NATIONAL CYBERWATCH CENTER

Innovations in Cybersecurity Education

2019

Table of Contents

01. EVIDENCE-BASED STRATEGIES

02. INSTRUCTION

Table of Contents

03. PRACTICE

04. PROGRAM DEVELOPMENT

05. HONORABLE MENTION

Message from the Director

On behalf of the National CyberWatch Center, I'm happy to present the 2019 Innovations in Cybersecurity Education booklet. A byproduct of our awards and recognition program, this publication showcases a range of creative and pioneering ideas across four categories: evidence-based strategies, instruction, practice, and program development. My hope is that this publication will accelerate the adoption and adaptation of new ideas throughout the academic and workforce development communities, while at the same time, recognizing individuals and organizations for their work.

Moving forward, we will be exploring the growth of the Innovations program by focusing on the quality of submissions, as well as continuing to promote your work beyond the confines of academia. If you have ideas on how we can improve this program, please feel free to contact me.

Thanks to all who submitted proposals this year and a special congratulations to the winners, who will be announced at the 2019 Community College Cyber Summit (3CS) in Shreveport, LA.

Sincerely,

Casey W. O'Brien
Executive Director & Principal Investigator
National CyberWatch Center

01

EVIDENCE-BASED STRATEGIES

WINNING SUBMISSION:
PATHWAY TO ADVANCEMENT IN CYBERSECURITY EDUCATION (PACE)

PATHWAY TO ADVANCEMENT IN CYBERSECURITY EDUCATION (PACE)

EVIDENCE-BASED STRATEGIES

DESCRIPTION

K-12 public education is developed on principles that all students need a solid foundation of core academic knowledge and lifetime skills to be successful. In reality, this has translated into a single goal of preparing students for 4-year colleges rather than providing a multifaceted approach to career development. As a consequence, high school dropout rates are still a major concern even for relatively affluent districts such as Anaheim Union High School with only 88% graduation rates in 2016 (EdSource.org). Furthermore, high school graduates are not necessarily ready to complete college or transfer to 4-year schools as is evident from the low completion rates. Only 53.1% of Cypress College first time students received a degree, certificate and/or transferred after six years beginning in 2010-2011 (scorecard.cccco.edu).

A guided Cybersecurity pathway that builds on cyber content developed during Middle school years is most likely to succeed. Introducing dual enrollment pathway as early as 9th grade with multiple educational and employment exit points is applicable to a wider student population and will positively impact high school and college dropout rates. The overall goal of this innovation is to develop and implement a Pathway to Advancement of Cybersecurity Education (PACE) from middle school all the way to 4-year College with multiple opportunities for employment exit points:

- Develop a plan based on Collaboration with all the stakeholders
- Embed Cybersecurity content in middle school/high school curricula
- Provide outreach activities to generate interest in Cybersecurity
- Develop/revise Cybersecurity certificate and Associate in Arts (AA) degree programs
- Provide articulation and alignment with 4-year institutions
- Recommend best practices

BENEFITS

The specific PACE strategy to attract students from early ages to the program and develop a strong pathway to prepare students for the cybersecurity field has been successfully tested during the past two years with our pilot middle school/high school cohort. The results for the 2018-19 academic year are as follows:

- Cybersecurity certificate, Cyber Defense Certificate and Associate in Science (AS) in Cyber Defense were developed and implemented
- A course "Cybersecurity Competition Fundamentals" was established that required CyberPatriot training and competition in addition to CompTIA's ITF+ certification. 154 middle school/high school students have completed this course which is also articulated with Magnolia High School
- 127 high school students completed industry certificates (i.e. CompTIA ITF+, Network+, Security+, CySA+ and Cisco CCENT, CCNA and IINS
- 37 HS students completed our College certificates (19 students in Cybersecurity 12 units; 12 students in Cisco Networking 12 units; 9 students in Cyber Defense; 24 units)
- 1,170 elementary/middle school/high school students participated in our Cybersecurity monthly trainings and 53 teams participated in the official CyberPatriot competition

CONTACT INFORMATION

Behzad Izadi
bizadi.cypress@gmail.com
(714) 801-3354
Cypress College

TVA (THREAT VULNERABILITY ASSET) METHODOLOGY

EVIDENCE-BASED STRATEGIES

DESCRIPTION

Research demonstrates that the use of vulnerability assessment (VA) tools are instrumental in identifying cyber threats and system vulnerabilities (Whitman and Mattord, 2018). Our innovation uses the TVA (Threat Vulnerability Asset) methodology to guide cybersecurity student project teams to generate a working TVA matrix.

The TVA matrix identifies and prioritizes an organization's most critical IT assets, identifies the cyber threats to those critical IT resources, identifies the organization's IT safeguards currently in place, and the resulting system vulnerabilities revealed from the triangulation of these three TVA matrix components. The development of the TVA matrix also provides cybersecurity students with useful insights for re-balancing the assignment of IT safeguards to better identify and address an organization's greatest system vulnerabilities.

The TVA methodology was selected as an open-source and effective VA tool that has been increasingly considered by cybersecurity educational programs that seek an uncomplicated but innovative approach to improve the current IT educational pedagogy for identifying cyber threats and system vulnerabilities.

BENEFITS

The use of the TVA methodology as a free and uncomplicated VA tool for identifying cyber threats and system vulnerabilities has become increasingly appealing to both organizations and educators. Higher education courses in IT and cybersecurity have the opportunity to go beyond mere classroom lectures about cyber threats, exploits and cyber attacks, and provide an engaging pedagogy of applied projects (such as the TVA methodology) that clearly demonstrate how cyber threat affect system vulnerabilities.

CONTACT INFORMATION

Dr. Roberto Mejias, Associate Professor of CIS
roberto.mejias@csupueblo.edu
(317) 432-8412
Colorado State University-Pueblo, Dept. of Computer Information Systems,
Center for Cyber Security Education & Research (CCSER)

FACULTY PERCEPTIONS OF OPEN EDUCATIONAL RESOURCES IN CYBER CURRICULUM

EVIDENCE-BASED STRATEGIES

DESCRIPTION

This innovation is part of my dissertation at Dakota State University for a Doctorate in Philosophy in Cyber Operations. The research involves a survey instrument geared towards faculty perceptions of open educational resources in cyber curriculum. At the time of 3CS, I will be in the data collection phase to procure responses for my survey based upon previous literature into OER perceptions.

Open educational materials provide a unique opportunity for individuals in reducing barriers to educational endeavors. No cost materials, cheap distributions methods, such as the Internet, and diversity of available topics is transforming learning for individuals across the globe. In particular, the availability of open materials on mobile devices is becoming increasingly popular for accessing information. Individuals seeking to transform the landscape of cybersecurity education can create and find resources to shape the technical, analytical and problem-solving skills needed for the cyber workforce. This research surveys the literature to discover the awareness, effectiveness, and potential barriers creators and adopters of Open Educational Resources (OER) may have when dealing with cybersecurity topics. The purpose of this study is to frame faculty perceptions of OER in the context of cyber curriculum usage.

BENEFITS

The study will set a foundation to study the awareness, perceptions of OER effectiveness, and perceptions of OER potential barriers to adoption of OER in cyber curricula. It will paint a big picture of the current perceptions of faculty surrounding OER usage in cyber course pedagogy. This will lead to further research on the utilization and efficacy of OER in different high-level functions of the cyber discipline and help cyber faculty make informed decisions when deciding content for cyber curriculum instruction.

CONTACT INFORMATION

Alan Stines
alan.stines@trojans.dsu.edu
(478) 972-1030
Middle Georgia State University | Dakota State University

ADVANCED CONCEPT MAPPING: AN ACTIVE LEARNING, MULTI-SENSORY LEARNING TOOL

EVIDENCE-BASED STRATEGIES

DESCRIPTION

At its core, a concept map is a hierarchical, visual representation of knowledge. A basic concept map is typically comprised of just two components: nodes and the lines connecting them. An advanced concept map (ACM) is comprised of five components; an anchor node, nodes, clusters, connections, and arcs. The anchor node represents the main topic and serves as the visual center and starting point of the ACM. It should stand out and is always a unique size, shape, and color. The nodes (shapes) are the individual concepts and are typically single words. The connections are what takes this approach beyond a basic concept map. The connections are the descriptive text between two individual nodes. The connections describe how and why the two nodes are related. Connections require students to demonstrate the depth and understanding of their knowledge. The deeper and more complex the connection, the higher the student's score. That can be done in three to five sentences.

Clusters are groups of related nodes (e.g. a chapter, module, or topic). Clusters (and their underlying hierarchy) should be visually similar. For example, each node in a cluster would be the same shape. The hierarchy would be illustrated through the use of color and size. Each cluster would be denoted by a different color. Each hierarchical level in a given cluster would be a different shade of that same color. Arcs are connections spanning from a node in one cluster of knowledge, to a node in a totally different, seemingly unrelated cluster. Connecting two widely dissimilar nodes typically requires a higher degree of understanding. These are always red so that they stand out from the other connections.

ACMs constructed using digital tools have some distinct advantages over those done with pen and paper. Digital maps have a virtually limitless canvas. They can accommodate small maps (5-10 nodes and connections) up to very large maps (those over 100 nodes and connections). In addition, digital maps are much easier to search, edit, and read. There are several freely available tools that can be used to build ACMs. Some of those include VUE from Tufts University and the web-based diagramming tool from LucidChart. Prior to their first exposure to Advanced Concept Mapping, learners should be introduced to the principles, components, and benefits of the ACM process.

BENEFITS

Advanced Concept Mapping is a "force multiplier" in terms of research-based benefits that enhance learning and recall. These benefits are well-established in the scientific research on learning. Our sense of sight has more effect on learning than any of our other senses. The ACM process is a visual representation of knowledge. As such, it leverages all of the considerable benefits of visual learning. While our sense of sight trumps all other senses in terms of learning benefit, using more than one sense is even more beneficial. ACMs require learners to organize and connect information into a hierarchical structure. In doing so, students must translate the information from a narrative form (books, notes, articles, etc.) to a visual form. In this way, it creates a multisensory process. The research makes it clear, engaging multiple senses during the learning process is much better than engaging only one. ACM construction requires significant effort on the part of the learner. When constructing an ACM, students must select, organize, combine, and process information. In working through these steps, student learning is improved. Done properly, ACMs require higher order thinking skills as defined by Blooms Taxonomy.

CONTACT INFORMATION

John Sammons
sammons17@marshall.edu
(304) 696-7241
Marshall University

02

INSTRUCTION

WINNING SUBMISSION:

THINKING OUTSIDE THE BOX - USING ESCAPE ROOM GAMES TO INTEREST TEACHERS AND STUDENTS IN CYBERSECURITY

THINKING OUTSIDE THE BOX - USING ESCAPE ROOM GAMES TO INTEREST TEACHERS AND STUDENTS IN CYBERSECURITY

INSTRUCTION

DESCRIPTION

It is no secret that there is a shortfall of cybersecurity teachers, students, and professionals across the globe. And to make matters worse, the interest level among diverse populations is very low. For this reason, it is necessary to find innovative ways to interest students as well as teachers in cybersecurity at the K12 level.

The prominent cybersecurity teaching tool has been the Capture the Flag (CTF) game. In one version of this game, players look for security flaws in a system/network. When they find a flaw, they capture a flag. In this manner, players learn about cybersecurity threats and how to fix them. The game is played in teams, often over a weekend. It is very competitive. Although it is an effective learning tool, it is usually for advanced students and is often frustrating for beginners to try to join in.

The cybersecurity-based escape room challenges participants to interact with their surroundings to uncover clues. At each step, players learn a new cybersecurity principle. Additionally, the puzzles are designed in such a way that participants must work together to find the solution. The most recent game we designed is an Escape the Suitcase challenge. This game is portable and easily taken to conferences. Conference goers are given a card set that simulates the suitcase and physical objects within it. They are also given a Python script where they may enter their guesses and advance to the next level. The first challenge is to unlock the briefcase using only a Happy Birthday card. This challenge invites students to think about password strength. The full game can be found here: https://drive.google.com/drive/folders/12r7MgGky2pX5EcwR_Ek2Y3CTOHefJtPG

BENEFITS

This game provides a non-competitive option as well as an opportunity for students to practice team work and to think outside of the box. It is a unique tool to help increase self-efficacy and an interest in studying cybersecurity. The game has had some early successes: we were invited to hold a workshop on this new teaching method at the 2018 Women in Cybersecurity (WiCyS) - see Workshop 4.4 - https://www.wicys.net/2018-workshop. We were the featured game at the 2018 USENIX Workshop on Advances in Security Education (https://www.usenix.org/conference/ase18). The game has been turned into an IOS application as part of a graphic design project at George Washington University. This game is also being used at several GenCyber camps sponsored by the NSA across the country. Currently, we are working on new levels of the game.

