Seattle
Making Value for Society
122nd ASEE Annual
Conference & Exposition
June 14 - 17, 2015
Seattle, WA

Paper ID #13338

# Developing and Piloting a Quantitative Assessment Tool for Cybersecurity Courses

**Dr. Richard Scott Bell, Northwest Missouri State University**

Scott Bell received his Ph.D. in Computer Science from Kansas State University in 2014 and his master's degrees in Computer Science in 2000 from the Missouri University of Science and Technology. His B.S., in Geological Engineering, with a minor in Communications, is also from the Missouri University of Science and Technology (1994).

**Dr. Eugene Vasserman, Kansas State University**

Eugene Vasserman received his Ph.D. and master's degrees in Computer Science in 2010 and 2008, respectively, from the University of Minnesota. His B.S., in Biochemistry and Neuroscience with a Computer Science minor, is also from the University of Minnesota (2003). His research interests include secure distributed systems, low-power computing and ad-hoc networking, and security usability. In 2013 he received the NSF CAREER award for work on secure next-generation medical systems.

**Dr. Eleanor C Sayre, Kansas State University**

Eleanor Sayre is a researcher in physics education, specializing in the intersection of undergraduate students' epistemologies, identity development, and community participation. Her PhD in physics is from the University of Maine, and she is currently an Assistant Professor in the Physics Department at Kansas State University.

# Developing and Piloting a Quantitative Assessment Tool for Cybersecurity Courses

**Scott Bell[1], Eleanor Sayre[2], and Eugene Vasserman[2]**
[1]**Northwest Missouri State University**
[2]**Kansas State University**

## Abstract

The rapid growth of the Internet over the past two decades has led to a proliferation of network-capable computing devices. This growth has occurred so rapidly that the academic pipeline is struggling to keep up with the demand for cybersecurity professionals capable of protecting the expanding infrastructure. Training a security-focused workforce has become a critical objective of government entities, businesses, and academic institutions.

As educators respond to this growing demand, developing new curriculum and methodologies for training cybersecurity professionals, there has been little systematic effort to assess student outcomes from the variety of pedagogical approaches being used. This paper presents the second stage in our work to develop an assessment tool designed to measure student interest and self-efficacy in relation to cybersecurity.

Such a tool will allow educators to detect changes in student outcomes and thus systematically improve pedagogical methods. Initial instrument development is based on a qualitative study of students enrolled in an introductory cybersecurity course. We piloted the survey during the Spring and Fall 2014 semesters, and present the results here along with discussions of our ongoing and future activities with this project.

## Introduction

Examining the current status of cybersecurity education, it is evident that few, if any, definitive "best practices" have been identified.[15] The problem of identifying those pedagogical methods which produce the best outcomes is compounded by the variety of stakeholders attempting to address this issue.[13] Government and industry are working internally to develop their own standards and methods for training employees on systems that are continuing to change even as the training occurs.[12,20] Meanwhile colleges and universities are adding to or updating courses each year to help students gain an understanding of the new challenges they will face upon graduation. The focus of our work is primarily on university courses although the assessment tool being discussed here could be utilized in other educational settings as well.

The depth and diversity of the content being taught in cybersecurity courses varies greatly among universities. These courses may look at the same topics in any of several different ways. For example, one course may investigate cryptography and the mathematical principles used to protect data while another might focus on the system-level implementation of those algorithms.[6]

Although these two courses cover the same concepts, the student perspectives and expected outcomes are drastically different. Course objectives can vary as well. For example, a given course might approach teaching cybersecurity as a set of practical, vocational skills, as good engineering practices, or as academic theories.

The methods used to teach these courses are just as varied as the content. Some courses focus on laboratory-based, experiential learning.[9,18] Others are lecture-based and involve the review and discussion of literature, and still others are challenge based courses where instructors and students work together to solve problems.[11] Numerous institutions participate in organized attack and defend scenarios, giving students hands-on experience.

In order to systematically improve the quality of cybersecurity education, we focus on developing a way to measure the outcomes from such a variety of courses in a manner that will help educators continuously improve their pedagogical approaches. This instrument must be able to assess student outcomes independent of the depth of coverage or method of instruction. Therefore, we do not focus directly on the level of knowledge students possess about individual topics. Instead, we set out to create an instrument which can be used to detect changes in student interest and self-efficacy as they relate to cybersecurity.

