Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE
Paper ID #46593

Successful Engineering Capstone Design Projects based on a collaboration between the US Army and an Electrical Engineering program with a focus on Cybersecurity

Dr. Virgilio Ernesto Gonzalez, University of Texas at El Paso

Virgilio Gonzalez, Associate Chair and Professor of Practice at the ECE department at The University of Texas at El Paso, and started his first appointment at UTEP in 2001. He focuses his research on communication technologies. He received the UT System Board of Regents Outstanding Teaching Award and is actively engaged in K-12 Engineering outreach.

Pilar Gonzalez, University of Texas at El Paso

Ms. Pilar Gonzalez, a Doctoral Research Associate at the University of Texas System Louise Stokes Alliance for Minority Participation (UT System LSAMP), is also a doctoral candidate in the Teaching, Learning, and Culture (TLC) Ph.D. program at the University of Texas at El Paso (UTEP) in the STEM strand. Her research, which uniquely stems from her Hispanic background, focuses on the impact of a STEM degree on Hispanic social mobility. With over 15 years of teaching experience, from early childhood (EC) through undergraduate school, she comprehensively understands the field. She has been instrumental in implementing STEM in grade school and observing the influence of students being exposed to STEM at an early age. Gonzalez's research focuses on STEM education, and she has contributed to the field through several presentations, where her work was published with the proceedings, such as at: Frontiers in Education (FIE, 2023, 2024, 2008), GradExpo (UTEP, 2024), Louis Stokes Midwest Regional Center of Excellence (LSMRCE, 2023, 2022), InSPIRE/UTEP Edge (2023), HACU Annual Conference on Hispanic Higher Education (2022), and Future African Space Explorers (FASESA, 2022), most recently. Gonzalez holds a master's degree in STEM education from UTEP and is a member of ASEE, the Texas Computer Education Association (TCEA), IEEE, and ASCD. In addition to her academic work, she actively supports schools and teams participating in For Inspiration and Recognition for Science and Technology (FIRST), with a particular focus on those comprised of minority students. She also researched teacher preparation programs for bilingual education (BED) and English as a second language (ESL).

Dr. Rodrigo Romero, University of Texas at El Paso
Dr. Oscar Antonio Perez, University of Texas at El Paso

Mr. Oscar Perez received his PhD. in Electrical Engineering from the University of Texas at El Paso (UTEP) with a special focus on control systems and data communications. He was Awarded the Woody Everett award from the American Society for engineering ed

Successful Engineering Capstone Design Projects based on a collaboration between the U.S. Army and an Electrical Engineering program with a focus on cybersecurity

ABSTRACT

Cybersecurity is an area of growing concern, both for the defense sector and industry. Traditionally, computer science programs have an explicit component of cybersecurity, but engineering programs are less likely to include it in their curriculum. A multi-year collaboration between the U.S. Army Combat Capabilities Development Command (DEVCOM) Analysis Center (DAC) and our institution has promoted several changes in the program curriculum, established new research avenues, and enhanced the capstone design course. We have described the overall impact of the collaboration elsewhere. This paper focuses on the strategies used in the capstone design interventions.

Our electrical engineering capstone project courses, a sequence of two semesters, have been significantly enhanced through collaboration with DEVCOM. The students now design and create electronic systems with a heightened awareness of cybersecurity impacts, thanks to the new requirement. This activity is achieved through security awareness modules in the capstone courses for all students and the opportunity for at least one student team in each cohort to develop a project focused on cybersecurity involving hardware. The design requirements are based on an Army need, resulting in a product that DAC can utilize. The primary application has been the development of self-contained portable systems to train soldiers and civilians on cybersecurity using a cyberphysical system to pinpoint vulnerabilities, launch attacks, and neutralize attacks through various countermeasures.

In previous papers, we used a two-phased explanatory sequential mixed methods study using quantitative data and then explained the quantitative results with in-depth qualitative data. This paper focuses on the qualitative analysis of the impact of the capstone design based on student interviews conducted in the last phase of the capstone design.

