A Longitudinal Study of Students in an Introductory Cybersecurity Course

Mr. Richard Scott Bell, Kansas State University

Scott Bell is a PhD candidate in the Computing and Information Sciences department at Kansas State University and is currently researching ways to improve Cybersecurity Education. Before beginning pursuit of his PhD, Scott worked as an Instructor at both Northwest Missouri State University, the University of Arkansas-Fort Smith and State Fair Communit College. He earned his Master of Science degree in computer science and his Bachelor of Science degree in geological engineering from the Missouri University of Science and Technology.

Eugene Y. 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). In 2013 he received the NSF CAREER award for work on secure next-generation medical systems.

Eleanor C Sayre, Kansas State University

Eleanor Sayre received her Ph.D. and M.S.T. degrees in physics in 2007 and 2005 (respectively) from the University of Maine, with research emphasis in physics education. Her B.A. in physics from Grinnell College in 2002 involved research in computer science education. Her current research interests include identity development in undergraduate STEM majors, time-evolution of student understanding, and community practices in physics and physics education. In 2012 and 2013, she and her collaborators received NSF WIDER awards for building faculty resources for assessment on the Physics Education Research User's Guide.

A Longitudinal Study of Students in an Introductory Cybersecurity Course

Scott Bell*, Eleanor Sayre*, and Eugene Vasserman*
***Kansas State University**

Abstract

While some aspects of information assurance can be traced back to the earliest implementations of cryptography, the field of cybersecurity is relatively new, and thus, pedagogical "best practices" have not been adequately investigated. The tremendous growth within the field over the past two decades has resulted in a substantial number of organizations (academic, governmental and commercial) implementing a wide variety of educational approaches in an attempt to meet the growing demand for graduates and employees possessing skills in cybersecurity. This growth has been so rapid that no one has taken the time to ask the question: *are we doing this the right way?* In order for us to identify and promote instructional best practices within cybersecurity courses, an instrument capable of measuring these values is needed. This paper contains the results of the initial phase in our development of such an instrument.

This work is a longitudinal and cross-sectional study of students enrolled in an introductory cybersecurity course. The purpose of the study is to identify course components and instructional approaches that affect both students' success in the classroom and the likelihood that they will continue to pursue cybersecurity both in the classroom and as part of their career. Given the variation in the content being presented in such courses, we focus this effort on student characteristics that have been shown to lead towards success in the classroom and influence student career selection. These characteristics include self-efficacy in relation to cybersecurity, student interest in further coursework, and research or jobs that involve cybersecurity concepts[3,12]. By interviewing students enrolled in a cybersecurity course, at multiple points during the semester, we are able to identify student interests and perceptions of cybersecurity and document changes in student self-efficacy and interest that occur as the semester progresses. Furthermore, we identify pedagogical practices which students found most useful through this semester-long investigation. The results from this study will be used to construct a Likert-type scale survey that will allow cybersecurity educators to evaluate student outcomes consistently between various teaching approaches. This will allow for systematic, informed pedagogical changes to improve outcomes in the cybersecurity classroom.

Course Background

The course being studied is a 3 credit-hour course offered once per year within the computer science department. This is the 8th iteration of this course being taught by the same instructor. Enrollment ranges from 20-35 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 overview 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.

Cybersecurity Education

Compared to other areas of study, cybersecurity is a very new field. Universities first began offering courses in cybersecurity during the 1970s[9]. Since that time, the importance and need for a workforce skilled in cybersecurity has grown rapidly[17]. Due to this rapid growth, and the tremendous breadth of material that falls under the umbrella of cybersecurity, a wide array of content and pedagogical practices have been incorporated into today's cybersecurity classrooms.

While this diversity reflects the reality of cybersecurity education, it is a major hindrance to the development of a consistent model for cybersecurity education. Areas which could be incorporated into this domain, include: computer architecture, criminology/law, cryptography, databases, human-computer interaction, information retrieval, information theory, management/business, mathematics, military science, mobile computing, networks, operating systems, digital forensics, philosophy/ethics, programming languages, software engineering, statistics/probability, and web programming[18]. Course content may range from cryptography, and the mathematical principles and algorithms used to protect data to system-level protocols[4]. Additionally, the goals of courses vary dramatically, such as teaching cybersecurity as practical vocation skills, as good engineering practices, or as academic theories.