CONTACT INFORMATION

Suzanne Mello-Stark
smellostark@ric.edu
(401) 456-4720
Rhode Island College

MAN-IN-THE-MIDDLE (MITM) ATTACKS ON IOT SYSTEMS

INSTRUCTION

DESCRIPTION

Internet of Things (IoT) comprises of interconnected "things" with unique identifiers that can be assigned IP addresses and possess the capability of transferring information over a communication medium without the need for any human or computer interaction. The information being communicated can range from configuration messages for heart implants to sensor readings to trigger a control system in industrial IoT. Secure transmission of this data is paramount to the safety and privacy of the owner and the correct working of the system.

Man-in-the-Middle attacks (MiTM) allow attackers to plug into the middle of a conversation without the knowledge of the communicating entities by relaying the traffic between the two. This grants the attackers the ability to intercept, eavesdrop, or alter the information in a manner of their choosing. All IoT devices rely on some form of radio frequency communication such as Wi-fi, Zigbee and Bluetooth. In the past, attackers have demonstrated that vulnerabilities in these protocols can be exploited if care is not exercised.

Students used a NodeMCU running a webserver and attached it to a temperature and humidity sensor to create an industrial IoT scenario where the environment could be remotely monitored over Wi-fi using a web browser. They then used a Wi-fi Pineapple to carry out a MiTM attack on the IoT. The goal of this exercsie is to try and understand different variations and repercussions of the attack, such as the use of rogue access points to display fake readings to the user, or delaying or modifying the readings via intermediate proxy software.

BENEFITS

This lab activity is used to expose students attending the IoT Security Cyberwarrior summer camp at Fontbonne University to some of the risks of IoT systems. The students learn about the importance of preserving the confidentiality, integrity, and availability of data in transit. Students differentiate between privacy and safety threats in traditional cyber-attacks versus attacks on cyber-physical systems. By applying adversarial thinking, students learn to analyze an IoT system for misconfigurations and inadequate security controls. Finally, they gain awareness about the risks of exposing personal information over insecure Wifi.

CONTACT INFORMATION

Zahid Anwar
zanwar@fontbonne.edu
(314) 719-8035
Fontbonne University

DEVSECOPS = DEVOPS + SECURE CODING

INSTRUCTION

DESCRIPTION

Software vulnerabilities are one of the key issues in cybersecurity. In a CA Veracode survey, 74% of respondents agreed that security threats due to software and code issues is a growing concern. If software vulnerabilities is one of the causes of cyber breaches, then why don't we start to think about protecting such software from the inception of the Software Development Life Cycle (SDLC)? Students who are new to coding should be taught about secure coding from their first programming course. Unfortunately, secure coding is rarely covered in introduction programming textbooks or courses. Software developers must understand how security risks are managed and mitigated by bad coding practices.

To address this issue, I have introduced DevSecOps = DevOps + Secure Coding concepts in all my programming courses. The main goal is for beginning software developers to understand and reduce the security risks and improve code quality during the SDLC. The majority of common software vulnerabilities are created during the handling of input and output of data. Requiring students to code using secure coding techniques for data validation helps them to understand that it reduces the software risks tremendously. By implementing the DevSecOps concepts we are teaching students to build security at the code level.

BENEFITS

The benefits of introducing the DevSecOps in the computer science curriculum is tremendous. According to a Gartner report, by 2021, DevSecOps processes will be used by 80% of development teams, growing from just 15% in 2017. In 2017 a DevSecOps Global Skills Survey by Veracode, they found that while 65% of DevOps professionals believe it is very important to have knowledge of DevOps when entering IT, 70% responded that they're not receiving the necessary training through formal education to be successful in today's DevSecOps world. The majority of students completing Bachelors or Masters degree in computer science and entering the workforce state that the security education they received is not adequate for what their current positions require. Thus, there is a skills gap; introducing DevSecOps in formal educational curriculum will benefit both the students and employers.

CONTACT INFORMATION

Rajiv Malkan
rajiv.malkan@lonestar.edu
(936) 273-7344
LoneStar College - Montgomery

CYBERSECURITY OPEN HOUSE/FAIR - PROJECT DEMO PRESENTED BY STUDENTS

INSTRUCTION

DESCRIPTION

This past year, I implemented a strategy for my students to prepare cybersecurity demos as part of their final research project. Students work in groups and fulfill a specific objective agreed upon by their team. For example, What does it take to sniff a wireless access point password and what are the implications? Their team segregates the workload among each other to research the technology and techniques required to answer this question. They build a project report identifying the steps in the process and the outcome. This report also includes a step-by-step walk through of how they implemented their project, which is then stored on our cyber range lab portal for future students to read. During their final, students then present their demo and project findings to open house attendees, such as industry partners, faculty, and students. This gives them the opportunity to communicate highly technical material with non-technical individuals. For this example, the students showcased the ease of sniffing wireless passwords, the risks involved with attaching to unsecured wireless networks, and hardening their home networks. They fielded questions from attendees and offered solutions for enterprise and home networks.

BENEFITS

The project is popular with cybersecurity students. It is interesting to see how the students interact with one another throughout the semester. By the end of the project and open house, they are comfortable and confident in identifying their project objectives within their team, and to others. It builds their non-technical skills, prepares them for communicating with upper level managers, connects them to project implementation skills, and bridges their understanding even further in the field of cyber defense. Attendees to the open house/fair responded with positive feedback and gained a better understanding of the risks associated with cybersecurity threats for home and business users.

CONTACT INFORMATION

Nicole Dyess
dyessn@easternflorida.edu
(701) 595-0978
Eastern Florida State College

GIRL SCOUT CYBER DAY AT AUGUSTA UNIVERSITY

INSTRUCTION

DESCRIPTION

In partnership with Palo Alto Networks, Girls Scouts of the USA (GSUSA) announced the development of 18 new cybersecurity badges to girls in grades K-12. Girl Scouts of Historic Georgia, area girl scout leaders, and Augusta University Cyber Institute faculty and staff have joined forces to plan and prepare the curriculum needed for area Girl Scouts to obtain cybersecurity badges in one event.

In recognition of October as National Cybersecurity Awareness Month, Augusta University's Cyber Institute hosted Girl Scouts of Historic Georgia Cyber Day on Saturday, October 13 on Augusta University's Summerville Campus. Over 80 Girl Scout Juniors and troop leaders across the state of Georgia participated in various activities learning about different cybersecurity topics to earn their cybersecurity badges. Station topics covered malware, coding, identity theft, username and password strength, and more. The day concluded with a "Women in Technology" panel discussion with industry and government members from the National Security Agency (NSA), U.S. Army Cyber Command, ADP, IBM, in addition to the Augusta University Cyber Institute Director, Joanne Sexton, and one of our female graduates of the new School of Computer and Cyber Sciences who was also a Dept. of Defense (DoD) Cyer Scholarship Program (CySP) recipient.

BENEFITS

Since women are vastly underrepresented in the technology industry, Girl Scout Cyber Day is a great event and way to educate and inspire more girls to pursue technology-related fields to help close the gap. This event allowed the University community to develop a partnership with the Girl Scout Council and provided additional opportunities for reaching more girls in the cybersecurity area. As a result of this event, Augusta University and Girl Scouts of Historic Georgia were one of ten councils nationally to be selected to host a Girl Scout Cyber Challenge for older girl scouts in October 2019.

CONTACT INFORMATION

Karen Ribble
kribble@augusta.edu
(706) 729-2374
Augusta University

CLASSROOM-READY INTERACTIVE CONTENT TO SUPPORT CYBERSECURITY INSTRUCTION

INSTRUCTION

DESCRIPTION

Funded by the National Science Foundation (NSF) Advanced Technological Education (ATE) program, this work develops classroom-ready interactive content to support courses in Networking and Cybersecurity. The project team engages internal subject matter experts (SMEs) at Brookdale Community College, external SMEs from around the country, and instructional designers. These so-called "interactives" explain complex, abstract, or dynamic concepts using analogies, animation, and interactivity.

The SMEs discuss and storyboard topics. The instructional designers build a first draft of the content and the team collaborates via bi-weekly video conferences to test and refine the interactive materials. Content is developed using HTML5 and therefore available for virtually any device running a modern web browser. The Creative Commons Licensed content can be hosted online, in a learning management system (LMS), and even used offline without an Internet connection.

To date, interactive content is available for the following topics:

- Addressing
- The OSI Model
- Public versus Private Addressing
- Three-Way Handshake
- SQL Injection
- Spoofing Attacks
- Buffer Overflows
- Opersting System (OS) Command Injection Attacks
- Cross-site Scripting
- Code Injection Attacks + Quiz
- Programing Primer
- Cyber Scenario
- Google Hacking
- Heartbleed
- Cryptography
- Memory Paging
- Permissions
- Cryptocurrency and Blockchain
- Cybersecurity Principles (CAE)
- Public Key Infrastructure
- Kerberos

Content can be viewed at the following sites:

1. https://mirrorlearning.org/emate2/web/emate2.html
2. https://mirrorlearning.org/emate2/web/emate2_preview2.html

E-MATE 2.0: Building Capacity for Interactive Teaching and Learning is a project supported by the NSF under Grant No. DUE 1601612.

BENEFITS

This work will benefit students that struggle to understand difficult concepts in networking and cybersecurity. In particular, these interactives target topics that are challenging to teach due to their complexity, and abstract or dynamic nature. As these materials are freely available online and offline, students can master topics through repetition and better prepare for quizzes, exams, and future content.

CONTACT INFORMATION

Michael Qaissaunee
mqaissaunee@brookdalecc.edu
(908) 209-0286
Brookdale Community College

EVIDENCE GATHERING / CALL DETAIL TRACKING

INSTRUCTION

DESCRIPTION

This semester, we will be introducing into our Evidence Recovery course a Virtual Reality Crime Scene. For now that scene is a physical evidence scenario. In the future we plan to create Digital Intrusion scenes. Call Detail Records from Cell Tower Dumps allow students to track mobile devices using Securcube. Using this technique students can take thousands of records and determine which if any devices do not belong. This process also can track suspected devices to determine direction, speed, and associations with other devices.

BENEFITS

Teaches students chain of custody, how to collect physical evidence, note taking in a environment that is interesting and as close to reality as possible without exposing students to dangerous environments. This also allows students to get ready for the 5G environment by understanding how 5G and Cellular networks work.

CONTACT INFORMATION

Peter La Monica
plamonica@ccsnh.edu
(603) 206-8034
MCC

MULTIDISCIPLINARY RISK MANAGEMENT IN CYBERSECURITY

INSTRUCTION

DESCRIPTION

This course provides a multidisciplinary approach to the management of organizational cybersecurity risks. This course includes not only technical cybersecurity risks, but also economic, legal, political, and social perspectives. The case studies provided with the course curriculum helps to improve analytical thinking and problem solving about risks of cyber incidents using real-world examples.

During the development of this course, a focus group meeting brought experts from government, industry, military, and academia together to reveal the issues of cybersecurity workforce and concluded that lack of communication skills of employees working on cyber risk management is a critical problem that needs to be solved. We designed the course to be used by different stakeholders within an organization (i.e., technical experts, legal advisors, senior managers, public relation experts, etc.) to help them have a common language for effective risk management within the enterprise.

The modular structure of the course enables instructors to plug the relevant parts of the course within their own curriculum or use it as a complete cybersecurity risk management course. The first module of the course presents the fundamentals of cybersecurity risk management, including discussions on risk management tools and techniques, cybersecurity risk governance, economic impacts of cyber attacks, and cybersecurity decision making. The second module presents the established government and industry standards and regulations about cybersecurity risk management, such as the Department of Defense (DoD) Risk Management Framework, FISMA, FAIR, and OCTAVE. The final module of the course focuses on application of cybersecurity risk management on emerging fields such as the Internet of Things (IoT) and Cloud Systems.

BENEFITS

- Multidisciplinary cybersecurity risk management curriculum that maps learning objectives to the NICE Cybersecurity Workforce Framework Knowledge/Skills/Abilities
- A modular structure that allows partial integration of the developed materials into existing courses
- Case studies that discuss specific cybersecurity incidents from different perspectives
- Hands-on lab activities on cybersecurity risk management.

All materials are available for the public at no cost at https://www.clark.center/users/capinto

The developed course materials include a syllabus, presentations, case studies, assessments, and lecturer guidelines.

CONTACT INFORMATION

Unal Tatar
utatar@albany.edu
(518) 545-7095
University at Albany - SUNY

TOWARDS THE USE OF CRYPTOGRAPHIC LIBRARIES IN BUILDING SECURITY SERVICES

INSTRUCTION

DESCRIPTION

I discuss the design and implementation of a set of pedagogical programming projects that supplement an undergraduate semester-long introductory course on information security, which I helped design at my institution. These projects introduce the students to the use of security software libraries in order to implement a diverse array of security mechanisms such as encryption, key exchange, and message authentication/integrity checking. These projects gradually increase in complexity as the semester progresses, and provide an opportunity for follow-up capstone projects suitable for honor classes and/or independent studies. The learning objectives of these projects include, but not limited to:

- applying symmetric-key cryptography to protect the confidentiality of arbitrary data
- using public-key cryptography for the exchange of session keys
- validating the integrity of messages and authenticate their senders
- launching a simple attack to exploit a vulnerable protocol
- mastering the use of big integer arithmetic to implement various cryptographic protocols

BENEFITS

Empower graduating software engineers with the necessary system/network security education and programming skills that various software developing houses expect. These skills include: how to use symmetric-key encryption, how to implement key-exchange algorithms, and how to use public-key cryptography for digitally signing documents.

