2022 CAE in Cybersecurity Community Symposium

June 8-10, 2022 The Westin Peachtree Plaza Atlanta, GA

Abstracts

CAE-CD Track Fast Pitch Talks

A Final Stop of the CWCT Journey: Training Participant Job Placement with Certifications

Mengjun Xie, University of Tennessee at Chattanooga
Stephen Reiter

While the job market for cyber talent has hit record numbers, employers have found it quite difficult to recruit quality individuals to fill the ranks. There are intense efforts to identify and hire employees with related experience, yet with limited success.

Beginning in 2020, a team of 4 higher education institutions established an NSA funded consortium named Cybersecurity Workforce Certification Training initiative or CWCT with the support from N-CAE. CWCT leadership projects by September of 2023 when this round of funding concludes, 1,100 people will be trained.

By design, 75% of the trainees in CWCT come from those who have served our nation, state, or local communities – via the military, law enforcement, 1st responders, etc. To date, our records show that 71.2% of the trainees are from underrepresented populations, 29.3% are women, which fits well with the desired demographic most employers are looking for. We are proud to announce our potential completion rate is currently running over 80%, well beyond our expectations.

Our CWCT workforce development program has fully recognized the importance of workforce preparation through academic training and competency measurement through the industry-government recognized certifications. The CWCT program goes one step further to develop a Job Placement program through workshops on resume building and interview skills development, and more importantly, introducing job opportunities to our training participants through CWCT virtual job fairs and other unique efforts.

This Fast Pitch talk will provide a quick synopsis of the CWCT initiative, then address our unique and successful approach to bringing employers and trained employees together.

Benefits from a Novel Outreach Project that Supports Cybersecurity Professional Development

Waleed Farag, Indiana University of Pennsylvania

This proposal discusses considerable benefits of a recent outreach project to strengthen relationships between Indiana University of Pennsylvania (IUP), an established CAE for over two decades, and several Community Colleges (CCs) and technical institutes across Pennsylvania. IUP has been working with several CCs for years to promote cybersecurity education and research in the western PA region. With support from a Capacity Building Project that focuses on outreach to technical and community colleges funded by the DoD and as a part of the Cyber Scholarship Program (CySP), IUP has built long-term relationships with several CCs throughout PA and provided engaging and highly rated professional development opportunities in cybersecurity to faculty and students at six institutions. The main goal of the project is to find additional ways to recruit qualified students into the cybersecurity field and DoD CySP to help protect the nation's cyber infrastructure. This goal was achieved through increased faculty and student development (via a series of collaborative cybersecurity workshops), and a wider network/partnership with several CCs and minority institutions. Specifically, our workshops have been designed in such ways to ensure that all participants will develop the following skills, abilities, and knowledge:

1. Faculty and students are able to self-organize their work, collaborate, and be successful in assessing and resolving vulnerabilities in digital space.
2. Faculty learn new cybersecurity teaching methods that help increase knowledge retention and develop plans for continuing education and professional development.
3. Students leave the workshops with a vast set of skills, including programming specialty computers and embedded systems.
4. Faculty and students learn procedures for ensuring software integrity through hands-on activities such as hash generation and verification.
5. Faculty and students develop interest in cybersecurity and are motivated to further their study of advanced techniques in cybersecurity to protect systems from vulnerabilities.

We have offered six workshops that each consist of two full days delivered over two successive Saturdays or during a semester break. Workshops were originally delivered face-to-face, but we shifted the delivery mechanism online due to the pandemic. We delivered workshops to the following CCs and technical institutes geographically distributed across PA: Westmoreland County CC, Pennsylvania Highlands CC, Laurel Business Institute, Laurel Technical Institute, Butler County CC, and Northampton CC. Below is a list of benefits and outcomes that resulted from this outreach project:

1. We built excellent relationships with faculty and administrators at six institutions across PA.
2. We were able to provide well-received, cybersecurity professional development to about 120 faculty and students at six different institutions.
3. Our offerings continued to be engaging after the shift to online delivery, which has been shown in the participants' high ratings of all sessions.
4. Efforts in this project have facilitated ongoing collaboration work that involves about half of PA community colleges working with IUP to enhance cybersecurity and STEM education.

Abstracts

CAE-CD is Not the End Goal, it is the First Door to a World of Opportunities for Cyber Initiatives

Shankar Banik, The Citadel

In this Fast Pitch Session, I will share with other CAE institutes how CAE-CD designation has helped The Citadel take Cyber Programs and Activities to the next level. The Citadel started with an undergraduate minor in Cybersecurity in 2012, and became CAE-CD in 2016 with the academic path of BS in Computer Science with a minor in Cybersecurity. The Citadel was the second college in the State of South Carolina with CAE-CD designation. Students from The Citadel Students have been awarded DoD CySP Scholarship every year since 2017. The Citadel hosted the first GenCyber Camp in South Carolina in 2016. The Citadel hosted All-Girls GenCyber Camp in 2019.

The Citadel was awarded the first NSF SFS Grant in South Carolina in 2020. The Citadel has started to offer BS in Cyber Operations in Fall 2020. The program has been designed based NSA Center of Excellence in Cyber Operations. The Citadel is working with University of South Carolina (CAE-CD, CAE-R) on a NCAE-C Research Grant. The Citadel is working with University of Memphis, University of West Florida, North Carolina A&T University on a NCAE-C Grant for Cyber Education for Critical Infrastructure. The Citadel has established Citadel Department of Defense Cyber Institute (CDCI) in Fall 2020. This is a joint initiative with five other Senior Military Colleges - Texas A&M University, Norwich University, University of North Georgia, Virginia Tech, and Virginia Military Institute. Students at The Citadel have formed Cyber Club, WiCyS Chapter.

The Citadel Cyber Team actively participates in different Cyber Competitions - National Cyber Exercise (NCX), Southeast Collegiate Cyber Defense Contest (SECCDC), NSA Code Breaker Challenge, Cyber Red Zone CTF, Palmetto Cyber Defense Contest, and National Cyber League (NCL). The Citadel hosted a Cyber Bootcamp for South Carolina Army National Guard in Summer 2021. The Citadel worked with Army Cyber Institute on Jack Voltaic Project. The Citadel hosted Jack Voltaic Conference on Cyber Resiliency for Critical Infrastructure on Feb 24-25, 2022. The conference program included sessions on Cyber Workforce Development for Critical Infrastructure, Cyber Education for Critical Infrastructure, Cyber Risk Assessment for Critical Infrastructure, Federal and State Policies and Capabilities for Critical Infrastructure protection against Cyber Threats. The conference program also included a Cyber Table-top Exercise and Student Case Scenario Exercise. The Citadel faculty actively participates in CAE Community by working as a mentor and reviewer for CAE applications.

Critical Infrastructure - Training

Dipankar Dasgupta, University of Memphis
Jim McGinnis

Critical Infrastructure training based on the current threat environment is at a high level throughout the nation and worldwide. A concerted effort by multiple professors, professional cybersecurity personnel, students and staff, a workshop has been developed based that provides training on current topics using in some cases actual examples of security incidents, demonstrations such as pen-testing and necessary remediation steps and methodologies. The current topics include the current state of cybersecurity, ransomware, threat level/surfaces, zero trust architecture, cyber risk assessment from a data-driven view and the work from home/remote office environment. The workshop/training provides not only research based initiatives but also insight and experience of cybersecurity practitioners.

