Teaching Computer Science with Cybersecurity Education Built-in

Chuan Yue, *Colorado School of Mines*

Abstract

Despite the remarkable cybersecurity education efforts from traditional approaches such as offering dedicated courses and even degree programs or tracks, the computer science curricula of many institutions still severely fall short in promoting cybersecurity education. We advocate to further explore *the security integration approach* to complement other approaches and better promote cybersecurity education. We contribute to this approach by concretely exploring a viable implementation solution and evaluating its effectiveness. Specifically, we explore to discuss relevant cybersecurity topics in upper and graduate level non-security courses to engage students in learning cybersecurity knowledge and skills from the perspectives of different computer science sub-areas, and help them understand the correlation and interplay between cybersecurity and other sub-areas of computer science. Our experience in six class sessions of five non-security courses is very encouraging: the majority of students found the discussed cybersecurity topics interesting, useful, and relevant; they would like to have cybersecurity topics discussed in other non-cybersecurity courses in the future; they improved their understanding of the discussed content. We hope our experience can be helpful for other educators to adopt and further explore the security integration approach in the future.

1. Introduction

The necessity and importance of cybersecurity research and education have been widely recognized by the National Science and Technology Council, NSF, NSA, DHS, NIST, many other organizations, and the whole society. However, large-scale and pervasive online malicious or even criminal activities will only increase in numbers and cause severer damages if we do not build an efficient cybersecurity education system and produce more high-quality cybersecurity professionals.

"Where a threat intersects with a vulnerability, risk is present [1]." Threat sources are persistent because attackers are always there, driven by either economic or political incentives. Therefore, fundamentally, widespread security vulnerabilities in the server-side and client-side software are the root causes of the pervasive security risks and rampant security attacks, and those vulnerabilities can be further attributed to the lack of sufficient security knowledge and skills in many software engineers who graduated mainly from the computer science degree programs.

Despite the remarkable cybersecurity education efforts from the traditional approaches such as offering dedicated courses and even degree programs or tracks, we strongly believe that the computer science curricula of many institutions still severely fall short in promoting cybersecurity education per our following observations:

- Cybersecurity courses are still not core courses in the computer science curricula of the majority of institutions (e.g., none of the top 50 CS programs in U.S. includes cybersecurity in the core per our survey in June 2016); many institutions even do not offer any cybersecurity elective course. One reason is that *Information Assurance and Security* was only officially added as a knowledge area in computing curricula by ACM and IEEE Computer Society in 2013 [2].
- Many computer science courses such as programming and software engineering traditionally do not include cybersecurity topics. However, cybersecurity is closely related to almost all the other sub-areas of computer science. For example, engineers can easily create many security vulnerabilities in the design, implementation, and deployment of their software if they do not have secure programming practices, do not follow secure software development and deployment processes, or do not properly include security components into the software.
- Even if cybersecurity courses are offered as electives in some institutions and are taken by some students, we missed the golden chances for helping students understand the correlation and interplay between cybersecurity and other sub-areas of computer science. The consequence is that cybersecurity is too often an irrelevance or at most an afterthought for students – not an indispensable ingredient that should be integrated into the basis of their computer science knowledge and skills.

We advocate to further explore *the security integration approach* to complement those traditional approaches and better promote cybersecurity education. This approach is not new, and indeed the necessity and importance of integrating cybersecurity concepts into existing computer courses have been emphasized for over one decade, for example, as highlighted in a SIGCSE 2002 panel [3]. ***Unfortunately, this approach***

has received insufficient attention, and it still severely lags behind in adoption (Section 2).

We contribute to this approach by concretely exploring a viable implementation solution and evaluating its effectiveness. Specifically, our cybersecurity researchers consulted with the instructors of five upper and graduate level non-security courses (*Computer Communication, Software Testing, Software Engineering, Operating Systems, and Computer Networks*), identified the relevant cybersecurity topics, and discussed the corresponding cybersecurity topics in six class sessions (Section 3). Students' responses to our anonymous questionnaires are very encouraging (Section 4): the majority of students found the discussed cybersecurity topics interesting, useful, and relevant; they would like to have cybersecurity topics discussed in other non-cybersecurity courses in the future; they improved their understanding of the discussed content. We hope our experience can be helpful for other educators to adopt and further explore the security integration approach in the future (Section 5).