Measuring change in student interest gives us an indication of how well a given course is motivating students to pursue further knowledge or work in this sub-field.[22] Building long-term student interest is vital within a new, fast-changing, field such as cybersecurity. Self-efficacy is defined as "...a person's belief in his or her capability to perform a task,"[8] Measuring student self-efficacy is important because it has been linked with outcomes such as persistence on task, academic success and long-term career success.[4,19] Studies have shown that students with higher self-efficacy in fields such as mathematics are more willing to discard faulty strategies and rework more problems than than students of equal ability but lower self-efficacy.[3]

Our instrument is designed to measure student interest and self-efficacy in relation to a variety of general cybersecurity topics ranging from "Install and run malware checking software on a home computer" to "Manage security for a Fortune 500 company." This paper presents the development of, and initial results from, a pilot study using a prototype survey measuring student interest and self-efficacy in relation to cybersecurity. It builds upon the findings from a qualitative investigation presented in our previous work.[5]

## Curriculum Standards

There is progress being made to improve the overall quality and consistency of cybersecurity education. In 2008, the ACM Special Interest Group for Information Technology Education (ACM-SIGITE) approved and published a model IT curriculum. Overarching all other pillars within this framework was information assurance and security (along with professionalism).[1] Similarly, the ACM and the IEEE recognized information assurance and security as a separate knowledge area within their recommended 2013 Computer Science Curricula.[24] As with the IT curriculum, the CS curriculum incorporates components of cybersecurity throughout the various other computer science knowledge areas.

These two documents provide educators with guidance as to what topic areas should be incorporated into classroom activities. However, neither set of guidelines includes pedagogical best practices or tools for assessing pedagogical methods. Currently there are a wide variety of pedagogical methods, content and training environments being used, with little progress being made to identify those practices that provide the best student outcomes.[9,11,18,23] By developing an assessment tool capable of measuring student interest and self-efficacy while meeting the goals set forth by these standards, we can help educators identify the pedagogical approaches that will best help us meet the growing demand for graduates who are willing and able to tackle the growing security problems in the computing industry.

## Background

Given the lack of formal assessment methods available for cybersecurity education, we looked at those available in other areas of computer science. There have been numerous research projects investigating ways to measure and improve student outcomes within introductory computer programming courses.[10,16,21,25] This type of course has existed since the earliest days of modern computing,[2] and while details such as the language used may change over time, the core concepts and expected outcomes have become relatively stable from year to year and even from university to university. This allows these instruments to focus on student exposure to, and comprehension of, specific topics.

Given the variety of pedagogical approaches, the diverse content, and the typically lower enrollment in cybersecurity courses, we determined that we would not be able to simply adapt the approaches used to develop these survey instruments into a new survey for cybersecurity. Instead, we would need to first identify how students relate to a course in cybersecurity. Therefore, we chose to first perform a qualitative study of students enrolled in an introductory cybersecurity course and then use those results to inform our development of the quantitative tool.[14]

## Initial Qualitative Study

Over the course of a semester, we performed 3 rounds of semi-structured interviews with students enrolled in an introductory cybersecurity course designed for upper division undergraduate and first year graduate students.[7,27] Our goal was to discover those topics and experiences that the students found most influential and interesting, and to identify ways we might be able to measure outcomes from those experiences. Fifteen students volunteered to participate in the first round of interviews, with 14 continuing on to the second round and 12 to the final round. Our primary objective was to study how student interest and self-efficacy in relation to cybersecurity changed over the course of the semester, and identify what experiences may have led to those changes. Specifically, we wanted to investigate student interests in cybersecurity as they pertain to future plans such as careers, research, and classwork. We also wanted to determine how to answer the question: *"Are students gaining confidence in their ability to handle cybersecurity issues?"*

Based on interview responses, it was apparent that there was student interest to further pursue cybersecurity in various ways (additional courses, performing research, and seeking jobs). Most of the students we interviewed considered cybersecurity to be a component of their overall education and career plans, but not the main focus. By the end of the semester, all students were glad they had taken the course. While there were a few students who had one or two topics they did not like, interest rates ranged from somewhat interesting to very exciting. When asked, most indicated they would be willing to take additional cybersecurity courses if those courses fit into their schedule and academic requirements. This interest was expected given that the students were enrolled in an upper-division elective course.

