Interdisciplinary Cybersecurity Projects Experience: Developing a Market Ready Workforce

Dr. Tamer Omar, California State Polytechnic University, Pomona

Tamer Omar is an Assistant professor with the Electrical and Computer Engineering Department at California State Polytechnic University. Dr. Omar earned his Ph.D. from the Electrical Engineering department at Iowa State University, USA and his MBA with emphasis on MIS from the Arab Academy for Science and Technology, Egypt and his B.S. degree in Electrical Engineering from Ain Shams University, Egypt. Dr. Omar research interests include wireless networks architecture, resources allocation in wireless networks, heterogeneous networks, self-organized networks, big data implementation and analysis, RDBMS and decision support systems. Dr. Omar has 8 years of experience in academia and more than 10 years of industrial experience in different ICT positions.

Dr. Abdelfattah Amamra

Dr. Abdelfattah Amamra joins California State Polytechnic University, Pomona as an Assistant Professor in the Department of Computer in the College of Sciences. Prior to coming to CalPoly, Pomona he was an Assistant Professor at the University of Connecticut. Dr. Amamra received his Ph.D. from the University of Quebec, Montreal, Canada. His primary research interests are in the field of cybersecurity and machine learning. Specifically, he is interested in smartphone security, and IoT security.

Dr. Kristina Rigden, California State Polytechnic University, Pomona

Dr. Kristina Rigden is the Director of Outreach Programs and the Women in Engineering Program for the College of Engineering at California State Polytechnic University, Pomona (Cal Poly Pomona). In her position, she provides several different outreach programming events to engage K-12 female students to pursue STEM majors and/or careers. Dr. Rigden holds a B.A. in Liberal Studies from Cal Poly Pomona, a TESOL certificate, a M.A. in Teaching with a multiple-subject credential and an Ed.D. from the University of Southern California.

Dr. Thomas Ketseoglou, Cal Poly Pomona

Thomas Ketseoglou received the B.S. degree from the University of Patras, Patras, Greece, in 1982, the M.S. degree from the University of Maryland, College Park, Maryland, USA, in 1986, and the Ph.D. degree from the University of Southern California, Los Angeles, California, USA, in 1990, all in electrical engineering. He worked in the wireless communications industry, including senior level positions with Siemens, Ericsson, Rockwell, and Omnipoint. From 1996 through 1998 he participated in TIA TR45.5 (now 3GPP2) 3G standardization, making significant contributions to the cdma2000 standard. He has been inventor and co-inventor in several essential patents in wireless communications. Since September 2003 he has been with the Electrical and Computer Engineering department of the California State Polytechnic University, Pomona, California, USA, where he is a professor. He spent his sabbatical leave in 2011 at the Digital Technology Center, University of Minnesota, Minneapolis, Minnesota, USA, where he taught digital communications and performed research on network data and machine learning techniques. He is a part-time lecturer at the University of California, Irvine. His teaching and research interests are in wireless communications, signal processing, and machine learning, with current emphasis on MIMO, optimization, localization, and link prediction.

Interdisciplinary Cybersecurity Projects Experience: Developing a Market Ready Workforce

ABSTRACT

The increasing advancement in Internet of Things (IoT) and Industry 4.0 inspires more connectivity of vital infrastructure to the cloud. Securing our infrastructure digital and control systems is currently a crucial demand in a cyber-world characterized by continuous cybersecurity attacks. Preparing qualified students to satisfy the current and future work force requirement in cybersecurity is deemed essential. One of the main cybersecurity domain challenges is its interdisciplinary nature that involves scientists, engineers, technologists, and business teams. It is almost impossible in real life to mitigate threats and defend against attacks without assembling teams and qualified team members with skills in all the aforementioned disciplines. This paper aims at presenting the plan and procedures required for creating an project based interdisciplinary course at cybersecurity of frontier technologies between the College of Engineering, College of Science, and College of Business Administration. The course objective is to bring students from the three disciplines into a multidisciplinary experience that aids students at replicating real life projects. Instructors from all three disciplines guide the students during the course work and supervise the project activities. The fifteen-week course can adopt different types of cybersecurity systems and provide a framework for students' collaboration on a practical project. The framework consists of four modules divided between the three disciplines: 1) project scope, system integration, and teamwork incorporation; 2) system engineering, cybersecurity design, and application development; 3) system cybersecurity algorithms, data collection, organization, and analytics; 4) system business planning, cybersecurity applications operations implementation, and maintenance. The paper also presents an example for an IoT based project to apply the framework and show the projected course model in developing the IoT project.

