Measuring the Effectiveness of Instruction Based on Material From a Hands-On Workshop in Information Assurance

Frank H. Katz
Armstrong Atlantic State University
Department of Computer Science and Information Technology
Savannah, GA 31419
912-344-3192
frank.katz@armstrong.edu

ABSTRACT
In computer science curricula, we teach our students to program on their own, while in the “real world,” programming is accomplished via cobbling together modules and subroutines stored in repositories that were written by others. Similarly, teaching Cyber Security or any other curricula does not occur in a vacuum. Instructors may want to be imaginative and create their own case studies and laboratory exercises, but time, and especially in the current era, financial constraints, affect all faculty members. The result is the reuse of labs and exercises obtained from colleagues and other sources. Consequently, it is important to measure the efficacy of using the material of others. This paper will evaluate before-and-after learning outcomes from two consecutive years of surveys of Armstrong Atlantic State University’s (hereafter referred to as Armstrong) ITEC 5001 Cyber Security I course to determine the effectiveness of the use of material obtained at the NSF-sponsored Summer Workshop in Information Assurance (hereafter referred to as the workshop) held at the University of Tennessee-Chattanooga, in May 2012.

Categories and Subject Descriptors
K.3.2 [Computers and Education]: Computer and Information Science Education – curriculum, information systems education.

General Terms

Keywords
Information security, Cyber security, Curriculum, Pedagogy.

1. INTRODUCTION
The creation of the minor in Cyber Security and graduate certificate in Cyber Security (now a graduate certificate in Cybercrime) at Armstrong was previously documented in papers presented at the Information Security Curriculum Development Conference in 2010 [1] and 2012.[2] Since the inception of Armstrong’s Information Security curriculum in 2006, laboratory exercises in Information and Cyber Security have been predominantly created from material provided in the course textbooks. The workshop provided me with new, challenging material to use in ITEC 5001, especially in the areas of encryption and access control. This prompted the use of a student survey of learning outcomes related to Cyber Security. Conducted at the beginning and end of the Fall 2011 and Fall 2012 semesters, the surveys provided a valid before-and-after measure of the effectiveness of the use of the material obtained from the workshop earlier in 2012.

2. COMPETITION TO ATTEND THE WORKSHOP
Notice of the competition for attending the workshop was received in November 2011. Since travel expenses were covered by a $2,000 National Science Foundation grant, selection to attend the workshop was a competitive process. Among the requirements was a statement by the applicant of how the workshop’s curriculum would be used in current and future courses, and a letter of endorsement by the applicant’s department head.

The purpose of the workshop was stated in the e-mail that contained the call for applicants: “This workshop is intended to promote hands-on labs and case-studies in Information Assurance (IA) education to enhance student learning experiences, and to foster collaboration among faculty in the Information Assurance (IA) field.” Targeted participants were: “(a) full-time faculty at a U.S. university who are currently teaching Information Assurance (IA) related courses or have strong interests to teach IA courses and (b) have a strong interest to incorporate case-studies and hands-on labs in their courses.” [4]

3. ARMSTRONG’S CYBER SECURITY CURRICULUM BEFORE THE WORKSHOP
Since its inception, laboratory exercises and hands-on projects have been an integral part of the Cyber Security curriculum at Armstrong. The early years of ITEC 5001 contained some lab exercises using port scanning software such as NetBrute, N-Map, enumeration software such as LanGuard and rudimentary web
reconnaissance using Sam Spade. However, missing from these exercises was hands-on lab work in cryptography. During two semesters, students did engage in a semester-long group project to perform a campus-wide scan of student laptops for malware and the installation of security software. [3]

Starting with the Fall 2008 semester, case studies have also been a fixture in ITEC 5001. Taken from Wright and Kakalik’s Information Security, Contemporary Cases, published in 2007 [8], they have been an asset in helping to define the different issues in Cyber Security in real-world terms.

Nonetheless, it is necessary to ensure that a curriculum does not get “stale.” Lab exercises either get outdated, or the software required to perform them changes, along with changes in operating systems. Case studies get old, outdated, and become irrelevant. Consequently, it was felt that the inclusion of new hands-on lab exercises and case studies obtained from the workshop would provide an infusion of interest in the ITEC 5001 curriculum.

4. THE WORKSHOP AND ITS CONTENTS

The workshop lasted four and one half days, from Monday, May 21, to Friday, May 25, 2012, and covered a wide variety of topics, including: cryptography, access control, cloud security, security management, wireless security, web hacking, secure web development, and forensics. Each day was devoted to a different topic or topics, presented by different faculty who had developed and used the material at their universities. All of the hands-on exercises were conducted on either personal laptops or desktop computers provided by UT-Chattanooga. Each exercise was performed in a virtual environment, using VMWare and VMPlayer, which had to be installed on personal laptops prior to attending the workshop. Of particular interest were the sessions on cryptography, the use of visualization tools as teaching aids, and the security management case studies, which covered a wide range of topics. A brief description follows describing the material that I felt would be most beneficial to students in Armstrong’s Cyber Security courses.

