ASEE 2022 ANNUAL CONFERENCE
Excellence Through Diversity
MINNEAPOLIS, MINNESOTA, JUNE 26TH-29TH, 2022 ASEE
Paper ID #37932

Towards Goal-Oriented Experiential Learning for Cybersecurity Programs

Eman Hammad (Assistant Professor)

Dr. Eman Hammad is a cybersecurity professional & interdisciplinary professional focusing on trustworthy & resilient complex systems and emerging technologies. She obtained her PhD in Electrical & Computer Engineering from the University of Toronto. Dr. Hammad is an is an assistant professor with Texas A&M University - Commerce. She combines practical experience and theoretical research to shape her vision for resilient-by-design solutions in the connected world. She is the director of the innovations in Systems Trust & Resilience (iSTAR) lab. Dr. Hammad's work has been published in more than 50 papers, and was recognized with merit awards (best paper award, best poster award) and has been featured on multiple outlets. Most recently, she was honored as one of Canada's Top 20 Women in Cybersecurity. Dr. Hammad is a senior IEEE member currently serving as Toronto ComSoc chair, and the co-chair of the IEEE 5G Security working group for the International Network Generations Roadmap (INGR). She delivered numerous invited talks in academic and industrial conferences, chaired and co-chaired several conferences and workshops, and participated in several panels. She serves on the advisory board of several initiatives. Dr. Hammad is an active advocate for diversity and inclusion in STEM and Cybersecurity. Her service has been recognized by IEEE exceptional, chapter achievement, and exemplary service awards.

James K. Nelson (Associate Vice Chancellor)

Associate Vice Chancellor in the Texas A&M University System and Director of the RELLIS Academic Alliance.

John Romero

Cybersecurity instructor, maker of IoT, techie, software developer, sailor, private pilot, Air Force veteran, and electronic warfare technician. Mentor, coach, and facilitator for young adults entering the workforce. Passionate instructor and influencer for positive ethical leadership. Research interests include cybersecurity social engineering, human element in cybersecurity, Smart Manufacturing, and Industrial Internet of Things (IIoT) hacking.

Towards Goal-Oriented Experiential Learning for Cybersecurity Programs

Abstract

The continuously increasing gap in the cybersecurity workforce, in numbers and skill levels, demands a fundamental shift in how we approach cybersecurity education and training. This is further complicated when considering the need to enable learners from a diverse set of backgrounds for a larger spectrum of career trajectories within the industry. In this article, we present our model for a goal-oriented experiential learning that was implemented in one cybersecurity course with interactive learning modules. In this model, a closed-loop learning environment is established, where students are actively involved and guided to include their goals in an interactive set of learning modules of the course. Students were provided with the needed infrastructure and technologies (such as IoT devices and the cyberrange platform) to enable them to proceed with those modules. The article summarizes the results based on students' feedback and observations, and concludes with a description of a methodology to generalize this to other similar courses.

Introduction

The global gap in cybersecurity talent remains highly unfulfilled with projections expecting this gap to extend with increasing market demand. Digital innovation continues to interconnect and embed digital components in virtually every industry including healthcare, education, finance, transportation, agriculture, manufacturing, oil and gas, mining, energy, aerospace, etc. This digital transformation comes accompanied with increasing risks of cybersecurity related disruptions and attacks. Thus, driving the demand for cybersecurity talent in most industries that employ or rely on technology for their business operations including security service providers.

The complex and ever-evolving cybersecurity industry and threat landscape underscores the need for cybersecurity professionals with versatile skillset, growth mindset and resilient character to support organizations' cyber capabilities, preparedness and resilience [1]. This makes it more challenging to develop and operate educational programs that effectively train cybersecurity talent, which is able to take on and perform in multiple roles and responsibilities, without tailoring the program to be very specific to such roles. Hence, cybersecurity educational programs must train professionals that can stand the test of time, in a fast-paced and quickly changing career [2].

Educators are quickly recognizing that the curriculum structure and delivery modalities must be developed to ensure foundational concepts and frameworks are clearly comprehended and translated into practice. This has motivated several efforts at different levels to outline the expected skillsets and proficiency levels through practical and experiential learning modules to enable effective integration between educational programs and workforce opportunities [2].

With such challenging goals and experiential learning approaches in mind, we focus and expand on the development of one course in this article; CSCI 310 Cybersecurity. The course is an introductory cybersecurity course at the Texas A&M University System at the RELLIS campus [3]. The course is offered as part of the Texas A&M University – Commerce Cybersecurity Bachelors (Cyber) academic program as a pre-requisite to subsequent more specialized offerings

in the program. Students in two other programs; Computer Science (CS) Bachelors and the Computer Information Systems (CIS) Bachelors can enroll in the course as an elective.

In the following sections of the article, we describe the evolution of the course structure, and the composition of learning modalities. We also detail the assessment survey used and expand on its findings. We conclude the articles with lessons learns and a generic approach that can be expanded to other similar courses.

