Using Cybersecurity Education Tool Assessment Method to Measure the Effective of Different Teaching Methods

Huiming Yu, Xiaohong Yuan, Jung Hee Kim, Jinsheng Xu and Taehee Kim

***Abstract*-In this paper, we present two teaching methods that are control group teaching and experimental group teaching to show how using Cybersecurity education tools to help students learn related topics. We develop an effective Cybersecurity Education Tool Assessment Method (CETAM) to measure effective of the teaching methods and evaluate these education tools. We adopt two different teaching methods with selected Cybersecurity education tools to Web Security class in Spring 2016. We use CETAM to measure the effective of the teaching methods and evaluate selected tools by student learning outcome, student motivation and student experience. The experimental results show the impacts of two different teaching methods and selected Cybersecurity education tools.**

***Index terms*-teaching methods, education tool assessment**

I. INTRODUCTION

There are many learning-based teaching tools that have been used to aid students learning on the extremely important topic of cybersecurity. These tools include hands-on labs, visualizations and simulations [1-10]. Hands-on laboratories require students to work on real-world systems. Visualizations and simulations can help students learn security concepts by letting students "see" the dynamics of changes in data structures that exist inside computers and networks. Chen et al. developed a set of portable teaching modules for secure web development [3]. Some of these modules include Introduction to Cryptography, Secure Web Transactions, Web Application Threat Assessment, Web Server Security Testing, and Java Security. Each module includes an introduction of the fundamental concepts as well as lab exercises on these topics [3, 11]. Yu et al. developed a visualization tool for SYN flood attack [9] and a Cryptographic Education Tool [1]. The SEED project [7] developed a series of lab exercises for computer security education. Some of these lab exercises demonstrate common vulnerabilities and attacks such as buffer overflow vulnerability, format string attack, Cross Site Scripting attack, SQL injection attack, and Click Jacking attack. Some of these lab exercises provide students with opportunities to apply security principles in designing and implementing systems, such as implementing firewall, access control mechanism, encryption, and sandbox. Some of these lab exercises allow students to apply security principles in analyzing and evaluating systems, such as exploring Linux firewall, packet sniffing and spoofing, and access control in Linux. OWASP WebGoat [12] is a J2EE web application that was designed to be intentionally insecure in order to teach web application security lessons. Each lesson requires users to demonstrate their understanding of vulnerabilities by exploiting security issues that are presented in the application. The application also provides hints and code that gives explanations of each lesson in further detail.

Various Cybersecurity education tools also are available. The availability of these tools has given educators a chance to choose different tools to aid teaching security related topics and let students get hands-on experience. The educators may also find it is difficult to determine which of these tools are best suited for their students. Many of the creators of these educational tools have primarily focused on research and development and have not put enough emphasis on assessment. Also, most of the assessments of available tools are anecdotal reports without the scientific validity gained from using control groups and scientific data analysis. For example, many assessments use surveys to ask whether the tool helped students learn. However, there is difference between what students think they know and what they actually know. The Cyber security discipline needs objective assessment methods that more accurately measure the effectiveness of teaching tools. Cybersecurity educators need better information about the effectiveness of these tools to make appropriate and accurate decisions when deciding which tools to use in their classrooms.

Manuscript received March 1, 2016; revised April 5, 2016. This work was partially supported by National Science Foundation under the award number DUE-1129136 and by National Security Agency under the award number H98230-15-1-0282.

Huiming Yu is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (Phone: 3362853699, e-mail: cshmyu@ncat.edu).

Xiaohong Yuan is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: xhyuan@ncat.edu).

Jung Hee Kim is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: jungkim@ncat.edu).

Jinsheng Xu is with the Department of Computer Science, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: jxu@ncat.edu).

Taehee Kim is with the Department of Human Development and Services, North Carolina A&T State University, Greensboro, NC 27411 USA (e-mail: tkim@ncat.edu).

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Therefore, we developed two teaching methods to let students get different experience and to assess the effectiveness of current cybersecurity teaching tools using educational research methodologies and scientific data analysis.