INTRODUCTION

The demand for qualified cybersecurity professionals is increasing in an unprecedented rate. Advancement in Internet of Things (IoT) and Operational Technologies (OT) domains add to the surface of attacks to the existing vulnerable Information Technology (IT) systems domain. These attacks include a number of diverse threats such as Distributed Denial-of-Service, ransomware, Advanced Persistent Threats and others. All these threats affect the operations of the IT/OT/IoT systems and cost globally \$148 million in 2018 [1, 2].

Cybersecurity is interdisciplinary by nature. The survey in [3] shows that cybersecurity science is not only related to computer and engineering science, but to many different sciences such as information science, business and management, psychology, criminal justice, and forensic science. We recommend in this work that a cybersecurity program should be interdisciplinary to provide students with strong skills and knowledge in different areas. The authors in [4] developed a Cyber Science course associate faculty from mathematics, science, engineering, computer science, and liberal arts colleges. The course aims at teaching students the benefits and dangers of cyberspace, in addition to drive them to fundamental concepts across these disciplines.

Creating larger populations of domain engineers with cybersecurity awareness explored in [5] illustrates that awareness can lead to expertise. The authors focus on cybersecurity between industrial control systems and other disciplines such as chemical engineers design refineries, civil engineers design structures, and mechanical engineers design industrial robots.

Multiple instructional approaches have been used to increase students' interest in cybersecurity. The game-based learning approach proposed in [6] provides motivation to students' willing to study the power grid through inclusion of the physics of power systems, cyber physical vulnerabilities, energy markets, and control systems. The game provides the mechanism for understanding the impact from computer security, growth of customer base, power generation assets, energy markets, automation, and human operator decisions on the stability of a small electric grid.

The study in [7] presents a peer-based learning approach with cybersecurity co-curriculum activities conducted and assessed using a student survey. Results demonstrate the efficacy of these activities in increasing students' technical skills and excitement about cybersecurity. From this study, students founded their own association to pursue coursework in the cybersecurity field. The association hosts multiple types of activities including peer-learning sessions that benefit students from participating in different hands-on activities.

Using a community-based learning approach, authors in [8] describe the development and evolution of an interdisciplinary seminar course that provide a cornerstone design experience addressing the national academy of engineering grand challenges [9]. The study elaborates on the collaboration between an engineer with expertise in biomedical engineering and design, and a political scientist with expertise in politics and gender of development in the global south. The offered seminar course aimed to address both the needs of non-engineering students to make a difference in the world through their academic scaffolds and curricula constructed to encourage research and community-based work. It also addressed engineering students' needs to develop critical thinking skills about the potential and limitations of engineering design methods, local social context, and economic and political systems.

The research-based learning approach introduced in [10] describes and advocates for the experiences of engaging undergraduate students in collaborative faculty cybersecurity mentoring. The approach focuses on the learning process of doing research rather than the product of research itself. Students start with a broad topic as they focus on creating a research question, read and learn about the research topic, discuss finding with faculty mentors, and present a talk or create a poster about their research and results.

The goal of the challenge/problem/puzzle-based learning approaches in [11, 12, 13] was to improve student learning via asking questions to understand complex problems. The studies elaborate the effect of challenges in motivating students. Students in these programs adopt this approach to participate in competitions, focus on active learning, and an interactive learning environment to help students better participate in course activities.