CONTACT INFORMATION

Mohamed Aboutabl
aboutams@jmu.edu
(540) 568-7589
James Madison University

DESIGNING DYNAMIC SECURITY ARCHITECTURES

INSTRUCTION

DESCRIPTION

In the course Designing Dynamic Security Architectures, we operate as a security architecture consulting firm designing secure architecture solutions for clients as a course long project. Students each choose their own client, either real or fictitious. We follow a step-by-step waterfall model to develop requirements and design a security architecture solution that addresses the problem to include technology, people, and processes. Students work together to assist each other throughout the process, along with guidance from the instructor, who is the Chief Security Architect of the firm. Students deliver five Milestones throughout the course including: Client overview, Requirements document, Risk register, Draft target architecture, and Key decision document. The milestones lay the foundation for the final deliverable, an Architecture Design Document, which the students present in class. Students perform in class activities such as interviewing stakeholders, discussing requirements, identifying risks, and developing their architecture solution.

BENEFITS

Students learn and apply concepts in a low-risk experiential learning format. Working as a security architecture firm builds teamwork, while still independently developing their own solution. The course design format enables the incorporation of emerging technologies as technology changes (i.e. cloud, blockchain, IoT, etc.). The final project enables students to apply concepts learned through critical thinking and problem solving. At the end of the course students have learned how to develop strategies and architecture solutions to protect an organization from security threats. The process and Architecture Design Document deliverable may be used as resume builders and examples in job interviews.

CONTACT INFORMATION

Angela Orebaugh
ado4v@virginia.edu
(571) 215-1210
University of Virginia

COMPROMISED BUSINESS SCENARIO

INSTRUCTION

DESCRIPTION

I developed a series of progressive assignments for my database security course that present the realistic scenario of a small business with an insecure business database. The sequence of assignments takes the students through important information security concepts and mechanisms while correcting the vulnerabilities in the database.

The small business is called "Mountain Sports and Game Guides" and has a database tracking both its sportsmen/naturalist customers and independent outdoor guides for whom it serves as a broker. The guides are allowed to use the database, but the database operations have no auditing, and almost no authentication or authorization. Each student individually remedies these defects in a stepwise fashion.

While this hypothetical business is very small, the fact that it nonetheless has external partners using its information systems gives it a very realistic "big business" problem.

BENEFITS

By providing the students with a realistic scenario, this innovation allows them to clearly recognize the risks around problems with database security. By guiding them through corrective actions, rather than simple and atomic exercises, it allows them to attach big-picture security perspective to those corrections.

CONTACT INFORMATION

Andrew Wolfe
adwolfe@loyno.edu
(781) 405-9118
Loyola University New Orleans; Boston University Metropolitan College

COMPETITIVE LABS AS A SERVICE (CLAAS) - A LEARNING SYSTEM FOR CYBERSECURITY EDUCATION

INSTRUCTION

DESCRIPTION

We implement a unique learning system, CLaaS, that incorporates competitions to provide comprehensive cybersecurity awareness education. The system includes multiple identical virtual learning environments with multiple virtual machines nested in each learning environment to serve both tasks of attack and defense. The virtualized system mimics a realistic network, providing real world experiences while containing dangerous lab traffic within its boundaries. Further, the system is easily reconfigured to meet the requirements of subsequent experiments and new learning outcomes.

Each learner has his/her own virtual learning environment. A graphical user interface (GUI) application is designed to provide access to the environment where cybersecurity activities are performed. The application menu includes a set of CyberSec labs, each containing a pair of attack and defense sub-labs. Each sub-lab is a combination of both cybersecurity theory and practice. The theory component introduces learners to the fundamental concepts, theories, and skills regarding a specific type of cyber-attack or cyber-defense mechanism. The practice component fosters learners' problem solving and critical thinking abilities with the help of hands-on activities. The system also facilitates a competitive component, encouraging learners to interact with each other, as other learners' virtual machines are the subject of attack sub-labs. Learners who successfully launch attacks will gain points; conversely, learners who do not successfully implement a mechanism to prevent the corresponding attack will lose points. This game-based learning strategy not only stimulates interest in learning the subject matter but also makes learning more exciting.

The system allows a learner to complete the cybersecurity activities at his or her own pace, anytime, from anywhere over the Internet from a browser. This self-guided learning experience allows the learner to be an active participant in the learning process. Also, this learner-centric approach provides a more enjoyable and effective learning experience for the learner, improving learning outcomes throughout the process. (This research is based upon work supported by the Secure &Trustworthy Cyberspace (SaTC) Program of the National Science Foundation under Grant Number 1723650).

BENEFITS

CLaaS is based on our country's need for highly educated and skilled cybersecurity professionals who can recognize, prevent, and mitigate threats to our nation's critical cyber infrastructure. The system is designed to be adapted for multiple uses. Leveraging virtualization technology and a user friendly GUI application, learners can accessing the learning system anytime and anywhere in the world to practice attack and defense techniques. Upon completion of the cybersecurity activities included in the system, learners will be well-prepared and ready to contribute their knowledge and hands-on experiences in cybersecurity to a high demand workforce.

CONTACT INFORMATION

Te-Shun Chou
chout@ecu.edu
(252) 737-1037
East Carolina University

NICERC INTEGRATES STEM, CYBER, AND COMPUTER SCIENCE INTO MORE THAN JUST K-12 CLASSROOMS ACROSS THE NATION

INSTRUCTION

DESCRIPTION

Since 2008, the Cyber Innovation Center (CIC) in Bossier City, LA has been working with K-12 partners to develop engaging, project-driven content for students. In 2012, the Department of Homeland Security (DHS) identified the CIC and its academic division, the National Integrated Cyber Education Research Center (NICERC), as the national model for cyber education in the country. Since then, NICERC has developed over 15 full courses for K-12 instruction and makes the materials and associated professional development available to all teachers in the country for free. NICERC's current network extends to approximately 16,000 teachers across the K-12 spectrum, in public and private schools, teacher mentors and educational coaches, district and regional administrators, and elective and after-school program providers.

NICERC's library of content includes a variety of titles across all grade levels. In the area of elementary school, content offerings include STEAM Fundamentals: an exploration into project-based learning of NGSS-based standards; Cyber Fundamentals: programming and IoT activities focused on the micro:bit platform; and, Computational Thinking: an opportunity for math, science, and ELA teachers to introduce computer science conversations into the classroom. In middle school, content offerings include STEM EDA: STEM content built around the engineering design process to allow students to work in small teams as they develop prototype solutions for challenging educational problems; Cyber Fundamentals: additional programming and IoT activities focused on the micro:bit platform but built to a higher level of rigor for middle school capabilities; and, Computational Thinking: multi-day lessons designed for math, science, and ELA teachers to use in the core classroom to infuse computer science language and build confidence in breaking down and solving hard problems. For high school classrooms, content offerings include Cyber Literacy and Cyber Literacy 2: liberal arts discussions with cyber engineering content based on a robotic platform that is available in three languages: BASIC (Parallax BoeBot), Arduino C (Parallax ShieldBot with Arduino), and Python (Parallax and NICERC cyber:bot with micro:bit); Cyber Society: humanities content aimed at engaging high school students in critical conversations about security, privacy, and the capabilities of technology in this new digital domain; Cyber Science: higher-level liberal arts and cyber engineering content aimed at presenting students with real-world challenges; Physics: a core physics course that uses robotics and technology to present topics in work and mechanics, electricity and magnetism, thermal fluids, light and optics, and waves and sound; Advanced Math: a senior-level mathematics course based on project based learning and a robotics platform that engages students in two dimensional coordinates, linear algebra, three dimensional coordinates, and polar coordinate mathematics; and, Computer Science: a core CS course based on the College Board's AP CSP guidelines and taught using the Raspberry Pi platform. New courses that are under development include Cybersecurity Fundamentals: a course that will be designed to introduce a high school junior or senior to the concepts that they might be exposed to in a college-level cybersecurity course, allowing them the opportunity to explore the career area before signing up for the course in college, and Cryptologic Mathematics: similarly, a high school senior level course aimed at exposing a student to college-level concepts in a high school setting, allowing them to make more informed choices about college courses.

BENEFITS

The ability of the DHS to see the value in making project-based STEM, cyber, and computer science content available to teachers across the country at no cost was tremendous. Since NICERC began working with the agency, policy influencers, academic educators, and students from all corners of the country have benefitted from NICERC content. Summer camps held at university partners have helped to spread the word about the importance of cyber hygiene and computer science education. States creating standards for cybersecurity or computer science have benefitted from NICERC's national network of content experts so that no one is left to feel like they need to recreate the wheel. National programs seeking to enhance the quality of cyber education among communities, regions, industries, and government have had the benefit of publicly-generated content to help shape their development. NICERC has been providing these services and more to all of its partners at no cost and will continue to do so for as long as the DHS is a partner in the project and even beyond.

CONTACT INFORMATION

Chuck Gardner
chuck.gardner@cyber.org
(504) 952-2195
National Integrated Cyber Education Research Center

CYBERSECURITY COURSEWORK, RESEARCH, INFORMATION LITERACY, AND PUBLICATION GO HAND IN HAND

INSTRUCTION

DESCRIPTION

Research and publishing is how the world and cybersecurity expand and grow. Research includes scholarly and creative activities that can lead to new knowledge, improve our ability to solve problems, result in new theories, and/or in the creation of cyber defense mechanisms. Participating in a research symposium or poster session at a conference is a opportunity for students to hone their professional skills in poster creation and presentation, public speaking, and the application process. Submitting a research paper for publication is an opportunity for students to learn about cybersecurity journals and publication outlets, learn about different paper formatting requirements, learn about paper review processes, and experience feedback by someone other than a professor.

Strong cybersecurity programs provide students numerous hands-on labs and assignments; some may also provide opportunities to physically build security related projects like home grown RFID readers with Arduinos and Raspberry Pis, but few community colleges require cybersecurity students to research a topic, demonstrate information literacy skills, and find a scholarly journal or conference to present. To better prepare community college students to write professionally in the workforce or in advanced courses at 4-year intuitions, research has been added as a component to the Lord Fairfax Community College Programming for Cybersecurity course. The course requires students to select a topic, research it, submit a proposal, write the paper in the format for the IEEE Technologies for Homeland Security, ACM XRDS: Crossroads, National CyberWatch Cybersecurity Skills Journal: Practice and Research Journal, or another cybersecurity related conference. Students must not only write the paper, they must show evidence of submission. This means students have to be aware of submission deadlines and practice time management in submitting not only for a course grade but for publication by the selected cybersecurity journal/conference.

Programming is not usually a strong skill or a desired skill by many novice cybersecurity students. They do not see how programming and other courses are connected. By researching they are able to visually take individual courses and see them as instead as a cohesive program and career foundation. In program development we discuss the C-I-A Triad which is critical for developing secure coding and protecting systems with automated scripts. Their research process may also be related to the C-I-A Triad simply as Confidentiality of data collected and ethical practices; Integrity: they have to be honest about their findings and they have to use trust worthy resources and information literacy skills; and Availability, because their resources have to be available and accessible to others.

BENEFITS

Students who have participated in the research project have benefitted in the following ways: greater problem solving skills; better understanding of research methods; deeper understanding of the cybersecurity discipline; more confidence and independence; better understanding of career paths versus academic paths; and building transferable skills while enhancing resumes. In addition, feedback from student participants and employers suggest students involved in research are more satisfied with their college experience, are retained and persist at a higher rate, both at college and within their major, and are more competitive when searching for jobs because of improved articulation skills and validation by their peer publications.

CONTACT INFORMATION

Melissa Stange
mstange@lfcc.edu
(540) 868-7003
Lord Fairfax Community College

AUTHENTIC COMPETENCY-BASED LEARNING TO DEVELOP AN INDUSTRY READY CYBER SCIENCE GRADUATE

INSTRUCTION

DESCRIPTION

This instructional approach focuses on five ways to ensure students are gaining the competencies and skills needed to successfully enter the workforce, while giving back to the community and future learners. The goal of this approach is to develop a graduate with an Ivy League mind-set for making a difference in society, while increasing their earning potential. The objectives of this approach are to ensure student's competencies for:

1. Meeting the needs of employers
2. Validating curricular program competencies and learning outcomes
3. Providing work-based learning and employer networking opportunities prior to graduation
4. Instilling the passion for giving back to the community through outreach and service
5. Increasing program enrollments and credentials

This approach builds a connection with employers and K-12 schools within a service region; provides multiple entry points into the activities in order to increase enrollment into the cyber science programs; has increased program completion, internships obtained, and industry certification embedding. Through community partnerships and securing grants, this approach is affordable to the college and student. The approach is sustainable through updating degree and certificate programs, relationships with employers within and outside the discipline-specific curriculum advisory committee, and by requiring community outreach to instill a "give back" and lifelong learning mindset into students.