Over the course of the three interviews, students' responses showed low self-efficacy levels when asked about performing various cybersecurity related tasks, with comments such as "I'm not sure I could do that" being common. Meanwhile interest levels seemed to grow, reflected in comments such as "That was really cool!". For some students, self-efficacy levels decreased over the course of the semester. Given that students admitted to having very little knowledge of cybersecurity at the beginning of the semester, this was not totally unexpected as students became aware of the volume and complexity of cybersecurity problems facing today's workforce. This is what we would like for our survey to help educators identify in their classrooms. A more detailed description and further analysis of this portion of our study can be found in our previous work.[5] The information gained from this investigation was used to develop the statements used in our current assessment tool.

Table 1: Statements included in survey

| | |
|---|---|
| 1 | Pursue an advanced degree(s) focused on cybersecurity |
| 2 | Find ways to exploit vulnerabilities in existing software |
| 3 | Perform research focused on cybersecurity |
| 4 | Learn how to crack users' passwords |
| 5 | Take additional courses focused on cybersecurity |
| 6 | Discover ways to protect personal data on the Internet |
| 7 | Write software that is safe from buffer overflow attacks |
| 8 | Manage security for a Fortune 500 company |
| 9 | Implement a protocol to allow data to be sent securely over a network |
| 10 | Perform network penetration tests for companies |
| 11 | Learn how to use SSL certificates |
| 12 | Find a job which involves cybersecurity |
| 13 | Learn how to intercept and read network traffic |
| 14 | Write an algorithm that uses asymmetric encryption to authenticate a user |
| 15 | Work for an organization that researches ways to make computing more secure |
| 16 | Learn how to verify a digital signature |
| 17 | Have cybersecurity concepts incorporated into other courses that I take |
| 18 | Remove detected threats from a home computer |
| 19 | Read articles/web posts about cybersecurity on your own |
| 20 | Install and run malware checking software on a home computer |
| 21 | Learn how to detect cyber attacks |
| 22 | Find a job which is specifically oriented towards cybersecurity |

## Survey Development

To measure these two attributes (interest and self-efficacy), we first developed 22 survey statements, derived primarily from the interviews performed in the qualitative study. Additional statements were chosen to provide data concerning specific areas of interest such as *"Take additional courses focused on cybersecurity."* The goal in selecting the topics was to cover a variety of ways in which students might further engage with cybersecurity material in both academic and work environments. The statements are shown in Table 1.

We then developed three measures which allow students to indicate their level of interest in, self-efficacy in relation to, and estimated time to accomplish or complete each of these 22 topics. The measures are shown in Table 2. Interest is related to student motivation, and measuring changes in this will show us to determine if a course is helping to motivate future learning or career choices within the student population.[22] Similarly, increases in self-efficacy have been shown to lead to greater persistence on tasks and long-term success in both academic and career endeavors.[4] The time metric was included to allow students to differentiate between topics they felt capable of achieving with minimal work and those they *could* become capable of if given enough time and/or resources.

Table 2: Measures and Likert Scale Values

| |
|---|
| I am interested in this topic<br>*(Strongly agree / Agree / Disagree / Strongly disagree / I don't know what this is)* |
| I am confident in my ability to undertake and succeed in completing this activity<br>*(Strongly agree / Agree / Disagree / Strongly disagree / I don't know what this is)* |
| Estimated time for me to prepare for and accomplish this<br>*At most a few days / A few weeks / Between a month and a year / A year or more / I wouldn't be able to do it on my own* |

For each statement, there are 4 options (forced-choice modified Likert scale) which provide students with the ability to rank their interest (4="Strongly agree", 1="Strongly disagree"), confidence (4="Strongly agree", 1="Strongly disagree"), and anticipated time to prepare for and accomplish a given topic (4="At most a few days", 1="A year or more"). A fifth option of "I don't know what this is" or "I wouldn't be able to do it on my own" was provided since some of the topics might be unfamiliar to the students. Questions which respondents left blank or for which they chose the fifth option were excluded from analysis.

The survey was reviewed for face validity by more than 20 graduate and undergraduate computer science students using a think-aloud protocol prior to being piloted.[17] This was done to check the clarity of statements, verify consistency of understanding of the questions by different students, and to ensure that students within the target audience would understand how to respond to the survey.