2. Related Work

We focus on reviewing the security integration approach in this section. The idea of this approach dated back to the late 1990s and early 2000s [4, 5, 6], while the 2002 SIGCSE panel on *integrating security concepts into existing computer courses* [3] is especially notable. The panelists emphasized the necessity and importance of integrating cybersecurity concepts into existing computer courses, and provided many detailed suggestions. For example, they suggested that using this approach, "even if no security-based courses are added, major and non-major courses in computer science, CIS, etc., can do a better job of raising awareness of threats, vulnerabilities, and risks"; they suggested that "security issues should be discussed throughout the undergraduate computer science curriculum"; they suggested that "the most effective way to incorporate security-oriented issues into the curriculum is to include them as natural aspects of normal course topics."

Some educators have further analyzed this security integration approach. Null proposed specific activities that provide the students with the proper motivation and the basic principles of computer security, but do not require instructors to be security professionals [7]. Perrone et al. termed the security integration approach as the "thread approach"; they analyzed that the single-course approach is of limited effectiveness, the track approach demands extensive resources, while the thread approach can effectively meet the cybersecurity educational needs using a minimum of resources [8]. Howles et al. outlined efforts to embed cybersecurity modules throughout the undergraduate years to ensure a greater understanding of security issues among diverse computing majors [9].

Some educators have also experimented with the implementation of this security integration approach. Taylor and Azadegan piloted security integration across sections of CS0 and CS1 using security laboratory modules [10]; their results show an increased security knowledge in students. Markham introduced information security in teaching CS1 with Python [11]. Kaza et al. experimented with disseminating the security integration approach at low level courses across five institutions, and they obtained promising results [12]. Siraj et al. focused on training non-security faculty members to integrate cybersecurity topics into their courses [13]; they found that students gained knowledge and awareness, but did not increase interest in computer security. Whitney et al. integrated secure coding education into an advanced Web programming course [14]; their results show an increased awareness and secure programming knowledge in students.

Unfortunately, the overall attention to this security integration approach is still insufficient and its adoption is still very limited. Our effort differs from and complements those existing efforts by providing a new viable implementation solution that leverages the expertise of cybersecurity researchers and focuses more on the (limited existing) integration in upper and graduate level non-security courses, as will be further justified in the next section.

3. Our Implementation Solution

The basic idea of our security integration implementation solution is very simple: leveraging the expertise of cybersecurity researchers to incorporate relevant security topics into upper and graduate level non-security courses. More specifically, cybersecurity researchers consult with the instructors of non-security courses, identify the relevant cybersecurity topics, and discuss the corresponding topics in the classes. Our implementation solution is viable from two perspectives.

On the one hand, asking cybersecurity researchers to conduct the integration can ensure a high quality of the integration and meanwhile avoid the overhead of training non-security faculty members [13]. The cybersecurity researchers can be faculty and students in universities, and can be experts in industry or government. They are ready and often willing to talk about cybersecurity research topics to a broader audience, for example, in the form of invited talks as we have practiced and observed.

Table 1. Class Session Information

Session Symbol	Course Title	Integrated Content	Course Level	Institution/ Semester	Class Size
CC	Computer Communication	SSL, TLS, HTTPS, DTLS (Datagram TLS), TLS Heartbeat Extension, OpenSSL Heartbleed Vulnerability/Impact/Security Patch, Security Recommendations	Grad.	I / I	11
ST	Software Testing	Commonly Used Crypto Primitives, Common Crypto Rules, Program Slicing, CryptoLint Static Analysis Tool and its Design/Implementation/Evaluation/Discussion	Grad.	I / I	5
SE	Software Engineering	Problems of Text-based Passwords, Popular Solutions, Password Creation, Password Management, Single Sign-On (SSO) Systems Security, Web SSO Phishing	Undergrad.	I / I	24
OS1	Operating Systems	Virtualization, VM, VMM, Virtualization and Security, IDS, Virtual Machine Introspection (VMI) and its Useful Applications in Security, Weak and Strong Semantic Gaps in VMI, Future VMI Research Directions	Grad. and Undergrad.	I / I	27
OS2	Operating Systems		Grad. and Undergrad.	I / II	23
CN	Computer Networks	Symantec Internet Security Threat Report, Vulnerability Analysis of Password Managers, Information Leakage Vulnerabilities in Browser Extensions, Phishing Attacks	Undergrad.	II / II	17