The first step is to embed faculty into professional organizations such as Society for Human Resources Management, National CyberWatch, and to network with community employers to better understand the workforce needs beyond technical publications and curricular advisory committee meetings. The second step is to ensure degree and certificate program outcomes provide students the competencies needed to not only find a job, but to progress in the selected career field. The next step is done through outreach to find paying and non-paying internships or co-op opportunities for students that will not only provide an opportunity to build skills by bringing classroom foundational learning to life, but to aid the students in developing a professional reference network. The fourth step is to expand student soft-skills such as communication, team-work, problem solving, global inclusion, and computational thinking through competition participation. The fifth step is to find opportunities for student inclusion in community service and outreach within the K-12 environment to foster a pay-it forward mind set, that it is their responsibility to help others learn and grow. The final step is to engage in continuous improvement - solicit feedback from students and employers - in order to evaluate the approach for relevance.

The first step is to embed faculty into professional organizations such as Society for Human Resources Management, National CyberWatch, and to network with community employers to better understand the workforce needs beyond technical publications and curricular advisory committee meetings. The second step is to ensure degree and certificate program outcomes provide students the competencies needed to not only find a job, but to progress in the selected career field. The next step is done through outreach to find paying and non-paying internships or co-op opportunities for students that will not only provide an opportunity to build skills by bringing classroom foundational learning to life, but to aid the students in developing a professional reference network. The fourth step is to expand student soft-skills such as communication, team-work, problem solving, global inclusion, and computational thinking through competition participation. The fifth step is to find opportunities for student inclusion in community service and outreach within the K-12 environment to foster a pay-it forward mind set, that it is their responsibility to help others learn and grow. The final step is to engage in continuous improvement - solicit feedback from students and employers - in order to evaluate the approach for relevance.

BENEFITS

Student responses show that 85% are members of PTK honor society, 95% transfer to 4-year institutions successfully, or are employed within six months of graduation. 75% of the students have recommended at least two peers to transfer into a cyber science program or to seek a second college credential in the field. Success is also evaluated by enrollment growth in Computer Science and Cybersecurity programs. Curriculum Advisory members count the activities in this program as job experience when interviewing applicants. While publication and industry credential prep are embedded within the cyber science programs, all students benefit from the organization meetings, competition participation, and community service. Outreach to K-12 is funded through grants. Minority and underrepresented students are welcomed by faculty who represent the same demographic and maintain a friendly environment. A Dept of Defense P3 grant provided funding for improved/updated classroom technologies enabling outreach and training for off-campus military and non-military students in the cyber skills necessary to meet workforce demand. This lab expansion benefits all students who use the classroom. This program model shows how two connected disciplines can work together to provide students writing, communications, problem solving, globalization, and community service skills without losing focus on critical discipline specific technical competencies.

CONTACT INFORMATION

Melissa Stange, Henry Coffman
mstange@lfcc.edu
(540) 868-7000
Lord Fairfax Community College

DEVELOPMENT OF AN ORIGINAL IOT DEVICE, WITH A FOCUS ON THE SCRUM FRAMEWORK, IN AN ONLINE, TEAM-BASED LEARNING ENVIRONMENT

INSTRUCTION

DESCRIPTION

Capstone students from all Information Technology AAS (Cybersecurity & Networking, Web Development, and Programming & Database) programs are put together on teams and charged with developing an original, Raspberry Pi-based IoT device. All projects are required to integrate a database, an online portal or dashboard, some sort of middleware (e.g., Python, Java), and students are expected to fully secure the device. Students are required to adopt the Scrum framework and provide daily updates as well as weekly Sprint reports to ensure that development is on track and artifacts are maintained.

Students must provide a complete submission for the initial concept work scope for the device to be built, including expected challenges in team knowledge and skills, as well as concerns for technology availability for developing or integrating technologies.

Final submission of the device must be accompanied by thorough documentation of the project and expected next steps to move the project to market. In particular, students are expected to identify security concerns that may not be directly addressed in their project. For instance, in an IoT device that is implanted in a human subject, additional security factors may need to be addressed external to the device they have developed. For projects where the scope of the project ultimately exceeds the skill of the team, clear documentation of the challenges that are still remaining and potential mitigations are expected.

Grading of the course is heavily weighted on communication of the team and the quality of the submitted documentation of the project with the completion of a functional device as a secondary expectation.

BENEFITS

Students quickly learn that challenges in group dynamics and communication have a far greater impact on product development than do technical skills. Teams learn to manage time and resources and, due to self-directed team nature of Scrum, learn to negotiate with each other to align time and resources to those needed to complete a project successfully. Students experience the unique challenges associated with pulling together multiple technologies into a single project and have to research the security implications of the decisions they have made in developing their project and address those concerns with a combination of technology and documentation.

CONTACT INFORMATION

B Bagby
bbagby@virginiawestern.edu
(540) 632-2429
Virginia Western Community College

THREE SECTION CLASS DEBATE: ATTACK, DEFEND AND DETER

INSTRUCTION

DESCRIPTION

In my graduate level class on international security titled "War, Peace, and Politics" at Saint Louis University, I ran a class debate by dividing the class into three teams: team attack (to generate the best way to conduct cyber attacks); team defend (to strategize the best ways to defend against cyber attacks); and team deter (to come up with the best way to deter cyber attacks).

In so doing, I assigned five book chapters and journal articles on this topic:

1. Thomas Rid, Cyber War Will Not Take Place (Oxford: Oxford University Press, 2017), pp. vii-10
2. Ben Buchanan, The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations (Oxford: Oxford University Press, 2016), pp. 1-9, 31-49, 141-156
3. Tim Maurer, Cyber Mercenaries: The State, Hackers, and Power (Cambridge: Cambridge University Press, 2018), pp. ix-xv, 3-28
4. Jon Lindsay and Erik Gartzke, " Coercion through Cyberspace: The Stability-Instability Paradox Revisited", in Kelly Greenhill and Peter Krause, eds., Coercion: The Power to Hurt in International Politics (Oxford: Oxford University Press, 2018), pp. 179-203
5. Carl von Clausewitz, On War, pp. 357-378, 523-531

First, we went over each of the assignments to make sure that students understood the main arguments of the readings. Then, we divided the class into the three teams and let them apply the main arguments to their own strategic conditions. Finally, they all had a 15 minute "strategizing session" to discuss how to approach their conditions and their rival teams' arguments, before we opened the floor to let each team make their own arguments.

BENEFITS

The student reaction was awesome and they seemed to enjoy drawing intellectual ideas from the engagement. They learned the attribution problem (that attribution is very difficult but not impossible and takes time and energy, and that dwell-time is still about 90 days), credibility problems stemming from use of deception and proxies in cyberspace, and the challenges of sending the right messages to deter through proper channels of communication. They also realized that attackers have inherent advantage in cyberspace over defenders and the difficulty of defending and deterring attacks. As a professor, I realized that this small-team debate really works for a relative small graduate course of about 12 students.

CONTACT INFORMATION

Nori Katagiri
nori.katagiri@slu.edu
(314) 977-3044
Saint Louis University

CYBERSECURITY STUDENT WORKBOOK

INSTRUCTION

DESCRIPTION

Our student workbook is an introduction to cybersecurity for middle school and high school students. Designed to accompany our Cybersecurity Career Guide or stand on its own, this 54-page .PDF helps students answer questions like:

- What is cybersecurity and why should I care?
- What can I do to stay safer online?
- How do I know if I like or can do cybersecurity?
- How do I figure out if a career in cybersecurity is right for me?

Students learn the answers to the above questions through lessons and activities. This is an introduction to cybersecurity for students, designed in a way to keep them interested and engaged. It's an affordable .PDF that teachers can easily use in the classroom to teach the basics of cybersecurity and to foster interest in students who might not be aware of the field.

BENEFITS

Opportunity for all: a career in cybersecurity can work for all kinds of students. Technical expertise is needed, of course, but soft skills, varied intellectual interests, and diverse life experiences are all crucial to the strength and vitality of the cybersecurity workforce.

Our Workbook offers lessons and exercises in cybersecurity basics, cyber ethics, relevant cognitive skills, and career assessment. Completing the four-chapter Workbook will show students what cybersecurity is all about and give them a strong start on finding a place in the field that can work for them.

CONTACT INFORMATION

Robert Black
bblack@start-engineering.com
(202) 841-1524

APPLIED CYBER DEFENSE

INSTRUCTION

DESCRIPTION

Applied Cyber Defense (ACD) is a new course offering at the University of Colorado, Boulder, as part of their recently re-designed program, Technology, Cybersecurity and Policy (TCP). ACD applies core cybersecurity concepts from prerequisite coursework, within a hands-on, gamified, virtual environment. Students practice offensive skills in password cracking and exploit development to understand vulnerabilities and then focus on defensive tactics to reduce cyber risk and respond to cyber-attacks. At the conclusion of the course, students will have experience using numerous real-world tools against actual threat attacks. Students successfully completing this course should have an understanding of how to become experts in the field of cybersecurity and the types of technical careers available.

The course is split into three units of study:

1. Unit 1: Adversary tools and tactics
2. Unit 2: Cybersecurity work roles (NICE & NIST Cybersecurity Frameworks)
3. Unit 3: Defensive team tactics and procedures

Learning Goals:

- Understand how an adversary develops a campaign to attack a network, including the types of motivations, tactics and kill chain. These concepts help defenders understand the elements that are present in an attack and where indicators of compromise can be found
- Understand the different types of work roles or technical competencies involved in cybersecurity defense. Students will be exposed to multiple work roles and then choose the one that fits them best for concentration (and the basis of their specific midterm exam on that role)
- Apply cybersecurity defense knowledge across the full scope of the NIST Cybersecurity Framework to understand what defenders should do before, during and after a breach.

BENEFITS

One of the biggest challenges employers face in recruiting cybersecurity professionals is around finding well qualified applicants. The innovation featured in this submission speaks to this need as it offers coursework that blends the conceptual/theoretical aspects of cybersecurity education with the practical application of hands-on, technical skills. Students walk away with a deep understanding of both the NICE and NIST Cybersecurity Frameworks (and how they differ/overlap), the affiliated work roles and responsibilities, and the applied knowledge to be impactful in their careers on Day 1. The outcome: cybersecurity talent that is both confident in their abilities and prepared to enter any sector of the workforce.

CONTACT INFORMATION

Laura Lee
bwolfenden@circadence.com
(858) 208-8003
University of Colorado, Boulder

A MULTIDISCIPLINARY APPROACH TO THE FIELD OF CYBERSECURITY EDUCATORS

INSTRUCTION

DESCRIPTION

Cyber education is critical to meeting the nation's priority for more professionals who will work in public and private sector organizations and businesses to protect the virtual space of modern life. To this end, the need for educators to keep pace with this demand is equally challenging. Using an innovative approach over the past year, the University of Maryland University College (UMUC) has successfully conducted a program to do just that.

The UMUC Cybersecurity Advanced Degree Fellowship (CADF) program, made possible from funding provided by the Dept. of Defense and the National Science Foundation, demonstrates the ability to increase the number of qualified college-level faculty in cybersecurity by offering an accelerated educational opportunity to degreed instructors and professionals in other fields. The initial UMUC CADF cohort consisted of a very multi-disciplinary and relevant group. Their employment backgrounds reflected companies and organizations such as American Express, IBM, community colleges, the U.S. Military, Deloitte, Touche, and MITRE where they performed duties related to project management, data analysis, database analytics, cyber risk analysis, engineering, adjunct teaching, and military activities.

The UMUC CADF program comprised ten fellows. To-date, nine fellows are certified for adjunct faculty positions in cybersecurity at the college level. The remaining fellow, who started later in the UMUC CADF program, is wrapping up the last requirement. The fellows are at various stages of finding adjunct college positions to fulfill their obligation to teach, with two fellows hired for positions within UMUC.

BENEFITS

Bringing multiple disciplines to the field of cybersecurity, and offering an accelerated quality learning experience for working adults, is a win-win situation benefitting cyber research, educators, and future generations entering the field. First, the CADF project supports the major initiative to increase the availability of qualified cybersecurity educators. Second, it creates a cyber academic environment comprised of multi-disciplinary fields. Understanding the complexity of cybersecurity needs the participation of faculty members with diverse backgrounds, though this need for educational diversity is not well-understood in cyber learning and practice. Academics in the fields of law, finance, human resources, political science and other fields need to mesh their backgrounds and careers with cybersecurity concepts in order to tackle today's problems in protecting cyber space. Lastly, the program produces valuable additions to the body of cybersecurity research through research, papers, and presentations prepared by CADF fellows.