The authors in [14] present an assessment of the educational benefits to undergraduates from participation in a research experience for undergraduates program on the topic of cyber-physical system cybersecurity. The assessment highlights a student benefit from participation, which is gaining technical skills. The study also shows other benefits to the students, such as system design and time management skills.

One of the prime motivations for the proposed course is to instill the concepts of entrepreneurship, science, technology, engineering, and interdisciplinary collaboration in students so they may pursue careers in areas related to Internet of Things (IoT) applications. These concepts can strengthen motivation and improve on student learning. Furthermore, the instructors of this course will work alongside the students to enhance their awareness of IoT and possible threats, attacks and defense techniques as well as to assist in learning new technologies and tools. In addition, students will be able to increase their skills, knowledge and abilities of IoT and cybersecurity. The course will develop their competency in innovation processes, develop their leadership/soft skills, and prepare them for a career in cybersecurity.

The second motivation for this course is the industry trend towards technology convergence in today's advanced manufacturing. Industries and organizations are rapidly converging their IT with their (Operational Technology) OT to provide new IoT systems. A persistent influx of networked industrial control solutions into the manufacturing processes has led to a rapidly growing demand for a new class of students; one that incorporates today's skillsets expected from engineering professionals and those skills traditionally associated with systems cybersecurity.

Students from the College of Engineering (CoE), College of Science (CoS), and College of Business Administration (CBA) will have the opportunity to join this interdisciplinary course. Students will select and complete a scientific/technological synthesis application project in the area of IoT under faculty supervision. Students will work in a multidisciplinary team project that include engineering, science and business disciplines. Each student in the group will work within the project team to:

- 1- Develop the scope of the project within the discipline of practice,
- 2- Prepare project workflow and logistics,
- 3- Develop project time and resources management,

- 4- Survey literature about technical aspects of the project,
- 5- Gather project requirements from stakeholders (e.g. industry)
- 6- Design the project and use appropriate tools for design implementation and design testing,
- 7- Write a formal report and prepare an oral presentation.

The proposed course will rely on project based learning practices and techniques to achieve the course goals, encourage student participation, innovation, and entrepreneurship. The authors aim that this course will be a unique, pragmatic, state-of-the-art multidisciplinary project experience for undergraduate students. The course will focus on the contemporary, high job demand area of cybersecurity applications. It will offer collaboration among three colleges (CoE, CoS, CBA) to leverage from delivered student knowledge transfer and deliver an effective, two-semester project based course.

CLASS OBJECTIVES & RESEARCH QUESTIONS

The class objectives are summarized into four folds:

1. Student engagement in interdisciplinary work of frontier technologies and its cybersecurity related aspects.
 - a. Build interdisciplinary teams comprising of three to six students from the Computer Science (CS), Electrical and Computer Engineering (ECE), and Computer Information Systems (CIS) departments to get involved in projects studying frontier technologies and their cybersecurity aspects.
 - b. Prepare students with the required skills and knowledge for joining a real interdisciplinary workforce environment.
 - c. Promote a cybersecurity culture in the three participating colleges and increase students' interest in cybersecurity in order to provide a pipeline of qualified candidates to the highly demanding workforce in the area of cybersecurity.
2. Motivate undergraduate student research on frontier technologies and their cybersecurity related aspects.
 - a. Develop a command and control system to collect, organize and analyze data collected from roadside units monitoring and autonomous and remote pilotless vehicles to test and the vehicle to infrastructure reliability and security.
3. Improve persistence and graduation rates among participants.
 - a. Increase retention and graduation of financially disadvantaged, underrepresented minority, and female students in the fields of ECE, CS, and CIS.
 - b. Measure participating students' capability to secure job offers before graduation.
 - c. Measure the retention and graduation rates of program participants.
 - d. Measure the effectiveness of the program to help students acquire skills and knowledge about frontier technologies.
4. Increase faculty impact on improved STEM teaching and learning through exploitation of frontier technologies.
 - a. Measure the impact of the faculty on increasing students' interest in cybersecurity.