### Initial Participant Selection

We would prefer to survey a large number of students enrolled in our introductory cybersecurity course. This would provide a statistically significant evaluation of the course and allow us to determine how the instrument performs in such an environment. However, this is an elective course only offered during the Fall semester each year at our university. This was the course which was used for the interviews discussed above during the Fall, 2013 term. Two other cybersecurity courses were offered during the Spring 2014 semester. Although enrollment was very limited, we did perform an initial pilot in these courses. We also surveyed a CS1 course to provide additional insight into student interest and self-efficacy concerning cybersecurity topics. We were able to survey the introductory cybersecurity course during the fall, 2014 semester.

Table 3: Student Participation Numbers

| | CS1 | Cyber Defense Lab | Adv. Security | Intro Security |
|---|---|---|---|---|
| When Surveyed | Spring 2014 | Spring 2014 | Spring 2014 | Fall 2014 |
| Course Enrollment | 138 | 14 | 6 | 32 |
| Pre-Course Survey | 93 | 11 | 5 | 30 |
| Post-Course Survey | 74 | 9 | 6 | 21 |
| Both Surveys | 61 | 8 | 5 | 17 |

“Both Surveys” value indicates students who completed pre AND post surveys.

The first course surveyed during the Spring 2014 semester was a 1 credit-hour lab course designed for advanced undergraduate and graduate students. Enrollment was 14 students. This course provides hands-on experience with tools and techniques often used by attackers, and presents ways to prevent such attacks. The second course, an advanced computer security systems design course, is primarily for graduate students (though advanced undergraduate students occasionally take the course) and had an enrollment of 6 students. We performed pre- and post-course surveys of the students enrolled in both courses during the Spring 2014 semester.

We also surveyed students enrolled in the introductory programming course (CS1), which had an enrollment of 138 students . This course does not contain significant cybersecurity content, and it is not a course for which we expect to regularly use the survey. It was selected because it has a fairly large enrollment and because it would provide data from students who are not likely to have much experience with cybersecurity topics (thus providing a baseline from students within the general CS population). This approach provides a broader view of student interest and self-efficacy in relation to cybersecurity within our program. Additionally, surveying this course allows us to measure how building general knowledge of computer science affects student interest and self-efficacy in areas students are not directly studying. This is a required course for CS majors and a large majority of the students enrolled in this course during the Spring term are in their second semester of the CS program. We cannot know how many of these students fit the profile for those who will go on to take cybersecurity courses. However, based on past enrollment numbers, we can estimate that 10%-20% of the students in CS1 will go on to take the introductory cybersecurity course. We can compare these outcomes to those from the cybersecurity courses to see how the interest and self-efficacy of students in the two groups differ.

The introductory cybersecurity course was surveyed during the Fall 2014 semester. This is a 3 credit-hour course with enrollment ranging from 20 to 35 students per year. Students who enroll in the course are expected to have taken an operating systems or computer architecture course, or have comparable background (there are some computer engineering and information systems students who take the course). Most are upper-division undergraduate or graduate students. Course content provides a broad survey of cybersecurity concepts, hands-on implementation of common software exploits, applications of cryptographic protocols, and discussion of various authentication methods, as well as concepts in network and web-based security. There are approximately 6 programming assignments and numerous external papers assigned for students to read. The course also includes a final paper on a current security topic of the student’s choice.

The survey was administered in all 4 courses within the first 3 weeks of the semester and within the last 2 weeks of the semester. Table 3 is a summary of the student enrollment and participation totals from each surveyed course.