INTRODUCTION

There is a growing concern in modern society about the rise of cybersecurity attacks, and the surface of cybercriminals continues to increase. The effects become more disruptive by affecting vital infrastructure, are more costly to organizations, and are part of global conflicts [13]. There is a need for a better-trained workforce [4]. Beyond the scope of common-sense practices [5], there is a need to adjust the scope and complexity of skills required by a modern workforce [6, 7]. Previous work has discussed the need to focus on preparing Electrical Engineers because cyberphysical systems require an understanding of hardware vulnerabilities. A multi-year collaboration between the Department of Electrical and Computer Engineering at the University of Texas at El Paso and the US ARMY Futures Command (AFC) DEVCOM [7-10]. The

partnership has many components, and this paper focuses on creating practical capstone design projects. Each semester, the entire cohort of students receives initial training in cybersecurity to generate awareness and include it as part of the considerations for all projects. Then, one of the student teams is selected to develop a project with a central security problem. We surveyed the students at the end of the capstone design sequence and used qualitative analysis methods to obtain insights into the interventions' impact. This study intends to evaluate the impact of cybersecurity interventions in capstone design projects, aiming at student learning outcomes and the efficacy of an academic-military alliance. The two research questions we intended to respond to are:

1. How much would you estimate you knew about cybersecurity before starting your Capstone Project Labs I & II?
2. How much would you say you learned about cybersecurity after cybersecurity lectures, your project vulnerability assessment, your final presentation, and your project documentation?

ECE CYBERSECURITY CAPSTONE PROJECTS SPONSORED BY AFC

The AFC's overarching goals of the projects were to develop cyberphysical systems to train cyber analysts on vulnerability detection in various environments, enhance vulnerability assessment methods, and train Electrical and Computer Engineering (ECE) students to become cyber analysts with skills for both the logical and the physical realm. To achieve these goals, the ECE capstone project teams were tasked with developing a series of cyberphysical systems called cybertutors, enabling users to explore vulnerabilities, attacks, and countermeasures of confidentiality, integrity, and availability. Each cybertutor was designed to model a specific context. The first one modeled an industrial control system, and the first student team to work on it focused on **C**onfidentiality as the security aspect to develop; subsequent teams handled **I**ntegrity and **A**vailability (CIA). The understanding of the CIA triad represents the three fundamental information security principles. Confidentiality ensures that the data is only available to authorized entities; integrity refers to maintaining the accuracy and consistency of the data, while availability guarantees that the data is accessible to authorized entities whenever needed.

AFC personnel met with each student team at the beginning of their capstone project to identify system requirements, which were in addition to the course requirements of ECE capstone projects. Each student team handled a security aspect of a cybertutor. Depending on the degree of development of the assigned cybertutor, a student team could work on a previously started system or start developing a new system, potentially modeling a new security context. The industrial control system was followed by a smart building, a field medical system, a virtual reality information technology environment, a system to monitor and neutralize unmanned autonomous vehicles, and other designs.

While developed cybertutors modeled diverse contexts, a standard architecture started evolving through the work of each student team. Based on traditional security concept introductions, each system was designed as a stand-alone network that could be monitored, attacked, and restored to expose vulnerabilities, launch attacks, and deploy countermeasures. This design would enable the

implementation of various Alice, Bob, and Eve scenarios. In cryptography, the "Alice, Bob, and Eve" framework is a conceptual model used to explain secure communication protocols. In this model, Alice is the sender, Bob is the receiver, and Eve represents an eavesdropper attempting to intercept their communication. This scenario demonstrates the necessity of robust cryptographic methods to safeguard sensitive information from unauthorized access. In the Network, victim nodes would include a master control node and a set of smart slave nodes with sensors or actuators, i.e., Alice and Bob's. For simplicity, each system would have a single, additional attacker node, i.e., Eve. Each node was implemented on a Raspberry Pi Model B per DAC requirements. Ensuring portability to enhance accessibility for multiple users, each cybertutor was fully contained in a single rugged case. See Figure 1 for examples of two cybertutors: an industrial control system and a smart building.