Related Works

The National Institute of Standards and Technology (NIST) developed the National Initiative for Cybersecurity Education (NICE) to help guide educational and training efforts bridge the cyber talent gap and maintain a healthy talent pipeline, [2]. NICE systematically defines cybersecurity roles within seven main categories that aligns with NIST's Cybersecurity Framework. NICE also establishes related capabilities, required skills and expected duties for each role. Moreover, it outlines the educational modules, named knowledge units related to each role. It can been observed in the NICE framework as well as in the related expected capabilities and skillsets, that experienced students not only would be more competitive, but would also be able to successfully perform.

Experiential learning is a learning process that combines reflection and review about the experience; abstracting and conceptualization of the experience; and ultimately engaging in active experimentation of what has been learned [4]. There has been multiple efforts focusing on the development of several experiential learning elements to enrich and support cybersecurity educational programs. One elements, which supported hands-on learning through cyberranges. A cyberrange is a set of dedicated computational resources to allow for safe cybersecurity exploration and testing, and are shown to enable experiential learning for academic and other educational settings. Cyberranges can be realized are specialized testbed focusing on certain security domains or more general virtualization environments [5]. A testbed for cybersecurity using cloud and software-defined networks is proposed in [6] to help with computer networks and security education. The benefits of the testbed were evaluated using surveys on student's satisfaction. The experiential activities developed as labs for students using the testbed focused on skills via pedagogical approaches.

In other approaches to enhance experiential learning, we examine existing work that considers engaging students and enacting their learner agency via structuring an environment where students participate in goal-oriented project-based problem solving [7]. A successful approach in experiential learning that has been consistently used in the past decades has been based on the pedagogy of play. Gamification tools of cybersecurity learning, such as capture the flag (CtF) challenges, are used in different contexts and settings and are found to be engaging and useful however more focused on technical concepts and skillsets.

Setting the Goals and Drawing the Course

The CSCI 310 Cybersecurity course outline (Figure 1) and student learning outcomes, listed below, are developed to map foundational concepts from leading professional certifications and industry standards at a high-level. This is combined with the objective of exposing the students to a wide spectrum or cybersecurity capabilities and roles from the beginning to enact their agency in shaping their course learning experience.

CSCI 310 Student Learning Outcomes:

Upon completing this course students should be able to:

- Understand the importance of information security / cybersecurity and associated risks
- Learn the key concepts of information security
- Learn about some of the different domains and capabilities of information security including identity and access management, network security, application security, data protection, etc.
- Understand basic cryptography algorithms and mechanisms The syllabus/schedule are subject to change.
- Learn and understand key concepts in threat & vulnerability management
- Learn concepts related to privacy & incidence response
- Understand basic cybersecurity issues related to emerging technologies (AI/ML, IoT, ICS/OT, 5G).

Week	Course Subject
Foundational Concepts: Security & Risk Management	
Week 1	Motivation: Threat Landscape and Recent Events
	Cybersecurity Concepts and Requirements
Week 2	Threats, Attacks and Assets
Week 3	Foundational Security Design Principles, Strategy, standards
	Legal, Ethical, and Professional Issues in cybersecurity
Security Engineering	
Week 4	Cybersecurity Governance, Compliance, and Risk Management
Week 5, 6	Cryptography
Week 7	Security Models, Design & Capabilities
Week 8	**Midterm exam #1**
Week 9	Threats, Vulnerabilities and Countermeasures
Communications and Network Security	
Week 10	Network & Communications Security
Identity and Access Management	
Week 11	Identity Management & Authentication
	Access Control & Monitoring
Security Operations	
Week 12	Security Operations, Threat Intelligence
Week 13	Incident Response & Preparedness
Advanced Topics	
Week 14	Data Trust & Privacy, Thanksgiving Holiday
Week 15	Cyber Crime & Digital Forensics
Finals Week	**Final Exam**

Figure 1. CSCI 310 Course Outline

Given the above learning objectives, we next examine the desired composition of course activities and learning modalities that take into consideration the following factors:

1) Diverse students' backgrounds: students from three different programs (Cyber, CS, CIS) can enroll in the course. While the three programs have significant overlap in the subjects of the freshman and sophomore years, they still represent student with fundamentally different characteristics and interests. Hence, the course structure must provide a venue for each student population to adjust its learning experience to their own set goals.
2) Wide variety of topics: cybersecurity is a "huge" field and it requires a careful balance and flexibility in structure to be able to fairly present it in one course with sufficient depth to allow those interested to further their pursuit within and after the course.
3) Technical vs non-technical roles: roles in cybersecurity are not strictly technical hands-on "hack" roles, and while most programs focus on the more interesting roles, a more balanced representation of technical and not so technical roles should be integrated in the course. This is necessary, due to the criticality of those functions in practical cybersecurity program operations.
4) Modalities of learning: availability of resources to enable the adoption of different modalities of learning including active and experiential learning.
5) Continuous feedback and enhancement: data collection points and tools must be set throughout the course offering and between course offerings to enable the assessment of

students learning outcomes and learning experience and the continuous improvement of the course.

Considering those factors, the CSCI 310 course evolved through three offerings in Fall 2020, Spring 2021 and Fall 2021. This evolution was informed by course evaluations and direct collection of student feedback, and using a customized survey for the last offering of Fall 2021. We illustrated the evolution of the course offering and highlight the main changes in Figure 2.