The rest of the paper is organized as follows. In the next section Web Security course related information will be discussed. Teaching methods will be discussed in section III. In section IV selected Cybersecurity education tools will be introduced. In session V the effective cybersecurity education tool assessment method will be presented. Experimental results will be presented in session VI and conclusions will be presented in section VII.

II. WEB SECURITY COURSE INFORMATION

COMP 621 Web Security has been taught in the Department of Computer Science at North Carolina A&T State University for years. In this course we broadcast the concept and technology of Web security, guide students to apply learned technologies to real world Web applications to practice information assurance and computer security. This course is intended for senior and graduate students in the Department of Computer Science or Information Systems. The Web Security course mainly focuses on the technologies that can be used to provide security services for the WWW. It introduces a set of procedures, practices, and technologies for protecting Web servers, Web users, and their surrounding organizations. It also provides the relevant information to help students understand and use security technologies for the World Wide Web and an overview about the technologies that can be used to secure real world applications.

In this course we 1) introduce the concept of Internet, WWW, vulnerability, threats, countermeasures and generic security model, security policy and organizational security; 2) discuss the concept of Hyper Text Transportation Protocol (HTTP) and its security methods, authentication and authorization techniques, as well as access control; 3) study cryptographic hash function, public key cryptographic, secret key cryptographic, digital envelopes and protection of cryptographic keys; 4) discuss security protocols at a network access layer, Internet layer, transport layer and application layer; 5) discuss certificate management and public key infrastructures; 6) study the authentication and authorization infrastructure; 7) study Client/Server security that includes looking at security issues from the point of views of server and client; 8) discuss real world application examples and how to apply learned technologies to secure these applications; 9) discuss why the Internet privacy and intellectual property protection are important, learn the technologies of anonymous browsing, anonymous publishing, voluntary privacy stands, usage control, digital copyright labeling and the digital millennium copyright act.

III. TEACHING METHODS

We develop two teaching methods that are control group teaching and experimental group teaching to teach the selected topics that are Cryptography and Web application security in Web Security course, and use Cybersecurity educational tools to help students learn cryptography and Web application security topics, and get hands-on experience.

A. Topic 1: Cryptography

Cryptography, a core topic in Information Assurance and Cybersecurity, is a method of storing and transmitting data in a secure format to ensure data confidentiality, data integrity, authentication, and non-repudiation. Cryptography involves multiple fields such as mathematics, computer science, communication, and information processing. Encryption and decryption algorithms are the basic tools to allow a sender to encrypt a message/data with a key and a receiver to decrypt the encrypted message/data with the key. Using the new teaching methods, we divide students into two groups that are Control group and Experimental group, and use different methods to teach them.

Control group teaching method: The students are given lectures and a simple education tool named Secret Key and Public Key Cryptographic Tool (SKPKCT) that was developed by faculty of the Department of Computer Science at NC A&T [1]. The lectures introduce Cryptographic hash functions, Secret key cryptography and Public key cryptography. Block ciphers and Stream ciphers are introduced. Cryptographic hash functions MD5, DES of Secret key cryptography and RSA of Public key cryptography are introduced. The SKPKCT tool exhibits how hash function, RSA and SDES work, and guides students step by step on how to generate keys and use these generated keys to encrypt and decrypt data. This tool has been used in the COMP 621 course to help students understand the concepts of cryptography, the processes of key generation and encryption/decryption, and gain hands-on experience. The students in this group will read SKPKCT user manual and learn how to use this tool in a laboratory exercise. For each algorithm the students will be given required data and plaintext, and will generate the key, use the generated key to encrypt the plaintext message and decrypt the encrypted message, and finally check the decrypted message to make sure it is the same as the original message/data.

Experimental group teaching method: The students are given the same lectures as the Control group along with a visualization-based tool named Visualization Systems for Cryptography that was developed by Michigan Technological University [4]. The tool visualizes DES, AES, RSA, SHA, and two other ciphers. The instructor will guide students do similar work as using the SKPKCT. The students will read the user manual and learn how to use this tool in a laboratory exercise. They will use this tool to

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

encrypt plaintext, decrypt cipher text, and practice encryption and decryption methods.