On the other hand, focusing on upper and graduate level non-security courses can help address one major concern that integrating cybersecurity topics "means something else will have to be sacrificed" [3] in those non-security courses. We observed that *instructors of upper and graduate level courses often travel to conferences and meetings during the semesters*, and sometimes are not able to make up all the missed class sessions. Such missed class sessions are excellent opportunities for cybersecurity researchers to integrate or inject relevant topics into non-security courses.

In our implementation, we talked with five instructors of upper or graduate level non-security courses at two institutions, and easily obtained such opportunities to discuss relevant cybersecurity topics in six 75-minute class sessions in two semesters as shown in Table 1. Note that *session symbol* is used for ease of presenting results in the next section, and *class size* is the number of students who attended the corresponding class session; OS1 and OS2 are the same course offered in two consecutive semesters, and we presented the same cybersecurity topic in the two sessions. The five integration opportunities obtained from Institution I were all due to the travels of the corresponding instructors. The integration opportunity obtained from Institution II was due to an invited talk, and the activity can be considered as a trial adoption of our implementation solution in an institution where no faculty member is actively doing cybersecurity research.

The cybersecurity topics are identified based on our discussions with the instructors. All the topics are very relevant to the corresponding non-security courses, and they meet the needs of those courses from different perspectives.

The OpenSSL Heartbleed vulnerability was publicly disclosed in April 2014; right after the instructor of the Computer Communication course introduced the TCP/IP protocols in the class, we used one class session to present the technical details, the impact, and the security patch of the Heartbleed vulnerability as well as the following up suggestions and recommendations from the cybersecurity research community. Students in the Software Engineering course had a strong demand on learning the knowledge and skills for building user authentication components in software; we used one class session to introduce the challenging problems, different solutions, and best practices in building password-based user authentication systems. Students in the Operating Systems course wanted to learn more about the security of the Virtual Machines (VMs) and Virtual Machine Monitors (VMMs); we used one class session to introduce the useful Virtual Machine Introspection (VMI) mechanisms and discuss the related research topics on bridging the semantic gaps in VMI. The instructor of the Software Testing course hoped to help students learn something about the security of mobile apps and about using software engineering techniques such as program slicing in security; we used one class session to illustrate the common cryptographic misuses in Android apps and explain the secure coding practices to the students. The instructor of the Computer Networks course at Institution II hoped to introduce some latest cybersecurity related topics to students for their potential undergraduate honor's projects; we used one class session to discuss the basic concepts and

problems as well as interesting research topics in Web security and privacy.

The instructors of those five non-security courses and many students informally praised our effort afterwards. In the next section, we present and analyze students' responses to our formal questionnaires.

4. Results

We designed five anonymous questionnaires and collected the data at the end of each class session from all the participating students. Basically, fourteen questions are common in those five questionnaires, and they include three general questions, ten questions based on students' overall perception of the cybersecurity topic discussed in the class session, and one open comments question. Meanwhile, in each questionnaire, there are eight to twelve questions specific to the cybersecurity content discussed in the class session for evaluating the corresponding learning effectiveness.

4.1. Common Questions and Results

The fourteen common questions are listed in Table 2, and we use S1~S14 to label them because most of them (except for S3 and S14) are designed as five-point Likert-scale statements. We converted the five answer options for Likert-scale statements to numeric values where value 1 stands for "Strongly Disagree", value 2 stands for "Disagree", value 3 stands for "Neither Agree Nor Disagree", value 4 stands for "Agree", and value 5 stands for "Strongly Agree". Similarly, we converted the knowledge and skills rating for S3 to numeric values from 1 to 5 corresponding to the five answer options from "clueless" to "total guru". Strictly speaking, since the responses are ordinal data, they do not necessarily have interval scales. We performed such conversions simply to ease the comparison of the responses from a relative perspective.