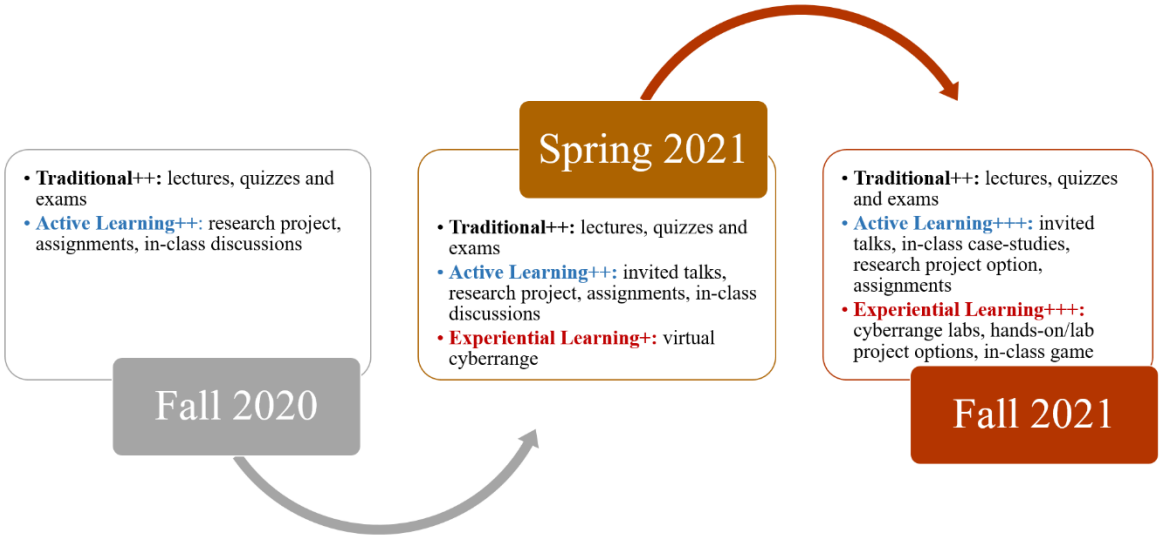

Figure 2. CSCI 310 Cybersecurity Course Composition Evolution Through three offerings between Fall 2020 – Fall 2021

Course Composition

As illustrated in Figure 2, the course evolved to include more active and experiential learning components based on instructor's observation and students' feedback, performance and input analysis. The CSCI 310 course composition evolved to incorporate multiple elements of active and experiential learning in its latest offering. Furthermore, this composition is structured in such a way that students can draft and guide part of their goals and select activities to help achieve those goals.

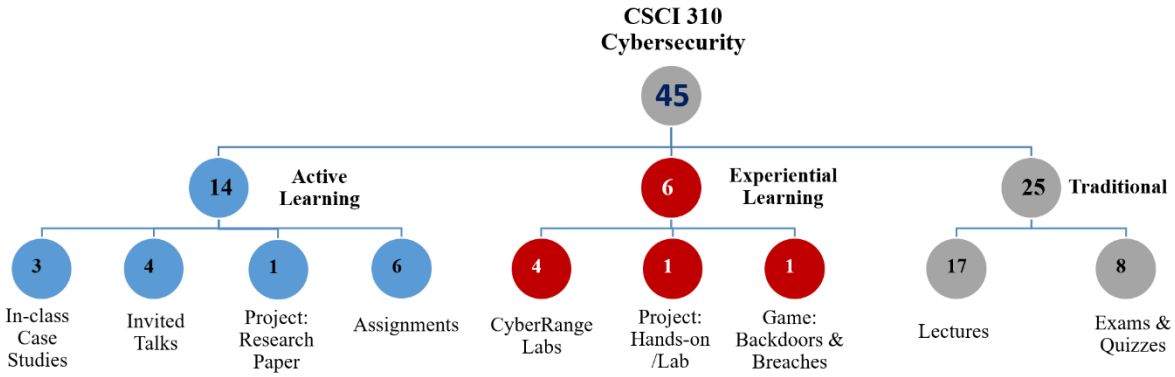

Figure 3. CSCI 310 Course Learning Modalities Composition, Fall 2021.

Figure 3 illustrates the final course composition for the Fall 2021 offering. The numbers in the circles indicate the number of activities.

It is important to note here that not all activities are graded such as the invited talks, in-class discussions and the integrated active learning game. For the learning activities that are graded, the weight (grade impact) assigned for each activity is not uniform and is set in accordance with the effort and related learning objectives. The grade distribution for the CSCI 310 course for the graded activities is detailed in Table 1 below.

Quizzes	Assignments	Cyberrange Labs	Exams	Project	Total
10%	10%	10%	45%	25%	100%

Table 1. CSCI 310 Fall 2021 grade distribution for graded activities.

A summary of the course activities is provided below:

1) **Active learning modules:**
   - In-class case studies: students are divided into groups and each group is assigned a a different and unique real-life case study. Each case study is described in sufficient detail, and is ended with a set of open-ended questions (guided query) that requires active discussion and research between members of the group. At the end of the discussion time, each group describes their case study to the whole class, and responds to some of the guided query questions. The rest of the class is then allowed to follow-up with additional questions. The topics of the case studies are carefully selected to synchronize with the course outline to discuss timely and relevant issues.
   - Invited talks: multiple experts are invited to deliver a class period on a topic theme that is aligned with the course outline. The invited speakers are given the flexibility to address the topic from their professional perspective and to support it using their tools and stories. The invited speakers are selected to represent different cybersecurity career roles, and student are provided with amble opportunity to ask questions and to ask for advice or insights.

