Layering Sociotechnical Cybersecurity Concepts Within Project-Based Learning

Brandt Redd
brandt.redd@utah.edu
University of Utah
Salt Lake City, Utah, USA

Ying Tang
yingtang@swu.edu.cn
Southwest University
Chongqing, China

Hadar Ziv
ziv@ics.uci.edu
University of California, Irvine
Irvine, California, USA

Sameer Patil
sameer.patil@utah.edu
University of Utah
Salt Lake City, Utah, USA

ABSTRACT

Motivation: The increasing volume and frequency of cyberattacks have made it necessary that all computing professionals be proficient in security principles. Concurrently, modern technology poses greater threats to privacy, making it important that technological solutions be developed to respect end-user privacy preferences and comply with privacy-related laws and regulations. Just as considering security and privacy must be an integral part of developing any technological solution, *teaching* security and privacy ought to be a *required* aspect of computer science education.

Objective: We set out to demonstrate that a project-based capstone experience provides an effective mechanism for teaching the foundations of security and privacy.

Method: We developed ten learning modules designed to introduce and sensitize students to foundational sociotechnical concepts related to the security and privacy aspects of modern technology. We delivered the modules in the treatment sections of a two-term capstone course involving the development of software solutions for external clients. We asked the students in the course to apply the concepts covered in the modules to their projects. Control sections of the course were taught without the modules as usual. We evaluated the effectiveness of the modules by administering pre-treatment and post-treatment assessments of cybersecurity knowledge and collecting written student reflections after the delivery of each module.

Results: We found that the students in the treatment condition exhibited statistically significant increases in their knowledge of foundational security and privacy concepts compared to those in the control condition without the modules. Further, student reflections indicate that they appreciated the content of the modules and were readily able to apply the concepts to their projects.

Discussion: The modules we developed facilitate embedding the teaching of security and privacy within any project-based learning experience. Embedding cybersecurity instruction within capstone experiences can help create a software workforce that is more knowledgeable about sociotechnical cybersecurity principles.

CCS CONCEPTS

• **Security and privacy** → **Human and societal aspects of security and privacy**; **Software and application security**;

KEYWORDS

Cybersecurity Education, Security, Privacy, Capstone Experience, Project-Based Learning

ACM Reference Format:
Brandt Redd, Ying Tang, Hadar Ziv, and Sameer Patil. 2024. Layering Sociotechnical Cybersecurity Concepts Within Project-Based Learning. In *ACM Conference on International Computing Education Research V.1 (ICER '24 Vol. 1), August 13–15, 2024, Melbourne, VIC, Australia.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3632620.3671093

1 INTRODUCTION

Security and privacy threats to users of computer systems are at or near an all-time high [9]. Yet, graduates from computing and technology-related programs are often unprepared to identify and address security and privacy issues when designing and implementing software solutions [29]. There is a worldwide shortage of professionals trained in cybersecurity principles [8]. Degrees or specialized curricular tracks dedicated to cybersecurity are one way to fill the shortfall. The US National Centers of Academic Excellence in Cybersecurity publishes requirements and offers designations for such programs [30]. However, not all computing students participate in these programs. Given that nearly all modern technologies impinge upon security and privacy, it is increasingly important that *all* students of computing-related programs, such as Computer Science, Software Engineering, and Informatics, graduate with at least a basic understanding of foundational security and privacy concepts. Imparting such an understanding as a component of every computing program would require that security and privacy training not be relegated merely to isolated elective courses as is typically the case [4]. Just as enhancing security and privacy support in technology requires incorporating it from the outset in all phases of design and development, enhancing the learning of foundational security and privacy concepts requires that *teaching* these concepts be a *mandatory* component within all computing curricula.

ICER '24 Vol. 1, August 13–15, 2024, Melbourne, VIC, Australia

ACM ISBN 979-8-4007-0475-8/24/08
https://doi.org/10.1145/3632620.3671093

Since project-based capstone experiences are mandatory in many computing programs, they offer a promising avenue for delivering knowledge about foundational sociotechnical concepts in security and privacy to students on the cusp of joining the technology workforce. Not only does the approach avoid the burden of an additional course on security and privacy, it also provides students the immediate opportunity for practical application of the learned concepts in real-world or realistic software projects. We measured the feasibility and effectiveness of the approach via the following research question:

> **RQ:** Can integrating learning modules on foundational sociotechnical cybersecurity concepts within a project-based capstone experience improve student understanding of these concepts?

To address the research question, we developed a set of ten learning modules on core cybersecurity concepts covering the most important technical and social aspects related to security and privacy. The modules covered topics such as threats and adversaries, risk assessment, data protection, intrusion detection, and network security. We integrated these modules within a section of a two-term capstone course in Informatics taught by the third author at the University of California, Irvine. The project-based capstone experience requires students to develop and deliver software solutions for external clients from industry, non-profits, or academia. We measured the effectiveness of the intervention to promote learning by developing and administering an assessment of cybersecurity knowledge at the beginning and end of the course and by including questions about the cybersecurity modules in the reports the students submitted after completing each module. In addition, we administered the same Cybersecurity Knowledge Assessment at the beginning and end of control sections of the same course taught by other instructors without the cybersecurity learning modules. At the end of the capstone experience, we found that the students in the treatment condition showed statistically significant improvement in their understanding of technical aspects of security and social aspects of security as well as privacy. Student reflections indicated that the students found the cybersecurity learning modules to be beneficial and relevant for their projects and their upcoming industry careers.

Our study makes the following contributions:

- We demonstrate the feasibility and effectiveness of embedding the teaching of foundational sociotechnical cybersecurity concepts within project-based courses, such as the capstone experience.
- We show that it is valuable to teach foundational cybersecurity concepts to upper-division computing students for application in real-world software projects.
- We provide ten cybersecurity learning modules and a Cybersecurity Knowledge Assessment that instructors can adapt and reuse to embed cybersecurity instruction within project-based software courses.

In the following sections, we first situate our research within the literature. We then describe the development, delivery, and assessment of the cybersecurity learning modules along with pertinent background on the capstone course in which we embedded the modules. Next, we present the results of analyses comparing cybersecurity-related learning in the treatment section of the course that incorporated the modules with that in the control sections without the modules. We proceed to discuss the salient insight from our findings and conclude with remarks on how our approach can help create a cybersecurity-proficient technology workforce.

2 RELATED WORK

We first discuss the approaches to teaching cybersecurity that are explored in the literature. We then delve deeper into research efforts that follow the embedded approach to integrate cybersecurity instruction within existing courses. In addition, we cover the assessment of cybersecurity-related learning connected to the instructional interventions.

2.1 Approaches to Teaching Cybersecurity

In 2017, a joint task force with representatives from the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers Computer Society (IEEE CS), the Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education produced Cybersecurity Curricular Guidelines (CSEC 2017) [18] targeted at higher education institutions. The guidelines are intended to be applied in three ways: 1) to develop dedicated cybersecurity programs, 2) to augment existing programs such as dedicated courses or program emphases, and 3) to incorporate cybersecurity content into existing courses. Yet, few computer science programs currently include mandatory cybersecurity courses or embed cybersecurity instruction within existing courses [6, 29].

Crick et al. [7] have described two approaches to teaching cybersecurity: 1) packaging cybersecurity instruction into a single course and then referencing the content in other courses as appropriate, and 2) embedding cybersecurity instruction across the entire curriculum. A dedicated course can make more effective use of the small number of faculty with relevant cybersecurity expertise and make it easier to focus the learning on cybersecurity-relevant issues. However, Crick et al. [7] did not comment on which of the two strategies is more effective.

