28th Annual Conference of the Australasian Association for Engineering Education (AAEE 2017)

ORDER OF PROCEEDINGS

SYDNEY, 10-13 DECEMBER 2017

Macquarie University CRICOS Provider 00002J

Australasian Association for Engineering Education

MACQUARIE University

Publication Information

All full papers accepted for publication in the Proceedings of the 28th Annual Conference of the Australasian Association for Engineering Education were submitted as full papers and were blind peer reviewed. Authors were given the opportunity to amend their paper in light of these reviews before the decision to accept and publish the paper was made. This process of reviewing is in accordance with the criteria set for research papers by the Department of Education, Employment and Workplace Relations (DEEWR) and the Department of Innovation, Industry, Science and Research (DIISR) of the Australian Government.

This Publication Title: Proceedings of the 28th Annual Conference of the Australasian Association for Engineering Education (AAEE 2017)

Author: Australasian Association for Engineering Education Conference (28th: AAEE 2017)

Editors: Nazmul Huda, David Inglis, Nicholas Tse, Graham Town

Published in Australia by: School of Engineering, Macquarie University, Sydney, Australia

ISBN: 978-0-646-98026-3

AAEE-2017 Proceedings

Quantitative Research Design to Evaluate Learning Platforms and Learning Methods for Cyber-security Courses

Kamanashis Biswas, Vallipuram Muthukkumarasamy
School of ICT, Griffith University, Gold Coast
{k.biswas, v.muthu}@griffith.edu.au

SESSION C1: Integration of theory and practice in the learning and teaching process

CONTEXT Teaching security courses is a challenging task in computer science program since it requires careful integration of theoretical concepts with their practical applications. In this paper, a quantitative approach is used to evaluate effective learning platforms and different learning styles for cyber-security courses. The outcomes of the study show that practice-based learning is the most effective learning method for cyber-security courses and student performance can further be enhanced significantly through social learning instead of solitary learning.

PURPOSE The main goal of this research is to understand the effects of learning styles and platforms for successful adaptation of different pedagogical practices. The following research questions are designed to achieve the expected outcomes.

- ✓ For cyber-security courses, does the performance of a student match with his/her self-specified learning performance?
- ✓ How learning platforms affect a student's performance in cyber-security courses? What factors play significant roles to successfully run a cyber-security course?
- ✓ Which type of learning mechanism is the most effective for cyber-security courses? Is learning in a group better than individual learning?

APPROACH Quantitative research is defined as a scientific method which follows a number of procedures such as generation of models, identifying theories and hypotheses, development of instrumentals and methods for measurement, experimental control and manipulation of variables, collection of empirical data, modelling and analysis of data and evaluation of results. This research follows experimental modes of inquiry which follows a standard form namely, participants, materials, procedures and measures.

RESULTS The results show that there is no single platform that includes all features to successfully run a cyber-security course. However, this problem can be solved by integrating those features with existing platforms. The study also suggests that learning performance can further be enhanced by choosing appropriate learning style.

CONCLUSIONS This paper investigates the impacts of learning platforms and learning strategies for cyber-security courses. Similar experiments from different aspects will be interesting to test their validity. The outcome can be used for further decision making e.g., the correlation of learning style difference could help to determine whether customized learning styles would be more effective for teaching cyber-security courses

KEYWORDS Quantitative research, Learning style, Cyber-security

Introduction

With the increased use of World Wide Web, malware and cyber-threats have also increased exponentially in the last few years. While cyber-attacks have been growing rapidly, it was predicted that there would be a global deficit of about two million cyber-security professionals in 2017 (Zantua, Dupuis, & Popovsky, 2015). This shortfall in critical cyber-security skills can mainly be overcome by promoting cyber-security programs in higher education. However, teaching cyber-security at undergraduate or postgraduate levels has been challenging for a number of reasons and has led to a shortage of qualified people with the right skills. This global phenomenon is due to lack of expertise and resources to develop and teach such programs, and keep up with continuously evolving discipline. The digital disruption and adoption of fast changing technologies by businesses and customers create a perfect environment for adversaries. The unknown vulnerabilities, zero-day exploits, high risk levels and possible consequences with lack of countermeasures leave the governments, businesses and industries off-guard. From world leading organizations to small businesses have fallen victims and became an embarrassing situation for nations.