Figure 1 is the box (and whisker) plot of the mean ratings to S1~S13 from the six class sessions. In other words, to focus on the comparison of different class sessions and to save space, we calculated the mean ratings to S1~S13 for each class session, and then drew the box plot of the six mean values (of the six class sessions) for each question; we further verified the rating distribution of each question for each individual course to make sure the wording in the following result presentation is accurate. In addition to representing the standard statistics such as quartiles, median, whiskers, and outliers, each box plot in this paper also depicts the mean value using a small solid square (▪) for us to more comprehensively capture the central tendency of the distribution. Overall, all the thirteen box plots have small spread (the interquartile range) values, indicating the consistence of the mean ratings among the six class sessions for all the thirteen questions.

Table 2. Fourteen Common Questions

General questions:
S1: Learning cybersecurity knowledge and skills is important for computer science students.
S2: I am interested in learning cybersecurity knowledge and skills.
S3: Please rate your current cybersecurity knowledge and skills: (clueless, beginner, intermediate, advanced, total guru)
Questions based on your overall perception of the cybersecurity topic discussed in today's class:
S4: The cybersecurity topic discussed in today's class is interesting.
S5: The cybersecurity topic discussed in today's class is difficult.
S6: The cybersecurity topic discussed in today's class is useful.
S7: The cybersecurity topic discussed in today's class is relevant to this course.
S8: The cybersecurity topic discussed in today's class improved my cybersecurity knowledge and skills.
S9: The cybersecurity topic discussed in today's class is helpful for me to prepare for my career.
S10: The instructor(s) effectively discussed the cybersecurity topic in today's class.
S11: I effectively learned the cybersecurity topic discussed in today's class.
S12 I would like to have cybersecurity topics discussed in other non-cybersecurity courses in the future.
S13: Today's class motivates me to systematically learn cybersecurity knowledge and skills in the future.
Open comments question:
S14: Please write down comments and suggestions about today's class and learning cybersecurity knowledge and skills in general.

For the three ***general questions S1~S3***, their box plots show most students in all the six class sessions agreed or strongly agreed that learning cybersecurity knowledge and skills is important for computer science students (S1), and they are interested in learning cybersecurity knowledge and skills (S2); however, they also acknowledged that their current cybersecurity knowledge and skills are still limited to the "beginner" and "intermediate" levels (S3). The lower outlier for S1 is the Software Testing class session, and its low mean rating value is attributed to one student who disagreed with that statement and is also related to the small size of the class; the upper whisker for S1 is the Software Engineering class session, indicating that its stu-

dents are well aware of the importance of cybersecurity. The upper outlier for S3 is the Computer Communication class session that has about half master students and half PhD students, while the lower whisker for S3 is the Software Testing class session.

The box plots for the ***questions S4, S6, and S7*** clearly show most students in all the six class sessions agreed or strongly agreed that the discussed cybersecurity topics are interesting (S4), useful (S6), and relevant to the corresponding courses (S7). The mean ratings to these three questions are highly consistent among the six class sessions; meanwhile, all the three box plots exhibit the symmetry (less skewness because the median is almost in the center of the box) of the distribution while none of them contains any outlier. The box plot for ***question S5*** shows that overall, the difficulty levels of those cybersecurity topics are neither too difficult nor too easy just as intended, with the first OS class session as the upper whisker and the Computer Communication class session as the lower whisker. The results of these four questions demonstrate that our efforts in discussing with the instructors and in selecting and preparing for the topics are worthwhile.