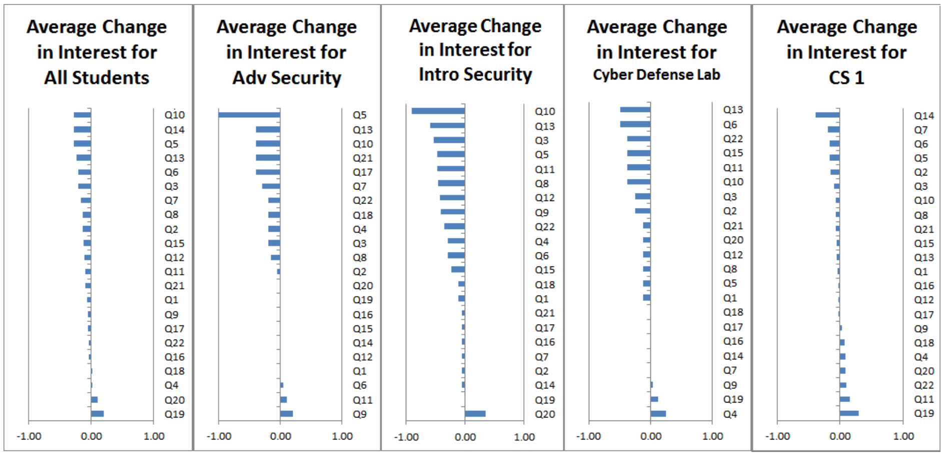

Figure 1: Average change in student interest for each survey question from pre- to post-survey. Each graph is ordered so that the questions with the largest change are at the top or bottom

## Analyzing Results

Figures 1 and 2 show the change measured for each interest and confidence statement in the survey, respectively. To make it easier to locate interesting data values, each graph is ordered so that the questions with the largest change are at the top or bottom of the graph. Graphs are included for the overall average change values as well as the average changes for each course.

Using a 1-4 forced-choice modified Likert scale, with 1 indicating less interest or confidence, we then average all responses containing a value on the ordinal scale for both the pre- and post-surveys. Comparing the pre- and post-survey averages shows the change in this tendency for each statement over the course of the semester. We compare results from the entire population to results from each course to see how each population is different from the overall results.

Within the pre-survey responses for the overall population, students indicate greater levels of interest than self-confidence in all but two of the topics based on the average response values. The two exceptions are “read articles/web posts about cybersecurity on your own” and “install and run malware checking software on a home computer.” These are topics which most students are likely familiar with, which is a reasonable explanation of students’ greater confidence in performing these tasks.

Estimated time selections tend to be conservative, with the average in most cases indicating more than “a few weeks.” The exceptions to this are the same 2 topics mentioned above along with “Remove detected threats from a home computer.” For these statements, average time estimates

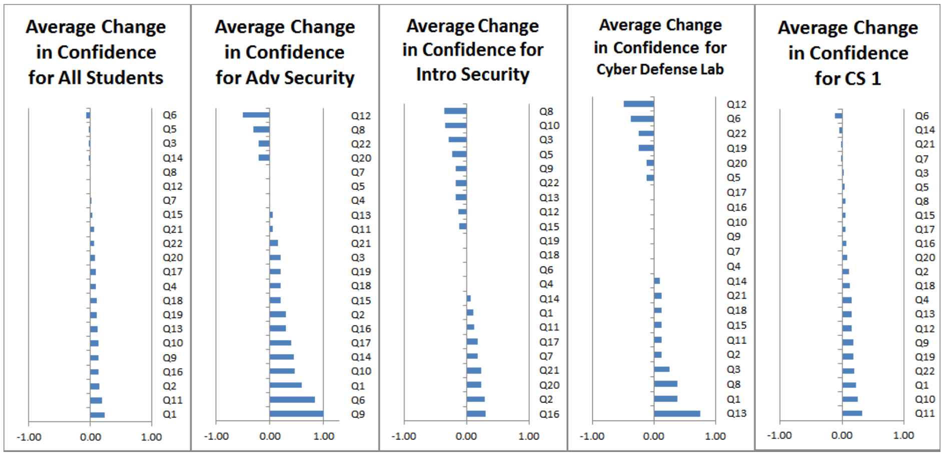

Figure 2: Average change in student *confidence* for each survey question from pre- to post-survey. Each graph is ordered so that the questions with the largest change are at the top or bottom

fall between a few days and a few weeks. Again, this is likely the result of the students being more familiar with these activities, and therefore more comfortable with a shorter time estimate to complete them.

Post-survey results are similar, although the difference between interest level and confidence level is reduced, with more cases (7) where the average confidence level exceeds the interest level. In fact, for 18 of the 22 statements, changes indicate student interest decreased, while confidence levels on 18 of the 22 statements increased. This seems to indicate that as students became more confident in their ability, they became *less interested* in the subject. This occurred in each of the courses studied. An alternative hypothesis is that students near the end of the semester have less interest in learning or taking on new tasks yet they have greater confidence in performing such tasks.