The solution to cyber-security challenges begins from creating skilled workforce in this space, who will have the fundamental knowledge and skills to evaluate and address issues. Since any security solution is a balancing act, the fact evolving nature of threats require understanding and appreciation of the issues at all levels. This demands immediate action to roll out programs by educational institutions at various stages: undergraduate, postgraduate, professional development, up-skilling of workforce etc. Scholarship of Learning and Teaching needs to happen to steadily improve cyber-security education and cope with future challenges. Since learning platforms and individual learning style play a significant role in students' performance, this study uses a quantitative approach to evaluate them in real classroom environment. Quantitative research deals with systematic and scientific investigation of quantitative properties and phenomena, and their relationships. One of the key benefits of quantitative approach is that the procedure ensures reliability and validity of experiments. The main goal of this research is to understand the effects of learning styles and platforms for successful adaptation of different pedagogical practices. The following research questions are designed to achieve the expected outcomes.

- For cyber-security courses, does the performance of a student match with his/her self-specified learning performance?
- How learning platforms affect a student's performance in cyber-security courses? What factors play significant roles to successfully run a cyber-security course?
- Which type of learning mechanisms is the most effective for cyber-security courses? Is learning in a group better than individual learning?

Related Works

Extensive research have been conducted to investigate the applicability of both new and existing learning styles and platforms during last few decades. This is becasuse learning platforms and learning strategies have significant impacts on learning outcomes. A learning platform is an integrated set of interactive services that provides the participants access to common resources and communication tools as well as exchange information with each other. Similar to learning platforms, learning strategies also offer a number of ways to enhance learning capabilities. For example, problem based learning provides an efficient way to acquire basic competencies where students learn about a topic through the solving of problems (Gorghiu, 2015). In contrast, students are presented with the problem in inquiry based learning and asked to demonstrate self-analysis and critical thinking required to solve the problem (Gordon, 2015).

Sheen (2015) proposed an extensible technology framework for cyber-security education. The paper explores different types of teaching methods, technology, and means used to

explain theoretical concepts. The framework uses a central engine to coordinate learning management with infrastructure in order to reduce administrative burden in cyber-security education.

Alshammari, Anane, and Hendley (2015) proposed an approach for learning style adaptivity and developed an e-learning system to facilitate personalized and adaptive learning. The authors also conducted experiments on sixty subjects and the results indicate that matching learning materials with learning style of the students significantly enhance learning gain and satisfaction.

Bell, Vasserman, and Sayre (2015) developed an assessment tool that can be used to measure student interest and self-efficacy in relation to cyber-security. This tool enables educators to detect changes in student outcomes and thus helps in systematically improve pedagogical strategies.

Cheung, Cohen, Lo, and Elia (2011) used Challenge Based Learning (CBL) methodology to cyber-security courses. In this approach, students are encouraged to collaborate with their peers, ask questions and develop a thorough understanding of the studied concepts and solve real world challenges. In addition to this, participating in cyber-security competitions, publishing research findings and making presentations are held regularly for guiding activities.

In this paper, our main emphasis is on different learning styles and platforms that can be used to enhance learning performance of students in cyber-security courses. Modern learning platforms like PebblePad, Blackboard and Facebook page are also evaluated in the experiments as they are most commonly used tools for interactive learning.

Quantitative Research Methodology

Quantitative research is defined as a scientific method, which generally follows a number of procedures such as generation of models, identifying theories and hypotheses, development of instrumentals and methods for measurement, experimental control and manipulation of variables, collection of empirical data, modelling and analysis of data and evaluation of results (Cresswell, 2003). The quantitative research methodology includes less rigorous experiments known as quasi-experiments, which are more suitable compared to true experimental designs as it does not have any time and logistical constraints. This research follows experimental modes of inquiry, which follows a standard form namely, participants, materials, procedures and measures. The following subsections describe these four forms of experimental methods used in this research.

Participants

For this experiment, 30 undergraduate students of the Network Security course and 21 postgraduate students of the Network Information Security course have been selected, who are studying Bachelor of Information Technology (BIT) and Masters of Information Technology (MIT) programs. This study follows a 2 × 2 × 2 factorial design: resources (learning platforms, learning styles), statement of values (implicit, explicit), and participants' identification (BIT, MIT). In addition, another dimension: individual versus group is also included in the experiments as a control and relevant for learning styles.

Variables

The main objective of this research is to evaluate the impacts of learning platforms and learning styles for cyber-security courses. A number of standard questions are designed for experiments to collect each student's individual preference. The collected data are tested and verified against real time responses conducted throughout the courses. The implicit statement of values condition is measured from the standardized format used in the experiment, whereas the explicit statement of values condition is obtained measuring the

responses of the participants (BIT and MIT). Group experiments are also designed to analyze the treatment variables and the performance measures of the students obtained from the experiments are used to draw the final conclusion.