B. Topic 2: Web Application Security

There are many techniques to secure Web applications. Secure Socket Layer/Transport Layer Security (SSL/TLS) protocol is one of these techniques. SSL/TLS is an intermediate layer between the transport and the application layers to provide the secure communication. The SSL/TLS protocol can be used to secure any TCP-based application protocols.

Control group teaching method: The instructor gives five hours of lectures to introduce Secure Socket Layer/Transport Layer Security protocol and certificate. First, the design consideration of SSL/TLS is discussed. Then the instructor introduces all subprotocals, and emphasizes the handshake protocol and data record protocol. How SSL/TLS supports authentication and authorization, and prevents various attacks such as Password Sniffing, IP Spoofing, etc. are discussed. Public key certificate, public key infrastructure and key management are introduced. Two relevant formats for public key certificates that are PGP (Pretty Good Privacy) certificates and X.509 certificates are discussed.

Experimental group teaching method: We develop an Implementing Https Training Tool to help students learn generating a digital certificate, signing and deploying a digital certificate, and implementing a secure communication (e.g. Https). The students are guided to create a public/private key pair, a SSL certificate under different operating systems, and a certificate signing request. Each student becomes a Certificate Authority. Students configure Apache and run https requests to test the result.

IV. SELECTED CYBERSECURITY EDUCTION TOOLS

We have studied many existing Cybersecurity education tools used by different universities. Based on our experience we select three Cybersecurity education tools. Two of them are used to aid teaching cryptography and one for Web application security.

A. Selected Cryptography Tools

Based on previous discussion we like to compare two teaching methods for cryptography topic. After teaching this topic we answer the following questions: Is one experiential-learning-based teaching tool (i.e., using a simple education tool) more effective than another experiential-learning-based teaching tool (i.e., visualization) in teaching cryptography concepts? Two encryption tools are selected. One is a simple education tool named Secret Key and Public Key Cryptographic Tool [1]. Another is Visualization Systems for Cryptography that is a visualization based tool [4].

A Secret Key and Public Key Cryptographic Tool

The Secret Key and Public Key Cryptographic Tool was developed by the Department of Computer Science at NC A&T SU [1]. The objective of this tool is to help students to effectively learn techniques of ciphers. It provides students an interactive tutorial and step by step demonstrations of ciphers, helps them better understand the concepts of cryptography, existing algorithms and the processes of key generation, encryption and decryption. The SKPKCT implements three categories ciphers that are Transmission of Password, Secrete Key Cryptography and Public Key Cryptography. First this tool demonstrates how these algorithms work, secondly it lets students get hands-on experience to encrypt and decrypt messages, and finally if the student cannot generate correct results it shows students step by step how to generate the correct result.

Visualization Systems for Cryptography

Tao el tl of Michigan Technological University have developed a set of visualization based tools for cryptography courses [4, 8]. It includes six different systems that are DES visualization system (DESvisual), AES visualization system (AESvisual), Finite field elliptic curve cipher visualization system (ECvisual), RSA visualization system (RSAVisual), SHA (Secure Hash Algorithm) (SHAvisual) and the Vigenère Cipher (VIGvisual). These systems allow students to visualize the steps of ciphers, conduct encryption and decryption, learn algorithms and perform some elementary attacks. These systems leverage visualization technology in order to meet the challenges for various encryption algorithms.

B. Selected Web Application Security Tool

We conduct a comparative study of these two teaching methods with the goal of answering the research question: Is using an experiential-learning-based teaching tool (i.e., a training tool) more effective in improving student learning than the traditional teaching method without using the teaching tool in teaching web application security concepts? One education tool named Implementing HTTPS Training Tool is selected.

Implementing Https Training Tool

We designed and implemented an Implementing HTTPS Training tool. The objective of this tool is to help students effectively learn what is HTTPS and how to implement HTTPS in a client-server network. This tool consists of four parts that are Creating a certificate, Distributing the certificate, Setup HTTPS and Testing HTTPS implementation. It provides an interactive tutorial to students and step by step demonstrations of generating a private key, creating a certificate signing request, creating a self-signed certificate, distributing the created certificate, setup HTTPS and testing HTTPS implementation. It helps students better understand the concepts of web security, HTTPS, SSL/TLS, secrete key and public key cryptographies algorithms and the processes of key

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

generation, creating a certificate and HTTPS implementation.