- Project – research paper: student must work on a project as part of the CSCI 310 course to further their learning experience and outcomes. The project part of the course affords the students the opportunity to select from three different types of projects. The intentional flexibility aim to enact students' agency and enable them to set their own goals for learning in this part of the course. Students, who are more adept with active learning, choose to do a research paper on a topic from a list of provided topics or could propose a topic that interests them. Once students select their research topic, they proceed to work on writing a technical survey paper on the subject. Students must use acceptable technical writing templates for their paper and should rely on an adequate number and type of references to ensure a balanced and credible coverage of the subject. In the Fall 2021 course offering, students followed the IEEE conference paper template. At the end of the semester, students present their research to the entire class, practicing appropriate public speaking and communication skills and responding to peer questions and feedback.
- Assignments: the course employs short assignments to help students gain confidence with foundational concepts. Assignments are graded in a timely manner and incorporate direct and individual feedback to the students. Once assignments are graded, they are discussed in the class to highlight the main objectives and learnings and to address any common students deficiencies/mistakes observed.

2) **Experiential learning modules:**
   - Cyberrange labs: as can be observed from the evolution of the course, the cyberrange was not available as a resource for use until the course last offering in Fall 2021. The cyberrange used is an active development project developed and supported by students using open source technologies. CSCI 310 students gain remote access to the cyberrange platform using an internet browser. Students use a set of credentials and multi-factor authentication to login to the platform and are provided with an instruction manual for each cyberrange lab. To address common challenges, we dedicate time in class for students to start working on the assigned lab modules, and we provide guidance during the class on the main steps of the lab and any potential difficulties or challenges that they should pay attention to. Once the students obtain good progress, the rest of the lab execution is left to the students with the support of the instructions manual. The cyberrange labs are designed to support guided experiential learning, and students' access to the platform is intentionally left open throughout the semester and between labs to allow student to continue with their own exploration and learning if needed.
   - Project – hands-on: students who are interested in more applied hands-on projects are offered two options, a) to develop and implement a cybersecurity project with real physical components. Students who chose this project were given the option to choose from a list of hands-on projects for which we have components such as IoT devices, controllers or hacking tools available. Once a project was selected, students were provided with the resources needed for their project. Alternatively, students can choose b) to develop cyberrange labs with proper documentation (instructional manuals) for future students. Students can select the lab focus from a list of topics or they can propose a topic of their choice. All students join the rest of the class to

present and demo their applied project during the scheduled project presentations at the end of the semester.

- Game – revised Backdoors & Breaches: at the end of the course, and after learning about the different capabilities, foundational concepts and main processes, students are divided into groups to play a cards game where the instructor is the facilitator. The game aims to teach incident response and preparedness through semi-real cyber incident scenarios with varying threat vectors and injections [8] [9]. We revised the games in consideration of available resources (class time and number of students).

3) **Traditional learning modules:**

- Lectures: lectures are infused with important discussion prompts and open ended questions. Foundational concepts are explained in sufficient details and students are often guided through relevant assignments on the challenging topics during class.
- Quizzes and exams: quizzes frequency and scope are designed to encourage students to remain current with the course material. Exams are designed to reemphasize main learning outcomes and to provide a fair coverage of materials in scope. Quizzes and exams are graded in a timely fashion and are always discussed in class with solutions explained and main issues, if any, addressed.

We typically offer CSCI 310 course in a 16 weeks semester. Figure 4 depicts the course timeline and the composition and schedule of course's active, experiential and traditional learning activities. As can be observed, the mix of activities may seem complex from the instructor perspective, but when structured and timed appropriately, they can be rewarding especially when the objectives of the student engagement and learning are achieved. To better assess the student perspective, a customized high-level survey was developed and distributed to students at the end of the semester independently from the general course evaluation.

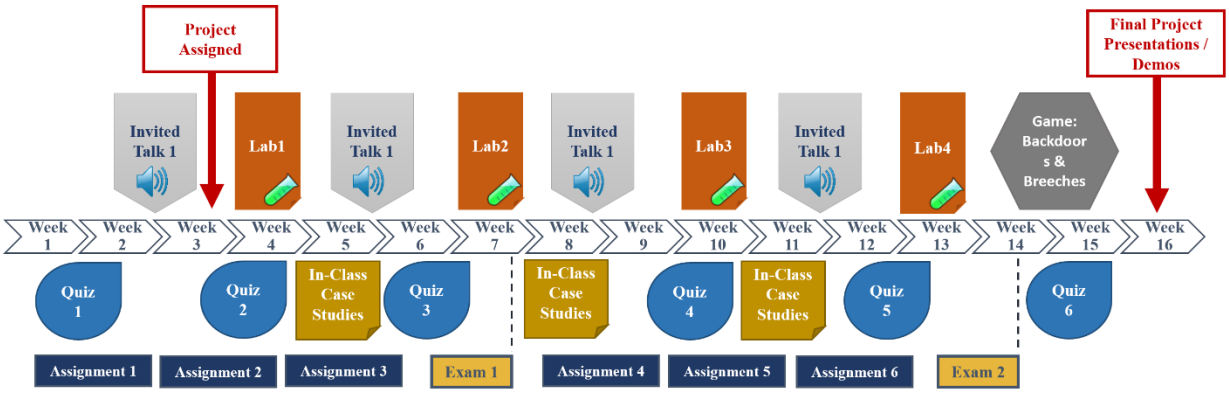

Figure 4. Course timeline overlapped with designed course activities.

