendley, R.Adaptivity in E-Learning Systems. *The 8th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS 2014)*, (2014), 79–86.
3. Alshammari, M., Anane, R., and Hendley, R.An E-Learning Investigation into Learning Style Adaptivity. *The 48th Hawaii International Conference on System Sciences (HICSS-48)*, (2015), pp11–20.
4. Anane, R., Purohit, K., and Theodoropoulos, G.An Animated Cryptographic Learning Object. *Computer Graphics, Imaging and Visualisation, 2008. CGIV'08. Fifth International Conference on*, (2008), 61–68 *http://www.cs.bham.ac.uk/research/projects/lemsys/DES/*.
5. Anane, R.The Learning Object Triangle. *Advanced Learning Technologies (ICALT), 2014 IEEE 14th International Conference on*, (2014), 719–721.
6. Brusilovsky, P. and Millán, E.User models for adaptive hypermedia and adaptive educational systems. *The adaptive web*, (2007), 3–53.
7. Brusilovsky, P.Adaptive Hypermedia for Education and Training. *Adaptive Technologies for Training and Education*, (2012), 46.
8. Buch, K. and Sena, C.Accommodating diverse learning styles in the design and delivery of on-line learning experiences. *International Journal of Engineering Education 17*, 1 (2001), 93–98.
9. Chrysafiadi, K. and Virvou, M.Student modeling approaches: A literature review for the last decade. *Expert Systems with Applications 40*, 11 (2013), 4715–4729.
10. Coffield, F., Moseley, D., Hall, E., and Ecclestone, K.*Learning styles and pedagogy in post-16 learning: A systematic and critical review*. Learning and Skills Research Centre London, London, 2004.
11. Cone, B.D., Irvine, C.E., Thompson, M.F., and Nguyen, T.D.A video game for cyber security training and awareness. *Computers & Security 26*, 1 (2007), 63–72.
12. Felder, R.M., Felder, G.N., and Dietz, E.J.The effects of personality type on engineering student performance and attitudes. *Journal of Engineering Education 91*, 1 (2002), 3–17.
13. Felder, R.M. and Silverman, L.K.Learning and teaching styles in engineering education. *Engineering education 78*, 7 (1988), 674–681.
14. Felder, R.M. and Spurlin, J.Applications, reliability and validity of the index of learning styles. *International Journal of Engineering Education 21*, 1 (2005), 103–112.
15. Hu, D. and Wang, Y.Y.Teaching Computer Security using Xen in a Virtual Environment. *Information Security and Assurance, 2008. ISA 2008. International Conference on*, (2008), 389–392.
16. Hu, J., Meinel, C., and Schmitt, M.Tele-lab IT Security: An Architecture for Interactive Lessons for Security Education. *Proceedings of the 35th SIGCSE Technical Symposium on Computer Science Education*, ACM (2004), 412–416.
17. Keefe, J.W.Learning style: An overview. *Student learning styles: Diagnosing and prescribing programs*, (1979), 1–17.
18. Klasnja-Milicevic, A., Vesin, B., Ivanovic, M., and Budimac, Z.E-Learning personalization based on hybrid recommendation strategy and learning style identification. *Computers & Education 56*, 3 (2011), 885–899.
19. Konak, A., Clark, T.K., and Nasereddin, M.Using Kolb's Experiential Learning Cycle to improve student learning in virtual computer laboratories. *Computers & Education 72*, 0 (2014), 11–22.
20. Marsa-Maestre, I., De La Hoz, E., Gimenez-Guzman, J.M., and Lopez-Carmona, M.A.Design and evaluation of a learning environment to effectively provide network security skills. *Computers & Education 69*, (2013), 225–236.
21. Mitrovic, A.An intelligent SQL tutor on the web. *International Journal of Artificial Intelligence in Education 13*, 2 (2003), 173–197.
22. Rößling, G., Joy, M., Moreno, A., et al.Enhancing Learning Management Systems to Better Support Computer Science Education. *SIGCSE Bull. 40*, 4 (2008), 142–166.
23. Schiaffino, S., Garcia, P., and Amandi, A.eTeacher: Providing personalized assistance to e-learning students. *Computers & Education 51*, 4 (2008), 1744–1754.
24. Sharma, S.K. and Sefchek, J.Teaching information systems security courses: A hands-on approach. *Computers & Security 26*, 4 (2007), 290–299.
25. Wang, Y.-S.Assessment of learner satisfaction with asynchronous electronic learning systems. *Information & Management 41*, 1 (2003), 75–86.