Collaboration program to disseminate cybersecurity in the ECE curriculum

Virgilio Gonzalez
Electrical and Computer Engineering
University of Texas at El Paso
El Paso, TX, USA
: email address or ORCID

Oscar Perez
CEAD
DEVCOM
WSMR, NM, USA
oscar.a.perez46.civ@army.mil

Rodrigo Romero
Electrical and Computer Engineering
University of Texas at El Paso
El Paso, TX, USA
raromero2@utep.edu

***Abstract*— Work in Progress: This paper presents innovative practices in Cybersecurity Education. This field is becoming a critical skill to protect the modern infrastructure. Traditionally cybersecurity has been perceived as a skill used mainly by computer scientists. However, there are concerns about the communication protocols operating at lower layers because the vulnerabilities closer to the physical systems do not receive the same attention as the user applications and human interactions. Consequently, Electrical and Computer Engineering programs must introduce cybersecurity awareness in those areas. A common solution is the addition of a cybersecurity class in ECE curriculums. We tried a more holistic approach by providing interventions in different aspects of the student preparation providing a richer experience.**

A partnership between the US Army Combat Capabilities Development Command (DEVCOM) Analysis Center (DAC) at White Sands Missile Range (WSMR), and the Electrical and Computer Engineering Department at the University of Texas at El Paso (UTEP) has resulted in students learning about cybersecurity through several methods. The partnership helped define the modification of the curriculum and offered opportunities for new research projects. The efforts include sponsorship of capstone projects and support for graduate teaching assistants specialized in promoting cybersecurity education to the entire cohorts.

The specialized teaching assistants offered training to the entire cohort of students participating in the capstone design course to provide everyone with cybersecurity awareness. Some of the capstone projects specialized in designing and building cyber-trainer devices that the soldiers use in the WSMR. Since the fall semester of 2020, three cohorts, including 115 senior students, have benefitted from cybersecurity awareness training. Three major capstone projects were developed, creating cyber-trainers used by the ARMY.

Two new courses were added to the Electrical Engineering curriculum, and a new track in security was proposed for a Computer Engineering program. Three graduate students were hired as teaching assistants to help the educational efforts while working on their research projects related to cybersecurity. Several students applied for internship experiences at the ARMY, and some are considering permanent job offerings in the field. Finally, the collaboration has opened other opportunities to apply for traditional research funds in the cybersecurity domain.

Keywords—Cybersecurity Education, Electrical and Computer Engineering, DoD Partnerships.

I. INTRODUCTION

Cybersecurity threats are growing in impact on our daily lives. There have been multiple incidents reported in the news. The trend is that they are becoming more costly to organizations [1, 2], and they are potentially weaponized as part of global conflicts [2, 3]. Those incidents have prompted different organizations to emphasize the need for a workforce better trained on cybersecurity aspects [4]. However, the typical approaches promote the best common-sense practices [5]. Therefore, there is a need to adjust the scope of skills required by a modern workforce [6, 7].

Computer science programs have taken the lead in introducing cybersecurity in their curriculum. However, Blair et al. [8] propose that cybersecurity teams must be composed of different specialties to be more effective. NIST has published the National Initiative for Cybersecurity Education (NICE) National Cybersecurity Workforce Framework (NCWF) [9], which decomposes the significant functionalities and skills needed in this field. Consequently, several professional organizations (ACM, IEEE, AIS, and IFIP) have jointly developed the CSEC2017 curriculum guidelines for cybersecurity degrees [10]. This framework proposes to structure the curriculum around several knowledge areas:

- 4.1 Knowledge Area: Data Security

- 4.2 Knowledge Area: Software Security
- 4.3 Knowledge Area: Component Security
- 4.4 Knowledge Area: Connection Security
- 4.5 Knowledge Area: System Security
- 4.6 Knowledge Area: Human Security
- 4.7 Knowledge Area: Organizational Security
- 4.8 Knowledge Area: Societal Security

Electrical engineering programs might benefit from introducing general cybersecurity concepts through their curriculum, and they are better prepared to focus on the *Component Security* and *Connection Security* knowledge areas.

II. Partnerships with the Department of Defense

The Department of Defense needs a well-prepared STEM workforce to support modern tools used by the defense sector. It has several initiatives to create a pipeline of students that will fill the positions in different DoD entities or related industries [11]. These activities range from K-12 education involvement [12] to University collaborations.