V. THE EFFECTIVE CYBERSECURITY EDUCTION TOOL ASSESSMENT METHOD

We develop an effective Cybersecurity Education Tool Assessment Method to assess the effectiveness of experiential-learning-based teaching tools for Web Security course and analyze the impacts of Cybersecurity education tools for student learning. Two teaching methods are developed and the Cybersecurity education tools are selected. We assess the effectiveness of the teaching methods via three measures that are improvement in student learning outcomes, improvement in student motivation in learning the topic, and improvement in the student experience such as student enjoyment, satisfaction, and perceived difficulty in learning the topics. The effective assessment method contains six main parts that are hypothesis, variables, procedure, data collection, data analysis, and validity and reliability of survey instruments.

A. Hypothesis

Based on the questions and measures of effectiveness of the teaching methods, we test the sets of hypotheses for each selected topic. The focuses are learning outcome, motivation and experience. For learning outcome, the hypotheses are: there is a statistically significant improvement in student learning outcomes using an experimental teaching method compared with the control group teaching method, or not. For motivation, the hypotheses are: there is a statistically significant improvement in student motivation in learning the topic using an experimental teaching method compared with the control group teaching method, or not. For experience, the hypotheses are there is a statistically significant improvement in student experience using an experimental teaching method compared with the control group teaching method, or not.

B. Variables

Stemming from the research questions and hypotheses, we identified one independent variable, and three dependent variables as shown below:

1) Independent variable: *Teaching method*
2) Dependent variables: *Student learning outcome; student motivation; student experience*

C. Procedure

The procedure for an assessment study is described below:

1) Participants in Web Security course are divided into two groups: control group and experimental group. The two groups should have an equal number of students (or close to an equal number of students), and have similar average GPAs.
2) Before an assessment is conducted, both groups of students are given an identical assessment test (pre-test) to test their knowledge of Cryptography and Web Application Security.
3) The two groups will be given two different teaching methods.
4) The two groups of students are given an identical assessment test (post-test) to test their knowledge of cryptography and Web application security topics.
5) The students in both groups will be given an identical survey on their motivation in learning the topic and their experience with the teaching method.

D. Data collection

Data to measure the variables are collected as follows:

Teaching method. We collect the type of teaching methods (such as lecture, visualization education tools) and a detailed description of each teaching method.

Student learning outcomes. We collect student pre-test and post-test scores. The improvement from pre-test to post-test is used as a metric to measure student learning outcome

Student motivation. We conduct survey to measure student motivation. We adopt and adapt previous validated survey instrument to measure student motivation.

Student experience. Data on student experience are collected through conducting survey and focus group interviews. Through survey and focus group interviews we ask the students questions on their enjoyment, satisfaction, and perceived level of difficulty in learning the topic.

E. Data analysis

Statistical tests will be conducted to compare the values of the dependent variables collected from experimental group with the values of these variables collected from the Control group. Multivariate ANOVA and associated t-tests are used for the comparisons in our analysis.

Open ended survey question answers, focus group interview answers, as well as instructor reflection reports are analyzed using qualitative methods to find re-occurring themes, and issues that hinder the effective implementation of the experiential-learning-based teaching methods as well as strategies to overcome these difficulties.

F. Validity and reliability of survey instruments

We develop a survey by adapting the SIMS to measure student motivation. We also develop a survey to measure student experience such as why are you engaged in this activity, and open-end questions, as well as student interview.

VI. EXPERIMENTAL RESULTS

Two different teaching methods that are control group teaching without using Cybersecurity education tools/or using simple tools and experimental group using visualization based Cybersecurity education tools are used to teach Web Security course in the Department of Computer Science at North Carolina A&T State University in Spring 2016. Twenty-three students in this class are

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

equally divided into Control group and Experimental group. The experimental results focus on student learning outcome, student motivation and student experience.