Much of the first day was dedicated to encryption and cryptography labs. [9] These labs included the Fair Play Cipher, Frequency Analysis, binary Exclusive-OR, Triple DES, RSA encryption, and hash generation. These labs were performed using Cryptool 1 and Cryptool 2, which had not been previously used in the Cyber Security courses at Armstrong.

On Wednesday, Dr. Kenneth Williams, and Dr. Xiaohong Yuan, both of North Carolina A&T University, presented a series of case studies in security management, wireless security labs, security visualization tools, buffer overflow labs, and firewall simulation games. [6] The case studies, presented online, with discussion questions mapped to Bloom’s taxonomy and references, appeared to be excellent supplements to existing material. They included web security and access control, application security, buffer overflow, cross-site scripting (XSS), and SQL injection. They also presented various Flash-based animated simulations, covering material such as packet sniffing, Kerberos authentication, wireless network attacks, and a SYNflood attack. Each simulation contained a series of challenge questions to actively engage the participant in order to ensure that he or she understood the material. [7]

5. APPLICATION OF WORKSHOP MATERIAL IN THE CLASSROOM

Prior to attending the workshop, there had not been any hands-on exercises in cryptography or steganography in ITEC 5001. Cryptographic exercises had been limited to pencil-and-paper assignments designed to test the students’ knowledge of the Vernam cipher, XOR functions, the Vigenère Square, and, given two key, the use of the RSA algorithm to encrypt a message. A discussion of steganography and steganalysis had been limited to just that, a discussion of material in the textbook. Instruction on packet sniffing, SYNflood attacks, and the use of Kerberos authentication had been textbook-based, without any practical applications or demonstrations in class. At the end of the workshop, while valid, had been limited to those in the Wright and Kakalik book; new cases had not been implemented in ITEC 5001 since the adoption of their book in 2008.

During the Fall 2012 semester, it was time to put into practice the material and instructional techniques that I had acquired at the workshop. Access Control had been traditionally discussed as a component on instruction of firewall concepts in order to limit access to a system. [5] Several different access control methods had been discussed, but in the curriculum, there had never been a case study regarding access control. To enhance their learning about access control, the students were required to read the case “Using Smart Cards with PKI to Implement Data Access Control for Healthcare Information Systems” [6], and answer the ten case discussion questions provided online.

Benjamin Franklin said: “Tell me and I forget, teach me and I may remember, involve me and I learn.” [10] In keeping with this principle, a change was also made to the teaching of cryptography. The students were given a hands-on lab using Cryptool 1 to perform cryptanalysis by various methods: Playfair, Vigenère, Triple DES, Rijndael (AES) and RSA encryption ciphers. Instead of learning by hand-cranking and calculating the results, they were able to learn by doing – applying each of those ciphers against the same message in order to understand how each cipher encrypted the message differently.

6. COMPARISON OF LEARNING OUTCOMES FROM 2011 TO 2012

In 2007, Armstrong’s Department of Information Technology underwent a process intended to produce a series of course assessments and learning outcomes for the future university-wide SACS Accreditation effort. As previously discussed, [2] these learning outcomes had been used in 2011 to measure the differences between Armstrong’s face-to-face “U” version of the ITEC 5001 course, taken primarily by undergraduate students majoring in Information Technology, and the online graduate “G” version of the course, taken primarily by students taking the Criminal Justice Cyber Security (now Cybercrime) certificate. At the start of the Fall 2012 semester, a new use of the learning outcomes became evident -- the comparison of the effectiveness of instruction in Fall 2011, prior to attending the workshop, versus the instruction in Fall 2012, after attending the workshop. In particular, there were two questions among the set that applied specifically to the teaching of cryptography, and one that applied
to access control. While all twenty-one questions in the survey were administered, only three questions were of interest to this analysis.

The two survey questions related to cryptography were:

16. I understand the basic principles of cryptography and can perform several very basic cryptographic schemes such as substitution and transposition ciphers.

17. I can describe the difference between symmetric and asymmetric encryption.

While these two questions do not specifically refer to some of the cryptographic methods employed in the labs acquired from the workshop, it would be expected that the performing those exercises would improve a student’s overall knowledge of cryptography.