- b. Measure the impact of the faculty on increasing students' interest in control systems including IoT and Internet of Vehicles (IoV).

Additionally, the pedagogical research related to the class development aims at answering the following research questions:

1. How does participation in this course engage students in interdisciplinary work on Frontier Technologies and its cybersecurity related aspects?
2. What is the impact of persistence and graduation rates among the students participating in the course versus the college population of students not participating in this course?
3. What is the impact of faculty participating in this course towards improving STEM teaching and learning of frontier technologies and their cybersecurity related aspects?

COURSE OUTLINES

Course Description

Students will select and complete an engineering/scientific/technological synthesis application project under faculty supervision. Students from CoE, CoS, and CBA will create a multidisciplinary project team with at least one student from each college to develop a project in frontier technologies and their cybersecurity aspects. Projects developed by students must include engineering, scientific, and technological aspects and must be conducted under the supervision of faculty from the three disciplines. An academic technical written report must be completed and submitted at the end of the course. Students will publish their research/final project report and present their project work at an undergraduate conference/event.

Course Learning Outcomes

After completing this course, students will

- 1- Identify a multidisciplinary project scope and state the project proposal.
- 2- Plan project activities and verify plan milestones accomplishment.
- 3- Outline the project literature review, find and evaluate resources.
- 4- Design project specification, and evaluate project constraints, needs, and risks.
- 5- Implement, assemble, test, validate and produce proposed designs using frontier technologies such as IoT design tools.
- 6- Report project findings and demonstrate the findings in an academic symposium.

Students Deliverables for Evaluation of Outcomes

- 1- Project proposal.
- 2- Literature review, introduction and references report.
- 3- Methodology, design, proof of concepts, and test bed implementation report.
- 4- Results, graphs, and discussions of findings report.
- 5- Completed project report draft.
- 6- Peer review and Comprehensive Assessment for Team-Member Effectiveness (CATME) survey for project team evaluation.

- 7- Project final report and academic symposium submission proof.
- 8- Project presentation and post

Course Schedule

The course uses a project-based approach and the students from CS, ECE, and CIS departments will form an interdisciplinary team to achieve the following milestones:

Fall Semester Milestones

Week 2: Each student shall enroll into one of the projects groups on Blackboard.

Week 3: The project topic shall be determined, and a two-page project summary will be submitted by each group.

Week 6: Each group will submit a five-page literature review with correct citations. The literature should cover the following aspects:

- a) State why the problem you address is important,
- b) State what is lacking in the current knowledge
- c) State the objectives of your study or the research question

Week 9: Each group will submit a 15-page paper with methodology, design, proof of concepts, and implementation test bed. The methodology section may contain some or all the following:

- a) Describe the context and the setting of the study
- b) Specify the study design
- c) Describe the “population” (participants)
- d) Describe the sampling strategy
- e) Describe the intervention (if applicable)
- f) Identify the main study variables
- g) Describe data collection instruments and procedures
- h) Outline analysis method

Spring Semester Milestones

Week 3: Methodology, design, proof of concept, and test bed implementation submission due.

Week 7: The written paper with results, graphs, and discussions of findings will be due. The results section may contain the following:

- a) Report on data collection and recruitment (response rates, etc.)
- b) Describe participants (demographic, experimental condition, etc.)
- c) Present key findings with respect to the central project scope
- d) Present secondary findings (secondary outcomes, subgroup analyses, etc.)

Week 8: Final report due

Week 9: Any required corrections on final report due

Week 12: Supporting material (e.g. codes, hardware) submission due

Week 13: Project poster/presentation submission due.