Instrumentation and Materials

The experiments are conducted for six consecutive weeks during lab hours and each week students are asked to answer or solve a number of questions. In first part, students are provided five technical questions and engaged in a repetitive question and answer session to find the correct solutions. The second part consists of five complex and challenging problems to be solved collaboratively. For the third part, a number of practice questions are provided and on the basis of knowledge acquired to solve those problems, the students are asked to solve five related questions. The answers are collected through three different platforms namely Blackboard, PebblePad and Facebook page. While submitting answers through PebblePad, students faced problems to upload their answers because of missing instructions. A mock experiment with dummy questions is held to overcome the problem. The following topics are used in undergraduate questionnaires: Unix Programming, Public Key Infrastructure, Hash and Digital Signatures, Security Tools, SQL Injection, and Same Origin Policy. On the other hand, postgraduate questionnaires include Advanced cryptographic schemes, Cipher modes, Secure Electronic Transaction (SET), Intrusion Detection System (IDS), Firewalls, and IP traceback. Some of these questions are descriptive (e.g., which features differentiate intrusion prevention system from IDS?) whereas some others are technical (e.g., for a given network scenario, what configurations should be changed to establish a telnet connection between two systems?). At the end of each week's workshop, students' answers are collected through learning platforms for evaluation. The outcomes are the average of the students' six weeks performance.

Experimental Procedures

The experimental procedure includes four steps: i) collection of demographic data, ii) learning platforms, instrument and materials, iii) learning styles and iv) learning tasks. In learning tasks, students answered a number of questions related to weekly lectures. Three learning platforms are used alternately to obtain the answers and the measurement is done on collected data to evaluate students' self-reported learning styles. As mentioned above, a mock session has also been conducted to overcome the PebblePad problem and the new results are recorded for analysis. Another experiment is done by randomly assigning students into groups (ten undergraduate and seven postgraduate groups) where each group consists of exactly two members. We have used the 2 × 2 × 2 factorial design experiment that uses two treatment variables to examine the performance as well as effects of the treatment variables on final outcomes. In this task, students are asked to develop a simple host based Intrusion Detection System. All students received the same background knowledge required to solve the task. The experiment has been conducted from two dimensions: one is problem/ practice based solution (*A*) that seems to be relevant to learning styles whereas individual/ group (*B*) dimension serves as a control. The first group only receives the treatment as shown below.

Group A: *R* ---------- *O* ---------- *X* ---------- *O*

Group B: *R* ---------- *O* ---------- *O*

Here, ***X*** denotes treatment, manipulation, induction, ***O*** denotes measurement, observation, and ***R*** is random assignment.

Threats to Validity

Threats of validity are classified into two categories: i) internal validity threats and ii) external validity threats. The following subsections describe each of these threats.

Internal Validity Threat Control

History- In this experiment, both groups have experienced the same current events. So no other current event affected the change in the dependent variable. *Maturation*- No changes occur in the dependent variable due to normal experimental processes because both groups experience the same experimental processes. *Selection*- As all the subjects are selected and all of them have received treatment or control condition, there is no impact on the dependent variable. *Experimental Mortality*- It means that whether some participants drop out and does it affect in the results or not. In the experiments, the same participants involved in the entire study in both experimental and control groups, so there appears to be no bias. *Testing*- Both groups get a pre-test in the experiment but a pre-test may have the experimental group more sensitive to the treatment. *Instrumentation*- The measurement method, materials and instruments have not been changed during the research.

External Validity Threats Control

Unique program features- A motivated set of facilitators for small group discussions may exist. *Effects of Selection*- probably applicable to other computer science courses. *Effects of Setting*- computer science students have their own culture, so it is doubtful if this would be applicable to other types of students such as medical students. *Reactive effects of experimental arrangements*- it would be better to imitate the results in other related programs.

Results and Analysis

The first experiment has been designed to test whether the performance of an individual student matched with his/her self-specified learning performance. The outcomes indicate that problem-based learning is more preferable compared to inquiry-based and practice based learning styles for cyber-security courses. *78.43%* students have found right answers through problem-based learning, whereas the amount for practice-based and inquiry-based learning is *62.74%* and *54.90%* respectively. This outcome is consistent with their self-reported learning styles as shown in Figure 1. The percentile representation of experimental outcomes shows that 40% students learn better through problem-based learning whereas the number is 32% and 28% for practice-based and inquiry-based learning respectively. These figures are very close to their self-specified learning styles where 46% students chose problem-based learning, 30% of them preferred practice-based learning, and the rest 24% students specified inquiry-based learning.