The methods used to teach these courses are just as varied as their goals. Some courses focus on laboratory-based, experimental operations[6,14]. 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[8]. This wide array of content and approaches shows how challenging it is to determine what content and pedagogical methods constitute the "best practices." Unfortunately, given this challenging environment, there is currently no valid way for those who are teaching these courses to systematically measure and improve student outcomes within their classrooms.

While the scope of the field is daunting, there is progress being made to improve the situation. 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 the framework was information assurance and security (along with professionalism)[2]. Similarly, in 2013, for the first time, the ACM and the IEEE have included information assurance and security as a separate knowledge area within their recommended Computer Science Curricula[1]. As with the IT curriculum, the CS curriculum also incorporates components of cybersecurity throughout the various other computer science knowledge areas. While both guidelines provide recommended cybersecurity topics that should be covered within the respective curricula, they do not include any pedagogical best practices to guide instructors as to how they should engage

students within the cybersecurity classroom or how to assess their own pedagogical methods.

There have been numerous research projects investigating ways to measure and improve student outcomes within introductory computer programming courses[7,10,16,19]. Unfortunately, the approaches taken do not readily apply to the cybersecurity classroom. First, the content of these courses has remained fairly consistent from year to year and even from university to university. Second, given the number of students enrolled in these courses (the introductory programming course in our program had over 110 students enrolled this past semester), researchers are able to conduct quantitative surveys and achieve statistically significant results over the course of a single semester and compare results from courses at various schools. Given the widely varying ways in which cybersecurity is taught, and the smaller number of students, we determined that while we wish to develop such a quantitative instrument, we needed to approach the problem from a different direction.

Qualitative Study

Due to the small class enrollment and our lack of understanding where student interests and attitudes lie in relation to the field of cybersecurity, blindly generating a paper-based survey would likely not produce statistically useful outcomes without several years of data. Additionally, with a survey-based assessment, we might entirely miss significant data. For these reasons, we chose to utilize a qualitative approach rather than a quantitative approach for this first stage of our research. While these results do not lend themselves to elaborate statistical analysis, they do give us greater flexibility to explore how or why things have occurred within this small population, reducing the ambiguity that comes with responses on paper based surveys. We can then use the knowledge gained from this study to more accurately focus future investigations.

Interviews are one of the most utilized qualitative methods in small-scale research. They tend to give high quality data with reduced ambiguity even with a relatively small sample size by allowing the interviewer to search for clarification of a respondent's answers when necessary. The drawback is that both the interviews and analysis of responses take substantially more time than survey-based assessments[11]. Interview format can range from a very structured set of questions that is to be followed explicitly to a nearly unstructured format with few guidelines, depending on the need and purpose of the research being performed[20]. This approach allows for new ideas to be uncovered and explored based on what the participants say, rather than potential preconceptions of study authors. The end goal of such a qualitative study is to gain an understanding of the participant's point of view concerning the course and its content[5,13].

Methodology

Student volunteers were solicited from an introductory cybersecurity course and included both upper division undergraduate as well as graduate students who participated in the semester long study. To help encourage student participation in the study and reduce the likelihood of participants not completing the study, volunteers who completed the entire study were promised and given a small financial incentive ($50) upon completion of the 3rd interview. From a course enrollment of 30 students, 18 initially agreed to participate. Participants were interviewed 3

times. Interviews took place during the 2nd, 10th and 15th weeks of the semester. Of the initial volunteers, 15 participated in the first round of interviews, 14 participated in the second round, and 12 participated in the third round. Of the 15 participants, 6 were undergraduate computer science students, 3 were undergraduate computer engineering students and 6 were graduate computer science students. Two of the graduate students were female; all other participants were male.

Interviews were semi-structured and lasted from 15 to 30 minutes. With the semi-structured format, a base set of questions was established for each interview but additional questions were asked when topics of interest were uncovered or points of clarification were needed. In cases where the new question would be useful for all students, these questions were carried over to the remaining interviews within that round. Interviews were video taped to allow for post-interview analysis. (Note that some of the sound content during the first round of interviews was not intelligible.) Also, in this format, participants are encouraged to elaborate and discuss their answers, so they might mention several topics in the answer to a single question. For these reasons, the number of items indicated for some questions does not always add up to the total number of participants. Topics covered included:

- reasons for taking the course
- experiences in the course
- specific topics of interest
- student's perception of his or her own ability in cybersecurity
- interest in cybersecurity as a career path and/or a topic of further study or research
- how well students felt the course was preparing them for future studies or positions in cybersecurity.