The literature indicates that the dedicated and embedded approaches to cybersecurity instruction offer complementary strengths. Courses dedicated to cybersecurity topics are well-suited for teaching concepts like secure coding practices and data security [4]. Moreover, courses in applied cryptography, information and communication security, privacy, and cybercrime can help address the growing need for cybersecurity-aware computing professionals [14]. Alternatively, embedding cybersecurity principles in existing courses serves to teach the principles *in context* [19, 22]. For instance, to ensure that students are able to connect the learned principles to real-world applications, embedded cybersecurity instruction can leverage techniques such as the case method [5], realistic games [15], etc.

2.2 Integration of Cybersecurity Instruction in Existing Courses

Embedded cybersecurity instruction has been characterized as a "security integration approach" [33]. Yue et al. [33] employed the

security integration approach in six courses by integrating a 75-minute presentation on security principles. Student responses to the post-presentation questionnaire on the learning experience demonstrated the promise of the approach to help students recognize the importance of learning about security and privacy [33]. However, the instruction was limited to a single session and the results are based only on post-session self-reports. In contrast, our study included significantly broader and deeper coverage of cybersecurity concepts, and we evaluated learning more systematically with a knowledge assessment carried out before and after the instruction.

In a more comprehensive application of embedded cybersecurity instruction, Taylor and Kaza [27] developed "security injection modules" in multiple programming languages to teach security awareness and secure coding practices within early programming courses (i.e., CS0–CS2). Comparison between pre-instruction and post-instruction assessments at five universities showed that the modules resulted in statistically significant improvement in student learning in most cases [27]. Our study uses a format similar to that used by Taylor and Kaza [27] with a pre-treatment assessment followed by the treatment (i.e., the learning modules), concluding with a post-treatment assessment. Instead of targeting introductory courses, we applied the embedded instructional approach in an existing upper-division course to be able to build on knowledge from lower-division courses. As a result, we could cover more advanced cybersecurity topics, such as applied cryptography, denial of service, data assurance, and network security.

Specifically, our study was conducted in the context of a project-based capstone experience. An advantage of project-based courses is that students can immediately apply the concepts they learn. For instance, students indicated being more comfortable with their major and having greater confidence in their ability to apply their computing skills after completing a course involving humanitarian free and open source projects [17]. In capstone experiences, students typically work on a project, often from an external client, and deliver a solution that requires them to engage in the full development cycle [32]. Therefore, project-based capstone courses provide a good opportunity for embedding the instruction of security and privacy principles within course content. The connection to industry is an additional valuable feature of project-based capstone courses. Faculty who teach information assurance and security courses have reported that industry-related content is relevant for their courses [31].

As a specific example, Jackson State University updated the learning objectives of their existing capstone course to include systems-security and software-security topics in coordination with two new elective courses—Systems and Software Security and Advanced Information Security—either of which could be taken concurrently with the capstone course [22]. The instructors of the capstone course strove to have at least one member of each project team take one of the two elective security courses. The approach raised student self-evaluations of security competency from a mean of 1.40 to 3.55 on a four-point scale [22]. The program-wide nature of the intervention meant that the results could not be compared with those from a control group that did not receive the treatment. In contrast, we incorporated a control condition without the embedded cybersecurity instruction to provide more robust results.

Moreover, the intervention at Jackson State University was limited to only the technical aspects of security, with the evaluation based on self-reports in faculty and student surveys [22]. We covered cybersecurity topics more broadly by including *sociotechnical* aspects of security along with privacy. Based on a survey of practices and recommendations regarding cybersecurity teaching in the United Kingdom, Crick et al. [7] have noted that there is a "need for both the academic and human skills." To that end, Parish et al. [23] have called for treating cybersecurity as a 'meta-discipline' with principles that span across conventional technical disciplines, such as Computer Science, Information Technology, Information Systems, and Computer Engineering, and non-technical fields, such as Sociology and Law.

2.3 Assessmment of Cybersecurity Learning

In seeking an objective assessment of basic cybersecurity knowledge to measure cybersecurity-related learning, we consulted various existing instruments to measure knowledge and behavior regarding computer security. For instance, Spitzberg's [24] measure of Computer-Mediated Communication (CMC) Competence focuses on competence in using online communication applications, such as email and social media. While the assessment touches on security and privacy awareness, it is not technical in nature. The Security Behavior Intentions Scale (SeBIS) measures security-related behavioral intentions [10]. Like Spitzberg's [24] measure, SeBIS focuses on *end-user* competence and does not measure the technical knowledge and skills needed by those who *develop* technology-based solutions. Having failed to identify an appropriate and up-to-date existing assessment of cybersecurity knowledge, we found it necessary to develop our own assessment to measure foundational security and privacy knowledge, covering relevant technical and social aspects (see Section 3.3).

3 METHOD

We developed a set of learning modules on foundational cybersecurity concepts covering the most important technical and social aspects related to security and privacy. We integrated these modules within a two-term capstone course in Informatics at the University of California, Irvine. In this section, we describe the development, content, and delivery of the modules, along with relevant information about the capstone course. To measure the pedagogical effectiveness of our instructional approach, we constructed an instrument for assessing foundational sociotechnical cybersecurity knowledge and used it in a quasi-experimental setup.

3.1 Learning Modules

We developed ten cybersecurity learning modules for embedding in upper-division undergraduate courses based extensively on hands-on team projects that typically span multiple academic terms and involve developing practical, real-world solutions for external clients. Capstone courses of such nature are increasingly *required* in core curricula in the computing disciplines [28].

We designed the ten modules to form a cohesive set to facilitate the learning of foundational sociotechnical cybersecurity concepts (see Table 1). Each module contains a short instructional video

Table 1: The delivery schedule and contents of each of the ten cybersecurity learning modules we developed to embed in project-based upper-division undergraduate courses in the computing disciplines.

Sprint	Module	Topics
3	1. Threats and Adversaries	– Threats to security and privacy with real-world examples – The Confidentiality, Integrity, Availability (CIA) triad – Common attack types
	2. Basic Risk Assessment	– Risk assessment: Threats, Vulnerabilities, and Consequences – The NIST (National Institute for Standards and Technology) standard for risk assessment – Risk identification tools
4	3. Vulnerability Management	– Examples of vulnerability exploitation – Vulnerability scans – Update management
	4. Secure Software Development Lifecycle	– Security by design – Security training, threat modeling, and secure development – Static code analysis, dynamic analysis, and incident response
5	5. Cryptography and Public Key Infrastructure (PKI)	– Symmetric and asymmetric encryption – Application of encryption and PKI – Securing the World Wide Web (WWW)
	6. Data Security	– Three data states: Data-at-rest, Data-in-transit, and Data-in-use – Network security implementation – Salted hashes for password storage
6	7. Intrusion Detection	– Intrusion Detection Systems (IDS) – Malware detection – Log analytics – Distributed Denial of Service (DDoS) attacks
	8. User Experience and Usability	– Human factors in system security – Secure user experience (UX) design – Privacy settings
7	9. Ethics	– Ethical responsibilities of application developers – Ethical security testing
	10. Compliance	– Regulatory compliance – Jurisdictional considerations – Important privacy laws and regulations

between 11 to 20 minutes in length, integrated within a corresponding lesson plan. We consulted industry professionals to help us determine the key topics to cover in the learning modules. We created the video content by incorporating input from the industry professionals regarding foundational sociotechnical security and privacy knowledge valued in the field. We designed the modules with the goal of *familiarizing* students with important sociotechnical privacy and security concepts, thereby encouraging them to consider these aspects in the context of their capstone projects. Since technical and social aspects of cybersecurity are too vast and complex to be covered in depth in a few short modules, the modules refer students to online cybersecurity resources should they desire more in-depth coverage beyond the introductory knowledge included in the modules. We used standard terminology common in the field and industry, further facilitating student searches for additional reference material on their own. Since the learning modules target upper-division undergraduates in computing-related disciplines, we assumed knowledge of computing fundamentals taught in lower-division computing courses.