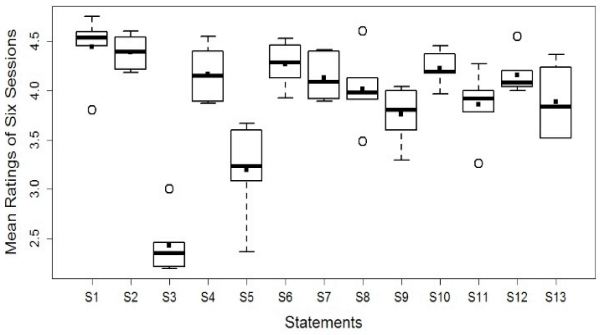

Fig 1. Mean Ratings of Six Class Sessions to S1~S13

For the ***question S8***, the mean ratings from four class sessions are centered on agreeing that "the cybersecurity topic discussed in today's class improved my cybersecurity knowledge and skills". The upper outlier for S8 is the Software Testing class session probably due to the limited prior cybersecurity knowledge and skills in its students (the lower whisker for S3), while the lower outlier for S8 is the first OS class session, probably due to the high difficulty level perceived by its students (the upper whisker for S5). For the ***question S9***, the overall agreement level is still positive, but it is not as high as those for most other questions probably because it takes time to predict if what students learned in the class will be helpful for them to prepare for their career.

The ***questions S10 and S11*** are more related to the teaching and learning effectiveness. Overall, most students agreed that the instructor(s) effectively discussed the corresponding cybersecurity topic in the class (S10), with the Computer Communication class session as the upper whisker and the first OS class session as the lower whisker. Most students also agreed that they effectively learned the corresponding cybersecurity topics discussed in the class (S11), with the Computer Communication class session as the upper whisker and the first OS class session as the lower outlier. Correlating these results to that for the question S5, while we cannot draw definitive conclusions as these results are only correlations, it is possible that more difficult topics will result in lower teaching and learning effectiveness ratings.

The mean rating distribution for the ***question S12*** is a very positive sign showing that most students in all the six class sessions enjoyed our activities and they would like to have cybersecurity topics discussed in other non-cybersecurity courses in the future. The upper outlier for S12 is the Computer Communication class session, while the lower whisker for S12 is the first OS session. The mean rating distribution for the ***question S13*** is also positive, indicating that our activities can to certain extent motivate students to learn cybersecurity knowledge and skills in the future. The upper whisker for S13 is the Computer Communication class session.

Some students also answered the open comments ***question S14***. In most cases, students appreciated our effort and further agreed to add more security contents into non-cybersecurity courses. Some students expressed that they need to study more cybersecurity knowledge and skills. Some other students commented about the technical details of the cybersecurity topics.

4.2. Specific Questions and Results

Each questionnaire also contains some questions specific to the cybersecurity content discussed in the class session. The questions are designed in pairs for us to evaluate the learning effectiveness in terms of the students' understanding of certain details of the discussed content (**B**)efore the class session and (**C**)urrently. All these questions are five-point Likert-scale statements (labeled as Special Statements SS#B and SS#C for "before" and "currently", respectively), and their answer options are converted to numeric values in the same way as described in Section 4.1. Due to space limitation, we only list the specific questions for two courses Software Engineering and Operating Systems in Tables 3 and 4, respectively; these two courses account for the three largest class sessions (SE, OS1, OS2) as shown in Table 1. We present the details of these three class sessions while only briefly summarize the results of the other three class sessions (CC, ST, CN).

Table 3. Specific Questions for Software Engineering

SS1B: I clearly understood that weak password, password reuse, and phishing are the essential problems of password security before today's class.
SS1C: Currently, I clearly understand that weak password, password reuse, and phishing are the essential problems of password security.
SS2B: I clearly understood that servers should use password checking techniques to help users avoid weak passwords before today's class.
SS2C: Currently, I clearly understand that servers should use password checking techniques to help users avoid weak passwords.
SS3B: I clearly understood that servers should only save salted and hashed passwords before today's class.
SS3C: Currently, I clearly understand that servers should only save salted and hashed passwords.
SS4B: I clearly understood the basic idea of Web Single Sign-On (SSO) user authentication systems before today's class.
SS4C: Currently, I clearly understand the basic idea of Web SSO user authentication systems.
SS5B: I clearly understood that HTTPS should be used by the Web SSO relying parties before today's class.
SS5C: Currently, I clearly understand that HTTPS should be used by the Web SSO relying parties.
SS6B: I clearly understood that Web SSO phishing attacks can be very profitable, insidious, and hard to detect before today's class.
SS6C: Currently, I clearly understand that Web SSO phishing attacks can be very profitable, insidious, and hard to detect.