The U.S. Army Combat Capabilities Development Command, known as DEVCOM [13], delivers future readiness as the Army's premier organization for the modernization cornerstones of science, technology, and engineering. The DEVCOM Analysis Center (CEAD) needs skilled personnel to study different cybersecurity threats.

For several years the CEAD has collaborated with the Computer Science Department at UTEP. However, the impact of the cyber domain requires other perspectives to have a complete analysis of different systems. In 2019 CEAD started collaborating with the Electrical and Computer Engineering (ECE) department sponsoring a capstone design project for EE majors each semester. In 2020 we proposed a comprehensive collaboration to include cybersecurity in a holistic approach and impact more students.

The UTEP is located in El Paso, Texas, and is a minority-serving institution where 83% of the students are Hispanic. The College of Engineering had a total enrollment of 4300 students, and 651 received BS degrees during the AY 2020-2021, 130 from Computer Science and 105 from Electrical Engineering, therefore offering an excellent opportunity to impact the graduating class instead of just a handful of students.

III. Interventions

The CEAD collaboration with the Computer Science (CS) department introduced a course in cybersecurity and has offered a capstone design theme for CS students for multiple semesters. We proposed interventions in three major areas for the ECE program, including capstone design projects, dissemination of cybersecurity awareness, and curriculum changes. The expansion to the Electrical Engineering program started in the spring of 2019 with a single project each semester and a team of 4 students. In 2020 we supported an expansion of cybersecurity awareness to the entire EE student cohort. We also proposed curriculum changes including new courses and a specialized concentration for ECE students

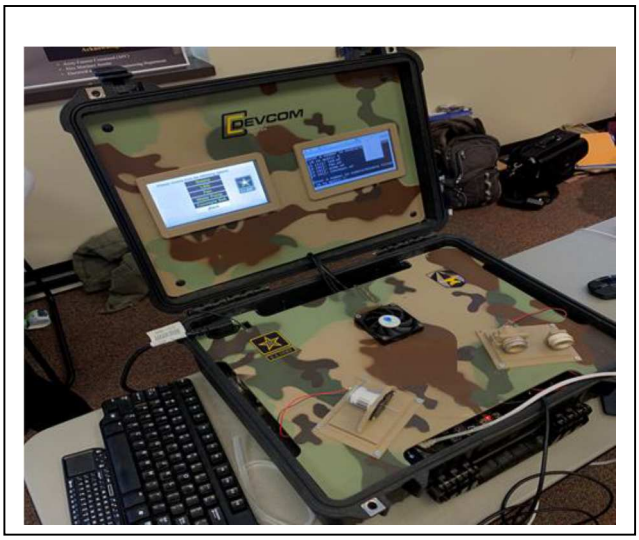

Fig. 1. Mobile Cybersecurity Trainer System

Capstone design projects in cybersecurity. The EE program has a two-semester capstone sequence called Senior Projects I and II (EE4220 and EE4230) offered every semester; thus, there are always simultaneous courses in parallel. Students must participate in a team consisting of three or four students, and all the topics are different. During the academic years 2019 and 2020, only two groups participated in cybersecurity projects each semester in the corresponding EE4220/4230. Their designs targeted the creation of portable cyber-trainer systems (Figure 1) that had an embedded demonstration of security concepts, such as Confidentiality, Integrity, and Availability. For example, a demonstration of a computer-controlled factory, and how it can be hacked. Other projects showcased spying attempts between unencrypted and encrypted channels, or a Denial-of-Service attack. The intended audience is soldiers that need to learn about cybersecurity.