We designed each learning module to cover the foundational knowledge pertaining to its respective topic while making explicit connections to relevant technical and social aspects of security and privacy. The second author (with expertise in learning sciences) created the initial module scripts and the accompanying learning aids, which subsequently underwent rigorous scrutiny and enhancement based on feedback from the fourth author (with expertise in security and privacy), followed by further refinement based on the input of the third author (the instructor of the treatment section of the capstone course with expertise in software engineering). Upon finalizing the module content, we employed a research assistant skilled in making e-learning resources to record the instructional videos.

We constructed each module by including the instructional videos within corresponding lesson plans that contained short learning activities to be performed before and after watching the

videos. The pre-video activities provided additional context and background for the video content, while the post-video activities were geared toward reflection on the video content and its application in the capstone projects. These activities were proposed by the second and the fourth authors, then vetted and refined in consultation with the third author (i.e., the course instructor) and two undergraduates who had previously taken the capstone course. The modules are included as supplemental material with the paper. They can be readily used by other instructors in their own courses.

3.2 Delivery of the Modules

We integrated the ten learning modules within a two-term undergraduate capstone course that is a *required* part of the Informatics curriculum at the University of California, Irvine. Students typically take this course in their final year, just prior to joining the workforce. The course involves teams of four to six students developing real-world solutions for external clients from large companies, startups, non-profits, government organizations, research labs, educational institutions, etc. Each project involves developing and delivering a software solution, at least at the functional prototype or proof-of-concept level. The teams employ typical software industry practices, including collecting requirements, documenting the design, developing mockups, and participating in regular reviews with clients. In the offerings of the course over a decade, only a handful of students within a cohort have had prior industry experience in the form of an internship or a job. The capstone course aims to provide real-world experience within a controlled and supervised setting to prepare students as future members of the technology workforce.

The capstone course spans two consecutive eleven-week terms, with ten weeks of instruction followed by a finals week. The teams follow the agile methodology [1], with projects organized in ten two-week sprints across the two terms. The finals week of the first term is used for intermediate presentations and demos of the projects. Similarly, the finals week of the second term is used for final presentations and demos.

For our research, we delivered the modules in the treatment section of the course ($n = 46$) taught by the third author in the Winter 2021 and Spring 2021 terms. Two other course sections, each taught by a different instructor without the cybersecurity learning modules, served as the control sections ($n = 96$). One control section was taught in the Fall 2020 and Winter 2021 terms, and the other was taught concurrently with the treatment section (i.e., Winter 2021 and Spring 2021 terms). All treatment and control sections were taught online due to the COVID-19 pandemic ongoing at the time. Students landed in the treatment or control sections depending on the section they chose when registering for the course. At the time of course registration, the students were unaware that some sections would include the cybersecurity learning modules. In all treatment and control sections, we administered the Cybersecurity Knowledge Assessment (see Section 3.3) at the beginning and end of the respective two-term course.

The students in the treatment section were organized into ten teams, each of which worked on developing a software solution commissioned by a different external client (see Table 2). As the treatment section of the course progressed, we delivered two modules per sprint. For determining the optimal schedule for delivering the modules, we leveraged our experience of embedding a privacy-focused design session within prior offerings of the course [25]. Since team formation and project detail are not completely finalized until the end of the first couple of sprints, we began the delivery of the modules at the beginning of the third sprint (see Table 1). The course schedule and logistics additionally required us to deliver all modules by the seventh sprint to leave enough time for applying the concepts during the last three sprints which typically involve heavy coding and implementation effort. Further, our module delivery schedule avoided creating an additional learning burden on the teams during the intense final weeks of the course.

Table 2: The clients and types of software projects for the ten teams in the treatment section of the capstone course.

Team	Type of Client	Type of Software Developed
1	Non-profit	Meeting and group management
2	Company	Remote and online therapy
3	University	Interactive information center
4	Company	Customer Relationship Management (CRM) systems integration
5	University	Medical imaging
6	Non-profit	Resource scheduling
7	University	Graphical social media
8	Non-profit	Business and charitable networking
9	Company	Custom content management
10	Company (startup)	Digital virtual assistance

We delivered the modules during the first week of the two-week sprints, enabling the students to use the second week to plan the application of the covered concepts to their projects during subsequent sprints. At the end of each sprint that contained the modules, we asked each team to respond to four learning reflection (LR) questions about the respective cybersecurity learning modules:

- LR1: What did you learn from the cybersecurity learning modules included in this sprint?
- LR2: What else would you like to know about the topics mentioned in the cybersecurity learning modules?
- LR3: Which of the topics covered in the cybersecurity learning modules apply to your project and in what ways?
- LR4: How could you implement these topics covered in the cybersecurity learning modules in your project?

The teams included the responses to the above questions as additional components in their sprint reflection reports for the respective sprints. While most learning reflections were submitted as collective team responses, there were a few cases in which students submitted individual answers to the reflection questions. Students in the control sections did not receive the learning reflection questions since they did not receive the cybersecurity learning modules. As mentioned above, we repeated the Cybersecurity Knowledge Assessment (see Section 3.3) after the projects were completed to measure changes in student understanding of foundational cybersecurity concepts between the beginning and the end of the course.

3.3 Cybersecurity Knowledge Assessment

We followed a pre-test—intervention—post-test pattern commonly used to evaluate educational interventions (e.g., [16, 21, 27]). Specifically, we used a quasi-experimental study design to measure learning [12]. As mentioned in Section 2, we created a new assessment for our research because we could not find a suitable existing one that covered technical and social dimensions of foundational security and privacy concepts.

We first determined that the assessment should cover technical and social aspects of security and privacy, measuring the level of understanding in each domain. The second author worked with two undergraduate research assistants in Informatics to brainstorm 36 questions and corresponding answer choices covering these four areas. The second, third, and fourth authors then collectively screened these questions and answer choices to select 15 of these questions by evaluating each candidate question via in-depth discussions based on their collective expertise in cybersecurity, software engineering, and learning sciences. The evaluation drew upon two inclusion criteria: 1) being closely related to either technical or social aspects of security or privacy and 2) being highly relevant to the security and privacy aspects likely to be encountered in typical upper-division software projects. We additionally sought to balance the number of questions in each area. We piloted the 15-question assessment by seeking feedback from undergraduate and graduate students and postdocs who were unconnected to the research. Feedback from this diverse set of individuals led to a few minor changes to the wording and composition of the questions and answer choices.

The 15 multiple-choice questions in the full assessment can be mapped into four quadrants: Security-Technical (5 questions), Privacy-Technical (3 questions), Security-Social (4 questions), and Privacy-Social (3 questions). Table 3 depicts the questions included in each quadrant. The full assessment with the answer choices associated with each question is provided in Appendix A. To counter potential order effects, we administered the assessment by presenting the questions in random order with the order of the answer choices corresponding to each question randomized as well.

All except one question (Q3) require the respondents to select multiple correct answer choices from the seven answer choices provided. We scored the assessment by awarding one point for each correct answer choice selected and one point for each incorrect answer choice *not* selected. In other words, we considered identifying the incorrect answers as equivalent to identifying the correct ones, yielding a maximum score of seven points per question. Since the sole multiple-choice question (Q3) has a single correct answer out of four options, we assigned seven points for the correct answer and zero for an incorrect answer in order to ensure that each question was weighted equally when scoring. Further, we normalized the total score for the questions in each of the four quadrants of the assessment to 25 points to assign equal weights to each quadrant within the maximum total score of 100.