STUDENT RECRUITMENT PROCESS

The course will be offered as an open enrolment course. However due to limitation of resources and available faculty, the Engineering Office of Outreach will manage the enrolment materials, the student application for the course, and rubrics to evaluate all applicants from the three colleges. The applications will be blind reviewed to choose the best candidates from each college to enroll in the course. The Engineering Office of Outreach will manage all student information for the course.

Selection Criteria

Priority during selection will be given to senior students. Students will be selected to enroll in the course based on reviewing a portfolio of information provided to the selection committee. The portfolio would include a transcript, a student statement, letters of recommendation, and a stipend application form.

Transcript

Transcript provides information about the student's academic potential and demonstrates the consistency of course work over a period.

Student Statement

Students should provide a statement that describes why they want to enroll in the course and outline their academic and career goals.

Letters of Recommendation

Letters of recommendation could come from any source such as faculty, community members, or supervisors. The recommendation letter should provide the student's characteristics and qualities against the course objectives. One recommendation letter will be required from a faculty member.

Applications Evaluation

The process of selection includes the examination of the curriculum vitae to evaluate student academic qualification and reference letters. The objective of our selection process is to identify students who are most likely to be successful in the course. The academic qualification of a student is evaluated based on the following criteria: current GPA, academic grades of related courses taken, relevant studies and training. The applicant is also required to have a recommendation letter from a faculty member.

EVALUATION PLAN

Mixed-methods sequential explanatory study is a procedure for collecting, analyzing, and integrating both quantitative and qualitative data for the purpose of gaining a better understanding of the research [15, 16]. The mixed-methods sequential explanatory design consists of quantitative data collection followed by qualitative. Quantitative and qualitative methods complement each

other and allow for a more depth analysis, taking advantage of the strengths of each method [17, 18].

The overall goal of this course is to increase interdisciplinary knowledge with a focus on cybersecurity of frontier technologies such as IOT among CoS, CoE, and CBA. To answer the research questions, students in the course will complete a pre- and post-test survey and participate in focus groups each semester of the course. The faculty will complete an interview with the evaluator each semester. Observations will also take place in the interdisciplinary classroom twice a semester noting interactions, processes, and behaviors related to cybersecurity of frontier technologies. In addition, document collection will take place consisting of the student's homework assignments and final project papers.

Evaluation will be ongoing for the class, a protocol will be developed to guide faculty interviews, student focus groups, and classroom observations. The research protocol will be approved by the university Institutional Research Board (IRB) before research will commence.

Evaluation of Class Objectives

The table below provides an overview of the formative and summative data sources that will be used to measure each class objective:

	Input	Objective 1: Student Engagement	Objective 2: Student Research	Objective 3: Persistence and Graduation Rates	Objective 4: Improved STEM Teaching and Learning
Class Development with class Pilot (Fall 2020)	Students	Pre-Survey and Post-test Survey; Focus Group; Formative feedback (quizzes & assignments) and posttest (exam); Observation Data	Document Collection; Focus Group; Formative feedback (quizzes & assignments) and posttest (exam/final class project)	College Data	
	Faculty	Interview	Perform project activities according to proposed curriculum		Interview
Pilot Refinement based on Formative Feedback (Fall 2021)	Students	Pre-Survey and Post-test Survey;	Document Collection; Focus Group;	College Data	

		Focus Group; Formative feedback (quizzes & assignments) and posttest (exam); Observation Data	Formative feedback (quizzes & assignments) and posttest (exam/final class project)		
	Faculty	Interview			Interview
Class Launch and Summative Results (Fall 2022)	Students	Pre-Survey and Post-test Survey; Focus Group; Formative feedback (quizzes & assignments) and posttest (exam); Observation Data	Document Collection; Focus Group; Formative feedback (quizzes & assignments) and posttest (exam/final class project)	College Data	
	Faculty	Interview			Interview
	Final Project Evaluation Report				
beyond longitudinal data			Post-Survey and College Undergraduate Research Data	College Data	Faculty Use Data

STUDENT's INTERDISCIPLINARY PROJECT EXAMPLE

The following description shows an example of a project using frontier technologies. A vehicle can be remotely controlled through wireless link using a car Virtual Racer X (VRX) simulator. The VRX racing simulator will use Internet of Vehicles (IoV) technology to support autonomous driving. Let us consider an extreme case in which there is a disaster zone that cannot be accessed by humans. A vehicle, controlled by a human through a simulator in a safe area, can be sent into this zone to collect useful data.