Course Evaluation and Improvement

The CSCI 310 course continuous improvement is guided through a systematic methodology to test and evaluate learning tools and modalities's effectiveness against a set of objectives and factors. We adopt the process improvement lifecycle illustrated by Figure 5.

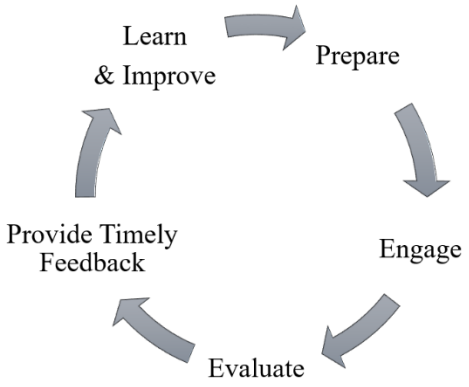

Figure 5. Adopted methodology for CSCI 310 improvement.

To enable continuous improvement of the CSCI 310 course, we structured our methodology considering two main categories of improvements.

- Agile modular improvements: such improvements were focused on enhancing the learning experience related to learning activities of the same type. For example, we needed to quickly adapt and develop a better cyberrange lab 2 based on the students' experience and feedback from cyberrange lab 1 during the semester. For this objective and support agility, we collected input for evaluation and improvement directly from students during and after each activity to better prepare and engage students with the subsequent similar activities. This type of feedback was collected verbally and was addressed in an agile manner following the same methodology illustrated in Figure 5. This type of improvements continuous to be part of the course process in its evolution.

- Strategic improvements: in this category, we focus on major changes to the course structure, outline, types/number and content of learning activities. To capture relevant input and feedback, we collected input using three channels: 1) direct student feedback through in-class reflections, 2) general student evaluation designed by the university in the first two offerings of the course, and 3) newly customized and more detailed student survey that was first conducted at the end of the most recent CSCI 310 Fall 2021 offering. The authors acknowledge this assessment survey needs to be further developed and improved in future offerings of the course.

As an indirect measure of students' engagement, we considered completion rate of assigned learning activities included in Table 1 for the Fall 2021 course offering. The results of the analysis shows that where the grade weight was the same, there was a higher completion rate for active and experiential learning activities, such as the cyberrange labs (89%), in comparison with traditional activities such as quizzes (82%). All students completed learning activities with higher-grade weights such as exams and the course project. Extensions of this work will expand

on identifying metrics to measure and analyze student's engagement and performance improvement as is described in the conclusion and future work part of this paper.

Course Student Survey and Discussion

Final feedback from students was collected using a customized survey that was distributed to the students towards the very end of the course after concluding all learning activities. Eighteen (18) students were enrolled in the class, out of which sixteen (16) responded to the survey, i.e. 89% response rate. The survey was high-level Table 2 provides a summary of the survey structure and questions types.

No	Section	Number of Questions	Example Question	Question Types
1	General	8	- Do you plan to further your interests in cybersecurity and possibly seek a career opportunity in the field? - What would you change about the class structure and the mix of class activities (lectures, invited talks, labs, quizzes/exams, discussions, case studies) so that it improves your learning experience?	• Multiple choice • Short response text field
2	Lectures	4	The lecture content of this course helped me gain foundational knowledge.	
3	Quizzes & Exams	2	On average, how much time did you spend on preparing for each exams/quizzes.	
4	Cyberrange Labs	4	Were the cyberrange labs useful in enhancing your learning experience of practical cybersecurity issues and tools?	
5	Invited Talks	4	What were the top 3 learnings you gained from the invited talks?	
6	Projects	3	Was offering more than one type of projects helpful to you to work on something more interesting and aligned with your interests?	
7	In-class Case Studies	1	Did you find the case studies and in-class discussions interesting and useful for your class experience?	

Table 2. Fall 2021 survey structure and question types

Students background, self-identified interests and course objectives:

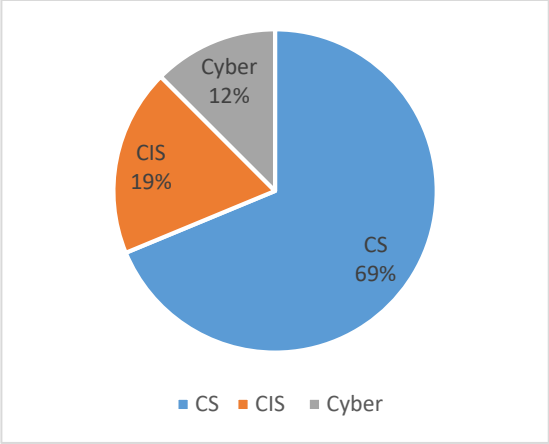

Figure 6. Student distribution by program

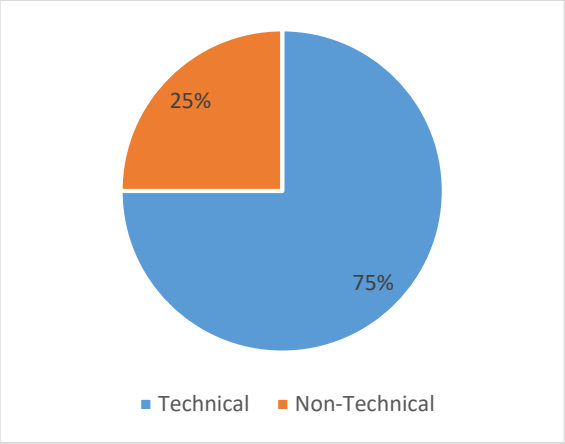

Figure 7. Student Self-Identification: Technical vs Non-Technical

The course offering had students from the three different programs (Cyber, CS, CIS) with a majority of CS students. This distribution loosely reflects the student population in the three programs at RELLIS. Students self-identified as technical or non-technical when asked: "Do you describe yourself as a technical or non-technical person?". The observation from responses to this question can be mapped to student's interests during the course and their project topic and type, this correlation was stronger for students who self-identified as non-technical.

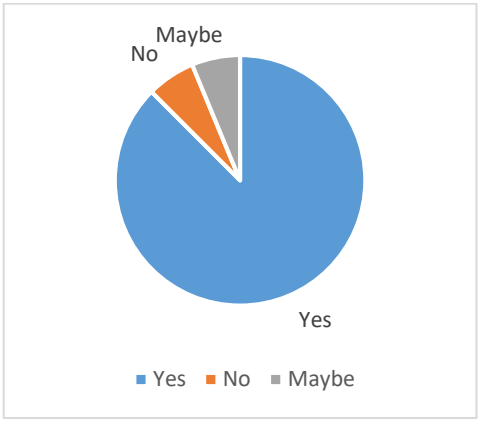

Figure 8. Response to question, "do you plan to further your interests in cybersecurity and possibly seek a career opportunity in the field?"

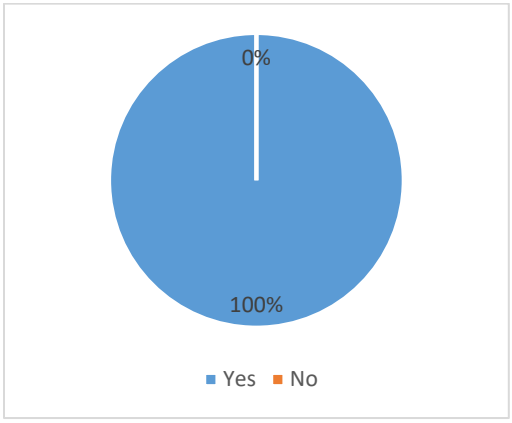

Figure 9. Response to question, "The course helped me understand the broader field of cybersecurity?"

All students who responded to the survey acknowledged that the course helped them understand the broader field of the cybersecurity. While majority of the students indicated that they are interested in furthering their interest in cybersecurity and possibly seek a career in the field.

Time spend on different learning activities

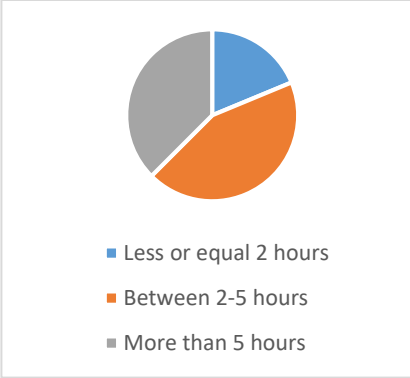

Figure 10. Average Time Spent Studying for the Course (hours/week)

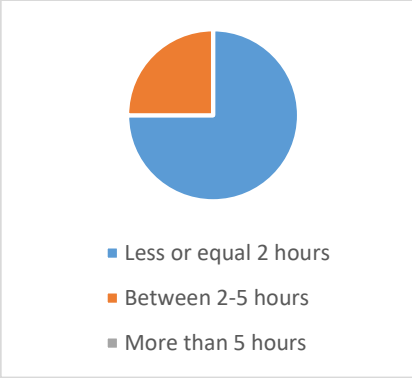

Figure 11. Average Time Spent on Cyberrange Labs (hours/lab)

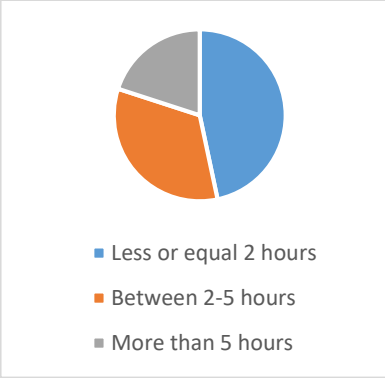

Figure 12. Average Time Spent Preparing for Exams (hours/exam)

The cyberrange labs were designed so that they are not time consuming on average. Students were observed to adjust according to their interests, their background and skillset level as they dedicated time for the course study and exam preparation.

Cyberrange labs

Figure 13. Response to the question, "Were the cyber-range labs useful in enhancing your learning experience of practical cybersecurity issues and tools?"