CONTACT INFORMATION

Loyce Pailen
loyce.pailen@umuc.edu
(240) 684-2766
University of Maryland University College

TEACHING CYBERSECURITY ACROSS THE DISCIPLINES

INSTRUCTION

DESCRIPTION

Cybersecurity has become a prevalent topic in many colleges, but how it should fit into the overall educational process is still not fully understood. A cybersecurity project at the University of Hawaii Maui College (UHMC), funded by the National Science Foundation (NSF) Advancted Technological Education (ATE) program, spans multiple disciplines and targets women and minorities. Many colleges in the United States and around the world have curriculum and educational programs that cover the core technical topics in cybersecurity. These topics are often geared towards students who have some degree of familiarity and interest in computer and networking technologies.

However, as the researchers at the UHMC have discovered, the above topics are often restricted to males who are aspiring towards a technical education that covers computer technologies or related fields of study. These above courses do not target women, minorities or students who aspire to study disciplines outside the core arena of computing. The project at UHMC attempts to address this problem by focusing on a few key disciplines that are outside the realm of core computing, but still relevant to cybersecurity. These disciplines include, but are not limited to: Accounting, Criminal Justice, Allied Health, Hospitality and Tourism and Electronics.

The innovation of this project is to ensure that a broad audience of faculty, students and practitioners get trained in the fundamentals of cybersecurity, without feeling intimidated or overwhelmed.

BENEFITS

Many community colleges and university across the United States and the world contain programs such as Accounting, Criminal Justice and Allied Health. Women and minorities enroll in these programs, not because they wish to specialize in cybersecurity, but because they wish to form careers and futures in these fields of study. As a result, these programs are often diverse and contain students and faculty who bring a diversity of experiences and backgrounds that are often unrelated to the core tenets of computing and cybersecurity. The benefit of this innovation is to train the faculty in these disciplines in the core tenets of cybersecurity and empower them to integrate cybersecurity into their own curriculum.

CONTACT INFORMATION

Young Choi
ychoi@regent.edu
(757) 352-4949
Regent University

EVIDENCE-BASED ASSESSMENT IN A BUSINESS SCHOOL-ORIENTED INFORMATION SECURITY MANAGEMENT CURRICULUM

INSTRUCTION

DESCRIPTION

My course, MIS755: Information Systems Security Management, focuses on how to do cybersecurity with the target audience being graduate business students in the Management Information Systems, Accounting Information Systems, MBA, Homeland Security, Accounting, and Management disciplines. Instead of relying on traditional exam-based assessments, I've innovated by using practice- and evidence-based assessments. The goal of the course is to prepare business students to manage information security activities and functions. To do this we focus on the areas of security planning, risk assessment and management, and security auditing. Three assignments are used to prepare students to perform the actual functions they will be expected to perform in industry.

The first assignment is to acquaint students with the capabilities of security tools and activities and is a portfolio of 10 security exercises using a lab book and tools obtained from the Internet. Each exercise is documented as a report to management saying what was done, what the result was, what was learned, and how it relates. The second assignment is designed to teach students how to do a Risk Management Framework approach to perform and document a risk assessment by performing a information asset inventory and subsequent risk assessment on themselves. I have the students use themselves as the subject of the assessment because they have the necessary contextual knowledge needed to truly do a risk assessment. The assignment prepares the student to do this function in an organization (note this exercise is the cornerstone for all security programs as it defines the scope of the organization's security plan). The third assignment is a team-based security audit on a small organization. The audit includes preparing an audit plan, audit execution, and preparation of an audit report that is delivered to the organization. Audit results are presented for quality control prior to being finalized. This exercise prepares students to do one of the more common entry-level jobs for graduate business security students: that of security auditor. Additionally, the assignment illustrates the challenges small organizations face in implementing information security by having them find the differences between what they learned in class and what an organization is actually doing, and then assessing it for adequacy and generation of a cost-effective road to success in information security.

BENEFITS

The main benefit of this innovation is that business students complete the course knowing how to plan and implement security in an organization because they have performed the needed functions rather than just read about them. Additionally, students learn the basic skills needed to be a script kiddie which gives them insight into the average cyber criminal and how easy it is for that criminal to attack the student and their organizations. I believe this is essential as all security managers need to understand the effectiveness and ease of use of security/hacking tools so that they can appreciate the scope of the risk faced by their organizations, and thus, prepare security plans and controls that will work. Finally, while the innovation does not test what a student remembers about security, it does test what the student can do in security and it is my experience that the student knowing what they can do leads to a better prepared and more confident applicant when they graduate. This confidence and skills leads to more successful and satisfied graduates as post graduation communications show.

CONTACT INFORMATION

Murray Jennex
mjennex@sdsu.edu
(619) 985-6209
San Diego State University

INTERGRATING A CYBERSECURITY OPERATIONS CENTER LAB TO ENHANCE STUDENT'S CYBERSECURITY SKILLS AND MEASURE COMPETENCIES

INSTRUCTION

DESCRIPTION

The SOC lab and cyber program expansion at Forsyth Tech around the SOC lab will allow the creation of engaging, hands-on learning through new technologies and expand work-based learning opportunities for cyber students. This will broaden the cybersecurity skills that are needed in the workforce and align with good paying careers in cybersecurity. The SOC lab will be used to train students in protecting and defending systems from attacks by adversaries and allow multiple scenarios for training purposes. Students will use software such as Alient Vault in a secure environment allowing them to learn asset discovery and inventory, vulnerability assessment, intrusion detection, incident response, endpoint detection and response, log management, and compliance reporting. The lab will also be utilized by our industry partners to train employees on advanced mitigation techniques (cyber hunting). It will also be utilized to assist Center of Academic Excellence (CAE) novice instructors to advance skills in mitigation and cyber operations as well as conduct hacking training from our certification partners.

There is also need to have IT and Cyber professionals learn through the use of developing technologies. Artificial Intelligence (AI) and Virtual Reality (VR) are two such technologies that will continue to transform student's learning experiences. Educators must being utilizing Virtual Reality and learn the role AI can have in student success and engagement. Utilization of VR for training purposes can transform learning, providing new opportunities for students to connect with people, visit places, and experiences they may never have the opportunity or capability to experience in person. VR will solve several problems as we see growth in utilizing this innovative technology including accessibility. The SOC lab will also include VR equipment.

BENEFITS

With the industry movement to an SOC model and the demand for expanded skill sets among all IT students, the SOC lab will assist students and faculty to enhance cyber mitigation skills, identify mailouts, packets and cyber intruders. While FT has several classes that currently address this content, there is not a dedicated operations lab that will specifically address these critical skills in a collaborative and hands-on environment. The SOC lab will further enhance our IT programs closing the learning gap in mitigating attacks from the novice to the advanced application level.

CONTACT INFORMATION

Deanne Cranford-Wesley
dwesley@forsythtech.edu
(336) 734-7305
Forsyth Technical Community College

HIGH SCHOOL 4-YEAR CYBERSECURITY PROGRAM

INSTRUCTION

DESCRIPTION

Troy High School has developed a four year cyber defense pathway as part of our Troy Technology academic magnet program. We chose as a school in 2016 to offer this innovative pathway based on a combination of growth in our after-school CyberPatriot competitive program and seeing our graduates choosing to earn cybersecurity related degrees in college in increasing numbers. Working with Coastline College, Troy combined six of their semester-long Computer Services Technology courses into three year-long courses.

Troy HS has offered computer science courses for 30 years, but our additional pathway for cyber defense has really boosted our interest in both taking classes and being on our after-school cyber teams. In only our second year of offering cyber defense classes, we have 52 students taking our Cyber Defense Fundamentals class and working towards their A+ hardware and software certifications. We have another 23 students enrolled in our Computer Operating Systems class which also earns the IT Fundamentals cert. Next year, we are adding a Cyber Defense Operations course which will focus on the Security+ certifications and we are expecting 150 students to be enrolled between the three course offerings.

Our class offerings have sparked even more interest in our cyber competitive teams. CyberPatriot is a scalable competition that allows us to offer every interested student a spot on a team even with no prior experience. Our 45 students in 2016 that prompted us to offer our academic program has grown to 295 students on 50 different teams in the 2018-2019 school year. Troy also has a Capture The Flag club and our students have competed in the National Cyber League (NCL) in large numbers since the Spring 2018 season.

BENEFITS

Students earn professional cybersecurity related certifications that demonstrate their IT and cybersecurity skills in a hands-on environment, while also having the chance to interact with cybersecurity professionals during their six week summer internship prior to their senior high school year. Initially motivated by engaging CTF and blue team competitions and spurred by career information from cyberseek.org, students are finding a true professional passion prior to graduating from high school. Troy High School benefits by attracting numerous students to a school that offers a mature cybersecurity academic program and highly competitive teams open to all new students with no prior experience.

CONTACT INFORMATION

Allen Stubblefield
astubblefield@fjuhsd.org
(714) 626-4464
Troy High School, 2200 Dorothy Ln, Fullerton CA 92831

03

PRACTICE

WINNING SUBMISSION:
INCENTIVE-BASED PLATFORM FOR TEACHING CRYPTOCURRENCY, BUG BOUNTY, RECONNAISSANCE, AND MORE

INCENTIVE-BASED PLATFORM FOR TEACHING CRYPTOCURRENCY, BUG BOUNTY, RECONNAISSANCE, AND MORE

PRACTICE

DESCRIPTION

GenCyberCoin is a web platform that teaches students the following concepts:

- Cryptocurrency and digital currency trading markets, including blockchain applications
- Cybersecurity principles (confidentiality, integrity, availability, defense in depth, keep it simple, think like an adversary)
- Bug bounty programs
- Password management and its strengths
- Social and ethical norms and values
- Reconnaissance and Social Engineering

GenCyberCoin was used in GenCyber summer camps as well as in college security classes. Students from gradesd 8-12 expressed high enthusiasm and actively participated in the GenCyberCoin platform, searching for bugs, performing reconnaissance, and earning coins for their leadership skills and willingness to learn cybersecurity. They later spent their coins at the GenCyberCoin marketplace to buy real items that the camp's Team has prepared for them. This platform has also been used in the Pentesting course (as midterm and homework assignments) at Arcadia University. Most of the things in this system are customizable to your specific needs. GenCyberCoin is available at [https://github.com/vitalyford/gencybercoin] and can be installed locally or in the cloud. Currently, it is also deployed on AWS at [https://gencybercoin.tk]. GenCyberCoin is a part of the NSA/NSF GenCyber grant.

BENEFITS

Educators can customize this platform, providing an incentive for students to finish their assignments and receive digital coins. It can be used as a fun activity to search for bugs, engage in a "social engineering the teachers" activity, and answer reconnaissance/security-related questions.

CONTACT INFORMATION

Vitaly Ford
fordv@arcadia.edu
(267) 620-4745
Arcadia University

RED VS. BLUE COMPETITION

PRACTICE

DESCRIPTION

For the first time in the Spring of 2019, we offered a competition that allowed students to demonstrate both offensive and defensive skills in the same competition (and to create teams that combined individuals with both types of skills). The competition placed teams in a bracket-based, head-to-head competition where they either attacked or defended a network and servers. The competition was scored based on uptime (with weighting) where operating services benefited the defending (blue) team and down services benefited the attacking (red) team.

Like many common sports (e.g., basketball, football, baseball) the competition required teams to be created that could both attack and defend. The teams were required to select a subset of their members (6 out of 10) to participate in each heat, so individuals that could contribute to both activities were particularly valuable.

The blue team got a slight head start to secure their systems before the red team was able to begin to attack them. The scoring engine was enabled concurrent with the start of the red team's participation. The event was hosted, and the systems for it configured, by a group of NDSU students.

BENEFITS

Having student teams on both sides of the competition allows students focusing on both areas of security to participate in the same competition. Virtually all existing competitions are targeted at either the offensive or defensive side, to the exclusion of the other. While some overlap between participants exists, teams excel at these other competitions by focusing in the respective area. The Red vs. Blue concept allows members of these two groups to compete together (potentially including traveling together, etc.), creating a cross-focus program bonding experience. Additionally, this approach may be beneficial to smaller programs that don't have separate offensive and defensive teams, allowing them to benefit from their skills in both areas. It also facilitates having defensive competitions

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
(701) 231-8196
North Dakota State University

CYBER DEFENSE STUDENTS RECEIVING REAL WORLD OPPOROTUNITIES

PRACTICE

DESCRIPTION

EdCC digital forensics students have the opportunity to work on real digital forensics cases, perform data recovery, and assist in performing security audits and penetration tests. One of the most important aspects of becoming proficient in cybersecurity and digital forensics related work is to be provided the opportunity to gain hands-on experience with industry professionals and experts. While most students typically perform work related to simulated scenarios in the classroom, EdCC instructors provide students the opportunity to work for actual clients under the supervision of their instructors or senior lab managers. Many students have documented work on their resumes before they even graduate.