This real-time vehicle simulator project aims at creating a vehicle that can be controlled by humans, making it unnecessary for a driver to be present inside the vehicle. With this in mind, the project hopes to facilitate the use of a vehicle when it is crucial that no driver be present, whether to avoid a dangerous zone or simply for practicality. The goal is to successfully establish a fast and reliable communication between the vehicle simulator and a remote pilotless vehicle.

In undertaking this project, the activities focus on creating a two-way communication, capturing simulator data (e.g. steer controls), and sending the controls to a vehicle using an Application

Programmable Interface (API) hosted on an intermediate server. First to capture the simulator data, C++ is used as the coding language to capture the VRX simulator driver actions and map the external environment to the driver on the simulator screens. Second, developing an IOT systems using controllers to control the vehicle steering, speeding, and other parameters by sending the VRX simulator controls over 4G network using mobile data and LTE Advanced vehicle router. Lastly, interpreting the data flowing between the vehicle and the simulator by relaying the data using an API server to primarily transmit and receive the vehicle control and environment surveillance, and secondarily to perform threats analysis using Intrusion Detection System (IDS) to support the control, communication, and vehicle systems. Figure 1 shows a system overview of the remote pilotless vehicle project.

Simulator

A communication system will link between a real-time simulator system and an remote pilotless vehicle system. There are multiple communication architectures and IOV is currently the most popular one. IOV includes different types of networks such as Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), Vehicle to Pedestrian (V2P), Vehicle to Device (V2D) and Vehicle to Grid (V2G). Vehicle to Everything (V2X) communication require three main components to construct the network and these include an On-board Unit (OBU) in each vehicle, a Roadside Unit (RSU) that make the transportation infrastructure, and a network infrastructure to connect the V2X networks. In this project, IoV will be used to provide the V2X connectivity using cloud and 4G LTE communication system. The data that needs to be collected will be coming from the VRX simulator, including laying out the necessary steps for data collection from vehicle's sensors. The network type implemented in this project is a client-server based network. The server listens to client connections and accepts commands from the connected client. Then, the server publishes the commands where they become available for the controller to read and relay them to the vehicle. The client accepts user input and transmits the corresponding commands remotely to the Server via an IP address connection over the 4G network.

In the client interface, the data collected from the simulator and the image port should be set for communication between the simulator and the game engine. The parameters of the IP address and the port should point to the server. The two predened formats for the data that will be transmitted are command data or sensing information (the communication server module is stand-alone and uses Linux). This server will connect to the vehicle through a 4G network provided by Sprint.

Therefore, the goal is to have the network successfully send information to the vehicle and the vehicle will receive this information using the 4G LTE modem and then distributes this information to the vehicle sensor and actuators using Wi-Fi and a Controller Area Network (CAN) of Raspberry PIs and Arduinos controllers.

The vehicle will have its own interface through which it receives control messages from the user terminal (vehicle simulator) of an operator and uploads various observation data obtained from its equipment. In the project, two interfaces will be implemented and data will be collected from both. One interface will connect the simulator to the server and the other interface will establish a connection between the car controllers and the server.