Cybersecurity Pathways: Implementing a Systems Based Approach Through Mentoring

Lonnie Decker, Davenport University
Teha Emmons

The need for cybersecurity workers is clear. With a documented current shortage of cybersecurity workers in the U.S. identified as over 300,000 openings, the need to attract, and retain more future cybersecurity workers could not be more clear. Many efforts have been created to address this need and have had clear positive results. These include the use of summer camps & competitions to increase interest in the field, reaching out to underrepresented populations to help fill the need, and providing scholarships and using shared curriculum to help students through their educational pathway.

This presentation will discuss the implementation of a Community Based Life Cycle (CBLC) approach to help address this need. With the development of a Cyber Education Task Force (CETF), the ability to use a systems development approach to identify and align the efforts that already have been developed to help retain students' interest in cybersecurity as a career. Through the use of professional and peer mentoring in a Cascade Advising approach, the professional mentors (and members of the CETF) would identify communities (summer camps, competitions, etc.), where peer mentors can be effective in helping newer and future students be successful.

Developing Competency Through Competitions

Dan Manson, Cal Poly Pomona
Morgan Zantua

Most young people do not know what a cybersecurity professional is, the skills required to reach and excel at a high level or a pathway to pursue the goal of a cyber-based career. The joy and impact of learning cybersecurity through competitions is still in its infancy.

Using the NICE framework, we are starting to use metrics to measure competencies in competitions. The NSA/CAE Evidencing Competency grant team is measuring competency using NICE Framework Tasks and Work Roles in labs, ranges, and competitions. This includes an ABCDE approach to competency statements. A = Who, B = What, C = How, D = How much, and E = Why.

This presentation will focus on how we can measure these competencies in competitions. In the future we can learn to measure cyber performance as well as we do athletic performance. We will create cybersecurity competition measurements enabling a spectator sport similar to traditional sports. This is not just a dream, it is a reality today for e-sports. It is time we put our passion, creativity, effort, and money where our future is.

Abstracts

Education on Cybersecurity Issues with Smart Power Grid

Mohd Hasan Ali, The University of Memphis

Modern power grids, such as smart grid and micro-grid systems, have various intelligent and sophisticated controllers at all stages of generation, transmission, sub transmission, distribution, and customer ends. Moreover, renewable energy sources (wind generator, photovoltaic systems, etc.) are being connected to the grids through various power electronics components and energy storage systems (ESS). According to a recent report, solar and wind together represent roughly 10 percent of the world's installed capacity. These power electronics devices as well as energy storage systems are also based on robust and intelligent controllers that may have internet-connectivity for their real-time operations.

However, there is a high possibility of cyber-attacks at those control and communication systems, which may be adversely effected and consequently major power disruptions or even blackouts may happen. ESS are important assets in power grids, capable of providing several essential services to systems dominated by intermittent renewable energy resources. Cybersecurity attacks exploit vulnerabilities in communications or control systems to disrupt system operations or execute malicious actions. With the advent of distributed energy resources (DER), which include consumer-owned small ESS often connected to public networks, the attack surface has greatly increased. This fast pitch will cover the basics of cybersecurity issues with the smart power grid, and also will discuss about the smart grid security workshop held at the University of Memphis on March 25, 2022, for a wide range of audiences.

Establishing New K-12 Pathways

Andrew Lutz, Johnson County Community College

This fast pitch session will describe how the Information Technology—Networking and Cybersecurity department at Johnson County Community College (JCCC) established a K-12 pathway with a large local district, Blue Valley Schools. The pathway provides students the opportunity to complete the JCCC Cybersecurity Certificate program tuition-free alongside their high school education. Successful students will receive both their diploma and the Cybersecurity Certificate upon graduation from high school. The session will discuss:

-Building the pathway
-Strategies for recruiting students into the program
-Working with the state department of education to increase opportunities

Hierarchical Multi-Blockchain Architectures for Autonomous Management of Medical Data/Devices

Mike Burmester, Florida State University
Xiuwen Liu

The healthcare ecosystem involves several interconnected stakeholders with different and sometimes conflicting security and privacy requirements. Sharing medical data, particularly remotely generated data, is a challenging task. Although there are several solutions in the literature that address the interoperability & scalability functional requirements of such services, as well as the security & privacy requirements, achieving a good balance between these is not a trivial task as off-the-shelf solutions do not exist. On one hand, centralized cloud based architectures provide interoperability & scalability, but make strong trust assumptions. On the other, decentralized blockchain platforms support independent trust management and data privacy, but typically do not allow dynamic changes of the underlying trust domains.

To address this challenge we propose a hierarchical multi-expressive blockchain architecture that addresses this challenge by providing: (a) dynamic trust management between different authorities, (b) flexible access control policy enforcement at the domain and cross-domain level and, (c) a global source of trust for all entities by an immutable forensics-by-design auditing mechanism.
Fine-grain access is enabled by using an attribute based encryption scheme that provides a single access point that cannot be bypassed by users or authorities and that supports flexible shared multi-owner encryption, when attribute keys from different authorities are combined to decrypt data.
The effectiveness of the proposed approach is validated experimentally. The multi-blockchain has also been implemented using the Hyberledger Fabric.

This work based on the following publications of the presenter.
1. JANUS: Efficient multi-authority & multi-domain attribute based access control in practice, submitted, 2022.
2. A hierarchical multiblockchain for fine grained access to medical data, V Malamas, P. Kotzanikolaou, TK Dasaklis, M. Burmester, IEEE Access 8, 134393-134412, 2020
3. A forensics by design management framework for medical devices based on blockchain, V Malamas, TK Dasaklis, P Kotzanikolaou, M Burmester, S Katsikas, IEEE World Congress on Services (SERVICES) 2642, 35-40, 2019

How Build Large Student Cyber Clubs

Mike Morris, Western Governor's University

Western Governors University (WGU) never had a club until 2020. Our Club went from 0 to 3,500 students in the first year. Currently We have 5,500 in our student club and 2,500 in our Alumni Club. In ten minutes I can provide an overview of how to build a robust club that helps students learn, network and prosper in today's educational landscape.

Abstracts

Incorporating AI Into Software Reverse Engineering Courses

Xiuwen Liu, Florida State University
Mike Burmester

Software reverse engineering skills are fundamental to producing a capable cyber security workforce. However, analyzing binaries is often difficult for computer science students and others in related areas due to the curriculum emphasis on efficient software development. At the same time, while artificial intelligence techniques, powered by machine learning and deep learning models, have shown promise to make software reverse engineering less labor intensive, there are a number of practical challenges software reverse engineers must overcome so that they are practically effective for program analysis and software reverse engineering. In this presentation, we will summarize our efforts in incorporating AI techniques to our software reverse engineering courses, where IDA Pro and Ghidra are used as the main tools. With proper setups, we show that the tools for control flow and data flow techniques along symbolic executions can be effective in malware analysis.

Lessons Learned from the Development of a Dual-Enrollment Programs with High Schools

Dr. Yair Levy, Nova Southeastern University

This talk will discuss the lessons learned from a project put in place by Nova Southeastern University (NSU), College of Computing and Engineering in collaboration with the Miami-Dade Public Schools (MDCPS) on a dual-enrollment program for high-school students from minority and underserved schools throughout the Miami-Dade district. The project allowed support for two entry-level Computer Science courses at the ABET CS program (under the Advanced Academics division at the school district) with additional extra-curricular activities (under the Career and Technology Education (CTE) division at the school district) focused on cybersecurity certificate using TestOut platform to prep the students outside the course for CompTIA Security+. The session will discuss the steps taken to address the course registration process, legal issues that the university faced and how we overcome those, along with coordination for advertising of the courses, student recruitment and continuous support for the enrolled students.