3.4 Data Collection and Analyses

All data collection procedures were reviewed and approved by the Institutional Research Boards (IRBs) of our universities. We carefully addressed important ethical considerations as follows: First, the cybersecurity modules were a mandatory pedagogical component of the treatment section of the course, independent of the research. Second, student grades for the course were unconnected to their scores on the Cybersecurity Knowledge Assessment. Third, we guarded against perceived coercion by separating the data collection for the Cybersecurity Knowledge Assessment such that the course instructors of the treatment and control sections (including the third author) did not have access to the individual answers and scores. Fourth, we anonymized the assessment scores by employing a randomly generated unique code for each student. Fifth, none of the researchers other than the course instructor (i.e., the third author) were involved in the instruction and grading for the treatment section of the course, nor did they have access to the grades (in compliance with legal privacy requirements stipulated in the Family Educational Rights and Privacy Act [FERPA] that applies to student academic records in the United States).

3.4.1 Quantitative Analysis. Two students in the treatment section and eight in the control sections completed the Cybersecurity Knowledge Assessment at the beginning of the course but did not do so at the end of the course. Conversely, four students in the treatment section and two in the control sections who completed the Cybersecurity Knowledge Assessment at the end of the course did not do so at the beginning. Since measuring student learning requires comparing the assessment scores at the beginning and end of the course, we excluded the responses of these 16 students from analysis. After excluding the above 16 cases, we obtained complete and valid assessment data from 46 students in the treatment section and 96 students across the two control sections of the course.

We measured the internal consistency of the assessment using Cronbach's alpha [2] for the initial (pre) scores. We calculated the Cronbach's alpha values for the assessment as a whole as well as for each of the four quadrants of the initial (pre) assessment. When calculating Cronbach's alpha values, we used the initial (pre) scores for the treatment as well as the control sections ($n = 142$) since these are unaffected by the treatment and other learning experiences in the course.

After confirming that the Cybersecurity Knowledge Assessment was reasonably reliable,[1] we analyzed the assessment scores with paired samples t-tests. The tests compared the initial (pre) and final (post) assessment scores for the treatment as well as the control sections of the capstone course. In addition to the total assessment scores, we conducted separate comparative analyses to examine the pedagogical effectiveness of each of the four quadrants (i.e., Security-Technical, Privacy-Technical, Security-Social, and Privacy-Social).

3.4.2 Qualitative Analysis. We further engaged in qualitative analysis of the student reflections on the learning modules. Before analysis, we separated the reflections on the modules from the rest of the content in the post-sprint reports and anonymized them by assigning non-identifiable unique identifiers to the individual students and the teams. We analyzed the data by employing thematic analysis [3], further informed by techniques from grounded

[1]We verified that the results were unaffected by the exclusion of the ten students who provided answers to the initial assessment without providing answers to the assessment at the end of the course.

Table 3: The Cybersecurity Knowledge Assessment we developed contains 15 questions covering four quadrants: Security-Technical, Privacy-Technical, Security-Social, and Privacy-Social. The answer choices associated with each question are provided in Appendix A. To counter potential order effects, the order of the questions and the order of the corresponding answer choices should be randomized.

Quadrant 1: Security-Technical	Quadrant 2: Privacy-Technical
Q1: Which of the following is true of ransomware?	Q6: When collecting, storing, and sharing user data, how can you protect user privacy?
Q2: Which of the following is true of buffer overflow?	Q7: How does the private browsing / incognito mode of a web browser work?
Q3: If Alice has locked a message with Bob's public key, which key does Bob need to decrypt the message?	Q8: Which of the following is true of a browser cookie?
Q4: Which of the following is true of Authentication and Authorization?	
Q5: Which of the following is true of HTTP and HTTPS?	
Quadrant 3: Security-Social	**Quadrant 4: Privacy-Social**
Q9: Which of the following is true of the dark web?	Q13: Why is it important to know privacy regulations, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), across the world?
Q10: What are some common features of a phishing message?	Q14: What is contained in a privacy policy?
Q11: Which of the following is true of multi-factor authentication?	Q15: How does social media increase the risk of privacy and security breaches?
Q12: Which of the following is true about social engineering?	

theory [13]. We coded and analyzed the learning reflections using the MaxQDA[2] software for qualitative analysis.

We marked the responses with the higher-level category corresponding to the specific reflection question that prompted the response — LR1: "Learning," LR2: "Enhancement," LR3: "Application," and LR4: "Action" (see Section 3.2). However, we found that the responses for a given reflection question sometimes addressed issues connected to the other reflection questions as well. In such cases, we additionally applied the category for the other reflection questions as applicable. For example, for a statement in response to LR1 (i.e., "Learning"), we additionally applied the category for LR4 (i.e., "Action") if the statement contained actions to be taken on the project.

Next, we assigned lower-level codes to each statement across all higher-level categories. For example, we assigned the lower-level code "How to apply security patches" to a statement in response to LR2 (i.e., "What else would you like to know about the topics mentioned in the cybersecurity learning modules?"). The first author performed the initial coding of each statement within the anonymized reflections. Subsequently, the first and fourth authors iteratively reviewed the codes together to ensure meaningful and consistent coding across all data. After coding all individual statements in the reflection responses, the first author clustered the lower-level codes to identify higher-level themes under each of the four categories mentioned above. For instance, we assigned the example code above (i.e., "How to apply security patches") to the higher-level theme of "More detail on implementation" under the category "Enhancement." The fourth author reviewed the clustering and the subsequent analysis to ensure their consistency and validity. Table 6 lists the final set of 22 themes we identified across the four categories.

[2]https://www.maxqda.com

3.5 Limitations

Our research was conducted within a real-world setting, so the procedures should be considered quasi-experimental since the setting cannot be tightly and fully controlled despite incorporating a control condition. In particular, the treatment and control sections were taught by different instructors. It is plausible that our results could have been influenced by differences in teaching styles and lesson plans between the treatment and control sections. That said, the three instructors who taught the sections engaged in higher-level coordination to ensure that the course was consistent and uniform across sections.

The student teams differed in composition. Moreover, the nature of the projects and the external clients varied across the teams. These differences could have contributed to variations in learning. It has been noted that variation in learning among students can be attributed more to their prior experiences than to their aptitudes or learning rates [20]. However, as mentioned above, most students in the treatment as well as the control sections had roughly similar levels of prior industry experience. Although we could not control for these differences, we can reasonably expect them to be distributed uniformly across conditions, thus not affecting the analyses comparing the outcomes between the study conditions.

We developed the Cybersecurity Knowledge Assessment specifically for this research because of the lack of a suitable existing assessment instrument. Therefore, additional verification is necessary to determine the reliability and validity of the assessment as a general-purpose instrument for measuring developer knowledge of foundational sociotechnical cybersecurity concepts.

Table 4: Cronbach's alpha values for the full Cybersecurity Knowledge Assessment as well as each of the individual quadrants within the instrument, indicating high internal consistency for the full assessment and acceptable consistency for each quadrant.

	Questions	α	95% Interval
Full Assessment	15	0.816	0.75 – 0.86
Security-Technical	5	0.533	0.39 – 0.63
Privacy-Technical	3	0.536	0.42 – 0.63
Security-Social	4	0.652	0.53 – 0.75
Privacy-Social	3	0.657	0.51 – 0.76

4 FINDINGS

Prior to answering the research question we posed in Section 1, we verified the internal consistency of the Cybersecurity Knowledge Assessment. After confirming the reliability of the assessment, we compared the assessment scores of each student at the beginning and end of the course. We then examined student learning reflections regarding the cybersecurity modules. The following subsections describe each of these analyses.