To meet ECE capstone project requirements, each student team follows at least one iteration of the engineering design process, aiming for a single forward pass but sometimes needing to cycle back to previous phases. A forward pass includes the following phases only once: problem identification, research, requirements specification, concept generation, design, prototype and construction, system integration, system test, delivery and acceptance, and maintenance and upgrade. In practice, the process is not entirely sequential because of the need to revisit previous phases, for instance, during the transition into the second semester of the project, and because testing is based on the Test-Vee in which requirements specification is concurrent with the design of user acceptance testing, system design is concurrent with integration testing design, and module construction is concurrent with unit testing design.

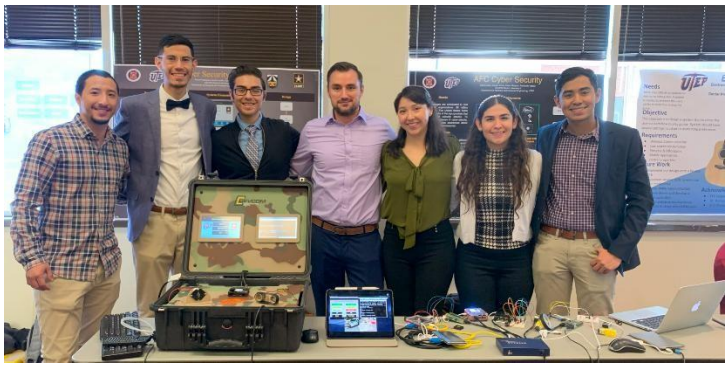

Fig. 1. On the left is a second-semester industrial control system with confidentiality and integrity measures. On the right, directly on the table, are the first-semester modules of a smart building system to explore availability.

This system design process provides multiple opportunities for teamwork, starting from problem identification and following all phases up to system design in the front end, then continuing from system integration to maintenance and upgrade in the back end. At the same time, the process also provides opportunities for individual work, starting from module design and following phases up to maintenance and upgrade. From the project management and personal accountability perspectives, the process is also advantageous because once the team completes the system design, producing a level-two functional decomposition, team members can proceed individually with a

more profound decomposition, detailed design, module construction, unit testing, and initial system integration either with their assigned modules or in collaboration with other team members.

Since student teams developing cybertutors follow the design process above, they have multiple opportunities to consider the security aspect they are handling from the point of view of each process phase. Considering confidentiality, for instance, which system requirements imply vulnerabilities to confidentiality? Which requirements are needed to protect it or restore it if attacked? At the same time, teams working on other projects attend two lectures on cybersecurity each semester, perform a vulnerability assessment after system integration, and analyze their findings, providing recommendations for future work in the final project report.

METHODS

This research follows a qualitative method. Qualitative data was collected through a survey at the end of the semester and then analyzed using a thematic framework. Said method identifies, analyses, and reports recurring patterns or "themes" within transcriptions by carefully discovering key concepts and meanings that emerge from the participants' perspectives. In this study, 25 students participated in the survey. The coding process was performed with the help of the software Intellectus [13]. Researchers analyzed codes and themes independently to triangulate the interpretation of the data.

QUALITATIVE ANALYSIS OF THE SURVEY "FALL 2024 CAPSTONE PROJECT II CYBERSECURITY LAB I AND II"

The analysis was performed by asking students to complete a survey at the end of the semester and then using qualitative methods to analyze the responses [11]. The process allowed the identification of the themes. The themes identified are:

1.1 Baseline Cybersecurity Awareness and Engagement

1.2 Absolute Beginner in Cybersecurity

2.1 Integrated Cybersecurity Education and Awareness

2.2 Enhanced Cybersecurity Competency

2.3 Incremental Knowledge Gains

Research Question

1. How much would you estimate you knew about cybersecurity before starting your Capstone Project Labs I & II?

1.1 Baseline Cybersecurity Awareness and Engagement

The theme "Baseline Cybersecurity Awareness and Engagement" directly helps answer the research question by providing insights into participants' initial levels of cybersecurity knowledge before starting their Capstone Project Labs I & II. This theme delves into the spectrum of

knowledge levels, from limited understanding to moderate foundational awareness, indicating participants' varying degrees of prior exposure and self-assessed competencies. By exploring this theme, researchers can understand participants' starting points regarding cybersecurity knowledge and their readiness to engage with the subject matter in the Capstone Project Labs.