Micro Transcripts: Quantifiable and Auditable Workforce Readiness Transcripts (WRT) for Internships

Ram Dantu, University of North Texas
Mark Thompson

Employers are citing a significant disconnect between the needs of their organizations and what higher education institutions are turning out in their cybersecurity-related education programs, with only 23 percent believing that college graduates are fully prepared to enter the cybersecurity industry with a certain knowledge set and applicable technical skills. One recent response from a major corporation to a request for information issued by NICE indicated that “the current [education] environment does not provide a common baseline set of skills from which to build the role-specific knowledge necessary to meet employer workforce requirements.

Problems in Matching to Internships: For a student without meaningful work experience, the only document is a university transcript that usually only contains the course information (i.e., name, number, credit hours) and accompanying letter grades along with the current and cumulative GPA, but they fail to provide specific information about the actual skills or rigor used to obtain that grade. The content and difficulty of each course can vary widely among institutions. Students cannot simply hope to stand out to employers based on their grades alone because universities lack normalized standards for the rigor of content in each course. Employers require a more work-skill specific transcript that matches the needs of the job specification.

The primary issue when hiring new graduates into the industry is correctly matching employer needs with student skills. For example, employers need web socket programming, or React API or Java Spring Boot but do not know how to measure the rigor of the skill. In this fast pitch, we present a workforce Readiness (WRT) transcript (we are building by crawling through the Canvas) tailored to the individual student with a quantifiable substantiation of preparedness for employment as a cybersecurity professional that includes a match percentage to an advertised internship and missing skills.

OpenStack Private Cloud for Cyber Capstone Development and Implementation

Chuck Bane, University of San Diego

This presentation outlines how we built the Openstack infrastructure, automated the implementation of student projects, and work with students so they treat the Capstone Projects as real-life jobs. At USD, we found that local businesses were reluctant to allow students the opportunity to evaluate, and implement security on an operational system. We developed the USD Cyber Cloud (a private cloud using OpenStack) to have an isolated sandbox that can be quickly configured to give the student (Student Groups) a fully functional business network system. In this safe environment they can perform all the required tasks to conduct a security engineering review of the client’s system, conduct Vulnerability Assessments, Penetration Testing, and based on findings, create and execute a hardening plan to make the system secure. The hardening plan is the “What”; execution of the hardening plan is the “How”. The development of an Information System Security Plan plus the other testing report builds a portfolio of achievements for the students.

We, Cybersecurity educators, understand what knowledge is needed to be successful in Cybersecurity and to foster a culture of ethical behavior. Now, we need an environment and method to allow students to execute and implement this knowledge safely risk free.

Abstracts

Stepping-Stone Intrusion Upstream Detection Using Round Trip Time Distribution

Jianhua Yang, Columbus State University

As the capability to detect network intrusion has increased, so has attackers' ability to avoid detection. Commonly, attackers use Secure Shell (SSH) to hide their identity. SSH securely connects two hosts together and encrypts their interactions. The first step to preventing Stepping-Stone Intrusion is to be able to detect if it occurs, in this regard, much research has been done to detect intrusion by looking at downstream network traffic, that is, the traffic flowing to the victim and back from them, but detection methods looking at upstream data, which is the traffic flowing from the attacker and back towards them from a sensor, are inadequate and underrepresented in the field.

To this end, a potential method for upstream detection has been devised. By observing the upstream connection, we can match a send packet with its respective echo packet, and as a result, determine the round trip time (RTT) of that packet. When looking at a series of these matches, we can find the average RTT of all the packets, and then the standard deviation of the RTTs among matches. We estimate that, as a result of the increasing routers, hops, and physical distance between them, transmission will vary more the further a sensor is from a victim. By observing the standard deviation of these RTTs at different places in a long connection chain, we may be able to discern a usable standard or pattern that can determine the length of a downstream connection, and with modification, estimate the length of an upstream connection.

The Easiest Interview Answers - Your Story

Robert Loy, Grand Canyon University

No matter how stressful the thought of an interview may be for you, there is an easy answer. Each person has a collection of responses that can be used to solve almost every question, and the best part is that there is no wrong answer! The answer that the interviewer is looking for is your personal story. It is a collection of events that shaped you as an individual and will ultimately be the deciding factor in your success in the role and within the company. Each of you has been on a project, worked on a team, failed, and succeeded. You all have experienced challenges and overcame them, or maybe not.

What we must do as interviewees is pull our experiences out and frame them so that it becomes a story with us as the main character. We need to us as a character who experiences conflict and then arrive at a resolution. The story will contain our experiences and are unique to use, which is essential when competing for roles.

In this fast pitch, the attendee will find examples relating their personal story to the most common interview questions. Finding the right mix of challenge and conflict in school projects, extra-curricular events, work, or class lessons is as easy as understanding what the interviewer is looking for in future team members. The storytelling takes some practice and polish, but it still is your story to tell.

The UAH Cyber Force Incubator

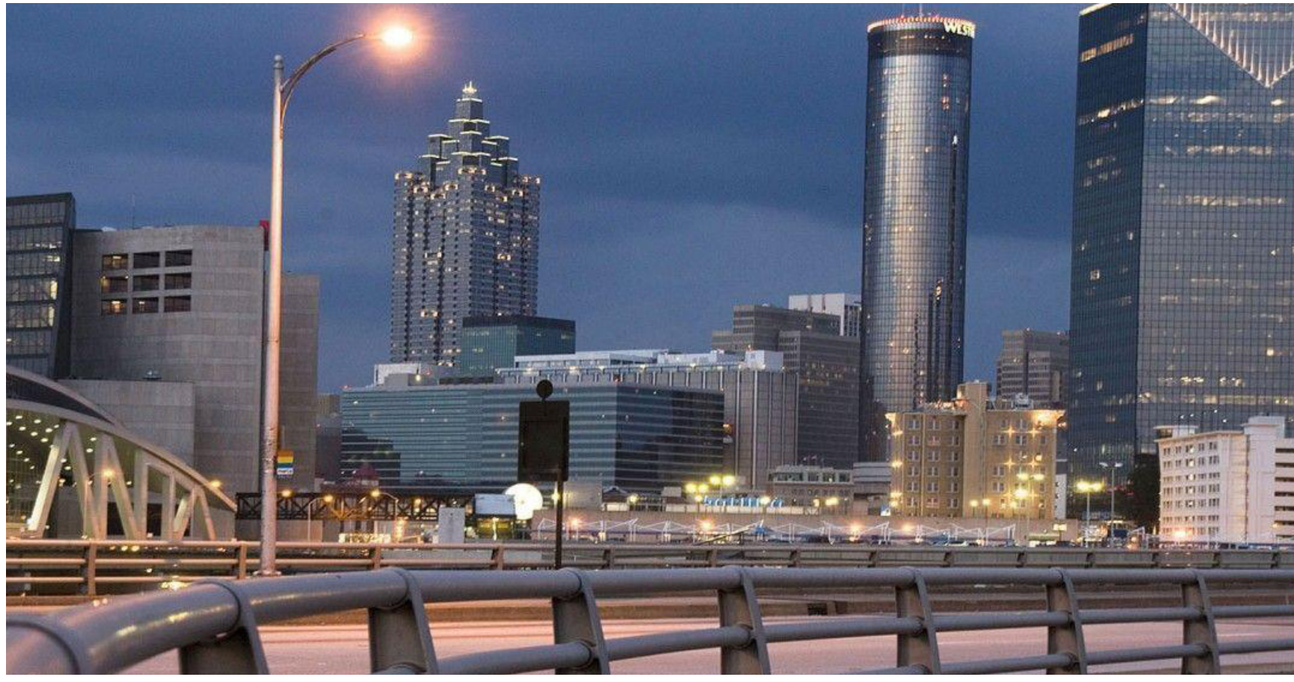
Tommy Morris, The University of Alabama in Huntsville

The UAH Cyber Force Incubator (CFI) is a cybersecurity workforce development program which recruits students from UAH, partner colleges and universities, and some Alabama high schools. CFI students are enrolled in an extracurricular cybersecurity and work place behaviors training program. Select students who pass the aforementioned training are nominated for security clearance. Students are hired to work on UAH cybersecurity research and development projects and students are placed into internships at government and industry partner locations.