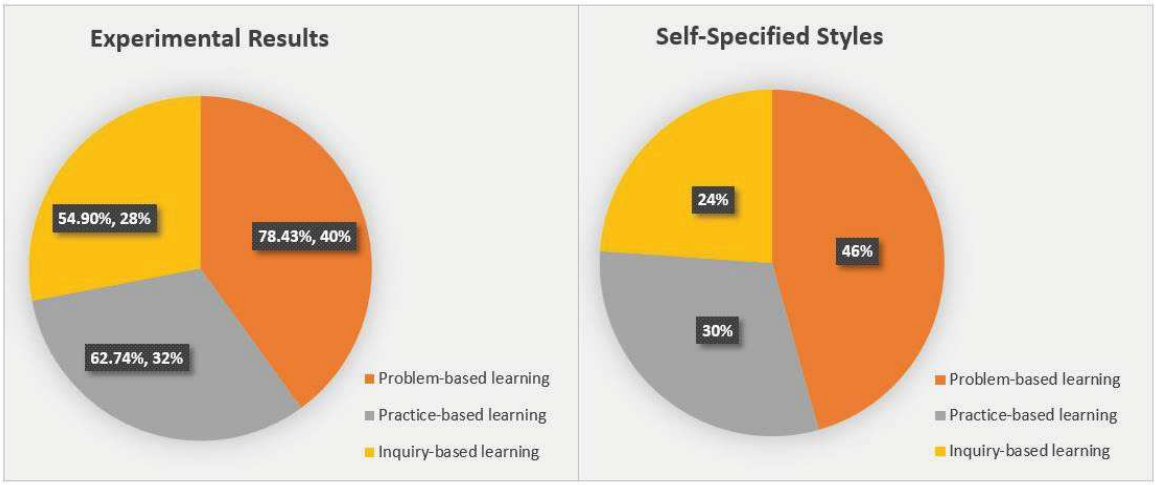

Figure 1: Learning performance outcomes for different learning styles

The second experiment is conducted to examine the impacts of different learning platforms. Students' responses are observed and accuracy is measured in terms of successful

collaboration and effective use of provided resources. The outcomes show that *67.78%* accuracy is achieved while using PebblePad, whereas the level of accuracy obtained for Blackboard and Facebook Page is *53.30%* and *49.23%* respectively. However, in self-specified instrument, *38%* students chose to use Blackboard while *33%* and *29%* of them specified PebblePad and Facebook Page as their preferred learning platforms as shown in Figure 2. Thus, experimental results do not support self-specified learning platforms. We noticed that PebblePad supports some unique features compared to other platforms such as individual feedback, group feedback, sharing workbook with any group member. PebblePad is a good learning platform for collaboration among group members and course instructor. Although Facebook Page is more user friendly, it doesn't provide most of the basic features such as setting submission deadline, student grading and integration of third party tools. On the other hand, Blackboard supports many third-party tools such as SafeAssign, TurnItIn, Tweak and WebAssign. However, in addition to other limitations, Blackboard is not user friendly like PebblePad and Facebook Page. From the experiments, it is understandable that there is no unique platform, which provides all necessary features to run a cyber-security course. In terms of students' satisfaction and learning performance, PebblePad outperforms other two platforms in our experiments.