The results of student learning outcome base on students' pretest and posttest results. For each topic students take a pretest to evaluate their knowledge in the area before the instructor gives lectures and students use selected education tools. Then the instructor gives related lectures. For encryption topic students in Control group learn how to use the simple tool that is Secret Key and Public Key Cryptographic Tool [1] and students in Experimental group learn how to use the Visualization Systems for Cryptography tool [4]. For Web Application Security topic students in Control group do not use any education tools and students in Experimental group learn how to use the Implementing HTTPS Training Tool. Finally, all participated students take the posttests.

For cryptography topic nineteen students took the pretest and posttest. Only seventeen of them took both pretest and posttest. The test questions include concepts of hash function, and secrete key cryptography as well as public key cryptography, using a given algorithm to generate a key(s), using a given key to encrypt message and developing a simple hash algorithm. Using SPSS, independent samples and paired t-tests were conducted to examine differences between the control group teaching method and the experimental group teaching method in student learning outcome. We performed paired T-test with 5% significance level. From the Control group pre and post test results, P(T<=t) one-tail=0.0003 < 0.05, therefore we reject the Null hypothesis. From the Experimental group pre and post test results, P(T<=t) one-tail=0.0004 < 0.05, therefore we reject the Null hypothesis. The results show there are significant improvement from pre to post test scores for both of Control and Experimental groups. We performed T-test with unequal variances with 5% significance level on the score difference between pre and post test scores (i.e., posttest score – pretest score) of the Control group and Experimental group. The result is that P(T<=t) two-tail=0.3466 > 0.05, therefore the Null hypothesis cannot be rejected, there is no significant difference between Control and Experimental groups in term of improvement from pretest to posttest scores.

For Web application security topic eighteen students took the pretest and posttest. Only sixteen of them took both pretest and posttest. The test questions include knowledge of creating and using certificates, knowledge of SSL and implementing HTTPS. Using SPSS, independent samples and paired t-tests were conducted to examine differences between the control group teaching method and the experimental group teaching method in student learning outcome. We performed paired T-test with 5% significance level. From the Control group pre and post test results, P(T<=t) one-tail=0.0000135 < 0.05, therefore we reject the Null hypothesis. From the Experimental group pre and post test results, P(T<=t) one-tail=0.0000626 < 0.05, therefore we reject the Null hypothesis. The results show there are significant improvement from pre to post test scores for both of Control and Experimental groups. We performed T-test with unequal variances with 5% significance level on the score difference between pre and post test scores (i.e., posttest score – pretest score) of the Control group and Experimental group. The result is that P(T<=t) two-tail=0.89 > 0.05, therefore the Null hypothesis cannot be rejected, there is no significant difference between Control and Experimental groups in term of improvement from pretest to posttest scores.

Overall, whether students were in either Control or Experimental group, students showed significant learning gains. However, there was not significant difference between two different teaching method conditions on students' learning gains.

The results of students' motivation bases on the online survey. The survey includes sixteen questions on different types of motivation such as intrinsic motivation, identified, external and extrinsic motivation. 5-point likert scale is used. Regarding students' motivation, overall, there were not statistically significant differences between students in the control group teaching method (M=3.53, SD= 1.28) and in the experimental group teaching method (M=3.00, SD= 0.79) on Intrinsic motivation, t (9)= .75, p = .46, between the control group teaching method (M=3.82, SD= 1.02) and the experimental group teaching method (M=3.50, SD= 1.24) on identified motivation, t (9)= .47, p = .65, and between the control group teaching method (M=2.75, SD= .66) and the experimental group teaching method (M=3.00, SD= 1.41) on external motivation, t (9)=-.407, p = .69, and between the control group teaching Method (M=1.25, SD= .66) and the experimental group teaching method (M=2.13, SD= 0.63) on motivation. t (9)= -2.15, p =.06. Even though there were not statistically significant differences between two teaching methods, overall, students in the control group teaching method showed higher average scores in their intrinsic and identified motivation while they showed lower average scores in their external motivation and motivation.