4.1 Internal Reliability of the Assessment

Because we created the Cybersecurity Knowledge Assessment ourselves, we checked the reliability of the instrument by computing Cronbach's alpha [2] values for the full assessment as well as for the four individual quadrants within it (see Table 4). The Cronbach's alpha value of 0.816 with a relatively narrow 95% confidence interval for the full assessment indicates good internal consistency on the whole. A higher value would suggest unnecessary redundancy among the questions. The Cronbach's alpha values for the individual quadrants are lower and have broader 95% confidence intervals, indicating less consistency than the full assessment. However, the individual Cronbach's alpha values for each quadrant are still above the minimally acceptable threshold of 0.5 [11].

4.2 Learning Effects of the Cybersecurity Modules

Table 5 shows the results of the pre and post scores for the Cybersecurity Knowledge Assessment for students in the treatment and control sections. Based on the score for the full assessment, students in the treatment section exhibited statistically significant improvement in their cybersecurity knowledge (Cohen's $d = 0.61$, $p < 0.001$), meeting Hattie's [16] assertion that effect size should be greater than 0.40 when measured over approximately one school year. In contrast, the scores on the full assessment for the students in the control sections exhibited no statistically significant improvement between the beginning and the end of the course (Cohen's $d = 0.04$, $p = 0.3244$). The results provide strong confirmation that our learning modules were effective in achieving the goal of promoting greater student learning of foundational sociotechnical cybersecurity concepts than possible organically (i.e., simply by working on the projects without the modules).

We consider the quadrant scores to be exploratory because they were not the primary goal of the assessment. Moreover, the scores for the individual quadrants have lower reliability based on their lower Cronbach's alpha values compared to the much higher Cronbach's alpha for the full assessment (see Table 4). We found that the students in the treatment section exhibited substantial learning in both quadrants related to security, with effect sizes of $d = 0.79$ and $d = 0.71$ for the Security-Technical and Security-Social quadrants, respectively. The effect size of $d = 0.34$ for the Privacy-Social quadrant for the treatment section fell just short of Hattie's [16] threshold of 0.40, suggesting moderate learning. We did not observe statistically significant increases in the scores for the Privacy-Technical quadrant in the treatment section. The mean scores on the initial (pre) assessment for the two Privacy quadrants (16.0 and 17.0, respectively, out of a possible score of 25 per quadrant) in the treatment section are low enough to leave room for improved scores in the privacy areas. The scores of the students the control sections improved statistically significantly only for the Security-Technical quadrant ($p < 0.001$), but the effect size ($d = 0.23$) was much lower than Hattie's [16] recommended threshold of 0.40.

4.3 Student Reflections on Learning

The thematic analysis described in Section 3.4.2 resulted in the themes listed in Table 6. In general, the student comments were consistently positive, expressing their appreciation for the contents of the modules:

> "I think that all of these things that we learned [in the module] apply to our project. We are dealing with personal and sensitive information that we really need to protect from outside attacks, and these lead to many risks that we need to address." — (Team 5, Collective Response)

> "In the module, we learned about the intersection among ethics, technology, and law. We now understand the tradeoffs between individual privacy and public safety as well as the differences between white hat (ethical) and black hat (exploitative, malicious) hackers. With all of these ethical concerns, it is important that the users of our system trust us developers and that we maintain transparency with the information we collect." — (Team 1, Collective Response)

Most teams reported that the modules served as a springboard for generating points to discuss with their clients:

> "This module has sparked an urgency to discuss cybersecurity matters with our client." — (Team 1, Collective Response)

> "We think there should be a simpler and faster way to authenticate users. . . . We will discuss this with our client." — (Team 4, Collective Response)

In addition, the modules helped the teams identify specific security- and privacy-related implementation tasks:

> "These topics spoke about more specific steps we could take in order to protect our software." — (Team 4, Collective Response)

Consequently, the modules led to material improvements in the projects:

Table 5: Comparison of the Cybersecurity Knowledge Assessment scores between the treatment and control sections of the course.

	Treatment Group (n = 46)							Control Group (n = 96)						
	Normalized Mean					Effect Size		Normalized Mean					Effect Size	
	Pre	SD	Post	SD	Diff		p	Pre	SD	Post	SD	Diff		p
Full Assessment	62.7	14.2	71.3	13.2	8.6	0.61	0.0000***	71.3	9.0	71.6	10.5	0.3	0.04	0.3244
Security-Technical	13.7	4.2	17.0	4.4	3.3	0.79	0.0000***	15.3	4.0	16.2	4.3	0.9	0.23	0.0098**
Privacy-Technical	16.0	3.6	16.8	2.7	0.8	0.24	0.0521	17.6	2.7	17.7	2.9	0.1	0.05	0.3509
Security-Social	16.1	4.3	19.1	3.6	3.0	0.71	0.0000***	19.0	2.8	19.0	3.4	0.0	−0.01	0.5491
Privacy-Social	17.0	4.4	18.5	4.8	1.5	0.34	0.0193*	19.5	3.0	18.8	3.3	−0.7	−0.21	0.9760

*$p<0.05$ **$p<0.01$ ***$p<0.001$

Table 6: The 22 themes identified in the thematic analysis across the four higher-level categories.

Category	Theme
Learning	– Foundational security concepts
	– Specific vulnerabilities
	– Protection from attackers
	– Foundational privacy concepts
	– Specific privacy violations
	– No prior knowledge of the concept
Enhancement	– More conceptual detail
	– More detail on implementation
	– More real-world examples
	– More information regarding a topic
	– Less information regarding a topic
	– Additional topics
	– Better delivery schedule
Application	– Gained security-related insight
	– Gained privacy policy and legal compliance insight
	– Gained software design (frontend and backend) insight
	– Gained development insight
	– Not applicable to the project
Action	– Implement a security feature
	– Address a vulnerability
	– Identify a software development task
	– Unsure whether the topic applies to the project

> "Right now, we do have security flaws within our system, and we're looking to fix those." — (Team 6, Student 1)

Although the students found the learning modules relevant and useful, they did offer a few suggestions for refining them to enhance their utility. In particular, the students suggested that the modules include more detail on the topics and more real-world examples of their application. It should be noted that we deliberately chose not to be overly detailed in the videos because the goal of the modules is to *introduce* students to the foundational concepts sufficiently well to equip them to seek more in-depth knowledge on their own. To that end, the modules do include references to resources with more detail on the topics. Moreover, the amount of content that could be included in each module was necessarily constrained by the timing and logistics of the larger course within which the modules were embedded.

Since we intended the capstone projects to serve as real-world examples of the application of the topics covered in the modules, we included explicit prompts to encourage the students to apply the material to their capstone projects. Comments from the clients and the students regarding the handling of security and privacy in the delivered projects confirmed that we succeeded in achieving our goal:

> "To abide by HIPAA [Health Insurance Portability and Accountability Act] rules, we would have to ensure that the data is protected from anyone outside the system and that it is sent correctly to the web server. We would have to integrate the encryption and hashing properly." — (Team 5, Collective Response)

> "We would vet the third-party libraries/frameworks we use in our application to ensure that user privacy is maintained." — (Team 3, Collective Response)

5 DISCUSSION

Based on prior studies of embedded cybersecurity instruction, we set out to determine whether a capstone course can serve as a suitable vehicle for such instruction by evaluating student learning based on comparing pre-treatment and post-treatment knowledge assessments coupled with student reflections. We expected that the capstone context would have the dual advantage of building on the foundation of prior learning [7] and immediate practical applicability in projects [17]. The assessment results and student reflections (see Section 4) confirmed our expectations.