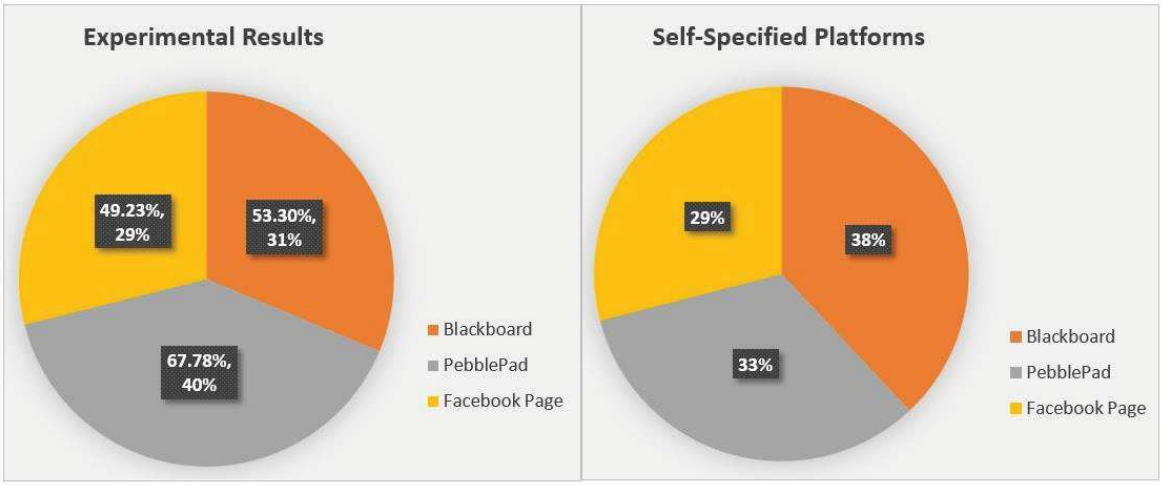

Figure 2: Impacts of different learning platforms on learning outcomes

To address third research question, students are divided into multiple groups with exactly two members: ten undergraduate groups and seven postgraduate groups. In this task, undergraduate and postgraduate students are asked to develop a simple IDS and an advanced IDS respectively using shell script in groups and individually. The IDS has two parts: i) verification file generation and ii) intrusion detection. Practice-based learning method has been implemented as a learning strategy for the first part whereas problem-based approach is followed for the second part. Students are taught basic shell script programming and essential features required to design the IDS. From obtained results, it was found that *88.23%* students in groups could solve the part 1 using practice-based method, whereas it is *64.70%* for individual. On the other hand, part 2 is solved by *76.47%* students working in groups, whereas it is *47.05%* for individual learning. We also calculated the *chi-square p* value with one degree of freedom. The *p value* is *0.478*, which indicates that there is no statistically significant difference between the observed value and the expected value. Thus, the experimental outcomes indicate that learning in groups is more suitable compared to individual learning for cyber-security courses. Similarly, practice-based learning is more effective than problem-based learning according to obtained results.

Conclusion

This paper investigates the impacts of learning platforms (Blackboard, PebblePad and Facebook Page) and learning strategies (inquiry-based, problem-based and practice-based) for cyber-security courses. Similar experiments from different aspects (e.g., Yammer platform and project based learning) will be interesting to test their validity. The results show that there is no single platform that includes all features to successfully run a cyber-security course. However, this problem can be solved by integrating those features, wherever possible, with existing platforms. The study also suggests that learning performance can be enhanced by choosing appropriate learning style. The outcome can be used for further decision making such as the correlation of learning style difference could help to determine whether customized learning styles would be more effective for teaching cyber-security courses. This paper will provide a good background for researchers interested to perform further research in cyber-security education. Our future work aims to evaluate other learning platforms and learning styles to examine their applicability for cyber-security courses.

References

Alshammari, M., Anane, R., & Hendley, R. J. (2015). *The Impact of Learning Style Adaptivity in Teaching Computer Security*. Paper presented at the Innovation and Technology in Computer Science Education Conference, (pp. 135-140). Vilnius, Lithuania: ACM.

Bell, R., Vasserman, E., & Sayre, E. C. (2015*). Developing and Piloting a Quantitative Assessment Tool for Cybersecurity Courses*. Paper presented at the 122nd ASEE Annual Conference and Exposition. Seattle, WA: American Society for Engineering Education .

Cheung, R. S., Cohen, J. P., Lo, H. Z., & Elia, F. (2011). Challenge Based Learning in Cybersecurity Education . Paper presented at the International Conference on Security and Management (SAM 11), (pp. 524 – 529).

Cresswell, J. W. (2003). *Research Design : Qualitative, Quantitative and Mixed Meth-ods Approaches.* SAGE publications.

Gordon, N. B. (2015). Inquiry based Learning in Computer Science teaching in Higher Education. *Innovation in Teaching and Learning in Information and Computer Sciences* , 22-33.

Gorghiu, G. D. (2015). Problem-Based Learning - An Efficient Learning Strategy In The Science Lessons Context. *Procedia - Social and Behavioral Sciences*, 1865-1870.

Sheen, F. J. (2015). An extensible technology framework for cyber security education. Brigham Young University. Retrieved May 12, 2017, from http://scholarsarchive.byu.edu/cgi/viewcontent.cgi?article=5374&context=etd

Zantua, M., Dupuis, M., & Popovsky, B. E. (2015). *RE-ENGINEERING THE CYBERSECURITY HUMAN CAPITAL CRISIS*. Retrieved May 17, 2017, from http://faculty.washington.edu/marcjd/articles/Re-engineering%20the%20Cybersecurity%20Human%20Capital%20Crisis.pdf