What is Missing in Cybersecurity Curriculum?

Bo Yuan, Rochester Institute of Technology

In this fast-pitch presentation, we will argue that the cybersecurity curriculum should include fundamental knowledge units such as information theory, game theory, and war game stratagems.



Abstracts

CAE-CD Track Presentations

A Slice of Raspberry Pi Dessert for GenCyber Teachers

Loyce Pailen, University of Maryland Global Campus
Kimberly Mentzell

This submission will be a 15 minute overview of a post-GenCyber Teacher Camp activity that provided guidance to teachers for a focused Raspberry PI project for their high school students. The project included post-camp follow-on meetings for teachers to develop their skills and proficiency in using the Raspberry Pi to teach Linux concepts and cybersecurity tools.UMGC trained eight dedicated H.S. teachers who were committed to implementing the project in their schools. All teachers had varying successes and challenges.

We feel that discussing the project outcomes to the larger CAE community will support the success of similar endeavors and remove roadblocks teachers often encounter. This session is unique for a few reasons. First, this was a very focused post-camp activity. Also, the teachers involved had to implement the Raspberry Pi project despite it not being an established part of their curriculum for the academic year. The session will provide an overview of how we planned and managed the teacher training and tool support in a virtual environment. A brief review of the lesson plan will be discussed. The theme of Pi project for students included using Kali Linux; Linux intro / basic commands; Network basics with Wireshark; and Password cracking. Session attendees will receive the excellent Raspberry PI lesson plan developed by one of the teacher participants.

Building a Smart Secure Manufacturing Testbed Using Zero Trust Model, Machine Learning and 5G

Loyce Pailen, University of Maryland Global Campus
Kimberly Mentzell

Manufacturing is not only the backbone of U.S. military-technical advantage, but also a major contributor to the U.S. economy. A healthy, innovative, and vibrant manufacturing sector is essential to the economic strength and national security of the United States. The Industrial IoT, coupled with 5G, security in IIoT, machine learning, and artificial intelligence, is impacting the future and growth of manufacturing. In this presentation, we will discuss and live demo how we use the zero trust model, machine learning, and 5G to design and implement a secure smart manufacturing testbed in a lab environment. The further discussion also includes how we collaborate with the manufacturing outreach center to engage local manufacturers and show business use cases that smart factories can drive value.

*The project is funded by NCAE-C Cyber Curriculum and Research 2020 Program.

Colorado's Cybersecurity Educational Diversity Initiative (CEDI): Urban/Rural HSIs & the Wild West

Jeffrey London, MSU Denver
Steve Beaty

Funded by the NCAE-C Cybersecurity Education Diversity Initiative (CEDI), our presentation describes a two-year collaboration between a large urban Colorado HSI and a small rural Colorado HSI. The cybersecurity program at Colorado's newest CAE designated university, MSU Denver, is growing rapidly with a new Cyber Range. In addition, MSU Denver also offers BS and MS degrees in CYB and is quickly becoming an established cybersecurity program with the Mountain West region. The satellite institution of Trinidad State College is in a very remote part of Colorado, Alamosa Valley and is just now establishing a brand-new cybersecurity program, spearheaded by Serena "Sully" Sullivan. Unlike Denver, Alamosa Valley is sparsely populated. The CEDI HSI collaborative between these two schools is an excellent example of how 4YR universities can work shoulder to shoulder with 2YR colleges throughout the KU-CLO mapping process.

By teaming up Colorado's preeminent CAE mentor, Joe Murdock (University of Colorado-Denver), Nikolaus "Klaus" Streicher (MSU Denver's Senior Cyber Range Instructor), and Serena "Sully" Sullivan (Director of Technology at Trinidad State College), Drs. London and Beaty were able to demonstrate the efficacy of simultaneously employing three different perspectives (i.e., student experience, instructor experience, and mentor experience) or three different levels of analysis to successfully negotiate and align KUs to TSC-Alamosa Valley CLOs. Drs. London and Beaty conclude that developing a new cybersecurity college curriculum should not take place in isolation. While a cybersecurity instructor often establishes a new cybersecurity program with a CAE mentor, Drs. London and Beaty recommend that adding an experienced cyber undergraduate student to the team can result in "added value" to the KU-CLO mapping process.

The undergraduate cybersecurity student has a valuable experiential knowledge base (as a learner) that informs the mapping process from the inside out. Students can often help instructors and mentors by adding a "third" perspective to the alignment process. As an important aside, the TSC CLO's (used for alignment) were provided by Ms. Serena Sullivan. During the alignment process, an effort was made to reduce the total number of courses used to align with KUs. The intention is to mindfully create advantageous outcomes to be shared with other CEDI partner institutions. In doing so, the intention is to streamline the CAE application process for other participating CEDI institutions. As an additional note, the Colorado Community College System (CCCS) utilizes a shared "statewide" course numbering system (CNS). Due to the statewide shared CNS for all courses within Colorado's publicly funded community college system, specific TSC CLOs used for this alignment will also work for the entire Colorado Community College System. In other words, the alignment of TSC CLOs holds promise for scaling up to statewide alignment with nationally recognized KUs.

Abstracts

Computer Forensics Teaching Resources

Jeffrey Duffany, Polytechnic University of Puerto Rico
Alfredo Cruz

The Computer Forensics Teaching Resources Workshop is designed to share our experience teaching CECS 7235 Computer Forensics and CECS 7237 Advanced Computer Forensics to Computer Science graduate students at Politechnic University of Puerto Rico over the last decade. We will begin with a brief overview discussing the relationship between Computer Forensics and Cyber Defense and our Computer Forensics Graduate Certificate Program. We will then describe the teaching resources that we are using in our courses with an emphasis on hands-on laboratory experience. This will include textbooks (Nelson-Phillips), lab manuals (Blitz) and internet resources such as NIST CFTT, CFREDS, Digital Corpora, and the DFRWS (Digital Forensics Research WorkShop Conference). We will also discuss our experience with Computer Forensics Software tools such as ProDiscover, Forensics Toolkit, OSForensics and Autopsy. In addition we will discuss the philosophy we used to decide what material to include in the advanced course and how we deal with operating system compatibility issues (Windows vs. MAC OSX).

Cyber Sleuthing: An Introduction to Cybersecurity Using Gamification

Curtis Coleman, Oklahoma Christian University

This presentation will review the development of a week-course for high school students. The course is designed to introduce students to the exciting science of Cybersecurity using an experiential gamification approach to learning Computer Science, with an emphasis on application and teamwork. The course includes practice using current Cybersecurity industry tools and technologies, development of cyber detective skills, and academic team competition. The course is offered during the Honors Summer Academy on the Oklahoma Christian University campus. Students attend 50-minute lectures and labs for 5 days. The last day students apply their acquired cyber sleuthing knowledge and skills to escape from the Sherlock Holmes Escape Room.