Table 1
Number of Excerpts by Code

Code	Excerpts
1. Moderate Initial Cybersecurity Knowledge	7
1. Rudimentary Cybersecurity Awareness	12
1. Limited Initial Knowledge with Active Learning	3

1.2 Absolute Beginner in Cybersecurity

The "Absolute Beginner in Cybersecurity" theme directly addresses the research question by identifying participants with no prior knowledge or exposure to cybersecurity before starting their Capstone Project Labs I & II. This theme helps quantify the baseline understanding of cybersecurity among the participants, allowing a clear distinction between those who started with a blank slate and those who had some prior knowledge. By understanding the prevalence of this theme among the participants, researchers can determine the effectiveness of the course in enhancing knowledge and skills in cybersecurity among absolute beginners.

Table 2
Number of Excerpts by Code

Code	Excerpts
1. Pre-Existing Cybersecurity Ignorance	3

Research Question Rationale

Research Question

2. How much would you say you learned about cybersecurity After cybersecurity lectures, your project vulnerability assessment, your final presentation, and your project documentation?

2.1 Integrated Cybersecurity Education and Awareness

The Integrated Cybersecurity Education and Awareness theme directly addresses the research question by highlighting the comprehensive nature of cybersecurity education. By emphasizing the importance of understanding various aspects of cybersecurity, such as vulnerability assessment, project documentation, and final presentations, this theme helps demonstrate how a well-rounded approach to cybersecurity education can lead to a deeper understanding and appreciation of the field. It shows that through integrated education and awareness, individuals can enhance their knowledge and skills in cybersecurity, enabling them to protect critical infrastructure better and contribute to the field's advancement.

Table 3
Number of Excerpts by Code

Code	Excerpts
2. Career Inspiration through Cybersecurity Learning	1
2. Holistic Cybersecurity Awareness	14

2.2 Enhanced Cybersecurity Competency

The theme of Enhanced Cybersecurity Competency directly addresses the research question by focusing on the development of foundational understanding and heightened awareness of cybersecurity principles. This theme highlights the initial stages of knowledge growth in cybersecurity, suggesting that participants have learned and recognized diverse cyber threats and their potential impacts through cybersecurity lectures, vulnerability assessment projects, final presentations, and project documentation. This theme indicates the extent to which participants have deepened their understanding and competency in cybersecurity through the various learning activities.

Table 4
Number of Excerpts by Code

Code	Excerpts
2. Incremental Learning	2
2. Cybersecurity Awareness Expansion	6

2.3 Incremental Knowledge Gains

The theme of Incremental Knowledge Gains is particularly relevant to answering the research question. It indicates that learning about cybersecurity may occur gradually and systematically through various activities such as cybersecurity lectures, vulnerability assessments, final presentations, and project documentation. This theme suggests that individuals are likely to experience slight enhancements in their cybersecurity knowledge over time, reflecting a continuous and evolving learning process rather than a sudden or transformative grasps of the subject matter.

Table 5
Number of Excerpts by Code

Code	Excerpts
2. Minimal Learning Increment	2

Theme Description for 1.1 Baseline Cybersecurity Awareness and Engagement

This theme encompasses participants' initial levels of cybersecurity knowledge, highlighting a broad spectrum from limited to moderate foundational awareness. The codes reflect varying prior exposure, ranging from rudimentary to baseline understanding and self-assessed competencies. The descriptions indicate a common characteristic of wanting to learn more, with varying

engagement levels in realizing practical security techniques. This foundational theme underscores the significance of pre-existing technical awareness, personal privacy consciousness, and the potential for growth through targeted learning experiences.

Codes

The codes contained within the theme are included in Table 6.

Table 6
Code Frequencies for 1.1 Baseline Cybersecurity Awareness and Engagement

Code	Frequency
1. Moderate Initial Cybersecurity Knowledge	7
1. Rudimentary Cybersecurity Awareness	12
1. Limited Initial Knowledge with Active Learning	3

Excerpts

Supporting excerpts for the theme are included below.