First Round of Interviews

During the first interview, students were asked why they chose to take the course. Most of them gave more than one reason, so we counted the number of times each reason was given:

- 5 students mentioned that it filled an elective for their degree
- 8 said it sounded interesting, 3 called it important
- 6 mentioned that they wanted to learn how to make code more secure
- 2 indicated that it was part of their research area.

Additionally, students were asked to give a definition of cybersecurity during the first and second interviews. The goal was to see whether and how student views of cybersecurity changed over the course of the semester. We noted patterns in specific terms that students mentioned during each interview. In both interviews, students linked actions such as protecting, securing, preventing, defending and finding with targets such as networks, hardware, systems, data, and programs. Table 1 shows the distribution of terms among the students. The most interesting change is the tripling in the number of students that mentioned data, files, or information as part of their definition. In fact, every 'category' was mentioned more frequently during the second set of interviews, showing that students were becoming more aware of the breadth of the threats faced today.

First Round		Second Round	
Protecting / securing / defending / preventing	14	Protecting / defending / preventing	17
Finding	2	Applying or using concepts	2
Network	6	Network / Internet	10
Hardware / computer / server	3	Hardware / computer / server	6
System	3	System	4
Data / files / information	4	Data / files / information	12
Software / programs	2	Bugs / weak spots	3
		Authentication / verification / authorization	4

Table 1: Topics mentioned by students when asked to define the term cybersecurity.

Students were also asked during the initial interview if they felt they could be successful conducting cybersecurity research. One student responded absolutely (this student withdrew from the course prior to the second interview). Other responses included "I think so," "probably," and "not sure." One student replied "I don't know enough yet to answer that question." Results are shown in Table 2.

Table 2: First interview questions related to future cybersecurity research and work.

Do you feel you could be successful conducting cybersecurity research?	
Absolutely	1
I think so / probably	7
Not sure	4
I don't know enough to answer that question	1
Is cybersecurity research something that you would enjoy doing?	
Yes / sure	10
Probably	4
Do you see cybersecurity involved in your career after you graduate?	
Definitely / yes	11
Depends	3
Do you plan to seek out jobs that involve cybersecurity aspects specifically?	
Definitely / yes	5
No	2
There are other, more important, aspects to job search	7

As a follow-up question, we asked students if they thought that cybersecurity research was something they would enjoy doing. Ten students responded with "yes" or "sure" and 4 students gave less certain but positive responses such as "probably." When asked if they felt that cybersecurity (not specifically research) would be involved in their career after graduation, all students felt that it would be involved in their career in some way, although 3 specified that it depends on the job. So, at the beginning of the semester, students felt that cybersecurity would likely be involved in their future careers and they were interested in cybersecurity research

Table 3: Second round interview questions.

How are you doing in the class?	
Well	6
Moderately well	1
Poorly	2
Unsure	3
Are you glad you decided to take this course?	
Yes	12
No	0
Is this course interesting?	
Yes	11
No	0
Do you feel that you could be successful in a job that involves cybersecurity?	
Definitely	1
Yes	6
With additional work / help	4
Not sure	2

although they were not very confident in their ability to do the work. Results from asking students if they would seek out positions that involved aspects of cybersecurity specifically are shown in Table 2.

During the first interview, we also investigated student experience with cybersecurity prior to the class. Students were asked to "Describe encounters you have had with cybersecurity prior to this course." While the students did mention some key concepts, nearly half (7) indicated they had little experience or were "oblivious" to cybersecurity prior to the course. Some of the previously encountered concepts that were mentioned included stack "smashing" and buffer overflow attacks, which were discussed in previous courses, finding and removing viruses on their computers, phishing attacks, and social account compromise.

Second Round of Interviews

The results from several of the questions asked during the second round of interviews are given in Table 3. First, students were asked how they were doing in the course. Three were unsure how they were doing (all were undergraduates), 2 felt they were doing poorly (one undergraduate). Another felt he was doing moderately while 6 thought they were doing well. Despite these mixed feelings about their performance, when asked, every student was glad they were taking the course. Reasons given included that they felt they had learned something useful or interesting and that it gave them a broader understanding of the subject.