Regarding student enjoyment, satisfaction, and perceived difficulty in learning the topic, overall, there were not statistically significant differences between the control group teaching method (M=3.64, SD= 1.32) and the experimental group teaching method (M=3.13, SD= 0.66) on students' satisfaction, t (9)= .722, p =.49, and between the control group teaching method (M=3.95, SD= 1.16) and the experimental group teaching method (M=3.17, SD= 1.03) on students' enjoyment, t (9)= 1.11, p = .29, and between the control group teaching method (M=1.40, SD= .74), and the experimental group teaching method (M=2.35, SD= 0.70) on students' perceived difficulty, t (9)= -2.09, p = .06. However, it is still noticeable that in line with the results of students' motivation, students in the control group teaching method showed higher average scores in their satisfaction and enjoyment in learning the topic than students in the experimental group teaching method even though there were not statistically significant

ISBN: 978-988-19253-0-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

differences between students in two teaching methods on students' overall experience. In addition, students in Control group show lower perceived difficulty in learning the topic than those in Experimental group.

VII. CONCLUSIONS

Two teaching methods that are control teaching and experiment teaching are discussed. An effective Cybersecurity educational tool assessment method that includes hypothesis, variables, procedure, data collection, data analysis, and validity and reliability of survey instruments is developed. We used two different teaching methods and selected Cybersecurity education tools to teach COMP 621 Web Security course in Spring 2016.

Students in Control group use a simple educational tool for encryption topic and without using any tool for Web application security topic. Students in Experimental group use a visualization based tool for encryption topic and using an interactive and visualization based tool for Web application security topic. Nineteen participated students took the pretest and the posttest for encryption topic. Eighteen participated students took the pretest and the posttest for Web application security topic. The T-test results show there are significant improvement from pre to post test scores for both of Control and Experimental groups, and there is no significant difference between Control and Experimental groups in term of improvement from pre-test to post test scores.

The results of students online surveys show no significant differences between the control group teaching method and experimental group teaching method regarding students' enjoyment, satisfaction and perceived difficulty in learning the topics.

ACKNOWLEDGMENT

This work was partially supported by National Science Foundation under the award number DUE-1129136 and by National Security Agency under the award number H98230-15-1-0282.

REFERENCES

[1] A. Abuzaid, H. Yu, X. Yuan and B. Chu, "The design and implementation of a cryptographic education tool", In Proceedings of the International Conference on Computer Supported Education, May 2011.

[2] Aleph One, "Smashing the stack for fun and profit", Phrack 49, Volume 7, Issue 49. Available: http://insecure.org/stf/smashstack.html

[3] L. Chen, L. Tao, X. Li, and C. Lin, "A Tool for Teaching Web Application Security", In Proceedings of the 14th Colloquium for Information Systems Security Education (CISSE 2010), Baltimore, MD. 17-24.

[4] Cryptography Visualization Software Downloads, Retrieved on March 23, 2015 from http://www.cs.mtu.edu/~shene/NSF-4/

[5] Z. Ni, H. Yu, X. Yuan and Z. Zhan, "Using a detection and prevention prototype to enhance cloud security", In Proceedings of International Conference on Computer Science and Technology, July 2014.

[6] "SDL Threat Modeling Tool", Available: http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx

[7] Syracuse University. 2015. SEED: Developing Instructional Laboratories for Computer Security Education. Available: http://www.cis.syr.edu/~wedu/seed/

[8] Tao, J., Keranen, M. and Mayo, J. 2014. RSAvisual: A Visualization Tool for the RSA Cipher. In Proceeding of SIGCSE.

[9] T. Terry, H. Yu, K. Williams, X. Yuan and B. Chu, "A visualization based simulator for SYN flood attacks", Poster, International Conference on Information Visualization Theory and Applications, March 2011.

[10] Yuan, X., Hernandez, J., Waddell, I. Chu, B. and Yu, H. 2012. Hands-on Laboratory Exercises for Teaching Software Security. In Proceedings of the 16th Colloquium for Information Security Education (CISSE 2012).

[11] Pace University, "Secure Web development teaching modules", Available: http://csis.pace.edu/~lchen/sweet/

[12] OWASP WebGoat Project. 2015. Available: https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project