One important issue with simulator data collection is that a common notion of time is a mandatory requirement, otherwise the needed realism cannot be achieved. The simulation environment needs to have a common notion of time and to achieve this clock synchronization needs to be implemented. Clock synchronization captures the time tick generated by the simulator, which is the main clock source. This distributes it to all the other components in order to allow the evolution of the simulation with a common knowledge of time. There are two known approaches used to achieve clock synchronization: event-driven and time-driven. In the event-driven approach, events are placed in a queue which is handled by a proper scheduler which retrieves and processes them accordingly. The time-domain approach is performed according to a certain sampling time in which for each iteration, it is assumed that a time interval equal to the sampling time elapses and state information is updated using an equation. The time-driven approach will be implemented since the project utilizes real-time data.

Application Programmable Interface (API)

API is an application programming interface and is a platform to connect varying forms of software in order to achieve a higher goal. The tasks of the API include creating subroutines between software to exchange data, creating connections and protocols, and being able to communicate what is happening with the user in order to acquire the desired outputs.

There exist many forms of APIs that have different functions, in the case of the specified objective, of vehicular control through a remote virtual controller, specific functions are required from the API. These include being able to: read the sensors of the virtual controller and vehicle, process the information through a dedicated server, transmit the read signals, and store testing data for future cybersecurity threat analysis research. The ability to store past trial information is important because it can be used for future simulations and troubleshooting.

Wireless Network

Two types of wireless networks are implemented in this project; the long-distance communication will be done through the 4G network provided by Sprint and the smaller radius wireless communication will be done through Wi-Fi using the wireless module. A specific server will be responsible for all communication data coming in and out from the 4G network. Another computer will be connected to the vehicle simulator which will be responsible for transferring data to and from the simulator and back to the communication server. Most of the data transmission will be happening through the 4G LTE network provided by Sprint. Internet of Vehicles is a good example

of how communication with the car is possible. The specific IP address will help to keep the flow of information private and undisturbed. This will ensure that a safe and intact flow of data is obtained from the car simulator to the server. Using a 4G network instead of a 3G network will help keep the real-time responses within a reasonable time limit. The modem will have a slot to insert a Sprint sim card. This will enable us to send the data from the server to the 4G network which will then transfer the data to the vehicle.

Cybersecurity Aspects

The traffic between the simulator and the vehicles is investigated to detect any possible attacks on the control system. To address the vulnerabilities in the control system, the project will utilize a statistical method (e.g. entropy) to address and recognize the difference between a normal and malicious network traffic. The effectiveness of attack detection solution will be studied and realized. The best solution will be proposed and implemented in the controller. A service will be implemented as an API to detect any malicious user who is responsible of any attacks (e.g. Distributed Denial of Service (DDoS)).

CONCLUSION

This course aims at developing new proposed interdisciplinary projects in Fall 2020 with a research-based learning approach that attracts and retains students interested in STEM fields. The course offers students interested in frontier technologies in the areas of Cybersecurity and IOT projects that will bring together students from three different disciplines: engineering, science, and information systems. Students will learn about frontier technologies in order to excel in their future practical workforce experience. An project example for remotely controlling a vehicle through wireless link using a car Virtual Racer X (VRX) simulator is presented to show a sample of the frontier technologies applications in the course. The VRX racing simulator will use IoV technology to support autonomous driving. IoV technologies rely on wireless communication to send the car and driving controls from the VRX simulator to an API. The API is a server that will be connected to the internet and thus transfer the data that is being collected to the vehicle. The server will act as a cloud service to communicate the data into the vehicle and receive the data back at the simulator side. The simulator controls the vehicle by using a communication link (4G LTE modem) attached to the vehicle and operated by Sprint. The modem connects the vehicle to receive controls and send feedback to and from the VRX simulator. IoV provides a dynamic mobile communication network that communicates between vehicles On Board Units (OBUs) and Roadside Units (RSUs) to provide the required support to vehicles during their routes and trips. If network intrusion attacks succeed to compromise IoV systems, intruders will control the autonomous vehicles communicating with the infrastructure, and this may lead to serious fatal consequences. Therefore, using an IDS to protect the IoV system is very crucial. In this project, students will use traditional IDS to protect the IoV system.