All 11 students who were asked if they thought the course was interesting agreed that it was, although the level of interest varied: "it is *very* interesting" versus "some of it is." Another question we asked students was "Do you feel that you could be successful in a job that involves cybersecurity?" Seven students felt they could be, while another 4 students thought that with work/help they would be. Only 2 students were not sure if they could be successful. No students

said they could not be successful in a cybersecurity job.

During the second round of interviews we asked students what topics they would like to learn more about. The list of topics included:

- everything just deeper
- more about buffer overflow attacks
- correct implementation of PKI (public key infrastructure)
- mobile security (mentioned by multiple students)
- newer attacks; the buffer- and heap-based attacks are out of date
- biometric authentication
- web security.

We asked this same question during the third round of interviews with similar results.

We asked students during both the second and third interviews if they planned to take additional cybersecurity courses. The department has several options for students to choose from. There is a cryptography course, a lab-based course focusing on common exploits and penetration testing tools, and an advanced (graduate level) cybersecurity course focused on network security, security protocols, and composition of security tools from building blocks. Since several (5) of the students will be graduating or leaving by the end of the academic year, there was some hesitation when answering this question. Student responses are given in Table 4. Note the trend toward more definitive positive answers – the number of students answering a definitive "yes" did not go down, but students who were previously uncertain moved from more negative to more positive answers.

Table 4: Do you plan to take additional cybersecurity courses?

	Second Interview	Third Interview
Yes	5	5
Not sure	2	4
Depending on schedule	3	2
I don't think so	3	1

Third Round of Interviews

During the third interview, students were asked to rank themselves on a scale from 1 to 10, with 1 indicating no knowledge of cybersecurity and 10 indicating being a cybersecurity expert. Two students rated themselves between 1 and 3, 3 students rated themselves between 4 and 5 while 5 students rated themselves between 5.5 and 7 and 1 student selected 8. The one remaining student first selected 4.7 then changed to 6.5 then 7 then 9.9, stating that compared to the rest of the world, he knows substantially more than a vast majority of people at this point. All of the students indicated that in order to rank higher, they felt they needed more experience and exposure to cybersecurity concepts either in the classroom, a work environment, or through research. One student noted that he might even rate himself lower as he learns more about cybersecurity. These results are shown in Table 5. During the final interview with each student, they were asked about their confidence in cybersecurity moving forward. The results were varied, with 6 students

expressing confidence in their abilities, 3 being somewhat confident, 2 being unsure and 1 having little confidence in his ability.

One of the main focuses of the course is having students perform attacks against various platforms. Several (7) students indicated that this was an eye opening or "aha" experience for them, making comments such as *"I was thinking to myself 'You can do that?' "* Other students also mentioned having a similar "aha" reaction when learning about the Kerberos authentication system[15]. There were numerous comments about this course being a good introduction and that the students were interested in learning more about various topics.

Table 5: Student self rating of cybersecurity competence.

Rating	Number of students
1-3	2
4-5	3
5.5-7	5
8	1
9 - 10	0
(One student changed from $4.7 \rightarrow 6.5 \rightarrow 7 \rightarrow 9.9$)	

Interview Summary

We performed 3 rounds of interviews of students enrolled in an upper-division cybersecurity course. Our goal was to determine student outcomes from the course. Specifically, we were interested in learning student interests in cybersecurity as they pertain to future plans such as careers, research, and classwork. We also wanted to investigate student self-efficacy as it pertains to cybersecurity: are students gaining confidence in their ability to deal with cybersecurity issues? Based on responses, there is student interest in cybersecurity at all levels (courses, research, and jobs) although many of the students see it as a component of their overall education and career plans, not the main focus. All students who were asked were glad they had taken the class and found the material at least somewhat interesting. This was expected given that the course is an upper-division elective course with many alternatives available to students.

Students' self-efficacy did not rate as highly as their interest. In fact, it decreased over the course of the semester. Given that students admitted to having very little knowledge of cybersecurity at the beginning of the semester and the enormous scope of the field, this was not unexpected. The fact that many were interested in continuing to learn more about cybersecurity and that they were glad they took the course shows that while the material was somewhat intimidating, they were not discouraged by the experience.

Conclusions and Future Work

From the interviews, we can learn quite a bit about students' experiences in and from this course:

- Students initially had varying ideas of what cybersecurity was, but by the second interview, they were very focused on network and data as being a major focus for protection.