Developing a “Hands On” Security Compliance Course

Joseph Jeansonne, Pitt Community College

The North Carolina Community College System’s Security Compliance course (SEC-258) introduces information security compliance and standards along with how they apply to corporate IT environments. Topics included in the catalog description of the course include ISO standards, government NIST frameworks, federal and state compliance requirements, security policies, incident response and business continuity planning. We have also added a CMMC module to the course. Unfortunately, many times the course content is dry and requires pure memorization. Join us, for this presentation to share and discover new ways to deliver a compliance course in a more “”hands-on”” format. In short, we intend to move students from remembering compliance regulations to understanding and applying security controls and governance.

Ensuring Consistency Across the Curriculum

Brandy Harris, Grand Canyon University

How do you ensure your CAE outcomes are consistently addressed from class section to class section? This workshop will provide some best practices to ensure student assessment and KU content is addressed in every section.

ERAU & A-ISAC CTF: Raising Awareness about Aviation Cybersecurity

Jesse Chiu, Embry-Riddle Aeronautical University - Prescott Campus
Krishna Sampigethaya

Aviation cybersecurity is an increasingly important problem for not only our nation but also the whole world. From vulnerabilities in avionics embedded system critical for flight operations in an aircraft to a wider network of international airports, cyber threats are more pervasive in aviation today. Airport and airlines face millions of cyberattack attempts annually and this trend will persist. A recent report from Europe in 2021, for example, shows cyberattacks on aviation increased by 530% in a year.

Embry-Riddle Aeronautical University—Prescott, AZ, is a NCAE-C leading aviation cybersecurity education and research. It is also a National Science Foundation (NSF) Scholarship for Service (SFS) institution for aviation and aerospace cybersecurity. The Aviation Information Sharing and Analysis Center (A-ISAC) is an international, non-profit organization that fosters information sharing and collaboration between different stakeholders in the community. They enable trusted sharing of vulnerabilities, threat intelligence, and best practices so that the aviation industry’s is better prepared to manage cyber risks and incidents.

In this presentation, we will talk about a recent collaboration between the NCAE-C at Embry-Riddle Aeronautical University—Prescott and the Aviation ISAC. The collaboration aimed at designing and developing an aviation-themed cybersecurity competition and offering the competition at DEF CON Aerospace Village and Aviation ISAC Annual Summit in 2020. The goal was to raise awareness both of aviation-specific challenges for the cybersecurity community and of cybersecurity issues to the aviation ecosystem, and foster talent in the subject areas.

This NCAE-C innovated and developed a novel aviation-themed Capture-The-Flag (CTF) competition. The story involved a group of hackers attacking and compromising a tier-1 airport with insider help, including ticketing kiosks, airline servers, flight information displays, transportation security, runway lights, aircraft, and more. The competition participants are the defenders, who are required to help regain control of compromised systems, prevent an aircraft from taking off, identify the insiders, and help bring normalcy back at the airport and its surrounding airspace. The CTF focused on knowledge, skills, and abilities in cybersecurity (e.g., password cracking, log analysis, computer forensics, and ethical hacking), intelligence (e.g., OSINT), and aviation (e.g., crew, avionics, air traffic control communications, airline operations, security screening, airport information systems, and aviation cyber-physical systems).

The presentation will overview the CTF project and discuss some challenges we faced in it. For example, following the pandemic outbreak, both DEF CON and Aviation ISAC Summit went into safe mode and all-virtual. The competitions were redeveloped and offered virtually, so that participants could register and participate in the competition from their remote locations. On the other hand, both competitions were free and open to anyone in the world. We had over 200 participants from many countries participate in our cyber competition. We will also talk about some of our future work in this area.

Abstracts

Honeypots and Knowledge Discovery in Teaching Network Defense

Ping Wang, Robert Morris University

This presentation shares a best practice in teaching network defense based on recent research on network security. Computer networks as part of critical infrastructure facilities and assets for most organizations are facing increasing challenges in defending against various and sophisticated cyber threats, intrusions, and attacks. Knowledge discovery is a key factor in cyber defense, and honeypots could be an effective tool for gaining knowledge for cyber defense. The research for this presentation draws upon a cyber defense knowledge model based on the classic of The Art of War and focuses on the use of honeypots for network intrusion detection. The cyber defense model highlights the role of knowledge (and the lack of knowledge) discovery of strengths and vulnerabilities of yourself and your opponent in cyber defense. This presentation illustrates the dynamics of the knowledge and its network security benefits using honeypots in a simulation of detection of intrusions and distributed denial of service (DDoS) attacks on a virtual network.

K12-University Cybersecurity Education Partnership Best Practices

Deveeshree Nayak, University of Washington

Cybersecurity Education for K-12 institutions and Universities across the USA is vital in the present time. In this presentation, I will be covering the best practices and approaches to enhance the partnership between K-12 institutions and Universities to enhance Cybersecurity education.

Long and Winding Road: Navigating to a Cybersecurity Performance Based Education (PBE) Curriculum

Norma Colunga-Hernandez, Texas State Technical College in Harlingen
Amy Hertel

While a Performance Based Education (PBE) conversion process was underway through an NSF grant at TSTC, the COVID-19 pandemic necessitated an accelerated and sharp turn in the Texas State Technical College hands-on technical model as courses were moved from an in-person to an online modality in the Cybersecurity program.

This brought multiple challenges and lessons learned including instructional content, access, hardware/equipment, software, and communication. This presentation will identify the challenges and solutions implemented for a successful PBE journey.

Making Knowledge Units Work for Your Program

Art Conklin, University of Houston
Seth Hamman

Knowledge Units are “owned” by the schools, yet schools do not take advantage of updating and modernizing them. This presentation will present how schools can update KU’s to have better alignment with their curriculum and improve the ecosystem for all. This presentation will include audience participation as a means of evangelism and outreach. The objective is to get more people involved in making the KU’s work for their program.

Mapping Low Cost and Open Source Labs to the NICE Workforce Framework

Chris Simpson, National University

In this presentation Chris Simpson will discuss National University’s mapping of low cost and open source labs to the NICE Workforce Framework and course learning outcomes using the online database Airtable. He will also provide updates on some new free and low cost lab environments that might be of interest to the CAE community.

Mapping of the NERC-CIP Standards with the NIST CSF

Guillermo Francia, University of West Florida

The Critical Infrastructure Protection (CIP) set of standards is developed by the North American Electric Reliability Corporation (NERC) to ensure the protection of assets used to operate North America’s Bulk Electric Systems (BES). Any entity that owns or operates any type of BES in the United States and Canada must be compliant with the requirements of the NERC-CIP Standards. This talk provides an overview of the NERC-CIP Standards to describe its relevance to the protection of one of our critical infrastructures: electric utility entities, to establish its harmonizing relation with the NIST Cyber Security Framework (NIST CSF), and to disseminate our workforce development program in this area of national need.

Abstracts

Meeting the Cybersecurity Workforce Challenge: One Goal, Innovative Solutions

Eman El-Sheikh, University of West Florida
Michael Tu

As the cyber threat landscape continues to evolve, the critical shortage of cybersecurity professionals continues to expand, particularly in Critical Infrastructure Sectors. This session will highlight three innovative cybersecurity workforce development programs, funded by the NCAE-C Program to address that challenge. An overarching goal is to support other CAE-C designated institutions in developing similar upskilling and reskilling training programs to complement their academic degree programs and multiply the pathways toward cybersecurity jobs. The presenters will offer a call to action to the CAE-C Community and discuss how other CAE-C institutions can leverage the programs' resources and platform to launch similar programs.