The interest graphs show that the overall average change values are influenced by those from the CS1 course due to the larger sample from that course. While the questions showing the greatest change are not in exactly the same order on these two graphs, they are nearly so, and the magnitude of the changes are similar. For the cybersecurity courses, it is surprising to see the large number of questions which exhibit a loss of interest. In fact, the introductory security course has lowered student interest in all but 1 area ("Install and run malware checking software on a home computer"). Given the small sample sizes for the the 3 cybersecurity courses, a few students can have a significant effect on the average, so a change of 0.5 is not necessarily a strong indicator of a trend in these courses. Additional assessment will be needed to determine if these results are significant.

In looking at the confidence graphs for the cybersecurity courses, unlike the interest graphs, there is a mixture of increasing and decreasing confidence among the statements. There is also a large difference in how statements performed within different courses. For example, statement 6: "Discover ways to protect personal data on the Internet" displays decreasing confidence for the introductory security course while it shows increasing confidence for the advanced security course. Similarly, question 14: "Write an algorithm that uses asymmetric encryption to authenticate a user" displays increases in confidence for all of the cyber defense courses while it trends toward less confidence for the programming course. Again, with relatively small sample sizes and an ordinal data scale, the magnitude of the changes does not provide a precise measure of the effects of the course, just a suggestion of how student interest and self-efficacy are trending. Future surveys with greater sample sizes are expected to provide stronger results.

### Statistical Analysis

In order to determine if the measured values from the pre- and post-course surveys were statistically different, we performed a statistical analysis of the data. To do this, only students who gave a valid response on the 4 point ordinal scale for a given statement on *both* surveys could be counted.

We used the Wilcoxon signed-rank test within R to validate the data.[28,26] Those statements with significant effects are shown in Table 4. We also calculated the Hedges' g values for each measure. This is a more conservative calculation of effect size. The results for the Hedges' calculation were similar to those found using the Wilcoxon test.

Table 4: Statistically Significant Statements

| Statement | p-value | Effect size | Hedges' g |
|---|---|---|---|
| Confidence in pursuing an advanced degree focused on cybersecurity | $< 0.01$ | -0.296 | -0.26 |
| Interest in taking additional courses focused on cybersecurity | $< 0.05$ | 0.209 | 0.27 |
| Interest in discovering ways to protect personal data on the Internet | $< 0.05$ | 0.228 | 0.26 |
| The time it would take to learn how to intercept and read network traffic | $< 0.01$ | -0.330 | -0.21 |
| The time it would take to learn how to verify a digital signature | $< 0.01$ | -0.345 | -0.29 |
| Interest in reading articles/web posts about cybersecurity on their own | $< 0.05$ | -0.266 | -0.19 |

Statements with p-values $< 0.05$ showing statistically significant changes between pre- and post-surveys and the measured effect sizes. Positive effect sizes indicate students became more interested or confident in the topic, or felt it would require less time to complete. Effect sizes: small $\geq .10$, medium $\geq .30$, large $\geq .50$

A negative effect size indicates that students have less interest/confidence in the statement, or felt it would require more time time to complete that task. While it would be better to have all measurements showing significance, there were at least two factors which made this unlikely. First, a majority of the students surveyed were not enrolled in a cybersecurity course. Second, the number of students enrolled in the cybersecurity courses who completed both parts of the survey is too small to provide statistical power.

### Per Course Analysis

The next question to investigate is how the responses are distributed within and between each of the 4 courses. For example, are introductory students more or less interested and more or less confident in learning how to use SSL certificates than students enrolled in cybersecurity courses? To determine this, we broke the responses down by course then averaged the responses for each option.

There was a noticeable difference between the CS1 students and the more advanced students. Students enrolled in the cybersecurity courses are self-selected and we would expect them to display greater interest than a population of students enrolled in a general computer science course. For many of the statements, students appear to become less interested over the course of the semester. The small sample sizes of the courses make this data less reliable for measuring the effects within a given course, but the results show that the survey measures differences between those that have chosen to take a cybersecurity course and the general population of CS students.