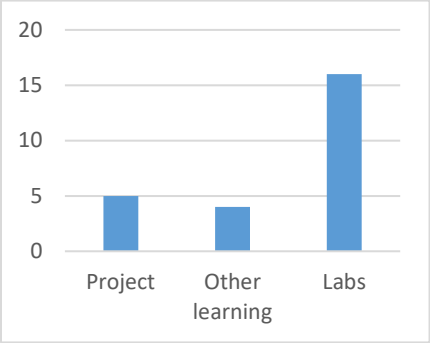

Figure 14. Cyberrange usage for labs, project and other learning.

Student mostly found the cyberrange experiential learning modules (labs) helpful and useful in gaining practical experience of cybersecurity tools and issues. Providing access to the cyberrange, supported some students in their chosen applied projects and empowered some students to further their learning on their own.

Projects

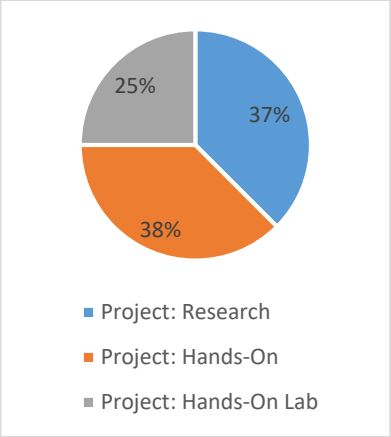

Figure 15. Student distribution by project type

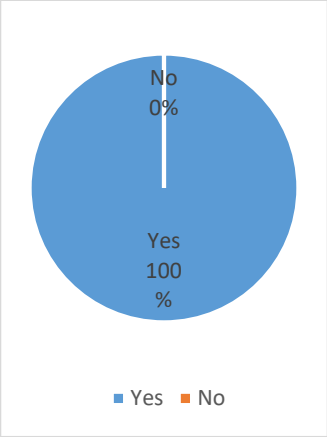

Figure 16. Offering different project types found helpful

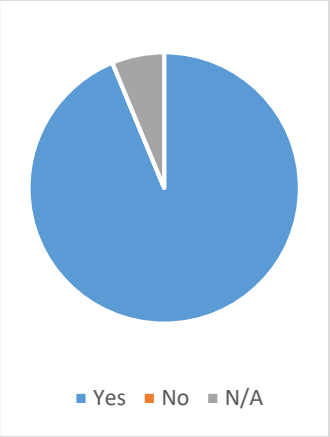

Figure 17. Students provided with resources when needed for their project

All students found offering different types of projects was helpful in allowing them to work on a project that is more aligned with their interests. Figure 15 depicts students distribution by project, where ~63% of the students, who responded, chose to work on an applied project when necessary resources were provided. The course project type and topic selection enacted students' agency in setting the goals for their own learning. For each project type included in the Fall 2021 offering, we include two examples in Table 3 below.

Project Type	**Project Examples**	**Required resources**	**Outcomes**
Hands-on applied	Security Hub Integration & Monitoring for Consumer IoT	Raspberry Pi Controller, Open-source software WebThings, Consumer IoT devices (smart plugs, cameras, home assistant, etc)	Working setup, technical report and presentation with demo
	Electric Load Switching Attacks	Smart plug, electric load (light)	Working setup, technical report and presentation with demo
Hands-on cyberrange lab	DNS Cache poisoning attacks	Cyberrange access, example online resources	Technical instructions lab manual and a working demo
	Deep-Learning data poisoning attacks	Cyberrange access, example online resources	Technical instructions lab manual and a presentation with demo
Research paper	Benefits and challenges of using machine learning in security automation	Online resources	Technical paper and presentation
	Analysis of deception techniques in cyber-attacks and defenses	Online resources	Technical paper and presentation

Table 3. Example CSCI 310 Course projects.

Invited talks and case studies

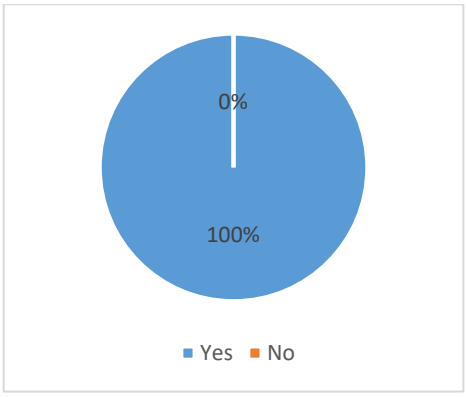

Figure 18. Invited talks relevant and interesting

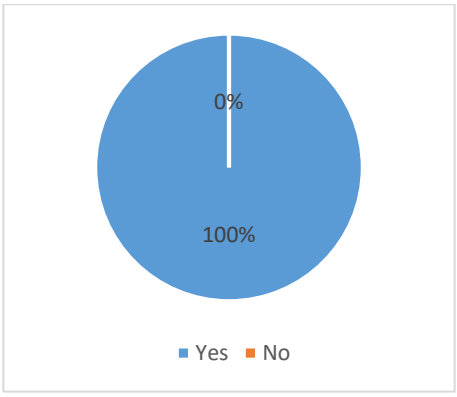

Figure 19. Case studies and discussion interesting useful for course learning

All survey respondents found the invited talks interesting, relevant and were able to articulate top three (3) learnings when asked in the survey. Most students found the invited talks insightful and helpful with respect to practical career advice. All respondents acknowledged the case studies discussions were interesting, engaging and useful for their learning in this course.