The National Cybersecurity Workforce Development Program is a nationally scalable program that focuses on recruiting, preparing, and placing over 1650 transitioning military, first responders, and veterans into cybersecurity roles across Critical Infrastructure Sectors. CyberSkills2Work is led by the University of West Florida and supported by a coalition of 10 NCAE-C designated institutions across the country, including CAE-CD, -R, -CO, 2Y, 4Y, and MSI institutions. The program offers 15 flexible training pathways that address 15 NICE Cybersecurity Framework work roles, help students develop hands-on skills via industry certifications, cutting-edge tools, and training courses, and document their competencies via digital badges and credentials. CyberSkills2Work includes a National Employers Network to connect students with employers and job opportunities, and a one-stop-shop web portal for students, employers, and institutions.

The University of Louisville-led Coalition (composed of 10 NCAE-C schools, including four HBCUs) Cybersecurity Workforce Development Program focuses on collaborating and leveraging resources and expertise to create cybersecurity curriculum addressing use cases in healthcare and logistics. The online asynchronous flexible cyber curriculum includes technology vendor credentials such as IBM, Microsoft, Google etc. matched with subject matter experts as well as participants partnered with success coaches networked within businesses. Three levels of progressive knowledge of cybersecurity (new/emerging cutting-edge technologies) are offered on topics, including blockchain, post quantum cryptography, artificial intelligence, and cognitive computing. A gaming app is available on the Google and App store free to anyone.

The CWCT, led by Purdue University Northwest and other three CAE institutions, has been launched to recruit and train over 1000 transitioning military, first responders, and other adult learners in the field of AI and Cybersecurity. Training participants have been engaged with educators and advisors at each phase of their CWCT journey including interest inspiration, pre-knowledge assessment, structured learning, certification preparation, career mentoring, and job placement. CWCT fully recognizes the importance of workforce preparation through online academic training and competency measurement through industry-government recognized certifications. CWCT goes one step further to develop a Job Placement Program through workshops on resume building and interview skill development, and more importantly, introducing job opportunities to training participants through virtual job fairs and other unique efforts.

Mininet as a Networking Tool for Simulating 4 Different Cyber Attacks: Experimental Results

George Meghabghab, Roane State

Software Defined Network (SDN) is a programmable network that separates the network data plane from the control plane. However, lots of security threats and issues are concerned in software defined network. In this work, in order to reasonably complete the cyber attack situation evaluation in the SDNs, we proposed a cyber attack situation evaluating method based on multi-dimensional features analysis in SDNs. Cyber attack detection features were considered and improved their computation methods about four typical cyber attacks in SDN. Correlations vectors between any two different cyber attack features using variety of measures was considered.
Mininet was used to establish our experiment environment, in which we simulated four typical cyber attacks to verify and analyze our method in the experiment.

Program of Study Validation: Cybersecurity Concentration at FDU

Ihab Darwish, Fairleigh Dickenson University

Fairleigh Dickinson University once again got designated as a National Center of Academic Excellence in Cyber Defense through the academic year 2026. During the process, NSA and a committee of academic peers has validated FDU's BSCS with Cybersecurity Concentration offered at FDU's Florham Campus through academic year 2026. At FDU, we have managed to achieve our goals after two years of extensive work on several Program of Study validation project activities involving planning, implementation and coordinating efforts that started in the year of 2019. The scope of the validation project consisted of four domains including program and curriculum enhancements, students' enrichment, faculty, and support, in addition to the continuous improvement's domain. Our success story in this program has been materialized in 2021 through securing four NSA Cybersecurity scholarships to our students. We shall continue to pursue continuous improvement and excel in the field of cybersecurity for the information security and safety of our nation. Hence, we are proposing to introduce our success story in obtaining this achievement and what has lead to reach our goals.

Furthermore, in April 2021, FDU was awarded the Expanding Access to Computer Science Education: Professional Learning Hubs grant from the NJ Department of Education to support the creation of a Computer Science Hub at FDU and to provide professional learning opportunities for New Jersey educators and to promote the growth of computer science. The services provided by the CS Hubs will help realize the strategic goals identified in the NJ Computer Science State Plan including Interactive Community Building to Support School Administrators, K-12 Teacher Professional Learning, Web Repository of Tools & Lesson Plans Accessible to All, and Culturally Responsive Teaching Practices.

Abstracts

Ransomware Incident Preparations with Ethical Considerations and Command System Framework Proposal

Stanley Mierzwa, Kean University

Concerns with cyber-attacks in the form of ransomware are on the mind of many executives and leadership staff in all industries. Inaction is not an option, and approaching the topic with real, honest, and hard discussions will be valuable ahead of such a possible devastating experience. This research note aims to bring thoughtfulness to the topics of ethics in the role of cybersecurity when dealing with ransomware events. Additionally, a proposed set of non-technical recovery preparation tasks are outlined to help organizations bring about cohesiveness and planning for dealing with the real potential of a ransomware event. Constraints from many factors come into focus during preparations for ransomware, and a method to categorize them is detailed. Finally, the use of Incident Command Systems is well known and documented in emergency management, and a proposed model for integrating this process for ransomware episodes is sketched.

RMF vs CSF: Which is Better for Higher Ed?

Matt Paulson, Weber State University

This is a presentation of research completed to compare higher education information security policies to the NIST risk management framework. A surprising event occurred when it was found that the higher ed institutions were using the NIST cybersecurity framework instead, which incorporates parts of the RMF. This workshop presents the results of this research along with a discussion.

Stepping-Stone Intrusion Detection using Crossover Packets

Lixin Wang, Columbus State University

Stepping-stone intrusion is a hacking strategy in which an attacker sends attacking commands through compromised hosts, called stepping-stones, in order to remotely access a target host. These stepping-stones form part of a connection chain that serves as an intermediary between the target and attacker hosts, providing the attacker with increased anonymity and detection avoidance capabilities. It is well-known that a long connection chain with three or more connections often indicates malicious activities. In a long connection chain, it is possible for the sender to transmit the next request packet before the sender receives the response for the previous request. In such a case, some request and response packets may cross each other somewhere along the chain, producing packet crossover. In prior work, it was demonstrated that the number of crossover packets in a given data stream should be proportional to the length of a connection chain. In this work, we develop an innovative detection method for stepping-stone intrusion based on crossover packets, referred to as Crossover-Packet Detection. Our network experiments demonstrate that our proposed Crossover-Packet detection method is resilient to hackers' session manipulation such as chaff perturbation or time jittering.

The Applications of Internet of Things in the Medical Field

Lixin Wang, Columbus State University

The Internet of Things (IoT) paradigm promises to make "things" include a more generic set of entities such as smart devices, sensors, human beings, and any other IoT objects to be accessible at any time and anywhere. IoT allows for the interconnectivity of devices or objects to collect, send, and receive information. IoT varies widely in its applications, but one of its most beneficial uses is in the medical field. Healthcare utilizes IoT and its emerging technologies to provide more efficient and quality care for patients while reducing the workload and burden on healthcare facilities. IoT provides a mainstream method for healthcare professionals to analyze patient data in real-time and make informed decisions regarding patient care. However, the large attack surface and vulnerabilities of IoT systems needs to be secured and protected.