- At the beginning of the course, students were uncertain if they could be successful doing cybersecurity research, yet all of them felt that it was something they might enjoy doing.
- All of the students felt that cybersecurity would be involved in their career.
- Other than overflow attacks, students reported very little exposure to cybersecurity concepts prior to this course.
- Responses were mixed on whether students would seek out a job that specifically involved cybersecurity.
- Students found the hands-on attacks and learning about the Kerberos authentication protocol especially interesting.
- About half of the students planned to take additional cybersecurity courses.
- During the second interview, just over half of the students thought they were doing well in the course.
- Reasons for taking the class included being an elective or part of their research area and making code more secure.
- Every student was glad they took the course, and thought that it was interesting.
- 11 of 13 students felt they could be successful in a cybersecurity job.

Overall, the students had a very positive experience in the course. The hands on experiences with exploits and cryptographic protocols within the course were definitely important to the students for building both interest and confidence in their ability to succeed in this field. Even with these positive responses, most students were still not sure that they would seek out a career in cybersecurity or take additional courses (though they all acknowledge that it is likely that cybersecurity will be involved in their careers).

We plan to use the data collected from this study to develop a paper-based survey tool designed to measure student self-efficacy and interest in relation to cybersecurity both in the classroom and in potential future jobs. This will involve the development of the survey instrument, an initial set of think aloud interviews with students of various levels, and then in-class validation within current cybersecurity courses.

Acknowledgments

The authors would like to thank Simon Ou for allowing us access to his class for this study. This work was funded by an NSF Scholarship For Service award.

References

1 IEEE ACM. Computer science curricula 2013, 2013. Retrieved from `http://ai.stanford.edu/users/sahami/CS2013//final-draft/CS2013-final-report.pdf`.
2 ACM-SIGITE. It2008 model curriculum, 2013. Retrieved from `http://www.sigite.org/`.
3 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.
4 Matt Bishop. Teaching computer security. In *SEC*, pages 65–74, 1993.
5 Robert C Bogdan and Sari Knopp Biklen. *Qualitative research in education. An introduction to theory and methods*. ERIC, 1998.
6 David Carlson. Teaching computer security. *SIGCSE Bull.*, 36(2):64–67, June 2004. ISSN 0097-8418.

7 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.
8 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.
9 Stephen Cooper, Christine Nickell, Victor Piotrowski, Brenda Oldfield, Ali Abdallah, Matt Bishop, Bill Caelli, Melissa Dark, E. K. Hawthorne, Lance Hoffman, Lance C. Pérez, Charles Pfleeger, Richard Raines, Corey Schou, and Joel Brynielsson. An exploration of the current state of information assurance education. *SIGCSE Bull.*, 41(4):109–125, January 2010.
10 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*, SIGCSE '13, 2013.
11 Eric Drever. *Using Semi-Structured Interviews in Small-Scale Research. A Teacher's Guide.* ERIC, 1995.
12 Heidi Fencl and Karen Scheel. Engaging students: An examination of the effects of teaching strategies on self-efficacy and course climate in a nonmajors physics course. *Journal of College Science Teaching*, 35(1):20, 2005.
13 Jack R Fraenkel and Norman E Wallen. How to design and evaluate research in education.
14 John M. D. Hill, Curtis A. Carver, Jr., Jeffrey W. Humphries, and Udo W. Pooch. Using an isolated network laboratory to teach advanced networks and security. In *Proceedings of the Thirty-second SIGCSE Technical Symposium on Computer Science Education*, SIGCSE '01, pages 36–40, 2001. ISBN 1-58113-329-4.
15 Steven P Miller, B Clifford Neuman, Jeffrey I Schiller, and Jermoe H Saltzer. Kerberos authentication and authorization system. In *In Project Athena Technical Plan*. Citeseer, 1987.
16 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.
17 Dale C. Rowe, Barry M. Lunt, and Joseph J. Ekstrom. The role of cyber-security in information technology education. In *Proceedings of the 2011 Conference on Information Technology Education*, SIGITE '11, pages 113–122, 2011. ISBN 978-1-4503-1017-8.
18 Eugene F Spafford. Teaching the big picture of infosec. In *2nd National Colloquium for Information System Security Education*, 1998.
19 Eric Wiebe, Laurie Williams, Kai Yang, and Carol Miller. Computer Science Attitude Survey. *computer science*, 14(25):0–86, 2003.
20 Jerry Willis. *Qualitative Research Methods in Education and Instructional Technology*. IAP, 2008.