NCAE-C Cybersecurity Annual Report Format

DoD and NSA requires colleges and universities participating in the NCAE-C Grant Programs to submit an annual report that explains their use of funds.

In addition to the technical reporting requirements listed in the official grant paperwork, grant recipients will be required to submit this report within 60 days of the grant completion. The report format is found below:

FORMAT: Please use the template below.

- Any items in blue should be filled in by the grant recipient.
- There is no page limit for the report
- CVs / Resumes should not be included
- Font – standard / readable 10 or 12 pt.
- **Please be as specific as possible in your reporting.**
- Attachments may be included

SUBMISSION: Final reports should be emailed to aeshaff@nsa.gov

Failure to submit the final report will result in point deductions for any future NCAE-C, DoD CySP, GenCyber, and/or STARTALK Grant opportunities.

UNIVERSITY OF MEMPHIS

NCAE-C in Cybersecurity Education Innovation
NCAE-C-001-2021

Grant No. H98230-21-1-0319

Second Year Report

DECEMBER 31, 2023

Grant Grand Total: **$1,014,075.66**

Project Director/Principal Investigator:

Name: Dr. Dipankar Dasgupta
Email: ddasgupt@memphis.edu
Title: Professor, Computer Science
Phone Number: 901-678-4147

Co-Project Director/Principal Investigator:

Name: Dr. Myounggyu Won
Email: mwon@memphis.edu
Title: Assistant Professor, Computer Science
Phone Number: 901-678-2792

Name: Dr. Mohd Hasan Ali
Email: mhali@memphis.edu
Title: Associate Professor, Electrical and Computer Engineering
Phone Number: 901-678-2225

University Information:

Address: Center for Information Assurance

Address: Dunn Hall – Rm 209

City: Memphis
State: Tennessee
Zip Code: 38152
Phone Number: 901-678-4271
Fax Number:

University Office of Sponsored Programs / Financial Management

University POC: Dr. Bill Hardgrave

Title: President

Address: Office of the President

Address:

City: Memphis State: Tennessee Zip Code: 38152

Phone Number: 901-678-2234 Fax Number:

PI Certification and Acceptance: I certify that the statements herein are true, complete and accurate to the best of my knowledge. I am aware that any false, fictitious, or fraudulent statement or claim made by me may be subject to criminal, civil, or administrative penalties.

Signature of Principal Investigator: _____ Date: _____

Sponsor and Sponsoring Institution Certification and Acceptance: I certify that the statements herein are true, complete, and accurate to the best of my knowledge. I am aware that any false, fictitious, or fraudulent statement or claim made by me may be subject to criminal, civil, or administrative penalties.

Signature of Sponsor Named: _____ Date: _____

1. Overview:

This report documents the activities and results of the **UNIVERSITY OF MEMPHIS** NCAE-C in Cybersecurity Education Innovation (NCAE-C-001-2021). In particular, the report provides information about project: ***CYBERSECURITY EDUCATION FOR CRITICAL INFRASTRUCTURE PROTECTION***.

2. Executive Summary:

All critical infrastructures are becoming tightly coupled with cyber-enabled systems and services. However, the degree of knowledge required to protect these may vary according to industrial sectors. Our mission is to prepare the current and next generation of professionals on complex cyberattacks on industry-specific critical infrastructures and how to identify and handle emerging threats. We propose to develop a comprehensive sector-specific cybersecurity program with a regional NCAE-C Coalition to better prepare for incident response and recovery in crisis. The overall project goal is to design and develop a multi-disciplinary critical infrastructure cybersecurity program to address the technical needs of NCAE-C students (future workforce), state and local government, and industry partners in energy, water and wastewater systems, and related Critical Infrastructure Sectors (https://www.cisa.gov/critical-infrastructure-sectors). More specifically, the project objectives include:

1. Design and develop an education and outreach program to enhance cybersecurity expertise for critical infrastructure security professionals in state and local government and industry, with an emphasis on energy, water and wastewater systems, and related CI sectors across the NCAE-C Southeast Region.
2. Develop and deliver competency-based training courses and workshops to upskill and reskill professionals in those organizations that leverage the expertise of the NCAE-C Coalition to provide fundamental knowledge, skills and competencies to critical infrastructures across different industrial applications.
3. Provide educational experiences for NCAE-C students to enhance their expertise and future support of CI security through (a) specialized courses and seminars offered at NCAE-C Coalition institutions, (b) internships to support the proposed cybersecurity consultation and services for the region's government and industry critical infrastructure partners, and (c) opportunities to network with the region's critical infrastructure partners to expand workforce development pathways.