Since we developed a new knowledge assessment specifically for our research, we performed a consistency test on the assessment results. The Cronbach's alpha for the full assessment is 0.816, with a relatively narrow confidence interval indicating robust internal consistency. To ensure full coverage of sociotechnical security and privacy concepts, it is important to include questions that address each of the four quadrants (i.e., Security-Technical, Privacy-Technical, Security-Social, and Privacy-Social). The Cronbach's alpha values for the assessment items corresponding to each of the four quadrants are lower with broader confidence intervals

(see Table 4), indicating that the individual components of the assessment are less reliable than the assessment as a whole. Adding questions to each quadrant would improve consistency at the cost of increasing the length of the assessment [26]. However, the lower internal consistency of the individual quadrants does not affect the results based on the full assessment.

With the caveat of lower reliability, we conducted exploratory analyses based on the assessment subscores for each quadrant. We found that student improvement was greater in the two security quadrants than in the privacy quadrants. Improvement was modest in the Privacy-Social quadrant, and there was no statistically significant learning gain in the Privacy-Technical quadrant. Given the lower reliability of the quadrant-level subscores, the differences in learning between the security and privacy quadrants could be an artifact of the assessment rather than a true difference in student understanding. Nevertheless, two plausible causes for the lower gains in privacy knowledge could be: 1) students not being pre-sensitized to privacy risks to the same degree as to security risks and/or 2) the learning modules not covering privacy topics as effectively as they cover security topics. Both of these aspects could be addressed by refining the privacy-related content in the modules. For instance, the modules could include more content on specific techniques for privacy protection since the student learning reflections suggest that the students seemed to have not learned as much about specific privacy-protection approaches (see Table 6). Further research is needed to uncover the underlying causes and refine the modules accordingly to enhance privacy-related learning.

The qualitative findings from the student reflections are consistent with the quantitative results obtained via the Cybersecurity Knowledge Assessment. Student comments indicate that the modules were the first formal training in cybersecurity for most of the students. Importantly, the material served to help the students learn by considering the applicability of the security and privacy concepts to their projects, even when the students felt that some of the concepts in a given module did not apply to their specific projects. In general, student reflections confirmed that they thoughtfully considered all material presented in each module and any lack of applicability was solely due to the specifics of their projects:

> "None of these topics apply to our project right now because we are not taking in or storing personal information from users. However, the topics should still be kept in mind as the features might expand in later stages of the project."
> — (Team 3, Collective Response)

Prior studies mentioned in Section 2 have shown the value of embedding cybersecurity instruction in introductory courses [27]. While we wholeheartedly agree that it is valuable to teach cybersecurity principles early in a computing program, our findings show that embedding cybersecurity instruction in an upper-level capstone course is effective as well. Prior efforts to incorporate cybersecurity considerations in capstone courses have typically involved coordinating the instruction with separate concurrent cybersecurity courses instead of embedding the instruction within the capstone course itself [22]. In contrast, our findings suggest that computing educational programs ought to consider embedding cybersecurity instruction within project-based courses. To that end, we offer ten learning modules we developed to cover foundational sociotechnical cybersecurity concepts. Further, we provide the modules in a form that could be easily adapted to any upper-division project-based course in the computing disciplines. In addition, the Cybersecurity Knowledge Assessment we developed for this research could serve as a useful resource to measure the learning of foundational sociotechnical cybersecurity concepts and provide feedback to students and instructors.

6 CONCLUSION

Developing a technology workforce informed about foundational sociotechnical aspects of security and privacy necessitates that cybersecurity be a mandatory curricular component in computing-related undergraduate education. We demonstrate that such an objective can be achieved effectively with relatively little additional burden if cybersecurity instruction is embedded within upper-division project-based courses, such as the capstone experience. Apart from benefiting instructors of project-based courses in computing-related disciplines, the sociotechnical learning modules and the Cybersecurity Knowledge Assessment could be incorporated within onboarding and upskilling training programs in industry settings. Importantly, the approach can help ensure that all computing professionals develop a *human-centered* understanding of security and privacy by going beyond technical detail to incorporate social aspects and the societal context that affect the practical deployment and use of technology.

ACKNOWLEDGMENTS

We are grateful to the students who participated in the study. We thank Matthew Bietz and Darren Denenberg for allowing us to administer the Cybersecurity Knowledge Assessment in their courses that served as the control sections. We acknowledge Katherine Hubeny, Preet Jyotpreet, Emma Lashley, and Danielle Muhlenberg for their help and support in tasks related to the development of the learning modules and the assessment. The paper benefited from the feedback of anonymous reviewers and the participants of the Human-Centered Computing seminar at the University of Utah. Part of the work described in the paper was carried out when Sameer Patil and Ying Tang were affiliated with Indiana University Bloomington. The research is supported by National Science Foundation (NSF) grants #1821782, #1821822, and #2221870. The contents of the paper are solely the work of the authors and do not necessarily reflect the views of the sponsors.

REFERENCES

[1] Joni K. Adkins and Cindy Tu. 2019. Applying an agile approach in an information systems capstone course. *Information Systems Education Journal* 17, 3 (2019), 41–49. https://isedj.org/2019-17/n3/ISEDJv17n3p41.html

[2] Douglas G. Bonett and Thomas A. Wright. 2015. Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organizational Behavior* 36, 1 (2015), 3–15. https://doi.org/10.1002/job.1960

[3] Virginia Braun, Victoria Clarke, Nikki Hayfield, and Gareth Terry. 2019. Thematic Analysis. In *Handbook of Research Methods in Health Social Sciences*, Pranee Liamputtong (Ed.). Springer Singapore, Singapore, 843–860. https://doi.org/10.1007/978-981-10-5251-4_103

[4] Jack Cable. 2019. Every Computer Science Degree Should Require a Course in Cybersecurity. *Harvard Business Review* (Aug 2019), 5 pages. https://hbr.org/2019/08/every-computer-science-degree-should-require-a-course-in-cybersecurity Accessed: 2023-08-18.

[5] Yu Cai. 2018. Using Case Studies to Teach Cybersecurity Courses. *Journal of Cybersecurity Education, Research, and Practice* 2018, 2 (Dec 2018), 24 pages. https://doi.org/10.62915/2472-2707.1041

[6] CloudPassage. 2016. CloudPassage Study Finds U.S. Universities Failing in Cybersecurity Education. https://web.archive.org/web/20160522051120/https://www.cloudpassage.com/company/press-releases/cloudpassage-study-finds-u-s-universities-failing-cybersecurity-education/ Accessed: 2024-06-13.

[7] Tom Crick, James H. Davenport, Paul Hanna, Alastair Irons, and Tom Prickett. 2020. Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes. In *2020 IEEE Frontiers in Education Conference (FIE)*. IEEE, New York, NY, 1–9. https://doi.org/10.1109/FIE44824.2020.9274033

[8] William Crumpler and James A. Lewis. 2019. The Cybersecurity Workforce Gap. *Center for Strategic & International Studies* (2019), 10 pages. https://www.csis.org/analysis/cybersecurity-workforce-gap Accessed: 2024-06-13.

[9] CyberEdge Group LLC. 2022. 2022 Cyberthreat Defense Report. https://cyberedge.com/cyberthreat-defense-report-2022/ Accessed: 2024-06-13.