Figure 2 illustrates the box plots of the ratings to the 12 (or six paired) specific software engineering questions listed in Table 3. Comparing the paired distributions of the ratings, we can clearly see that students improved their understanding of the password security and password-based user authentication systems by attending our cybersecurity session. Median and mean ratings for all the six paired questions are improved ("currently" vs. "before"), and the spread for all the ratings to the current understanding are relatively small. Except for two lower outliers (for SS4C and SS5C) and two lower whiskers (for SS3C and SS4C), all other ratings are very positive. Using the paired t-test to compare the mean ratings (solid squares ▪) for each pair of the questions, we found that the mean rating improvements are statistically significant (at the 0.05 significance level) for all the six pairs, with p-values: $p = 0.032$, $p = 0.002$, $p < 0.001$, $p < 0.001$, $p < 0.001$, and $p < 0.001$ for the six tests, respectively.

Figures 3 and 4 illustrate the box plots of the ratings to the 10 (or five paired) specific operating systems questions listed in Table 4 for class sessions OS1 and OS2, respectively. Note that although we have the words "before reading the paper …" in those SS#B statements, the link to the paper was not available to students in advance due to technical issues. Comparing the paired distributions of the ratings in each individual figure, we can clearly see that students improved their understanding of the IDS and VMI related concepts by attending our cybersecurity session. Median ratings are improved for three paired questions in Figure 3, and for all the five paired questions in Figure 4. Mean ratings for all the five paired questions are improved in both class sessions, and the spread for all the ratings to the current understanding are also relatively small in both figures. Using the paired t-test to compare the mean ratings for each pair of the questions in both sessions, we found that the mean rating improvements are statistically significant (at the 0.05 significance level) for all the five pairs in both sessions: in the OS1 session, the p-values are: $p = 0.011$, $p < 0.001$, $p < 0.001$, $p < 0.001$, and $p = 0.003$ for the five tests, respectively; in the OS2 session, the p-values are: $p = 0.005$, $p < 0.001$, $p = 0.009$, $p < 0.001$, and $p < 0.001$ for the five tests, respectively.

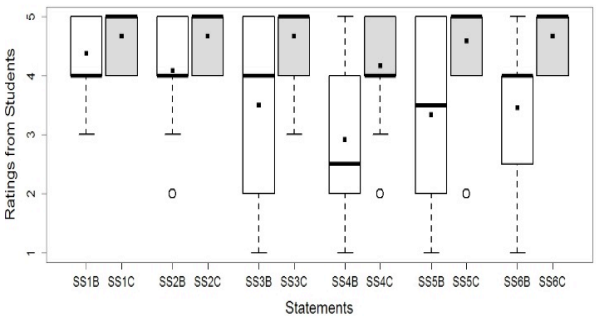

Fig 2. Ratings to Specific Software Engineering Questions

Further using the unpaired t-test, we compared the ratings to the 10 questions between the two OS sessions, i.e., between SS1B in OS1 and SS1B in OS2, between SS1C in OS1 and SS1C in OS2, and so on. For all the 10 tests, the mean rating differences are not statistically significant (at the 0.05 significance level) with all the 10 p-values greater than 0.05.

We also analyzed the ratings to the specific questions for the other three class sessions (CC, ST, CN). We have 8 (or four paired) specific questions for each of those three class sessions. While the rating distributions are improved for all the questions in the three class sessions, the mean rating improvements are statistically significant (based on the paired t-test at the 0.05

significance level) only for some of those questions partially due to the small sample sizes in those three class sessions.