EdCC instructors Steve Hailey and Mike Andrew are industry professionals that maintain a working relationship with companies throughout Washington state as well as various law enforcement agencies. Work performed with their students is done on a pro bono basis, so it is truly a win-win situation for students as well as members of the community and businesses throughout the state. EdCC students are trained to perform physical data recovery in a cleanroom environment, and performed data recovery for victims and families of the Oso tragedy:

- https://www.heraldnet.com/news/edcc-team-retrieves-delicate-data-damaged-in-oso-slide
- https://mynorthwest.com/gallery/edmonds-students-to-recover-data-photos-memories-from-oso-mudslide-computers

All students are afforded the opportunity to sit for the CyberSecurity Forensic Analyst exam, with the $750 exam fee waived. Also, any students assisting with a security audit or penetration test much pass the Certified Ethical Hacker (CEH) exam, which is part of the cybersecurity curriculum.

BENEFITS

The benefits of the EdCC program are many: all work performed involving students is done on a pro-bono basis for members of the community as well as businesses throughout the state, so it is truly a win-win situation for all involved; this has resulted in many students gaining employment before they graduate or shortly thereafter. The opportunity for students to be involved in performing actual work related to cybersecurity is invaluable. EdCC instructors also cover how to start a consulting business performing digital forensics and cybersecurity work, and many students are successful in this.

CONTACT INFORMATION

Steve Hailey
shailey@edcc.edu
(425) 640-1377
Edmonds Community College

'HACK NDSU' CAMPUS PENETRATION TESTING EVENT

PRACTICE

DESCRIPTION

With penetration testing, getting the proverbial 'foot in the door' is difficult. To give students real world penetration testing experience, we hosted a 'Hack NDSU' penetration testing event. The event was suggested by and held in conjunction with our Information Technology Division. During the event students were led by two industry penetration testers (Tim Jensen from AppSec Consulting and Mike Saunders from Red Siege) and got the opportunity to practice their ethical hacking techniques on the campus network and servers.

NDSU's Information Technology Division provided the professional penetration testers and the students with a scope of work that constrained what areas of the network they were allowed to test. From this point, the professional penetration testers and the students conducted reconnaissance and scanning activities. Then, from the potential targets identified, multiple attacks were conducted to test various servers and networking equipment.

The professional penetration testers and the students used both tool-automated attacks and several manual attacks. Students got to demonstrate their existing skills, developed through coursework, and learned several new techniques that were demonstrated by the professionals during the event. Most importantly, they got to see how all of the parts of the penetration testing process come together for an actual engagement.

BENEFITS

The 'Hack NDSU' event provided students with an opportunity to perform a full penetration test on an actual network. Students that participated can list their involvement on their resume and discuss the experience and their role in it with prospective employers. This provides a unique experience that most students don't have when graduating from college. For NDSU, it also provided the opportunity to identify vulnerabilities in its network and configurations at minimal expense.

CONTACT INFORMATION

Jeremy Straub
jeremy.straub@ndsu.edu
(701) 231-8196
North Dakota State University

PENETRATION TESTING OF HUMAN MACHINE INTERFACES AND MODBUS PROGRAMMABLE LOGIC CONTROLLERS

PRACTICE

DESCRIPTION

Today's critical infrastructures such as utilities, defense systems, manufacturing, and production rely more upon the use of control systems for daily business than ever before. As smart technologies increase in use, so does the need for a trained cybersecurity workforce to protect such systems from threat actors seeking to steal information or cause damage to processes critical in daily life. Many colleges and universities reported that control systems cybersecurity was not part of the current curriculum taught. This project was developed to introduce students and faculty to various Human Machine Interface (HMI) and Programmable Logic Control (PLC) penetration testing tools currently available in Kali Linux and the Metasploit framework. The series of labs introduced in this project is designed for basic and intermediate cybersecurity courses to expose the learner to the concepts of data communication in control systems.

The Penetration Testing of Human Machine Interfaces and Modbus Programmable Logic Controllers project consists of five lab modules that are designed to teach students in the career fields of Cybersecurity and Industrial Systems the framework of Modbus communication control in HMI and PLC networks. In the project, students were introduced to the Metasploit and Armitage security testing framework that provide Modbus auxiliary payloads, which allow remote takeover of PLC and HMI communication in Modbus networks. The ultimate goal of the project is to train students on the hacker methodology and critical system vulnerabilities.

The five sections of the project teach students how to:

1. Build a reverse_tcp payload using Veil Evasion
2. Create a fraudulent Web site using SimpleHTTPServer for deployment of the reverse_tcp payload
3. Deliver Modbus commands and device pivoting using Metasploit
4. Exploit a PLC and HMI device using Armitage auxiliary scanners
5. Once students are able to gain control of the PLC or HMI device through the reverse_tcp connection, they are able to issue

BENEFITS

Since the delivery of this project at various colleges across the United States, an overwhelming number of faculty reported that students were very engaged with the hands-on portions of the modules related to PLCs, HMI, and critical system security testing. Student surveys found the labs very rewarding from a knowledge standpoint and fostered a desire to expand their education of critical infrastructures. The overarching intent of this project was to increase awareness of critical systems and broaden the base of understanding of students in cybersecurity and industrial system fields of study.

CONTACT INFORMATION

Greg Randall
greg.randall@snead.edu
(256) 840-4166
Snead State Community College

USING PRACTICE-LABS FOR REMOTE ONLINE LAB ACTIVITIES TO AID INSTRUCTION

PRACTICE

DESCRIPTION

Teaching technology requires a combination of theory and hands on labs to reinforce course objectives. Most of the courses in our degree program are professional certification-aligned and require extensive and complicated Lab setups. The addition of Practice-Labs into our classroom has greatly improved teaching effectiveness and most importantly the student learning experience. Labs objectives align with vendor certifications including CompTIA, Microsoft, Cisco, VMware, and others. Disciplines include IT Networking, Cybersecurity, and Programming. Students are able to complete labs at home or in the classroom, as long as they have Internet access and a browser. The Labs include periodic snapshots to collect student performance data and the inclusion of mini quizzes to validate understanding. Students are now better engaged with theory and can increase their confidence through directly related hands-on Lab activities.

BENEFITS

Students graduating from our program are better prepared and more competent in local and remote network management due to the extensive hours they have spent performing a range of remote hands-on Labs, including but not limited to configuring equipment or performing network management. Every semester, the number of course sections completing Labs continue to increase as students are better able to perform network tasks and find solutions to their assigned labs. We are also able to integrate Practice-Labs with our Canvas Learning Management System so students can launch their assignments from a single portal. Students going through our program are getting access to training 7 days a week. As students complete a variety of courses through our program, and are performing labs in each course, they will be ready to manage online equipment and will feel much more confident at job interviews. Use of real online equipment that is readily available for training has greatly improved our overall teaching effectiveness and our student learning experience across our program.

CONTACT INFORMATION

Edmond Garcia
egarcia@vcccd.edu
(805) 558-8340
Moorpark College

THINKING LIKE A HACKER

PRACTICE

DESCRIPTION

Within different Introduction to Cybersecurity textbooks, information about malware (e.g. Viruses, worms, etc.) and its impact on a company's network computer systems are well known. Students in a first level cybersecurity course learn about famous malware such as Slammer and CryptoLocker, to name a few. But how many students in cybersecurity programs nationwide understand the concept of how to create a virus? From an ethical hacking point-of-view, this skill set is important and allows students to think like a hacker.

The purpose of this lab assignment is to provide students hands-on training on how to create a harmless virus to better understand the concepts of malware. This lab assignment also provides students the opportunity to understand why cybersecurity can be challenging and how easy it is to create dangerous malware. The impact of this lab assignment is that it's fun, powerful, and educational.

After the instructor demonstrates to the students how to create a harmless virus, students are required to create their own harmless virus that consists of 100 lines of code, and use different special effects within the virus as if it was real (e.g. Make the CD-ROM drive open, display snowflakes on the screen, make the monitor screen change color, etc.). Students are required not to use any code that would shut down a computer system or network. Students are allowed two to three weeks to complete this lab assignment.

BENEFITS

Since cybersecurity is a forever changing field of study, it is essential that students entering the field are knowledgeable about the basic concepts of malware. This hands-on lab assignment allows students to be innovative and "think outside the box" as if they are a hacker. This lab assignment is simple, but the learning experience for students is rewarding.

CONTACT INFORMATION

Charles DeSassure
charles.desassure@tccd.edu
(817) 515-3747
Tarrant County College, Southeast Campus

PURDUE UNIVERSITY GLOBAL CYBERSECURITY INTERNSHIP PROGRAM - TECHNOLOGY

PRACTICE

DESCRIPTION

Purdue University Global offers an internship in Cybersecurity to provide graduating seniors with real-world experience in our simulated company called Purdue Global Internship Program - Technology (PGIP-T). The interns work as a department/team to fulfill the total requirements of an IT company from forming an Information Security Steering Committee (ISSC) to reviewing information security policies, proposals and charters, and information classification, to data management and data retention policies. Incoming interns are required to pass the ESET Cybersecurity Awareness training prior to getting credentials and access to the Amazon Web Services (AWS) cloud to ensure foundational knowledge of the information security policy governance framework. AWS cloud computing allows PGIP-Tech to scale up or down as needed to train interns on different servers and security software. The intent of the cybersecurity internship is to establish and maintain comprehensive protection, effective operation and clear accountability for all PGIP-Tech confidential and proprietary information assets and resources which, if subject to inadvertent or unauthorized disclosure, would potentially cause financial, legal, regulatory and/or reputational damage to PGIP-Tech.

Interns become familiar with the five stages of the information security policy lifecycle which encompasses assessment, design, deployment, management and support, and sustenance. Projects are robust and ongoing, such as exploring different options for Intrusion Detection Systems (e.g., Security Onion); an open-source solution that monitors incoming traffic in promiscuous mode. It listens on all interfaces and has several tools that generate reports on various types of inbound connections. The tool also scans traffic that runs against our systems and puts that data into real-time diagrams to track IP addresses. The interns install the tool on an Ubuntu machine keeping PGIP-Tech up-to-date on any potential intrusion attempts.

The interns also learn how to prevent SQL injections to PGIP-Tech databases. These attacks are prevented through learning how to sanitize inputs and parameterizing statements. Training occurs through creating an instance of a local virtual machine (running Microsoft Windows) that are vulnerable to SQL injection. This allows interns to access their own copy of the VM using the remote desktop protocol (RDP). Additional experiences offered to interns include penetration testing to flush out the weaknesses in PGIP-Tech's network perimeter and website security from cyber threats of all kinds.

BENEFITS

The internship program has measurable value-added benefits for cross-over students and those technology students who have no direct experience in cybersecurity. The internship is experiential, with hands-on projects, where teams of students actually work with cybersecurity tools that protect the "PGIP-Tech company," which includes protecting the company's other departments: IT Support, Network, Database, Systems and Web Development, that deliver real-world services to non-profit organizations. Graduates report gainful employment related to their experiences in the internship.

CONTACT INFORMATION

Desiree DePriest
ddepriest@purdueglobal.edu
(816) 941-8119
Purdue University Global

STICKER HEIST CHALLENGE

PRACTICE

DESCRIPTION

Sticker Heist contains two boxes physically locked and under the guard of a security system. The first box is simple: it's a locked container containing lots of Defcon, Hacking, tech, geek laptop stickers. The second box is the system securing the first. It contains a Raspberry Pi 3B, Arduino Uno, network and various other components (RFID, keypad, buzzer, lights). The goal is to tackle physical, network, and software security flags to disable the alarm and get the loot (stickers). https://www.linkedin.com/pulse/sinclair-college-hacking-team-sticker-heist-prof-mike-libassi-sc-d

BENEFITS

A hands-on challenge that requires the use of critical thinking and creativity to defeat the alarm system. The "flags" are actual security vulnerabilities seen in real-life. The challenge also offers the ability to work as a team and divide and conquer.

As a cybersecurity professor, the setup also allows the challenges to be changed-up, offering varied levels of vulnerabilities to adapt to different teams and classes. All the parts are easily obtainable and building the challenge is a rewarding experience for the instructor/coach.

CONTACT INFORMATION

Mike Libassi
mike.libassi@sinclair.edu
(937) 231-0888
Sinclair College

04

PROGRAM DEVELOPMENT

WINNING SUBMISSION:

THREE COLLEGES + THREE DEGREES = ONE SUCCESSFUL CYBER CAREER

THREE COLLEGES + THREE DEGREES = ONE SUCCESSFUL CYBER CAREER

PROGRAM DEVELOPMENT

DESCRIPTION

Through the leadership of our provost, Dr. Debbie Ricker, Hood established a formal cyber pipeline - the first in the nation as far as we can tell - with two nearby colleges: Frederick Community College (FCC) and Mount Saint Marys University (MSMU).

This "cyber tripod" provides students in the region with opportunities to obtain cybersecurity training at every level of higher education (associates, baccalaureate, and masters) with shared exposure to big names in cybersecurity and experiential opportunites, like hacking events with mixed-member teams and more.