The successful outcome of this project will create a strong southeast regional coalition, leveraging the NCAE's expertise in cybersecurity in assisting local and state governments and critical infrastructure partners in the region and the nation. Moreover, this cybersecurity community development project will design activities to be continued with supports from our industry partners beyond the project period as outlined in the proposal.

3. Accomplishments: (You may include images, tables, charts, and/or other graphics in support of the accomplishments)

a. What are the major goals of the project?

The major goals of the project are to enhance cybersecurity expertise in critical infrastructure security, provide upskill and reskill opportunities for current cybersecurity professionals, and provide educational experience opportunities for NCAE-C student and future professionals.

b. What was accomplished under these goals (you must provide information for at least one of the 4 categories below)?

- **Major Activities:**
  a. Faculty team members are incorporating CECIP training module concepts in their Fall 2022 classes where appropriate.
  b. Smart Grid Security Workshop was held at the University of Memphis on March 25, 2022.
  c. Cybersecurity for Critical Infrastructure Workshop was held at the University of Memphis on April 1, 2022.
  d. Five Workforce Development courses were implemented:
     a. ICS-RE Security (at UWF) was conducted May 16-27, 2022.
     b. Cybersecurity Maturity Model Certification (CMMC at UWF) was conducted June 13-24, 2022.
     c. NERC-CIP Standards and Compliance (at UWF) was conducted August 1-12, 2022.
     d. ICS-RE Threat Intelligence (at UWF) was conducted August 22-26, 2022.
     e. ICS-RE Security (at UWF) was conducted October 22 – November 6, 2022.
  e. Hybrid IoT Security Workshop was held at North Carolina A&T State University on September 23, 2022. The University of Memphis helped co-host the event.
  f. Cybersecurity Resilient EV Charging Station & Critical Infrastructure Workshop was held at the University of Memphis in conjunction with the Electrical/Computer Engineering Department on August 25, 2023.
  g. Cybersecurity Education for Critical Infrastructure Protection Workshop was held at Citadel College on October 19-20, 2023.
  h. A Virtual Workshop on AI Enhanced IoT Security was held at North Carolina A&T State University on October 27, 2023.

- **Specific Objectives:**

  1. Design and develop an education and outreach program to enhance cybersecurity expertise for critical infrastructure security professionals in state and local government and industry, with an emphasis on energy, water and wastewater systems, and related CI sectors across the NCAE-C Southeast Region.

  2. Develop and deliver competency-based training courses and workshops to upskill and reskill professionals in those organizations that leverage the expertise of the NCAE-C Coalition to provide fundamental knowledge, skills, and competencies to critical infrastructures across different industrial applications.

  3. Provide educational experiences for NCAE-C students to enhance their expertise and future support of CI security through (a) specialized courses and seminars offered at NCAE-C Coalition institutions, (b) internships to support the proposed cybersecurity consultation and services for the region's government and industry critical infrastructure partners, and (c) opportunities to network with the region's critical infrastructure partners to expand workforce development pathways.