[10] Serge Egelman and Eyal Peer. 2015. Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 2873–2882. https://doi.org/10.1145/2702123.2702249

[11] Stephen O. Ekolu and Harry Quainoo. 2019. Reliability of assessments in engineering education using Cronbach's alpha, KR and split-half methods. *Global Journal of Engineering Education* 21, 1 (2019), 24–29. http://www.wiete.com.au/journals/GJEE/Publish/vol21no1/03-Ekolu-S.pdf

[12] Darren Gergle and Desney S. Tan. 2014. Experimental Research in HCI. In *Ways of Knowing in HCI*, Judith S. Olson and Wendy A. Kellog (Eds.). Springer, New York, NY, 210–211. https://doi.org/10.1007/978-1-4939-0378-8_9

[13] Barney G. Glaser and Anselm L. Strauss. 1967. *The discovery of grounded theory: Strategies for qualitative research.* Routledge, New York, NY. https://doi.org/10.4324/9780203793206

[14] Jan Hajny, Sara Ricci, Edmundas Piesarskas, Olivier Levillain, Letterio Galletta, and Rocco De Nicola. 2021. Framework, Tools and Good Practices for Cybersecurity Curricula. *IEEE Access* 9 (2021), 94723–94747. https://doi.org/10.1109/ACCESS.2021.3093952

[15] John Grady Hall, Abhinav Mohanty, Pooja Murarisetty, Ngoc Diep Nguyen, Julio César Bahamón, Harini Ramaprasad, and Meera Sridhar. 2022. Criminal Investigations: An Interactive Experience to Improve Student Engagement and Achievement in Cybersecurity Courses. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education - Volume 1* (Providence, RI, USA) *(SIGCSE 2022)*. Association for Computing Machinery, New York, NY, USA, 696–702. https://doi.org/10.1145/3478431.3499417

[16] John Hattie. 2009. The Nature of the Evidence. In *Visible learning*. Routledge, New York, NY, Chapter 2, 7–21. https://doi.org/10.4324/9780203887332-8

[17] Gregory W. Hislop, Heidi J.C. Ellis, S. Monisha Pulimood, Becka Morgan, Suzanne Mello-Stark, Ben Coleman, and Cam Macdonell. 2015. A Multi-Institutional Study of Learning via Student Involvement in Humanitarian Free and Open Source Software Projects. In *Proceedings of the Eleventh Annual International Conference on International Computing Education Research* (Omaha, Nebraska, USA) *(ICER '15)*. Association for Computing Machinery, New York, NY, USA, 199–206. https://doi.org/10.1145/2787622.2787726

[18] Joint Task Force on Cybersecurity Education. 2017. Cybersecurity curricular guidelines: CSEC 2017. https://cybered.hosting.acm.org/wp/ Accessed: 2024-06-13.

[19] Frank H. Katz. 2018. Breadth vs. Depth: Best Practices Teaching Cybersecurity in a Small Public University Sharing Models. *The Cyber Defense Review* 3, 2 (2018), 65–72. https://cyberdefensereview.army.mil/CDR-Content/Articles/Article-View/Article/1620289

[20] Kenneth R. Koedinger, Paulo F. Carvalho, Ran Liu, and Elizabeth A. McLaughlin. 2023. An astonishing regularity in student learning rate. *Proceedings of the National Academy of Sciences* 120, 13 (2023), 11 pages. https://doi.org/10.1073/pnas.2221311120

[21] Kees Leune and Salvatore J. Petrilli. 2017. Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. In *Proceedings of the 18th Annual Conference on Information Technology Education* (Rochester, New York, USA) *(SIGITE '17)*. Association for Computing Machinery, New York, NY, USA, 47–52. https://doi.org/10.1145/3125659.3125686

[22] Natarajan Meghanathan, Hyunju Kim, and Loretta A. Moore. 2012. Incorporation of Aspects of Systems Security and Software Security in Senior Capstone Projects. In *2012 Ninth International Conference on Information Technology - New Generations*. IEEE ITNG, New York, NY, 319–324. https://doi.org/10.1109/ITNG.2012.54

[23] Allen Parrish, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. Global perspectives on cybersecurity education for 2030: A case for a meta-discipline. In *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (Larnaca, Cyprus) *(ITiCSE 2018 Companion)*. Association for Computing Machinery, New York, NY, USA, 36–54. https://doi.org/10.1145/3293881.3295778

[24] Brian H. Spitzberg. 2006. Preliminary Development of a Model and Measure of Computer-Mediated Communication (CMC) Competence. *Journal of Computer-Mediated Communication* 11, 2 (2006), 629–666. https://doi.org/10.1111/j.1083-6101.2006.00030.x

[25] Ying Tang, Morgan L. Brockman, and Sameer Patil. 2021. Promoting Privacy Considerations in Real-World Projects in Capstone Courses with Ideation Cards. *ACM Trans. Comput. Educ.* 21, 4, Article 34 (Oct 2021), 28 pages. https://doi.org/10.1145/3458038

[26] Mohsen Tavakol and Reg Dennick. 2011. Making sense of Cronbach's alpha. *International Journal of Medical Education* 2 (2011), 53. https://doi.org/10.5116/ijme.4dfb.8dfd

[27] Blair Taylor and Siddharth Kaza. 2016. Security Injections@Towson: Integrating Secure Coding into Introductory Computer Science Courses. *ACM Trans. Comput. Educ.* 16, 4, Article 16 (Jun 2016), 20 pages. https://doi.org/10.1145/2897441

[28] Saara Tenhunen, Tomi Männistö, Matti Luukkainen, and Petri Ihantola. 2023. A systematic literature review of capstone courses in software engineering. *Information and Software Technology* 159 (2023), 21 pages. https://doi.org/10.1016/j.infsof.2023.107191

[29] Robert Thomas. 2016. Behind the Numbers on Why Universities Lag Behind in Cybersecurity Education. https://web.archive.org/web/20190516182303/https://blog.cloudpassage.com/2016/04/13/behind-numbers-universities-lag-behind-cybersecurity-education/ Accessed: 2024-06-13.

[30] U.S. National Security Agency / Central Security Service. 2023. National Centers of Academic Excellence in Cybersecurity. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/ Accessed: 2024-06-13.

[31] Sander Valstar, Caroline Sih, Sophia Krause-Levy, Leo Porter, and William G. Griswold. 2020. A Quantitative Study of Faculty Views on the Goals of an Undergraduate CS Program and Preparing Students for Industry. In *Proceedings of the 2020 ACM Conference on International Computing Education Research* (Virtual Event, New Zealand) *(ICER '20)*. Association for Computing Machinery, New York, NY, USA, 113–123. https://doi.org/10.1145/3372782.3406277

[32] Jari Vanhanen, Timo O. A. Lehtinen, and Casper Lassenius. 2012. Teaching real-world software engineering through a capstone project course with industrial customers. In *2012 First International Workshop on Software Engineering Education Based on Real-World Experiences (EduRex '12)*. IEEE, New York, NY, 29–32. https://doi.org/10.1109/EduRex.2012.6225702

[33] Chuan Yue. 2016. Teaching Computer Science With Cybersecurity Education Built-in. In *2016 USENIX Workshop on Advances in Security Education (ASE '16)*. USENIX Association, Austin, TX, 8 pages. https://www.usenix.org/conference/ase16/workshop-program/presentation/yue

A CYBERSECURITY KNOWLEDGE ASSESSMENT

The Cybersecurity Knowledge Assessment is designed to cover four quadrants: Security-Technical (5 questions), Privacy-Technical (3 questions), Security-Social (4 questions), and Privacy-Social (3 questions). To counter potential order effects, the assessment is delivered by randomizing the order of the questions as well as the order of the answer choices corresponding to each question. In the list of answer choices below, the correct answers are marked with a black square or circle (■ ●), and the incorrect answers are marked with an empty square or circle (□ ○).