Students who graduate with an Associate of Applied Science degree in cybersecurity from FCC and complete certain academic requirements can transfer up to 60 credits to MSMU, with a maximum of 24 credits meeting MSMU's cybersecurity major requirement. There are two options for degree articulation between Hood and MSMU: first, the 4+2 Program that grants qualified MSMU students preferred admission into the cybersecurity M.S. program at Hood and second, the 3+2 Program, an accelerated track that will allow qualified MSMU students to earn both a B.S. in cybersecurity from MSMU and M.S. in cybersecurity from Hood in only five years, one year less than the typical time. MSMU students accepted to either program will be able to take courses at Hood that will count toward their B.S. degrees and have the opportunity to waive foundational courses upon entry into Hood's M.S. program.

In an effort to support the growing need for trained professionals in the cybersecurity field, both regionally and nationally, the three colleges have collaborated to provide a single, unified degree pathway into this field. All three cybersecurity degrees, associate's (FCC), baccalaureate (MSMU), and master's (Hood), will be marketed together to encourage all students in the region to pursue advanced cybersecurity training. All three institutions will promote these programs, hoping to attract qualified students and streamline their path to pursuing higher education and succeeding in the cyber field.

BENEFITS

There are a variety of benefits from this three-way partnership:

- Tuition and time savings for the students
- Unique learning opportunities for students by seamless sharing of computer lab facilities and software
- Unique cross-mentorship opportunities for students with faculty from multiple institutions
- Unique faculty collaboration opportunities to improve pedagogy and engage in research projects and scholarly activity
- Unique student networking opportunities with cyber teams practicing and participating in hackathons and other cybersecurity related events
- Access to "cyber VIPs" with two events annually, which allow cyber-pipeline students from all three institutions to have a private session with experts in the field from black- to white-hat speakers. Recent sessions with Hector Monsegur (de facto head of Anonymous) and NIST Fellow, Dr. Ronald Ross, gave cyber-pipeline students a unique window to the most pressing issues in cybsecurity
- Shared public outreach opportunities across three institutions
- Shared marketing opportunities for program exposure and student recruiting across three institutions

CONTACT INFORMATION

April Boulton
boulton@hood.edu
(610) 209-5012
Hood College

CYBER FUTURES: EXTENDING CYBERSECURITY EDUCATION TO PRE-COLLEGIATE PROGRAM THROUGH CAPSTONE EXPERIENCE

PROGRAM DEVELOPMENT

DESCRIPTION

Cyber Futures was developed as a partnership between the University of the Virgin Islands' CECOR (Consortium Enabling Cybersecurity Opportunities and Research) program and the Peter Gruber International Academy, which offers an End Session, or capstone experience in the last weeks of the school calendar. Increasingly popular in high schools, capstone experiences allow students a chance to explore a topic of personal interest. Students with a strong interest in computer science selected the Cyber Futures program as their preferred option for this experience. For the University of the Virgin Islands (UVI) the Cyber Futures program thus offered an opportunity to bring CECOR programming to students interested in the area but without formal access to cybersecurity education in core coursework. As an HBCU partner in the K-20 Cybersecurity Workforce Development Program guided by Minority Serving Institutions Partnerships Program of the U.S. Department of Energy, UVI was able to target a talented and motivated student group for an immersive experience.

Students participating in Cyber Futures were introduced to cybersecurity careers, simulations, Capture the Flag challenges, and phish-spotting tests. A field trip to the university's academic computing center provided a look at cutting edge systems and the chance to meet IT professionals making real world cybersecurity decisions. Concepts in physical security, the pros and cons of remote access, and Internet of Things (IoT) were included through hands-on learning. Students used SSH (Secure Shell) to access Raspberry Pis, which were then used to create projects such as motion sensors, signal lights, and temperature alarms.

BENEFITS

Cybersecurity education at the pre-collegiate level suffers from lack of qualified instructors. While colleges and universities are often willing to engage in partnerships, faculty cannot often commit to full or even part-time positions at high schools. Capstone programs are already in place at many schools as a way of motivating students to take a renewed interest in learning just prior to the end of a school year. Partnerships like this one provide high-impact experiences and have great potential to improve both student preparation and recruiting for college programs.

CONTACT INFORMATION

Rebecca Hoffart
rhoffart@vimsia.org
(407) 284-0290
Peter Gruber International Academy, partnership with University of the Virgin Islands, St. Thomas, USVI

LAREDO COLLEGE CYBERSECURITY INSTITUTE

PROGRAM DEVELOPMENT

DESCRIPTION

Laredo College has developed a Cybersecurity Institute. The Institute consists of two specialty labs that focus on a multitude of new technologies, as well as research and instruction in all Internet realms. The labs have a dedicated demarcation point isolating the Institute from the regular college network. The Institute's primary mission will be to enhance program instruction and create collaboration opportunities with other schools, industry, government, and law enforcement entities. Collaboration with other partnering institutions to create Cyber Ranges is currently under development. Students will gain broader hands-on experience with defense tools while experiencing non-simulated cyber attacks. The Institute will also partner with Laredo College's newly established Drone Specialization to explore new ventures in cyber and surveillance technologies. The Institute will increase the college's opportunities to pursue federal grants promoting innovation and new technologies.

A curriculum pathway has been established with the public school systems. High school students will begin a dual credit certificate that leads to completion of an Associate Degree at Laredo College and then continue towards a baccalaureate degree at Texas A&M San Antonio.

BENEFITS

- Enhanced instruction
- Better prepared graduates for the workforce
- Collaboration with Industry, government, law enforcement, and other institutions
- Increased opportunity for federal grants
- Technology innovation

CONTACT INFORMATION

Robert Moore
rmoore@laredo.edu
(956) 721-5317
Laredo College

INCREASE K-12 CYBERSECURITY COMPETENCIES TO INCREASE CYBERSECURITY COURSE ENROLLMENT

PROGRAM DEVELOPMENT

DESCRIPTION

This successful approach has been two years in the making. It started in 2017, when a dual enrolled student became a CSTA Certified Cyber Teacher to include NSA Day of Cyber into the new technology club and to incorporate it into CIS I and CIS II courses after taking a course at Lord Fairfax Community College. Then in 2018, the outreach expanded to middle schools through a Girl Scout-hosted Cyber Tween event prior to the Girl Scouts creating cybersecurity badges; again in partnership with Lord Fairfax Community College. The Virginia K-12 system was then just starting to explore adding cybersecurity into the curriculum and realized that the issue was that K-12 tends to teach cyber bullying, cyber safety, and certifications without providing educators the needed education to fully understand the fundamentals of cybersecurity. This is often due to administrators and educators themselves not understanding what cyber competencies are actually needed due to the constantly changing field. At the same time, K-12 continues to teach the GenY (Millennials) way. Studies show that social engineering, hacking and defending, cyber awareness, and personal connections have more impact on Generation Z and Generation Alpha students.

Through the support of the Virginia Education System and the state's pathway approach between K-12 and higher education, I have been able to design a unique approach to increasing K-12 educator cyber competencies, reducing student cyber distress, and increase interest in cybersecurity as a career. The first step is to provide training for educators and staff to ensure they know the cyber competencies and can identify cyber distress. This step requires K-12 systems to go beyond simply downloading cybersecurity lesson plans from Cyber Ranges or other free websites. It involves educators attending weekend workshops to learn about the C-I-A Triad; not only what a tool like Wireshark is, but what it is actually doing; and that cybersecurity is not just hacking or getting a Security+ credential. This training is done through a partnership with Dr. Melissa Stange and Dr. Henry Coffman at Lord Fairfax Community College. The second step is to create a Cyber Task Force to integrate grade-level specific cyber competencies into all grades, not just Fundamentals of Cybersecurity Courses or Networking courses at the high school. Also, during this step I met with school officials to convince them to be open to student suggestions on cyber related topics, presentations, and course content. Presentations on cyber topics have to be engaging and Generation Z and Generation Alpha students have to be able to relate to them, instead of being a speaker from across the nation that they have no connection with. This means bringing in people like local cyber survivors, organizations like Safe Surfin' and BACA, current cybersecurity students, and industry professionals that are creating the IoT devices they are using. These presentations must be cross-curricular to demonstrate how cybersecurity is not an independent course or discipline, but that it is weaved into everything we do in society. In the third step, school systems must notify parents of all Web and mobile communications required to be used within the classroom and provide offline options. It was discovered that some educators require students to create accounts, even though the student was below the minimum age listed on the website, because the educator wanted to use it in the classroom and the school systems technology manager approved it for use. The final step is critical as it requires a continual review and maintenance process of the cyber plan.

School systems that are using this approach have found a decrease in K-12 cyber distress and an increased interest in cybersecurity courses. To ensure that K-12 and higher education expectations are aligned, community college professors should serve on K-12 program advisory boards and K-12 representatives should serve on the community college curriculum advisory committee. Lord Fairfax Community College takes this approach and it has allowed open discussions on how to better connect K-12 cybersecurity to Community College cybersecurity. My efforts to improve K-12 Cybersecurity education and increase Cybersecurity enrollment has evolved through national organizations such as Safe Surfin' Foundation by providing speakers at schools and education material, National Center for Women & IT (NCWIT) Aspiration in Computing Awards and AspireIT grants, and National CyberWatch Center of early steps in the 2017 and 2018 Innovations for Cybersecurity Education. This national support has validated this two-year cybersecurity educational approach. This solution was initially presented at the 2019 Association for Computing Machinery (ACM) SIGCSE and continues to evolve into a duplicatable K-12 to Higher Education cybersecurity curriculum model that engages students in cybersecurity at the elementary school level, so they want to continue in the field.

BENEFITS

Incorporation of cross-curricular security problems leads to students that are actively engaged in solving the problems. Educators and staff are more competent in the C-I-A Triad and can encourage student learning beyond a canned lesson plan to produce better mastery of and interest in cybersecurity. This method focuses on the outcome of increasing the number of cybersecurity professionals while keeping students involved and providing a solution that they can have a voice in. Educators are held accountable for understanding the risks involved with using free tools. Finally, this method is a source of open communication and partnerships between K-12 school systems, higher education institutions, and cybersecurity organizations.

CONTACT INFORMATION

Rachel Stange
rms25145@email.vccs.edu
(540) 877-5571
Lord Fairfax Community College

STATEWIDE COLLABORATIVE: CALIFORNIA MAYORS CYBER CUP - REACHING UNDERSERVED STUDENT POPULATIONS FOR CYBER EDUCATION AND CAREERS

PROGRAM DEVELOPMENT

DESCRIPTION

Determined to bridge the gap between K12, communities, industry, and higher education, a pilot launch of the collaborative California Mayors Cyber Cup (CMCC) occurred in 2017, hosted by community colleges in four regions consisting of 32 teams and 191 students. CMCC, an educational and workforce program of California Cyberhub, a synEd initiative, utilizes cyber competitions, educational training, and higher education, government, and industry partnerships to spread awareness about cybersecurity and the many opportunities that exist within cyber career fields. Critical to the CMCC outreach, is reaching underserved communities and student populations to build a strong, ethical, future cyber workforce for California and our nation.

As an outcome to our alpha year, our beta version, led to a true statewide collaborative engaging the California Community College Chancellor's Office, economic development partners, statewide legislative representatives, and wide-ranging industry representation. More importantly, however, was the ability of this collaborative endeavor to reach and serve diverse socio-economic, cultural, and ethnically diverse participants in a fun, appealing, community event. The 2018 CMCC fostered community spirit by providing a live video link from our state capital to 12 host sites representing 150 cities, 270 teams, 1,300 participants, and a plethora of community spectators. A key objective, stipulated by all stakeholders, was to ensure that the platform was easily accessible to all, free of charge, and include community youth groups and organizations. This was achieved by centralizing the competition game designed by Haiku Cyber Range along with access and technical support through Amazon Web Services and Sentek Global. Local hosting time investment and technical equipment was cut substantially, with accessibility through a cell phone, Chromebook, tablet, PC, or iPad. Participants explored, played, and competed in a fun, engaging, four-hour cyber challenge requiring critical thinking, team collaboration, communication skills, and cyber hygiene governance. Teams of middle school and high school-age participants detected and thwarted attacks and infiltration on our nation's critical infrastructure in an effort to obtain cumulative points towards winning the perpetual Mayors Cup Trophy for their city. For their exemplary efforts, each were awarded recognition certificates by their State Assembly Representative. Significant local impact is achieved with the regional Mayors Cup Trophy presentation, by the winning team, at each of the respective city council meetings as it provides powerful awareness to local government, business, and general citizens and serves as a catalyst for their involvement. The students' testimony of the CMCC impact and their personal endeavors towards a cyber career pathway, is the launch pad that embeds cyber opportunities in their community and grows new teams.