- *I knew some basic cyber-security concepts but did not know how these concepts related to real-world situations. By developing the game around cyber-security, I researched real-world implementations of these concepts and how an attacker would use these concepts for malicious intent.*
- *I have some knowledge of cybersecurity. I have created software for encryption previously, so this was a topic I already knew about.*
- *Not much, just a basic understanding of the concept.*
- *I knew small details here and there but nothing in-depth.*

Theme Description for 1.2 Absolute Beginner in Cybersecurity

This theme captures participants without prior knowledge or exposure to cybersecurity concepts before engaging with the course or project. It highlights the starting point of absolute ignorance in the field, presenting a clear opportunity for substantial learning and skill acquisition.

Codes

The codes contained within the theme are included in Table 7.

Table 7
Code Frequencies for 1.2 Absolute Beginner in Cybersecurity

Code	Frequency
1. Pre-Existing Cybersecurity Ignorance	3

Excerpts

Supporting excerpts for the theme are included below.

- *I knew nothing about cybersecurity before starting the class.*
- *Nothing*
- *0 (zero)*

Theme Description for 2.1 Integrated Cybersecurity Education and Awareness

This theme encapsulates the dual impact of cybersecurity education that inspires career growth within critical infrastructure protection and fosters an understanding of the multifaceted nature of cybersecurity. It highlights the importance of holistic awareness that blends technical knowledge with a broader comprehension of safeguarding software and hardware systems against vulnerabilities.

Codes

The codes contained within the theme are included in Table 8.

Table 8
Code Frequencies for 2.1 Integrated Cybersecurity Education and Awareness

Code	Frequency
2. Career Inspiration through Cybersecurity Learning	1
2. Holistic Cybersecurity Awareness	14

Excerpts

Supporting excerpts for the theme are included below.

- *I learned a lot about cyber security, especially in a field I like, such as the smart grid. By working on this project, I was able to stop and think about how I could make a career in this field and became excited to think about the possibilities of working to improve the cyber-security of critical systems, such as power systems.*
- *After finishing the capstone project, I realized that cybersecurity is a huge aspect of any system. Our team learned that cybersecurity is about software and hardware that can be vulnerable and exploited if unprotected.*
- *I have a much clearer perspective on the importance of building systems that are functional and secure.*
- *Intermediate, I gained a significantly more profound understanding of cybersecurity, particularly assessing and mitigating hardware and software systems vulnerabilities.*
- *Throughout the project, I gained a much better understanding of cybersecurity. I learned about securing communication protocols like UART, identifying*

vulnerabilities in hardware, and designing systems with security in mind. The lectures and assessments helped me see the importance of incorporating cybersecurity into the design process.

- *A lot more, thinking about security in detail and further problems that could arise based on our design and program.*

Theme Description for 2.2 Enhanced Cybersecurity Competency

Development of a foundational understanding and heightened awareness of cybersecurity principles, showcasing the initial stages of knowledge growth and the recognition of diverse cyber threats and their potential impacts.

Codes

The codes contained within the theme are included in Table 9.

Table 9
Code Frequencies for 2.2 Enhanced Cybersecurity Competency

Code	Frequency
2. Incremental Learning	2
2. Cybersecurity Awareness Expansion	6

Excerpts

Supporting excerpts for the theme are included below.

- *I understand more about cybersecurity, although I believe more time and knowledge would be needed to fully understand how to utilize it more effectively in the project and future projects, primarily how to create countermeasures.*
- *I learned a lot and have a deeper understanding of the subject.*
- *After the lectures, I learned a lot about the importance of cybersecurity and how it could affect all types of electronics. I also became more familiar with the different types of attacks.*

Theme Description for 2.3 Incremental Knowledge Gains

Captures the notion of small, gradual increases in understanding, where individuals experience slight enhancements in their cybersecurity knowledge. This theme highlights more evolutionary than revolutionary learning, indicating awareness of new concepts without a profound or transformative grasp.

Codes

The codes contained within the theme are included in Table 10.

Table 10
Code Frequencies for 2.3 Incremental Knowledge Gains

Code	Frequency
2. Minimal Learning Increment	2

Excerpts

Supporting excerpts for the theme are included below.