- **Significant Results:**
    a. Smart Grid Security Workshop was held at the University of Memphis on March 25, 2022.
    b. Cybersecurity for Critical Infrastructure Workshop was held at the University of Memphis on April 1, 2022.
    c. Five Workforce Development courses were offered via UWF/IRCC:
        a. ICS-RE Security (at UWF) was conducted May 16-27, 2022.
        b. Cybersecurity Maturity Model Certification (CMMC at UWF) was conducted June 13-24, 2022.
        c. NERC-CIP Standards and Compliance (at UWF) was conducted August 1-12, 2022.
        d. ICS-RE Threat Intelligence (at UWF) was conducted August 22-26, 2022.
        e. ICS-RE Security (at UWF) was conducted October 22 – November 6, 2022.
    d. Hybrid IoT Security Workshop was held at North Carolina A&T State University on September 23, 2022. The University of Memphis helped co-host the event.
    e. Cybersecurity Resilient EV Charging Station & Critical Infrastructure Workshop was held at the University of Memphis in conjunction with the Electrical/Computer Engineering Department on August 25, 2023.
    f. Cybersecurity Education for Critical Infrastructure Protection Workshop was held at Citadel College on October 19-20, 2023.
    g. A Virtual Workshop on AI Enhanced IoT Security was held at North Carolina A&T State University on October 27, 2023.

- **Key outcomes or other achievements:**
    1. Faculty team members have incorporated CECIP training modules into some of their classes.

c. What opportunities for training and professional development has the project provided?

- Smart Grid Security Workshop was held at the University of Memphis on March 25, 2022.
- Cybersecurity for Critical Infrastructure Workshop was held at the University of Memphis on April 1, 2022.
- The University of West Florida implemented five workforce development courses for veterans, first responders, professional, and adult-learners.
- Hybrid IoT Security Workshop was held at North Carolina A&T State University on September 23, 2022. The University of Memphis helped co-host the event.
- Cybersecurity Resilient EV Charging Station & Critical Infrastructure Workshop was held at the University of Memphis in conjunction with the Electrical/Computer Engineering Department on August 25, 2023.
- Cybersecurity Education for Critical Infrastructure Protection Workshop was held at Citadel College on October 19-20, 2023.
- A Virtual Workshop on AI Enhanced IoT Security was held at North Carolina A&T State University on October 27, 2023.

d. What student opportunities has the project provided?

- University of Memphis students were employed as research assistants and helped develop some of the IoT project demonstrations. A video recording of their project was presented during the Hybrid IoT Security Workshop by Dr. Myounggyu Won.

e. What outreach opportunities has the project provided?

- Invitations were sent to members of the professional community (i.e., including veterans, first responders, adult learners, and students) to gain training in IoT Security and cyber defense workforce development raining. Additionally, the five Workforce Development courses (i.e., ICS-RE Security, CMMC, NERC-CIP Standards & Compliance, and ICS-RE Threat Intelligence) hosted by UWF emphasized the recruitment of transition military personnel, transitioning first responders, and other qualified adult learners.

f. What diversity opportunities has the project provided?

- Minority and female faculty, staff, and students have been engaged in the project.

g. How have the results been disseminated to communities of interest?
The proposed workshops were be advertised through website postings, university newsletters, the CAE community, radio and television broadcasts, the dissemination of opportunities at professional meetings, and the use of other social media avenues.

4. Products: Please list any products produced as a result of your project. These may include but are not limited to: *Journals, books, book chapters, thesis/dissertations, conference papers/presentations, other publications, technologies or techniques, patents, inventions, licenses, websites, or other products. Please be specific.*

a. Certificate-based Workforce Development Courses
The implementation of four courses related to the protection of our critical infrastructures. These courses are Industrial Control Systems and Renewable Energy (ICS-RE) Security, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) Compliance, Cybersecurity Maturity model Certification (CMMC) Compliance, and ICS-RE Threat Intelligence. The courses provided verifiable digital credentials for the specific cybersecurity work roles in critical infrastructures with emphasis on transitioning military personnel, transitioning first responders and other qualified adult learners. A fifth course was also implemented that was designed for faculty development.

b. Explainable AI-based Intrusion Detection Systems for Cloud and IoT: North Carolina A&T State University master's student had her paper entitled "Explainable AI-based Intrusion Detection Systems for Cloud and IoT" accepted for publication into the workshop program for The 2nd IEEE International Workshop on IoT in Emerging Fields at the ICCCN 2023. The paper was presented in July 2023 in Hawaii.

c. Zero Trust Architectures: A Comprehensive Analysis and Implementation Guide: University of Memphis graduate student (e.g., Nathan Seymour) master's thesis submitted for approval entitled "Zero Trust Architectures: A Comprehensive Analysis and Implementation Guide."