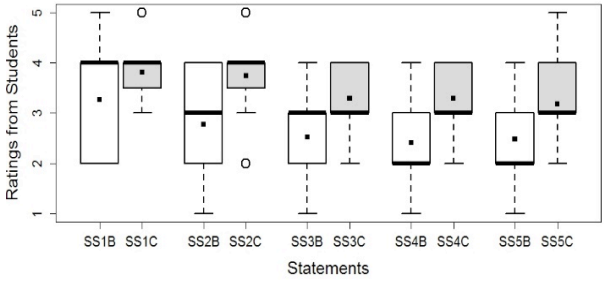

Fig 3. Ratings to Specific OS Questions for Session OS1

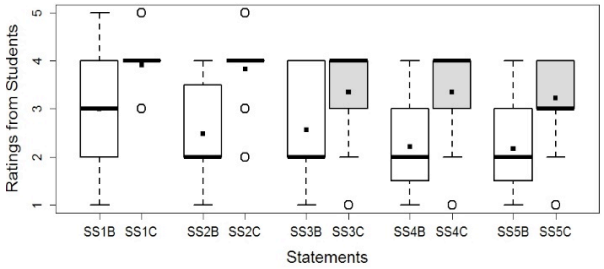

Fig 4. Ratings to Specific OS Questions for Session OS2

4.3. Summary of Results and Discussion

Overall, from the results for the common questions presented in Section 4.1, we can clearly see that most students agree with the importance of learning cybersecurity knowledge and skills (S1), they consider their cybersecurity knowledge and skills as limited (S3), and they are interested in learning more about cybersecurity (S2); most students agree that our discussed cybersecurity topics are interesting (S4), useful (S6), and relevant to the corresponding courses (S7); most students agree that the discussed topics are neither too difficult nor too easy (S5), and our activities improved their cybersecurity knowledge and skills (S8); most students agree that instructor(s) effectively discussed the corresponding cybersecurity topics in the class (S10), they effectively learned the corresponding topics (S11), and they would like to have cybersecurity topics discussed in other non-cybersecurity courses in the future (S12). Our activities also to certain extent help students prepare for their career (S9) and motivate them to learn cybersecurity knowledge and skills in the future (S13). From the results for the specific questions presented in Section 4.2, we can clearly see that students effectively learned the corresponding cybersecurity topics discussed in the class sessions; the paired t-test results indicate that the improvements of students' understanding on the discussed topics are statistically significant at least in the three sessions with the largest sample sizes.

Table 4. Specific Questions for Operating Systems

SS1B: I understood the basic idea of the Intrusion Detection System (IDS) before reading the paper recommended by the instructor(s) and before today's class.
SS1C: Currently, I clearly understand the basic idea of IDS.
SS2B: I understood that VMI can be useful in security systems such as IDS before reading the paper recommended by the instructor(s) and before today's class.
SS2C: Currently, I clearly understand that VMI can be useful in security systems, especially IDS.
SS3B: I understood the technical details about using VMI in security systems, especially IDS, before reading the paper recommended by the instructor(s) and before today's class.
SS3C: Currently, I clearly understand the technical details about using VMI in security systems, especially IDS.
SS4B: I understood the meaning of the semantic gap in VMI before reading the paper recommended by the instructor(s) and before today's class.
SS4C: Currently, I clearly understand the meaning of the semantic gap in VMI.
SS5B: I understood the difference between the weak semantic gap and the strong semantic gap in VMI-based security systems, especially IDS, before reading the paper recommended by the instructor(s) and before today's class.
SS5C: Currently, I clearly understand the difference between the weak semantic gap and the strong semantic gap in VMI-based security systems, especially IDS.

While we justified in Section 3 that our implementation solution to the security integration approach is viable, we acknowledge that some limitations exist in our solution and in its effectiveness evaluation. For example, in terms of the implementation solution itself, the identified cybersecurity topics are discussed only through presentations and Q&A in one class session, while other methods such as laboratory exercises [15, 16] and capstone projects are not explored in our study; in terms of the effectiveness evaluation, we only used questionnaires and did not try other techniques such as quizzes and formal knowledge and skill assessments yet. Although these limitations can be largely attributed to the limited amount of time available for us to inject the cybersecurity topics into the non-security courses, we are still very grateful to those instructors who enabled us to make our existing solution viable. In the future, it is possible for us to further address some of those limitations by having discussions with more educators and

incorporating some other appropriate methods and techniques into our implementation and evaluation.