- *A little more than before.*
- *2/10 (20%).*

CONCLUSIONS

The formal collaboration resulting from the funded proposal occurred during the COVID-19 pandemic. We observed that before the interventions, most students had little awareness of how cybersecurity topics related to Electrical Engineering applications. Taking the training in class and applying it to solve a real problem enabled a better understanding and confidence in including cybersecurity requirements in their projects. Many of the curriculum changes were possible thanks to the support from DAC. Their letters and constant communication describing their needs helped shape the new curriculum.

The straightforward program changes provided all the students in a cohort with awareness of cybersecurity concepts. Such changes can be implemented at any institution without needing an external sponsor. However, adding specialized cybersecurity projects benefits us from having external customers. We believe this type of collaboration can be replicated in other institutions with different levels of involvement from the DoD agencies. Some of the changes are generic and only require focusing on the capstone design and some existing courses in the curriculum. Some projects might require external sponsors, but cybersecurity is in high demand, and many private organizations could be interested in sponsoring specific projects.

ACKNOWLEDGMENT

The research was sponsored by the Army DEVCOM Analysis Center and was accomplished under Grant Number W911QX20D0002. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies of the Army or the U.S. Government, either expressed or implied. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes, notwithstanding any copyright notation herein.

REFERENCES

[1] S. Furnell, H. Heyburn, A. Whitehead, and J. N. Shah, "Understanding the full cost of cyber security breaches," *Computer fraud & security*, vol. 2020, no. 12, pp. 6-12, 2020, doi: 10.1016/S1361-3723(20)30127-5.

[2] D. Woods and P. Hirsch. "*Cracking the code on cyber insurance*." NPR. https://www.npr.org/transcripts/1093656544 (accessed 04/22/2022, 2022).

[3] Chang. "*The role cyberattacks and information campaigns have played in the war in Ukraine*." NPR. https://www.npr.org/transcripts/1089774585 (accessed 04/22/2022, 2022).

[4] J. Blazic, "Changing the landscape of cybersecurity education in the E.U.: Will the new approach produce the required cybersecurity skills?" *Education and information technologies*, vol. 27, no. 3, pp. 3011-3036, 2021, doi: 10.1007/s10639-021-10704-y.

[5] K. Daimi and G. Francia, III, *Innovations in Cybersecurity Education*, 1st 2020. ed. Cham, Switzerland: Springer, 2020.

[6] Steven Furnell and M. Bishop. "*Addressing cyber security skills: the spectrum, not the silo*." https://www.magonlinelibrary.com/doi/abs/10.1016/S1361-3723%2820%2930017-8 (accessed 04/22/2022, 2022).

[7] S. Furnell, "The cybersecurity workforce and skills," *Computers & Security*, vol. 100, p.

[8] 102080, 2021/01/01/ 2021, doi: https://doi.org/10.1016/j.cose.2020.102080.

[9] V. Gonzalez, O. Perez, and R. Romero, "Collaboration program to disseminate cybersecurity in the ECE curriculum," in *2022 IEEE Frontiers in Education Conference*, FIE 2022, October 8, 2022 - October 11, 2022, Uppsala, Sweden, 2022, vol. 2022-October: Institute of Electrical and Electronics Engineers Inc., in Proceedings - *Frontiers in Education Conference*, FIE, doi: 10.1109/FIE56618.2022.9962613. [Online]. Available: http://dx.doi.org/10.1109/FIE56618.2022.9962613

[10] Gonzalez, V., O. Perez and R. Romero (2023). Cybersecurity in ECE Curriculum, an

[11] Expanded Collaboration Program to Disseminate Real Security Experiences in Cyberphysical Systems. 53rd IEEE ASEE *Frontiers in Education International Conference*, FIE 2023, October 18, 2023 - October 21, 2023, College Station, TX, United States, Institute of Electrical and Electronics Engineers Inc.

[12] V. Gonzalez, O. Perez, R. Romero, P. Gonzalez, and H. Erives-Contreras, "Multi-year collaboration between the US Army and an ECE program to develop student skills in cybersecurity of cyberphysical systems," in *2024 IEEE Frontiers in Education*, Washington, DC, October 2024, 2024.

[13] Intellectus Qualitative [Online computer software]. (2025). Intellectus360. https://qualitative.intellectus360.com