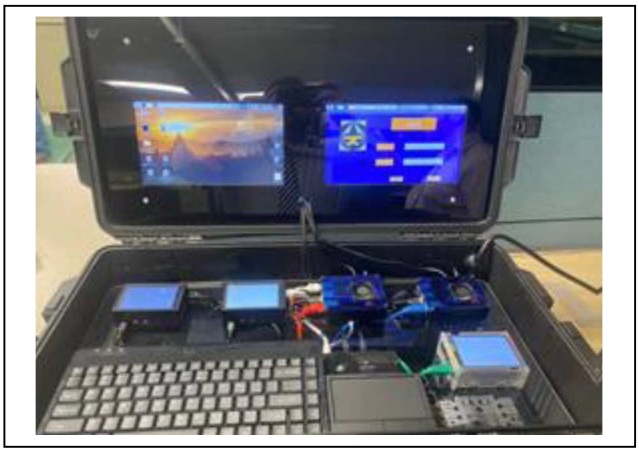

Fig. 2. Biomedical sensor

Entire ECE cohort awareness. In spring 2020, we sent a proposal to DEVCOM to expand the collaborations, and we got additional funding to support several efforts through DEVCOM DAC's Cyber Center for Analysis and Assessment. The capstone design continues with more advanced projects, and now they are incorporating ideas to test biomedical sensors (Figure 2) and add Augmented Reality (Figure 3) devices. Besides the teams developing a cyber-trainer each semester, we incorporated a Graduate Teaching Assistant into the capstone course. The TA is specialized in cybersecurity topics and created training materials to provide awareness to all the students in each Senior Projects cohort. The training included concepts in preserving the confidentiality of information in the system, maintaining data integrity, and keeping the system available. The students had to make a simple vulnerability analysis of their system with those considerations for all the projects. That enables the addition of cybersecurity risks as a consideration by all student teams.

The cost for each senior project ranges from $1k to $5k depending on the requirements of DEVCOM. This part of the budget changes every semester. We have about $20k per year budgeted for the teaching assistant. There are other indirect institution costs added.

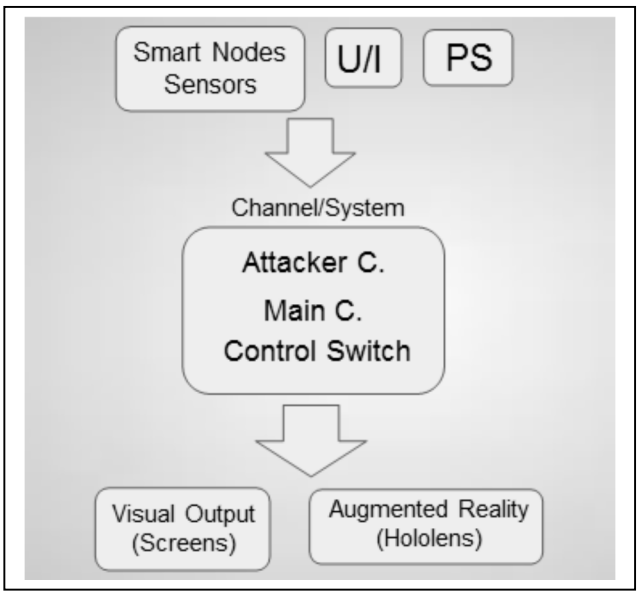

Fig. 3. Augmented Reality Project

Curriculum changes. The ECE department created two formal courses in cybersecurity geared toward embedded systems and provides foundational knowledge to EE students. One class is for undergraduates, and the other is for graduates. Other courses, such as Software Design II, Introduction to Communication Networks, and Data Communications, added some awareness topics in security. These courses emphasize the knowledge areas of *Component Security* and *Connection Security*.

The ECE department initiated the process to offer a new B.S. degree in Computer Engineering. The process was already underway, and the collaboration influenced the decision to include a concentration track in cybersecurity. The new degree offering is expected for 2023.

IV. Results and Pending Work

The proposal for additional funding was awarded in Fall 2020, and there have been four advanced capstone projects supported directly with this grant. There were 16 students involved. They benefited from the direct application of cybersecurity knowledge in their projects.

	Course							
Sem.	3354	3372	4220	4230	5330	4395 5390	Cyb Part.	Grad cohort
Fall 18	28	37	50	42			0	42
Spr 19			37	50	21		4	50
Sum 19			6	6			4	6
Fall 19	28	31	61	36		15	19	36
Spr 20			51	63			8	63
Sum 20			5	11			8	11
Fall 20	9	21	52	45		27	35	45
Spr 21			21	51	16		88	51
Sum 21			8	2			10	2
Fall 21	19	20	36	28		23	126	28
Spr 22			26	34			60	34

Since the spring 2021 semester, 115 students have completed the Senior Projects sequence, all of whom have been exposed to cybersecurity concepts in the class and gaining awareness of its application to other problems.