5. Conclusion

We advocated to further explore the security integration approach to complement other approaches and better promote cybersecurity education. We contributed to this approach by concretely exploring a viable implementation solution and evaluating its effectiveness. Specifically, we explored to discuss relevant cybersecurity topics in upper and graduate level non-security courses to engage students in learning cybersecurity knowledge and skills from the perspectives of different computer science sub-areas, and help them understand the correlation and interplay between cybersecurity and other sub-areas of computer science. Our experience in six class sessions of five non-security courses is very encouraging: the majority of students found the discussed cybersecurity topics interesting, useful, and relevant; they would like to have cybersecurity topics discussed in other non-cybersecurity courses in the future; they improved their understanding of the discussed content. We will continue to discuss with instructors and obtain opportunities to integrate relevant cybersecurity topics into other non-security courses. We share our developed materials including questionnaires with other educators to make our effort more duplicable. We hope our experience can be helpful for other educators to adopt and further explore the security integration approach in the future.

Acknowledgments: We sincerely thank anonymous reviewers for their valuable comments and suggestions. We also sincerely thank all the instructors and students who have participated in our security integration activities. This research was supported in part by the NSF grant DGE-1619841.

References

[1] P. Bowen, J. Hash, and M. Wilson, "Information Security Handbook: A Guide for Managers", in NIST Special Publication 800-100, 2007.

[2] "Curriculum Guidelines for Undergraduate Degree Programs in Computer Science", The Joint Task Force on Computing Curricula, ACM and IEEE Computer Society, 2013.

[3] P. Mullins, J. Wolfe, M. Fry, E. Wynters, W. Calhoun, R. Montante, and W. Oblitey, "Panel on integrating security concepts into existing computer courses", In Proc. of the ACM Technical Symposium on Computer Science Education (SIGCSE), 2002.

[4] G. White and G. Nordstrom, "Security Across the Curriculum: Using Computer Security to Teach Computer Science Principles", In Proc. of the National Information Systems Security Conference, 1996.

[5] C. E. Irvine, S. K. Chin, and D. Frincke, "Integrating Security into the Curriculum", Electrical Engineering and Computer Science, 1998.

[6] R. Vaughn, "Application of Security to the Computing Science Classroom", In Proc. of the ACM Technical Symposium on Computer Science Education (SIGCSE), 2000.

[7] L. Null, "Integrating security across the computer science curriculum", J. Comput. Sci. Coll. 19, 5, 2004.

[8] L. F. Perrone, M. Aburdene, and X. Meng, "Approaches to Undergraduate Instruction in Computer Security", In Proc. of the American Society for Engineering Education Annual Conference & Exposition (ASEE), 2005.

[9] T. Howles, C. Romanowski, S. Mishra, and R. K. Raj, "A Holistic, Modular Approach to Infuse CyberSecurity into Undergraduate Computing Degree Programs", In Proc. of the Annual Symposium on Information Assurance (ASIA), 2011.

[10] B. Taylor and S. Azadegan, "Moving beyond security tracks: integrating security in CS0 and CS1", In Proc. of the ACM Technical Symposium on Computer Science Education (SIGCSE), 2008.

[11] S. A. Markham, "Expanding security awareness in introductory computer science courses", In Proc. of the Information Security Curriculum Development Conference (InfoSecCD), 2009.

[12] S. Kaza, B. Taylor, H. Hochheiser, S. Azadegan, M. O'Leary, and C. F. Turner, "Injecting Security in the Curriculum – Experiences in Effective Dissemination and Assessment Design", In Proc. of the Colloquium for Information Systems Security Education, 2010.

[13] Siraj, S. Ghafoor, J. Tower, and A. Haynes, "Empowering faculty to embed security topics into computer science courses", In Proc. of the Conference on Innovation & technology in computer science education (ITiCSE), 2014.

[14] M. Whitney, H. L-R, B. Chu, and J. Zhu, "Embedding Secure Coding Instruction into the IDE: A Field Study in an Advanced CS Course", In Proc. of the ACM Technical Symposium on Computer Science Education (SIGCSE), 2015.

[15] W. Du and R. Wang, "SEED: A Suite of Instructional Laboratories for Computer Security Education", Journal on Educational Resources in Computing, 8, 1, 2008.

[16] C. Yue, W. Zhu, G. Williams, and E. Chow, "Using Amazon EC2 in Computer and Network Security Lab Exercises: Design, Results, and Analysis", In Proc. of the American Society for Engineering Education Annual Conference & Exposition (ASEE), 2012.