There is a discernible difference between the populations within the confidence data as well, but it is not as clear as the difference seen in the interest response data. Considering that all of the students surveyed are enrolled in computer science courses, they would be expected to have confidence in their ability to solve problems within a computer science context. Some differences can also be seen between the cybersecurity courses. For example, the statement “Learn how to intercept and read network traffic” averages $1.32 \pm 0.13$ for CS1, and $1.37 \pm 0.26$ for cyber defense lab while the average is $2.2 \pm 0.58$ for the advanced security course, and $2.29 \pm 0.14$ for the introductory security course. The more advanced students appear to be more confident than students in the other 2 courses in their ability to learn how to intercept and read network traffic. Again, the sample sizes were small for the courses, but the ability to see a difference in the measures is promising.

We analyzed the responses from the CS1 course to see if they contained additional significant changes. Given that the student population is more uniform, there was the potential that this might occur. Since these students had little or no exposure to cybersecurity subjects, we expected

Table 5: Statistically Significant Statements from CS1 Course

| Statement | p-value | effect size | Hedges’ g |
|---|---|---|---|
| Confidence in pursuing an advanced degree focused on cybersecurity | $< 0.05$ | -0.276 | -0.258 |
| The time it would take to learn how to intercept and read network traffic | $< 0.05$ | -0.33 | -0.357 |
| Interest in writing an algorithm that uses asymmetric encryption to authenticate a user | $< 0.05$ | -0.326 | -0.38 |
| Interest in reading articles/web posts about cybersecurity on their own | $< 0.05$ | -0.319 | -0.28 |

Positive effect sizes indicate more interest or confidence. Effect sizes: small $\geq .10$, medium $\geq .30$, large $\geq .50$

little change in values over the course of the semester. Inspecting the values revealed that 4 results had a p-value below the 0.05 threshold as shown in Table 5. The one new statement is "Interest in writing an algorithm that uses asymmetric encryption to authenticate a user."

## Summary and Future Work

We have developed a survey instrument that focuses on student interest and self-efficacy in relation to jobs, classes and/or research involving cybersecurity. This survey was piloted during the Spring 2014 and Fall 2014 semesters. Pre-course survey results show that student interest was generally higher than confidence. These differences were reduced, and in some cases reversed, in the post-course survey data. Further analysis of the individual course results showed that there is a noticeable difference in student responses between courses. Upper division students in cybersecurity courses had greater interest and confidence than introductory programming students in all but four of the interest and self-efficacy items.

These results show that the survey is capable of differentiating between outcomes from a cybersecurity course and those from an introductory programming course. We were also able to detect significant changes between the pre- and post-course responses for some of the topics even with limited sample sizes. Unfortunately, the enrollment in the cybersecurity courses was too small to allow for statistical analysis of the responses from those courses individually.

Implementing the survey in a variety of cybersecurity courses with larger enrollment numbers is the ongoing next step in the development of this instrument. This work is being conducted during the Spring 2015 in courses at two universities. These results will allow us to begin validation of survey questions and provide us with the opportunity to perform more rigorous data analysis. This data will be used to adjust the survey and enable us to begin working within the classroom to identify pedagogical activities which produce improved student interest and self-efficacy in relation to cybersecurity.

## Acknowledgments

The authors would like to thank Xinming Ou for allowing us access to his classes for surveys and interviews. This work was funded by NSF grant 1241721: the CyberCorps®Scholarship for Service.

### References

1 ACM-SIGITE. IT2008 model curriculum, 2013. Retrieved from `http://www.sigite.org/`.

2 Richard H. Austing, Bruce H. Barnes, Della T. Bonnette, Gerald L. Engel, and Gordon Stokes. Curriculum '78: Recommendations for the undergraduate program in computer science&mdash; a report of the acm curriculum committee on computer science. *Commun. ACM*, 22(3):147–166, March 1979. ISSN 0001-0782. doi: 10.1145/359080.359083. URL `http://doi.acm.org/10.1145/359080.359083`.

3 Albert Bandura. Perceived self-efficacy in cognitive development and functioning. *Educational psychologist*, 28 (2):117–148, 1993.

4 Albert Bandura, Claudio Barbaranelli, Gian Vittorio Caprara, and Concetta Pastorelli. Self-efficacy beliefs as shapers of children's aspirations and career trajectories. *Child development*, 72(1):187–206, 2001.

5 Scott Bell. A longitudinal study of students in an introductory cybersecurity course. In *Proceedings of the 121st Annual ASEE Conference and Exposition*, 2014.

6 Matt Bishop. Teaching computer security. In *Proceedings of the 9th IFIP International Symposium on Computer Security (IFIP/ SEC)*, pages 65–74, 1993.