This work investigates various applications of IoT in healthcare and focuses on the security aspects of the two internet of medical things (IoMT) devices: the LifeWatch Mobile Cardiac Telemetry 3 Lead (MCT3L), and the remote patient monitoring system of the telehealth provider Vivify Health, as well as their implementations. Our research explores the security issues with these IoMT devices and proposes efficient solutions to better protect them. Security is a requirement for IoT systems in the medical field where the Health Insurance Portability and Accountability Act (HIPAA) applies. While there is a risk that sensitive and protected health information may be compromised in the use of IoT systems, effective implementation of robust security measures and risk mitigation techniques can ensure that IoT can be an invaluable system of technologies that enhances the quality and efficiency of patient care.

The Lack of Incident Response Curriculum in the CAE Community: Call to Action

Casey O'Brien, University of Illinois Urbana-Champaign
David Umphress

In September 2020, the Critical Infrastructure Resilience Institute (CIRI) - a DHS Science & Technology (S&T) Center of Excellence at the University of Illinois Urbana-Champaign - led a Cybersecurity and Infrastructure Security Agency (CISA)-funded project and team of academic partners (Auburn University, Purdue University, University of Tulsa) in the creation of a comprehensive plan to develop a nationwide cybersecurity education and training hub & spoke network to address the nation's chronic and urgent cybersecurity workforce shortage. The envisioned national network will develop and deliver Incident Response (IR) and Industrial Control Systems (ICS) curricula conformant with the NIST National Initiative for Cybersecurity Education (NICE) Framework.

This presentation discusses the research findings from this project related to the current state of IR curriculum (degrees, certificates, technical courses) in the CAE community and makes the case for an increase in the number of CAE schools focusing on this critical area.

Abstracts

CAE-CD Panel Presentation

The “Power of Six”: Creating Cyber Experiences and Building a Diverse Talent Workforce Pathway

Sharon Hamilton, Norwich University
Colonel Linda Riedel, Citadel DoD Cyber Institute
Dr. Bryson Payne, University of North Georgia

In 2017, six universities (five NCAE-C and one candidate) joined together (“Power of 6”) to establish a pilot program to demonstrate their ability to develop cybersecurity talent pathways for women and underrepresented students for civilian and military positions in the Department of Defense (DoD). Norwich University, University of North Georgia, The Citadel, Texas A&M, Virginia Tech, and Virginia Military Institute share a common identity as senior military colleges but had never previously teamed to create and fund academic, experiential, and research opportunities for cybersecurity students.

In 2018, the “Power of 6” built bipartisan Federal support of Senators and Congresspersons to insert language in the 2019 National Defense Authorization Act to establish DoD Cyber Institutes. In 2019, the “Power of Six” gained federal appropriations support to fund this pilot effort to help fill the cybersecurity workforce gap. Using a common framework, the Cyber Leader Development Program, the “Power of Six” successfully completed their first pilot program year and are fully engaged in Phase II!

Panel focus: Now in Phase II (2022-2024), the DoD Cyber Institute team is excited to share their pilot program insights on outreach activities, collaboration with government and military organizations, student professional development and experiential opportunities, and strategies for other NCAE-Cs to develop similar cybersecurity opportunities for students and faculty.

The panel moderator, Dr. Sharon Hamilton, Colonel (Retired, US Army), Norwich University, has led the “Power of 6” team since its inception in 2017 and is the Principal Investigator and Program Director for this initiative and grant.

Panel members will consist of Dr. Hamilton and two cybersecurity leaders from NCAE-C universities partnered in this pilot program.
- Dr. Bryson Payne, University of North Georgia, Professor, Cybersecurity
- Colonel (SC Army National Guard) Linda Riedel, Citadel DoD Cyber Institute (CDCI) Deputy Director, Operations and Outreach

CAE-R Workshop

Transformational Research in Usable Security

Heather Lipford, UNC Charlotte
Cori Faklaris, Carnegie Mellon

This workshop will bring together usable-security researchers at CAE-R institutions to discuss transformational ideas for addressing the nation’s cybersecurity challenges. The outcomes of the workshop will be an agenda for an integrated approach in usable security that will involve (1) gathering data on problems and solutions for uptake of end-user security practices (such as quickly installing software updates, creating unique passwords, and staying alert for scams, phishing, and misinformation), then (2) bringing this research back to the next generation of cyber students.

The need for a human-centered perspective to inform better tools, better designs, and improved educational approaches is clear. Proofpoint has cited human interaction as a factor in more than 99 percent of cyberattacks (2021). Yet, existing cybersecurity approaches do not necessarily monitor for such critical interactions, such as when carelessness or negligence leads to a security breach (Greitzer et al. 2014). The failure to address such carelessness can have severe downstream effects. However, the use of basic end-user tools has been shown to help forestall network intrusions and catch cyberattacks in progress. These issues can be solved by people adopting and following certain security practices such as staying alert for and reporting phishing; implementing and using strong, multi-factor authentication protocols; quickly installing needed software updates; and following basic security practices for their phones, laptops, and other hardware. Usable security researchers provide critical understanding of the security behaviors people do and do not adopt, to improve technology designs and education. The fact that too many people do not do these simple things is evidence that we need to do better at bridging the gap between applied research and education and examine approaches to encourage more adoption by end users and by systems administrators.

We aim to identify a range of cybersecurity challenges that could be addressed through usable security methods. Thus, this workshop has the goal of accomplishing an integrated research agenda for usable security in the next five years. Example questions this will address are:
- What is the overall picture of needed research? What are the pressing issues now that were not present previously?
- What are the touchpoints between this research and education, and what types of education? How do these line up with what a lot of agencies and places are already funding and requiring, and how do we marry these together?
- How do we bring usability researchers together with technical researchers?

Abstracts

Technical Director Panel Presentation

Panel of Technical Directors for the INSuRE Program

Session Chair: Susanne Wetzel
Timothy Davison, Johns Hopkins University Applied Physics Laboratory
Roland Varriale, Argonne National Laboratory
Edward Zieglar, National Security Agency

Currently, the INSuRE program is one of the main efforts of the Community of Practice in Research (CoP-R). As part of this panel, Technical Directors from four different government agencies and national laboratories will share information on their backgrounds, research interests, as well as their involvement and experience with the INSuRE program. A major focus of the panel is for the Technical Directors to not only discuss the benefits of the INSuRE program to the three stakeholders of the program (i.e., students, academic institutions, and to the government - represented by the agencies and labs) but also address the challenges that may arise as students, faculty, and Technical Directors jointly carry out the various projects.

INSuRE+C Presentations

Towards a Rigorous Approach for Zero Trust in the 5G Core

Norbert Ludant, Northeastern University
Guevara Noubir, Northeastern University
Marinos Vomas, Northeastern University

By combining technologies such as Network Function Virtualization and Service-Based Architecture with decentralized and cloud deployments, the fifth generation of cellular networks (5G) aims for unprecedented Quality of Service, and use-cases in smart industry, emergency operations, remote medicine, and more. The increased attack surface introduced by this transition as well as the critical nature of the 5G communications require, more than ever before, a rigorous analysis of 5G security. In this talk, we analyze the security implications introduced in the 5G Core, and the existing security solutions proposed in the 5G standard. We explore the model of Zero Trust Architecture (ZTA) and we discuss how it is supported by the 5G Core standard. With Virtualization and Cloud deployment being significant factors in the increase of the attack surface, we expand ZTA principles to include the software and hardware of the deployment stack. We leverage Trusted Execution Environments (TEEs) to ensure confidential computing on untrusted deployments and our analysis shows how our proposed model handles the increased attack surface and reinforces the ZTA principles in the 5G Core, without any changes to the 5G standard. Finally, we provide experimental results that demonstrate the overhead incurred by our model in terms of performance and monetary cost.