REFERENCES

- [1] Cisco, "Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper," 2019.
- [2] IBM, "The demand for cybersecurity professionals is outstripping the supply of skilled workers," 2019.
- [3] T. Omar, S. Venkatesan and A. Amamra, "Development of Undergraduate Interdisciplinary Cybersecurity Program: A Literature Survey," in *ASEE Annual Conference & Exposition*, Salt Lake City, 2018.
- [4] T. Heath, C. Krystal, Galen and Turner, "Cyber Science - Interdisciplinary Approach to Cyber Studies," in *ASEE Annual Conference & Exposition*, Atlanta, 2013.
- [5] G. Rhonda, M. Thomas, D. Rishabh, L. Yu, A. Thiago, Z. Hongyu and F. Farbod, "Work in Progress: Layering Cybersecurity on Domain Engineering Instruction," in *ASEE Annual Conference & Exposition*, Tampa, Florida, 2019.
- [6] T. R. McJunkin, C. G. Rieger, A. Rege, S. K. Biswas, M. Haney, M. J. Santora, B. K. Johnson, R. L. Boring, D. S. Naidu and J. F. Gardner, "Multidisciplinary Game-based Approach for Generating Student Enthusiasm for Addressing Critical Infrastructure Challenges," in *American Society for Engineering Education (ASEE)*, New Orleans, LA, 2016.
- [7] J. Straub, "Assessment of the Educational Benefits Produced by Peer Learning Activities in Cybersecurity," in *American Society for Engineering Education*, Tempa, FL, 2019.
- [8] J. S. Rossmann and H. Stewart-Gambino, "Cornerstone Design for Sociotechnical ”Grand Challenges”,," in *American Society for Engineering Education (ASEE)*, Tempa, FL, 2019.
- [9] National Academy of Engineering, "NAE Grand Challenges for Engineering," National Academy of Sciences on behalf of the National Academy of Engineering, 2019. [Online]. Available: <http://www.engineeringchallenges.org/>.
- [10] C. E. Frank, J. W. McGuffee and C. Thomas, "Early undergraduate cybersecurity research," *Journal of Computing Sciences in Colleges*, vol. 32, no. 1, pp. 46-51, 2016.
- [11] R. S. Cheung, J. P. Cohen, H. Z. Lo and F. Elia, "Challenge Based Learning in Cybersecurity Education," in *Proceedings of the International Conference on Security and Management (SAM). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp)* , 2011.

- [12] P. Stephens, "Problem-based learning in cybersecurity at CCCU.," in *12th Annual Teaching Computer Forensics Workshop*, Sunderland, UK, 2016.
- [13] D. Dasgupta, D. M. Ferebee and Z. Michalewicz, "Applying Puzzle-Based Learning to Cyber-Security Education," in *Information Security Curriculum Development Conference (InfoSecCD '13)*, Kennesaw GA, USA, 2013.
- [14] J. Straub, "Experiential Research Education: A Report on the First Year of a NSF-sponsored Cyber-physical System Cybersecurity Research Experience for Undergraduates Program," in *ASEE Annual Conference & Exposition* , Tampa, Florida, 2019.
- [15] N. V. Ivankova, J. W. Creswell and S. L. Stick, "Using Mixed-Methods Sequential Explanatory Design: From Theory to Practice," *Field Methods*, vol. 18, no. 1, p. 3–20, 2006.
- [16] S. R. Terrell, "Mixed-methods research methodologies," *The Qualitative Report*, 2012.
- [17] J. W. Creswell, *Research Design.: Qualitative, Quantitative, Mixed Methods Approaches*, University of Nebraska-Lincoln, 2016.
- [18] O. M. Mugenda, *Research methods: Quantitative and qualitative approaches*, African Centre for Technology Studies, 1999.