Quadrant 1: Security-Technical

Q1: Which of the following is true of ransomware?
(*Select all correct answers.*)

- ■ It is a form of malware.
- ■ It requires victims to send payment in return for their data.
- ■ It is a technique hackers use for monetary gain.
- ■ It prevents users from accessing their files.
- □ It is a paid antivirus tool.
- □ It is a technique for withholding credentials from a suspicious user.
- □ It posts a victim's personal information online as revenge.

Q2: Which of the following is true of buffer overflow?
(*Select all correct answers.*)

- ■ It happens when the memory buffer storage is exceeded.
- ■ It triggers a program to write data to adjacent memory locations.
- ■ It permits attackers to overwrite the memory of an application.
- ■ It causes the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.
- ■ It is a software security vulnerability.
- □ It is a security tactic that stores information in a buffer until the user is properly authenticated.
- □ It uses a computer's network connection to flood a router with packets.

Q3: If Alice has locked a message with Bob's public key, which key does Bob need to decrypt the message?
(*Select one answer.*)

- • Bob's private key.
- ◦ Bob's public key.
- ◦ Alice's private key.
- ◦ Alice's public key.

Q4: Which of the following is true of Authentication and Authorization?
(*Select all correct answers.*)

- ■ Authentication determines whether users are who they claim to be, while authorization determines what users can and cannot access.
- ■ Authentication is usually done before authorization.
- ■ Authentication transmits info through an ID token, while authorization transmits info through an access token.
- ■ Some authorization mechanisms rely on IP addresses.
- □ Authorization determines whether users are who they claim to be, while authentication determines what users can and cannot access.
- □ Access to a resource is protected by authentication, while authorization is used to try and override the authentication process.
- □ Authorization includes passwords, single sign-on, etc., while authentication includes role-based access control, openID, etc.

Q5: Which of the following is true of HTTP and HTTPS?
(*Select all correct answers.*)

- ■ HTTP is not secure, while HTTPS is secure.
- ■ HTTPS is the extension of HTTP that works in conjunction with SSL.
- ■ HTTP involves no data encryption.
- ■ HTTP sends data over port 80, while HTTPS uses port 443.
- □ HTTPS was created to offset the amount of traffic going to HTTP addresses.
- □ HTTP is the free version of HTTPS. HTTPS needs to be purchased when choosing a domain name.
- □ Sites using HTTPS do not use browser cookies, while sites using HTTP do.

Quadrant 2: Privacy-Technical

Q6: When collecting, storing, and sharing user data, how can you protect user privacy?
(*Select all correct answers.*)

- ■ Encrypt the information entered by the user.
- ■ Use secure databases.
- ■ Salt and hash user passwords.
- ■ Be transparent about how the data will be used.
- □ Use HTTP rather than HTTPS.
- □ Encourage the user to use a private browsing session.
- □ Collect the data necessary to build a detailed user profile.

Q7: How does the private browsing / incognito mode of a web browser work?
(*Select all correct answers.*)

- ■ When a user visits a website in the private browsing / incognito mode, the browser does not store the session in the user's history.
- ■ Although the private browsing / incognito mode sessions prevent browsing information from being stored in the web browser, the cookies used during the session can provide information about browsing behavior to third parties.
- ■ In the private browsing / incognito mode, browsing activity may still be visible to the ISP as well as the organization involved in the connection, such as the user's school or employer.
- ■ The private browsing / incognito mode prevents third parties from collecting the user's data.
- □ When a user visits a website in the private browsing / incognito mode, the web browser is unable to track any information about the user.
- □ Web browsing is completely private and anonymous when using the private browsing/ incognito mode.
- □ The private browsing / incognito mode sends all web browsing data through a VPN, keeping it private from the ISP.

Q8: Which of the following is true of a browser cookie?
(*Select all correct answers.*)

- ■ It can store user preferences.
- ■ It may specify that a secure connection is necessary.
- ■ It enables core website functionality.
- ■ It can record personal information.
- □ It contains the entire content of the webpage the user is browsing.
- □ It records the user's browsing history.
- □ It saves the username and password of the user.

Quadrant 3: Security-Social

Q9: Which of the following is true of the dark web?
(*Select all correct answers.*)

- ■ It is a part of the Internet that is not indexed by search engines.
- ■ It is an avenue often used for illegal activity.
- ■ It is the place where stolen user information is often sold.
- ■ It contains content that can be accessed only with specific software, configurations, or authorization.
- ■ It is accessible only through networks such as Tor and I2P (Invisible Internet Project).
- ■ It helps people maintain privacy.
- □ It is a tactic for hiding browsing data from other users of the computer.

Q10: What are some common features of a phishing message?
(*Select all correct answers.*)

- ■ It often presents unrealistic threats or demands.
- ■ It often asks for personal/sensitive information.
- ■ It often has poor grammar and misspellings.
- ■ It normally contains links that do not go to the site from which the message claims to originate.
- ■ It often contains alarming content and suggests taking immediate action by following a link.
- ■ It is a fraudulent message that can look reputable.
- □ It installs a virus on the victim's machine.

Q11: Which of the following is true of multi-factor authentication?
(*Select all correct answers.*)

- ■ It is a strategy for verifying user identity.
- ■ It adds an additional layer of security to prevent brute-force attacks.
- ■ It verifies user identity by requiring multiple credentials.
- □ It is a hacking strategy that tricks users into entering multiple pieces of information through a fake login portal.
- □ It is a paywall that ensures that the users are real people.
- □ It uses IP addresses to ensure that logins are occurring in the same location as the sign-up.
- □ It asks users to enter their login information twice.

Q12: Which of the following is true about social engineering?
(*Select all correct answers.*)

- ■ It is a manipulation technique to obtain personal information from targeted users.
- ■ It is a hacking tactic that exploits the trust of victims.
- ■ It takes advantage of a potential victim's natural behavioral tendencies and emotional responses.
- ■ It uses psychological manipulation to trick users by pretending to be someone else.
- □ It is the act of learning hacking tactics through online forums and private groups.
- □ It refers to the selling of user credentials gathered from data breaches.
- □ It is a precaution users can take to avoid being hacked.

Quadrant 4: Privacy-Social

Q13: Why is it important to know privacy regulations, such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), across the world?
(*Select all correct answers.*)

- ■ Companies are expected to know and follow regulations in the locations where their users are using their products and services.
- ■ Regulations vary by location.
- ■ Regulations help protect user data from unauthorized use.
- ■ Regulations help identify and protect against reasonably anticipated threats.
- □ Following regulations allows companies to increase advertising.
- □ CCPA will soon be a global regulation.
- □ Companies need to follow the privacy regulations of the states and countries where they have offices.

Q14: What is contained in a privacy policy?
(*Select all correct answers.*)

- ■ The kind of information collected from users.
- ■ The purpose of collecting data.
- ■ The legal basis for data collection.
- ■ The rights users have regarding the data collected about them.
- ■ Affiliated organizations with which user data may be shared.
- □ The repercussions of attempting to breach the database.
- □ Information about the developers and tools used to create the website, application, or service.

Q15: How does social media increase the risk of privacy and security breaches?
(*Select all correct answers.*)

- ■ Social media is used for social engineering tactics by hackers to gain access to a user account and target that user's network.
- ■ Malicious actors create fake social media accounts with the purpose of exploiting vulnerable users.
- ■ People have become accustomed to sharing high amounts of personal information on social media.
- ■ Social media can be used to impersonate a person, cause, or business through the use of fake profiles.
- □ User data and metadata of social media activity is typically unencrypted.
- □ Social media companies have too many users to store user data on secure servers.
- □ Social media is available on most devices.