Although the California Mayors Cyber Cup competition is over, the work of Team California to educate the next generation of cybersecurity professionals is just beginning. Over the next year, parents, educators, employers, employees, and leaders from business and government will work together to create 1,000 new middle and high school cyber competition teams by 2020. It's an ambitious goal but one that can be achieved through statewide cooperation. Cybersecurity jobs provide a pathway to a secure, high-paying career that can't be outsourced. The goal of the Team California initiative is to bring cybersecurity awareness and education into communities across the state, and expand to other states in the same way youth soccer or little league baseball became common generations ago.

BENEFITS

The CMCC initiative provides the following benefits with full accessibility to the educational curriculum, community and team resources, and tools at no cost to the public (www.ca-cyberhub.org):

- Accessibility to all communities; diverse and balanced representation of socio-economic, cultural, and ethnically diverse participants to explore and engage in cyber education and careers
- Exposure for participants, community members, industry representatives, and civic leaders to cyber educational pathway opportunities at their local K12, community college, and university institutions
- Building and expanding vital community partnerships
- True collaborative engagement by community members, civic leaders, educators, and business leaders
- Access to methodologies, tools, and support readily available for duplication in other states and community colleges
- Building strong, viable cyber pathways for our youth to develop our future cyber workforce

CONTACT INFORMATION

Liz Fraumann
lfraumann@ca-cyberhub.org
(858) 735-2288
12 Host Locations - Multiple Community Colleges and Education Centers: Butte Community College, East Los Angeles College, Fresno City College, Long Beach City College, Mendocino Community College, Moorpark Community College, Moreno Valley College, Mt. San Jacinto College, Sacramento City College, San Jose College; San Diego Salvation Army Kroc Center, and Troy High School.

VICYBER RAPID DEVELOPMENT OF CYBERSECURITY CURRICULUM BASED ON THE NICE CYBERSECURITY WORKFORCE FRAMEWORK

PROGRAM DEVELOPMENT

DESCRIPTION

In an effort to encourage and support innovations in curriculum development, the National Institute of Standards and Technology (NIST), published the National Initiative for Cybersecurity Education (NICE). It is a partnership between the government, academia and the private sector focused on cybersecurity education, training, and workforce development. The NICE framework consists of seven categories, 31 specialty areas, 369 Knowledge, Skills and Abilities (KSAs), 65 competencies, and 444 tasks under various specialty areas. It is meant to guide curriculum developers to choose the right knowledge areas that would serve the desired competencies. However, two major difficulties faced in this regard are: 1) the lack of cybersecurity experts who can interpret the framework and make effective use of it; 2) the large number of competencies, KSAs and tasks in the framework that need to be considered along with their relationships during curriculum development.

In viCyber, we've addressed the issues identified above by developing an interactive system to assist rapid cybersecurity curriculum and training development using visual mapping and artificial intelligence techniques. It has been released as an online application freely accessible to curriculum designers across the nation (https://vicyber.columbusstate.edu/home).

BENEFITS

The growing number of reported cyber-attacks pose a difficult challenge to individuals, governments and organizations. Adequate protection of information systems urgently requires a cybersecurity-educated workforce trained using curricula that cover the essential skills required for different cybersecurity work roles. The viCyber curriculum development tool is designed to assist inexperienced as well as experienced instructors in designing cybersecurity courses and training programs. It is an intelligent interactive system that uses visual feedback to guide the user through the design process. Over time, it is designed to become a repository in the cloud for curriculum and course exemplars. ViCyber is a cloud-based free application open for use to anyone with access to the Internet.

CONTACT INFORMATION

Shamim Khan
khan_shamim@columbusstate.edu
(706) 507-8184
Columbus State University

THE INTELLIGENCE COMMUNITY CENTER FOR ACADEMIC EXCELLENCE (ICCAE) CONSORTIUM ON CRITICAL TECHNOLOGIES STUDIES PROGRAM

PROGRAM DEVELOPMENT

DESCRIPTION

San Juan College has partnered with the University of New Mexico in Albuquerque and other institutions of higher education across New Mexico to form a New Mexico consortium of schools aiding in the creation of UNM's Critical Technologies Studies Program (CTSP), under The Intelligence Community Centers for Academic Excellence (ICCAE) program. ICCAE helps undergraduate students in the development of the essential skills needed to work in the 17 federal U.S. intelligence agencies (i.e. the Intelligence Commnity). ICCAE specifically focuses of the development of students' analytic, critical thinking, and communication skills needed within the IC.

BENEFITS

ICCAE comprises a wide spectrum of institutions of higher education dedicated to study of issues related to the intelligence community (IC). ICCAE assists in the development trained personnel who possess the technological, analytic and critical language skill sets needed to successfully navigate the 21st Century's Intelligence landscape.

CONTACT INFORMATION

Cameron Cooper
cooperc@sanjuancollege.edu
(505) 566-3372
San Juan College

SOUTHWEST VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY & CYBERSECURITY INITIATIVE

PROGRAM DEVELOPMENT

DESCRIPTION

The purpose of the cybersecurity Initiative is to build a pool of cybersecurity professionals and bring new jobs to the region, leveraging significant investments that have been made in the region's fiber infrastructure, robust and redundant broadband capacity, place-based economic development strategies (including outdoor recreation and cultural assets), as well as a decade-old investment toward developing an IT workforce. This initiative builds upon the work already completed to create an environment complete with amenities attractive to cybersecurity professionals and information security companies.

A critical shortage of individuals with information security skills and industry-recognized credentials exists in Southwest Virginia; therefore, training is crucial to developing an adequate workforce. Partnerships have facilitated a major role in the success of the Information Technology pathway at Southwest Virginia Community College. These partnerships came from local employers, community organizations, public-school systems and other regional colleges.

The Cybersecurity initiative is targeting the critical shortage of individuals with information security skills and industry-recognized credentials that exists. Every class in the curriculum is focused on the use and integration of technology to meet the critical needs of businesses. Many of the course objectives were based on various third-party certifications to provide a skillset needed for employment.

This program provides students with knowledge and training so that they can implement defense, recognize unauthorized access, and take action to minimize threats to their network and computing environment. Our program is designed to provide students with technical and problem solving expertise needed to actively protect assets connected to a network.

The course work of the Career Studies Certificate in Cyber Security is designed to be completed within two terms to provide expertise in security. The curriculum will prepare students for employment as network security specialists, Internet security specialists, or similar security related employment fields. The CSC in Cyber Security also helps prepare students for the CompTIA IT Fundamentals, A+, Network +, Security+, and Certified Ethical Hacker (CE) certification exams.

CONTACT INFORMATION

James Dye
james.dye@sw.edu
(276) 964-7277
Southwest Virginia Community College

COMPETENCY-BASED GLOBAL CYBERSECURITY EDUCATION

PROGRAM DEVELOPMENT

DESCRIPTION

Modern organizations exist in a new hyperconnected world of machines and humans. Crime, news, and even warfare is digital today. Information risk and intellectual capital risk is now integral to the success of organizations. IT security evolved from a technology focus to a business focus. Cybersecurity strategy must be tailored to the mission of organizations. Modern cybersecurity is defined as the mission-focused and risk-optimized governance of information, which maximizes confidentiality, integrity, and availability using a balanced mix of people, policy, and technology, while perennially improving over time (Hasib, 2015, p. 3). Modern organizational executives need a holistic business approach, which includes a cybersecurity strategy based around people, policy, and technology and perpetual innovation. In such a manner cybersecurity strategy becomes a revenue, innovation, and productivity driver for organization.

We created groundbreaking interdisciplinary Master of Science degree programs in various cybersecurity tracks to teach graduates to think as business professionals and modern executive leaders. With our open admissions policy, we embrace people from all previous backgrounds such as criminal justice, human resources, politics, psychology, criminal justice, law - even linguistics and art into the program with no GRE or other artificial barriers. We made the program and all accompanying lab exercises available online from any global location. We hired practitioner scholars to lead and teach in the program so students are mentored by professionals who have worked in the field.

Since cybersecurity is not a one brain sport, we made teamwork an essential feature of the programs. So students apply each other's knowledge and work in teams to approach problems through an interdisciplinary lens. Students therefore learn from each other as much as they learn from the curriculum and professors. Students also learn to make executive presentations, create podcasts, and build their personal brands in order to achieve success and gain higher market value for their skills. We have partnered with several large federal government and private business organizations to provide job opportunities to our students and graduates. The programs already has thousands of successful graduates who are stars or rising stars in the field.

BENEFITS

Knowledge is not enough. Graduates need to be able to apply knowledge to a particular situation, problem, or organization. Students complete practical real world type projects and develop marketable skills instead of taking memory based tests. Thus they are ready for employers when they graduate. Since business mission, risk principles, and perpetual deep learning are deeply embedded into the programs, these programs are better executive preparation programs than most MBA programs today. We eliminated textbooks and provide students everything they need to learn. Thus, they save $400 per term. Students have multiple attempts to successfully complete projects. Thus there is no fear of failure and more students succeed in the programs. Furthermore, full time working professional can earn our 36 credit Master's degrees in 18 months for under $25,000 while taking only one course at a time from anywhere in the world. We have won multiple awards including Best Cybersecurity Higher Education Program in the USA Award from SC Awards two years in a row (2018 and 2019) and (ISC)2 Information Security Leadership Award for the Americas (2017). Our programs have also experienced phenomenal growth in global enrollment and with more than 12,000 students in graduate and undergraduate programs, we are currently the world's largest cybersecurity university.

CONTACT INFORMATION

Dr. Mansur Hasib
mansur.hasib@umuc.edu
(240) 684-2425
University of Maryland University College
(UMUC)

IMMERSIVE EDUCATION: ACCELERATING THE AVAILABILITY OF CYBERSECURITY WORKERS TO THE WORKFORCE

PROGRAM DEVELOPMENT

DESCRIPTION

There is a great need for cybersecurity personnel. Schools are not producing enough graduates right now to fill the increasing need for cybersecurity workers. Ivy Tech, in partnership with the Indiana National Guard and the National Center for Complex Operations (NCCO), has put together a program to graduate around 40 students in 11 months with the A.A.S. in Cybersecurity, with plans to start 80 students in the fall of 2019. The program is being hosted at the Muscatatuck Urban Training center in Butlerville, IN, which will give students access to real life situations, like a fully-outfitted smart house, a working water treatment plant, a jail, and many other features. Ivy Tech Community College has the honor of being designated as a National Centers of Academic Excellence in Cyber Defense 2-Year Education through a rigorous process supported by the Department of Homeland Security and the National Security Agency.

BENEFITS

There are several innovations with our Muscatatuck Cyber Academy. One is that the program gives community college students the experience of living in dorms like traditional 4-year colleges. It also gives students a built-in peer group. Everyone is taking the same classes at the same time, and it makes for a really good group to evaluate curriculum, teaching methods, etc. Having an accelerated program allows students to get into the workforce more quickly, and it makes it easier for companies from a recruiting perspective. The coolest part of this program, though, is the students having access to the Muscatatuck facilities - from the smart house to the jail that all can be manipulated in a cyber-physical environment.

CONTACT INFORMATION

Pam Schmelz
pschmelz@ivytech.edu
(812) 374-5214
Ivy Tech Community College

05

HONORABLE MENTION

WINNING SUBMISSION:
PCI CREDIT CARD SECURITY

PCI CREDIT CARD SECURITY

HONORABLE MENTION

DESCRIPTION

I work full time on Payment Card Security at the University of Virginia. I created this training module to train staff and students how to properly handle credit card data (http://training.foc.virginia.edu/UVAFrontline/index.html). I am also a student both at Piedmont Virginia Community College in the Computer Information Associates program with a specialization in Cyber Security as well as a student at The University of Virginia in the Graduate Cyber Security Management program.

This training covers cybersecurity protection of unauthorized use of customer's credit cards, who pay the University for a numerous types of transactions ranging from Athletics to the Virginia Festival. This is an interactive streamlined approach that has DocuSign at the end providing a time date receipt for the training. This training is available to share with other colleges and universities to help enhance rolling out interactive training to all staff and students.

BENEFITS

There are two links available, the open link http://training.foc.virginia.edu/UVAFrontline/index.html and the non-public internal link. The internal link ties to our education portal, will give the person taking the training credit for HR purposes, and will automatically email the person taking the training annually that they need to take it again.

Both links provide the following benefits:

- ADA accessible, allowing for tablet touch screens, laptop tabbing, or desktop mouse input
- Closed Captions and audio/visual combinations
- UVA Branding color scheme
- Interactive games to reinforce key concepts: drop and drag the definitions, true/false covering multiple policies, and identify important parts of a credit card that must be safeguarded
- Then the training splits into choose your job function and has detailed cybersecurity training for the webpage departments and the physical machine safety
- Lastly, the training goes into DocuSign that the trainee fills out. Once filled out, the Docusign is sent to the employee, their supervisor, and the Payment Card Services department for Audit purposes
- The entire training module is under 20 minutes and also paperless

CONTACT INFORMATION

Ruth Parcells
rp9d@virginia.edu
(434) 924-4362
University of Virginia

NATIONAL
CYBERWATCH
CENTER

WWW.NATIONALCYBERWATCH.ORG