Changes to the course structure

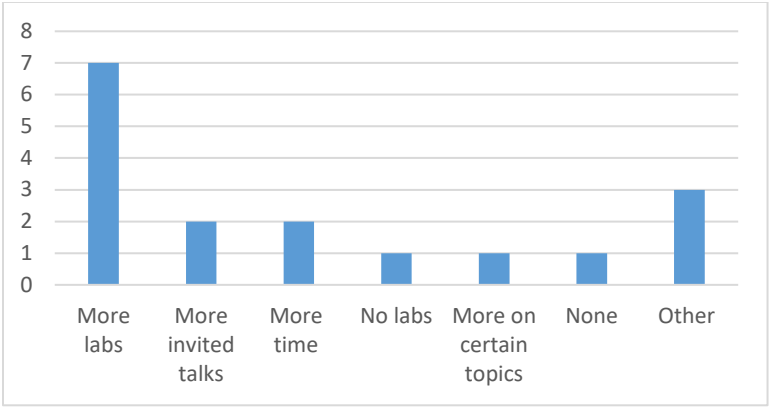

Figure 20. Response to the question "What would you change about the class structure and the mix of class activities (lectures, invited talks, labs, quizzes/exams, discussions, case studies) so that it improves your learning experience?".

Finally, when students were asked for suggestions on course structure, most students who sked for changes wanted more cyberrange labs (experiential learning).

Conclusions and Future Work

In this article, we presented our work on the development and evolution of an introductory cybersecurity course, CSCI 310 Cybersecurity, that integrates multiple active and experiential learning modalities in addition to tradition learning. We described our pedagogical approach and our embedded processes improvement life-cycle that guided our course improvement and evolution through three course offerings between Spring 2020 - Fall 2021 at the Texas A&M University System - RELLIS campus. The presented course is built around enacting students' agency, experiential learning, empowering diverse skills sets, and collective learning. We presented some observations on the learning experience based on collected student feedback.

The outcomes of this study underscores the criticality of integrated education approaches for cybersecurity that include a mix of learning activities such as traditional, active and experiential learning. It also underscores importance of adopting adaptive and agile evaluation and improvement framework. The presented approach will be further developed and extended to other cybersecurity courses in the program. We plan to continue our CSCI 310 course agile and strategic improvements including improvements of evaluations tools such as the end of semester survey where to have additional in-depth questions and multi-level scoring, to help assess the improvement in learning and measure students' engagement (detailed survey and analytics). The authors are working on other related studies, where in one project, we are developing a cyberrange environment that includes real-time measurement and monitoring of student engagement while working on cyberrange related activities.

References

[1] (ISC)2, "A Resilient Cybersecurity Profession Charts the Path Forward, CYBERSECURITY WORKFORCE STUDY," (ISC)2, 2021.

[2] W. K. S. S. B. &. W. G. Newhouse, "National initiative for cybersecurity education (NICE) cybersecurity workforce framework," NIST special publication, 2017.

[3] J. K. a. B. L. D. Nelson, "Partnership to Prepare Students for Careers in the Emerging Field of Cybersecurity," in *ASEE Virtual Annual Conference*, 2020.

[4] D. A. Kolb, "What Is Experiential Learning?," Institute of Experiential Learning, 2021. [Online]. Available: https://experientiallearninginstitute.org/resources/what-is-experiential-learning/. [Accessed 10 February 2022].

[5] E. M. A. B. F. H. H. D. B. D. K. R. A. C. T. M. B. I. A. a. X. B. Ukwandu, "A review of cyber-ranges and test-beds: Current and future trends," *Sensors,* vol. 20, no. 24, p. 7148, 2020.

[6] M. K. X. a. J. L. Rahouti, "Leveraging a cloud-based testbed and software-defined networking for cybersecurity and networking education," *Engineering Reports,* vol. 3, no. 10, 2021.

[7] X. L. A. A. M. A. N. K. K. &. H. A. Du, "Examining engineering students' perceptions of learner agency enactment in problem-and project-based learning using Q methodology," *Journal of Engineering Education,* vol. 111, no. 1, pp. 111-136, 2022.

[8] "Backdoors & Breaches," Black Hills Information Security, [Online]. Available: https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/. [Accessed 25 3 2022].

[9] J. a. F. S. Young, "Backdoors & Breaches: Using a Tabletop Exercise Game to Teach Cybersecurity Incident Response," in *Proceedings of the EDSIG Conference ISSN*, 2021.

[10] ABET, "Accredited Programs," ABET, 11 February 2022. [Online]. Available: https://amspub.abet.org/aps/name-search?searchType=program&keyword=cybersecurity. [Accessed 11 February 2022].

[11] T. K. W. C. L. J. S. L. C. D. H. A. a. B. A. W. Holloman, "The assessment cycle: Insights from a systematic literature review on broadening participation in engineering and computer science," *Journal of Engineering,* vol. 110, no. 4, pp. 1027-1048, 2021.