The survey question related to access was:

19. I can describe the various different types of access control.

Responses to each question were given in terms of Strongly Agree, Agree, Neutral, Disagree, and Strongly Disagree, with the responses weighted 5, 4, 3, 2, and 1, respectively. A weighted score was calculated pre- and post- for both Fall 2011 and Fall 2012. In order to better assess these three specific questions for the two consecutive years, the responses for ITEC 5001U and 5001G were combined for each year. The results (graphically shown in Appendix A) were striking:

In 2011, prior to including material from the workshop in the course’s curriculum, the responses for Question 16, pre- (beginning of the semester) versus post- (end of the semester) showed a percent improvement of 11.11% (a weighted average improvement of 10.8 to 12.0). In 2012, after the inclusion of the material from the workshop, the responses for the same question showed a pre- versus post- improvement of 48.81% (an weighted average improvement of 16.8 to 25.0). For Question 17, the 2011 pre- versus post- improvement was 14.29%. In 2012, the improvement was 29.38%. And for Question 19, on access controls, the improvement in 2011 jumped from 7.69% in 2011 to 77.14% in 2012.

7. RECOMMENDATIONS AND CONCLUSIONS

7.1 Recommendations

Surveys of learning outcomes can be an important tool to measure the effectiveness of instruction in Information Assurance. This paper has not only made a comparison between before-and-after outcomes, but compared the effectiveness in consecutive years, of two different types of instruction in cryptographic methods. However, it is important to ensure that the questions in the survey truly provide a valuable comparison between two different methods of instruction. The learning outcomes referenced in this paper did indicate an improvement in understanding of general cryptographic concepts, but not in specific cryptographic methods.

For future work, perhaps even in this semester, a set of survey statements could be created and administered that compare the instructional value of paper-and-pencil cryptographic exercises versus the use of hands-on experimental and visualization tools. For example, after completing a paper-and-pencil exercise using the Vigenère cipher and using a visualization tool such as Crypt Tool to perform the same cipher, the students would be asked to respond to statements designed to measure their comprehension of each method. One such learning outcome statement might be: “Performing the Vigenère cipher via the paper-and-pencil exercise improved my understanding of this cryptographic method.” Then students would respond to a similar question, only regarding the use of Crypt Tool: “Performing the Vigenère cipher via Crypt Tool improved my understanding of this cryptographic method.” Students would answer using the Strongly Agree, Agree, etc., responses, and the responses would be weighted, calculated, and compared as described previously in this paper. In this way, a more effective comparison may be made between methods of instruction used prior to the inclusion of material from the NSF workshop and those based on materials obtained from the workshop.

7.2 Conclusions

The impressive improvement in learning outcome data may not be totally attributed to the inclusion of the material from the NSF-sponsored Workshop in Information Assurance, but the effect of having students learn by doing cannot be totally discounted. Instead of calculating cryptographic results by hand, students actually saw the various ciphers in action, leading to what can only be described as a greater understanding of the concepts. Instead of just going over course material on access control from the textbook, students were required to read and respond to a real-world case study that had not been previously used in the course.

Just a small amount of material obtained in the workshop was actually used in the Fall 2012 course. The extraordinary improvement in understanding means three things: more of the material from the workshop will be used in upcoming semesters; the method of comparing instructional techniques described above in the recommendations should be implemented; and the adage from Ben Franklin suggesting that students learn by doing is still true today.

8. REFERENCES


APPENDIX – TABLE DATA (CONDENSED)

Below is a table depicting the combined results of the survey, by year, for the undergraduate and graduate sections of ITEC 5001, Cyber Security I, from 2011 and 2012. The tables are condensed in that they do not contain the raw number of responses per question. They contain the specific survey questions as discussed above.

ITEC 5001U and ITEC 5001G Combined, 2001 vs. 2012, Specific Survey Questions, Pre- and Post- Weighted Averages, and Percent Increase (Decrease)

<table>
<thead>
<tr>
<th>Q#</th>
<th>Description</th>
<th>2011 Pre Weighted Score</th>
<th>2011 Post Weighted Score</th>
<th>2011 Pct incr (decr)</th>
<th>2012 Pre Weighted Score</th>
<th>2012 Post Weighted Score</th>
<th>2012 Pct incr (decr)</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>I understand the basic principles of cryptography and can perform several some very basic cryptographic schemes such as substitution and transposition ciphers.</td>
<td>10.8</td>
<td>12.0</td>
<td>11.11%</td>
<td>16.8</td>
<td>25.0</td>
<td>48.81%</td>
</tr>
<tr>
<td>17</td>
<td>I can describe the difference between symmetric and asymmetric encryption</td>
<td>9.8</td>
<td>11.2</td>
<td>14.29%</td>
<td>16.2</td>
<td>24.2</td>
<td>49.38%</td>
</tr>
<tr>
<td>19</td>
<td>I can describe the various different types of access control.</td>
<td>10.4</td>
<td>11.2</td>
<td>7.69%</td>
<td>14.0</td>
<td>24.8</td>
<td>77.14%</td>
</tr>
</tbody>
</table>