Path-Aware Risk Scores for Access Control in Zero-Trust Systems

Philip Brown, University of Colorado, Colorado Springs

The growing adoption of zero-trust architectures brings the principle of complete mediation to the forefront of well-designed, secure systems. Despite the potential for zero-trust to improve the security and resilience of systems from cyberattack, practical adoption of these architectures is hindered by lack of sufficiently trustworthy origin authentication within untrusted networks such as the Internet. Notably, problems with authentication exist due to stolen credentials and mobile clients used by remote workers that are easier for threats to compromise than traditional workstations hiding behind boundary firewalls. The result is that access control for the protection of critical assets increasingly depends not just on user authentication but also on context-sensitive techniques, e.g., behavior and location, to monitor and isolate such threats.

In this talk, we introduce path-aware risk scores for access control (PARSAC), a novel context-sensitive technique to enrich access requests with risk scoring of the path taken by those requests between the authenticated user and the resources they access. These path-aware risk scores enable another layer of security for traditional access control systems that addresses the need for fine-grained monitoring and enforcement within a zero-trust architecture. We define rules for general functions that can be used to determine risk and instantiate a specific approach to calculate path risk scores. We have evaluated our approach with realistic network graphs and discovered that PARSAC finds more paths with lower risk when compared with traditional routing algorithms that select the shortest path.

Exploration of Heuristic and Probabilistic Tools in Quantum Computing with Applications to Cryptography

Hugo Delgado, Polytechnic University of Puerto Rico

Recent advances in the development of quantum computing hardware have accelerated the interest of preparing information systems for the post-quantum world. Grover's unstructured search and Shor algorithm for period-finding have potential applications in security, cryptography, and communications in general. We present in this paper the evaluation and simulation of proofs of concepts, gates, and experiments for quantum circuits along with explanations of their potential applications to computing and security. The circuits explore several aspects of quantum computers such as superposition, parallel calculations, amplitude amplification and phase estimation. These circuits and gates were also tested on real quantum computers to assess their behavior.

Abstracts

CanarySat: A Virtual CubeSat Model for Cybersecurity Research and Education

David Coe, Aleksandar Milenkovic, Jeffrey Kulick and Letha Etzkorn, The University of Alabama in Huntsville

Presented here is an overview of CanarySat, which is an open, virtual model of a cube satellite (CubeSat) and a satellite ground station. The goal of this project was to produce a high-fidelity, extensible modeling framework that will allow cybersecurity researchers and satellite designers to investigate cybersecurity solutions targeted specifically at CubeSats and other small satellite platforms. Unlike the typical desktop and server computer systems, space-based systems have significant limitations in terms of their computational resources, the available energy resources, and communication bandwidth. CanarySat facilitates evaluation of competing cybersecurity solutions based upon the effectiveness of the technique, the computational overhead, and the energy consumption.

To guide development of CanarySat, we have acquired the ISISpace CubeSat Development Platform, which is a flight-proven, cost-effective system which serves as the engineering model for training, development, and testing. Prior to selection of this cubesat platform, we performed a trade study which examined and compared the available commercial-off-the-shelf cubesat and ground station systems. The platform we selected includes the actual flight computer, electrical power system, communications system, and attitude control system as well as the ground station.

Our student researchers have constructed both a Satellite Power Scheduling Application and the baseline CanarySat model. The Satellite Power Scheduling Application is an application that allows satellite designers to estimate the energy requirements of their missions and explore trade-offs between performance and power consumption for different on-board computer systems. The application includes a database of performance and power consumption data that was collected via a sequence of experiments performed on representative single-board computers (SBCs).

The baseline CanarySat model includes an orbital physics model built within Simulink and the open-source COSMOS command and control software which serves as the satellite ground station. The orbital physics model is deployed on a representative single board computer, and the COSMOS ground station software executes on a desktop or laptop computer. Our student team demonstrated the ability to issue commands from the ground station and view the satellite attitude changing in the Simulink model. The students have also demonstrated successful operation of an image processing workload to simulate an earth observation mission.

We are currently engaged in the development of proof-of-concept cyberattacks against the CanarySat model to demonstrate the utility of CanarySat for cybersecurity research.

Juicing V8: A Primary Account for the Memory Forensics of the V8 JavaScript Engine

Ibrahim Baggili, Samuel Bergami, and Enoch Wang, Connecticut Institute of Technology

V8 is the open source interpreter developed by Google to enable JavaScript (JS) functionality in Chrome and power other software. Malicious threat actors abuse the usage of JS because most modern-day browsers implicitly trust script code to execute. To aid in incident response and memory forensics in such scenarios, our work introduces the first generalizable account of the memory forensics of the V8 JS engine and provides practitioners with a list of objects and their descriptors extracted from a memory image. These objects can be used to reveal key information about a user and their activity. We analyzed the V8 engine and its garbage collection process. We then developed and validated a Volatility plugin – V8MapScan – to reconstruct V8 objects from a memory image. The runtime of the V8 engine is housed within the V8 isolate which contains its own heap manager and garbage collector. Within the heap of the isolate exists a root object map known as the MetaMap. By using the MetaMap and a object-fitting technique, we were able to extract objects, object-maps, and object properties. The V8MapScan plugin scans process memory for the MetaMap data structure contained within the V8 isolate using its data structure, references to objects can be found and extracted. Our findings were verified with Chrome DevTool's Heap Profiler. Our approach recovered the majority of objects indicated by the heap profiler with common types such as the ONE BYTE INTERNALIZED STR type returning more than 98.9%. Lastly, we provide a case study using our tools on the Monero Cryptocurrency Miner. This material is primarily based upon work supported by National Security Agency (NSA) and Department of Defense (DoD) under grant H98230-20-1-032.

CAE-C Community Leads

Northeast

Hub Lead: Blair Taylor (btaylor@towson.edu)
Hub Lead: Sidd Kaza (SKaza@towson.edu)
Hub Lead: Jake Mihevc (JMihevc@mvcc.edu)
Hub Lead: William Butler (whbutler@captechu.edu)

Northwest

Hub Lead: Gretchen Bliss (gbliss@uccs.edu)
Hub Lead: Gurvinder Tejay (gtejay@uccs.edu)

Midwest

Hub Lead: John Sands (sands@morainevalley.edu)
Hub Lead: Stanley Kotska (kostkas@morainevalley.edu)

Southwest

Hub Lead: Kim Muschalek (kmuschalek@alamo.edu)
Hub Lead: Glenn Dietrich (Glenn.Dietrich@utsa.edu)

South East

Hub Lead: Eman El-Sheikh (eelsheikh@uwf.edu)
Hub Lead: Anthony Pinto (apinto@uwf.edu)

CAE-CD

CoP Lead: Yair Levy (levvy@nova.edu)
CoP Lead: Anne Kohnke (kohnkean@udmercy.edu)

CAE-CO

CoP Lead: Seth Hamman (shamman@cedarville.edu)
CoP Lead: Drew Hamilton (hamilton@exchange.tamu.edu)

CAE-R

CoP Lead: Agnes Chan (ahchan@ccs.neu.edu)
CoP Lead: Susanne Wetzel (swetzel@stevens.edu)

To learn more about the CAE in Cybersecurity Community, visit caecommunity.org

Thank you for attending the 2022 CAE in Cybersecurity Community Symposium! All materials from the symposium will be available to view on the CAE in Cybersecurity Community website at caecommunity.org. If you have any questions, comments, or concerns, please contact us at info@caecommunity.org