7 Robert C. Bogdan and Sari Knopp Biklen. *Qualitative Research in Education. An Introduction to Theory and Methods*. ERIC, 1998.

8 Nancy G Boyd and George S Vozikis. The influence of self-efficacy on the development of entrepreneurial intentions and actions. *Entrepreneurship theory and practice*, 18:63–63, 1994.

9 David Carlson. Teaching computer security. *ACM SIGCSE Bulletin*, 36(2):64–67, 2004.

10 Simon Cassidy and Peter Eachus. Developing the computer user self-efficacy (CUSE) scale: Investigating the relationship between computer self-efficacy, gender and experience with computers. *Journal of Educational Computing Research*, 26(2):133–153, 2002.

11 Ronald S Cheung, Joseph P Cohen, Henry Z Lo, and Fabio Elia. Challenge based learning in cybersecurity education. In *Proceedings of the 2011 International Conference on Security & Management*, volume 1, 2011.

12 Wm Conklin, Raymond E Cline, Tiffany Roosa, et al. Re-engineering cybersecurity education in the us: An analysis of the critical factors. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, pages 2006–2014. IEEE, 2014.

13 Stephen Cooper, Christine Nickell, Victor Piotrowski, Brenda Oldfield, Ali Abdallah, Matt Bishop, Bill Caelli, Melissa Dark, Elizabeth K Hawthorne, Lance Hoffman, et al. An exploration of the current state of information assurance education. *ACM SIGCSE Bulletin*, 41(4):109–125, 2010.

14 John W Creswell. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications, 2013.

15 C.R. Dodge, Costis Toregas, and Lance Hoffman. Cybersecurity workforce development directions. In *Proceedings of the Sixth International Symposium on Human Aspects of Information Security and Assurance*, 2012.

16 Brian Dorn and Allison Elliott Tew. Becoming experts: measuring attitude development in introductory computer science. In *Proceeding of the 44th ACM technical symposium on Computer science education*, pages 183–188. ACM, 2013.

17 Arlene Fink and Mark S. Litwin. *How to measure survey reliability and validity*, volume 7. Sage, 1995.

18 John Hill, Curtis A. Carver Jr., Jeffrey W. Humphries, and Udo W. Pooch. Using an isolated network laboratory to teach advanced networks and security. In *ACM SIGCSE Bulletin*, volume 33, pages 36–40. ACM, 2001.

19 Robert W. Lent, Steven D. Brown, and Kevin C. Larkin. Self-efficacy in the prediction of academic performance and perceived career options. *Journal of counseling psychology*, 33(3):265, 1986.

20 Celia Paulsen, Ernest McDuffie, William Newhouse, and Patricia Toth. Nice: Creating a cybersecurity workforce and aware public. *IEEE Security & Privacy*, 10(3):0076–79, 2012.

21 Vennila Ramalingam and Susan Wiedenbeck. Development and validation of scores on a computer programming self-efficacy scale and group analyses of novice programmer self-efficacy. *Journal of Educational Computing Research*, 19(4):367–381, 1998.

22 Kusum Singh, Monique Granville, and Sandra Dika. Mathematics and science achievement: Effects of motivation, interest, and academic engagement. *The Journal of Educational Research*, 95(6):323–332, 2002.

23 Eugene F. Spafford. Teaching the big picture of infosec. In *2nd National Colloquium for Information System Security Education*, 1998.

24 The Joint Task Force on Computing Curricula Association for Computing Machinery (ACM) IEEE Computer Society. Computer science curricula 2013, 2013. Retrieved from `http://ai.stanford.edu/users/sahami/CS2013//final-draft/CS2013-final-report.pdf`.

25 Eric Wiebe, Laurie Williams, Kai Yang, and Carol Miller. Computer science attitude survey. *Computer Science*, 14(25):0–86, 2003.

26 Frank Wilcoxon, SK Katti, and Roberta A Wilcox. Critical values and probability levels for the wilcoxon rank sum test and the wilcoxon signed rank test. *Selected tables in mathematical statistics*, 1:171–259, 1970.

27 Jerry Willis. *Qualitative Research Methods in Education and Instructional Technology*. IAP, 2008.

28 Chi Yau. R tutorial. http://www.r-tutor.com, 2014.