Table 1, Enrollment and Participation

In addition, the following courses started offering some topics in cybersecurity:

- EE3372 Software Design 2.
- EE3354 Intro to Communication Networks.
- EE4395 / 5390 Special Topics in cybersecurity.
- EE5330 Data Communications.

Table 1 shows the enrollment in different courses from fall 2018 until spring 2022. Before Fall 2019 there was no formal course offering or awareness of cybersecurity in the EE program. Between the spring of 2019 and the fall of 2020, there were 4 students per capstone project involved in a specific cybersecurity project (8 total per semester). Also, we started offering an elective course that included about half senior and half graduate students. The "Cyb Part" column indicates the number of students involved in some cybersecurity topics during

the semester (green highlight) and the “Grad Cohort” column is the total number of students graduating during the same semester. The grant from DEVCOM, in spring 2021, enabled the expansion of course offerings (yellow highlight) and promoted the broader participation of students.

We found, through different questions, how many students had some level of cybersecurity training in the program. The EE program graduated 110 students during the academic year between fall19 - sum20, however, only 12 obtained cybersecurity knowledge through projects or the new course, and the rest of the cohort did not have any exposure. In comparison during the last academic year between sum21 - spr22, we graduated 64 students. About 24 reported a deeper cybersecurity experience, but the entire cohort obtained some basic awareness through the capstone class or other supplementary courses. There are more students participating in cybersecurity efforts than the graduating class each semester. Notice that the recent decrease in cohort enrollment was due to the COVID impact on the university in general.

We recently submitted a proposal to offer a new degree in Computer Engineering. An important component of the new degree proposal requires industry support. The backing from DEVCOM and the inclusion of the cybersecurity concentration attracted other companies to also offer letters indicating their interest in the new program and convinced the UTEP to approve the proposal in Spring 2022 at the institution level. Now the proposal is just pending approval from the State Higher Education Coordinating Board.

As a secondary effect, these efforts have increased the interaction between faculty and engineers from DEVCOM. Consequently, we have obtained new grants or contracts to support studies on wireless security or the use of A.I. to train Intrusion Detection Systems. As a result, two more graduate students were hired to support the collaborative efforts.

V. Conclusions and Future Work

The formal collaboration resulting from the funded proposal occurred during the COVID-19 pandemic. For this "Work in Progress," we focused only on implementing the activities required by the proposal and the total number of participants. We observed that before the interventions, at most 12 out of 110 students obtained some cybersecurity experience. After the intervention 24 out of 64 students gained a deeper understanding of cybersecurity and the entire cohort gained awareness.

For the next cohort in fall 2022, we plan to collect additional data to understand the level of expertise gained by different students in their capstone projects. In addition, the other courses that offer cybersecurity topics, are only offered in the fall.

Many of the curriculum changes were possible thanks to the support from DEVCOM. Their letters and involvement in describing their needs helped shape the new curriculum.

The simple program changes provide all the students in a cohort with awareness of cybersecurity concepts. Those can be implemented at any institution without the need of an external sponsor. However, adding specialized cybersecurity projects benefits 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.

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] A. 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] B. 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. 102080, 2021/01/01/ 2021, doi: https://doi.org/10.1016/j.cose.2020.102080.

[8] J. R. S. Blair, A. O. Hall, and E. Sobiesk, "Educating future multidisciplinary cybersecurity teams," Computer, vol. 52, no. 3, pp. 58-66, 2019, doi: 10.1109/MC.2018.2884190.

[9] W. Newhouse, S. Keith, B. Scribner, and G. Witte, "National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework," NIST special publication, vol. 800, no. 2017, p. 181, 2017.

[10] Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery Joint Task Force on Cybersecurity Education, 2018.

[11] N. Lim, A. Haddad, D. M. Butler, and K. Giglio, "First steps toward improving DoD STEM workforce diversity: response to the 2012 Department of defense STEM diversity summit," Rand National Defense Research Inst Santa Monica CA, 2013.

[12] "DoD STEM." Department of Defense. https://dodstem.us/ (accessed 04/22/2022, 2022).

[13] "ARMY DEVCOM." https://armyfuturescommand.com/devcom/ (accessed 04/22/2022, 2022).