5. **Participants:** There are no limits on the number of participants you list for this section; however, you must list participants who have worked one-half person month or more for the project reporting period.

   a. **What individuals have worked on the project?**
   The successful outcome of this project is predicated upon the creation of a strong southeast regional coalition, leveraging the NCAE's expertise in cybersecurity in assisting local and state governments and critical infrastructure partners in the region and the nation. As such, the following individuals have been actively engaged in the development of workshop, classroom course, and technical materials associated with cybersecurity:

   Dr. Dipankar Dasgupta (University of Memphis – Professor of Computer Science), Dr. Shankar Banik (Citadel College – Professor and Head of the Department of Cyber & Computer Science), Dr. Guillermo Francia (University of West Florida – Professor and Faculty Scholar at the Center for Cybersecurity), Dr. Kaushik Roy (North Carolina A&T State University – Associate Professor of Computer Science), Dr. Myounggyu Won (University of Memphis - Assistant Professor of Computer Science), Dr. Mohd Hasan Ali (University of Memphis – Associate Professor of Electrical & Computer Engineering), Dr. Eman El-Sheikh (University of West Florida – Associate Vice President and Professor of Computer Science), Dr. Kevin Cooper (Indian River State College), Dr. Tarek Youssef (University of West Florida - Associate Professor), Guy Garret (University of West Florida – Instructor), Anthony Pinto (University of West Florida - Instructor), Steven Nicholson (Indian River State Colle – Instructor), Dr. Kelvin Bryant (North Carolina A&T State University – Associate Professor of Computer Science), Dr. Xiaohong (Dorothy) Yuan (North Carolina A&T State University – Professor and Chair of the Computer Science Department), Dr. Cory Nance (Citadel College – Assistance Professor of Cyber & Computer Science), Dr. Melissa Graves (Citadel College – Assistant Professor of Intelligence & Security Studies), Nathan Seymour (University of Memphis – Graduate Student), Cody Seymour (University of Memphis – Undergraduate Student), Nathan Farrar (University of Memphis – Graduate Student), Luke Carrington (University of Memphis – Undergraduate Student), Douglass Espinoza (University of Memphis – Undergraduate Student), Adam Thieme (University of Memphis – Undergraduate Student), Hans Siegfried Amelang (University of Memphis – Undergraduate Student), Allison Plank (University of Memphis – Undergraduate Student), Tiffany Geistkemper (University of Memphis – Graduate Student), Arturo Perez ((University of Memphis – Undergraduate Student), Doris Allen (University of Memphis – Staff Member), Debera Pittman (University of Memphis – Staff Member), Tony Pinson (University of Memphis – Project Coordinator),, Bianca Govan (NC A&T State University – Program Manager), Malory H. Saunders-Gooding (Citadel College – Project Coordinator)

   b. **What other organizations have been involved as partners?** None
      - Type of Partner Organization
      - Name
      - Location
      - Partner's contribution to the project

c. **Have other collaborators or contacts been involved? Yes or No. If yes, please elaborate.** Yes. Dr. Andrew Neel served as an "Internal Reviewer/Subject Matter Expert" for the Smart Grid Security and Zero Trust Architecture Clark Library modules.

6. Impacts:

a. **What is the impact on the development of the principal discipline(s) of the project?** Critical infrastructure cyber protection topics are being incorporated into the classroom instruction.

b. **What is the impact on other disciplines?**
The primary project objective is to raise awareness of the need to implement better practices associated with cybersecurity for the various sectors of critical infrastructure. According to CISA, there are 16 critical infrastructure sectors. These sectors include the chemical, communications, defense, emergency services, financial, food, energy, and healthcare among others. Consequently, critical infrastructure protection requires a wide variety of disciplines to incorporate sound cybersecurity principles in their design and technology.

c. **What is the impact on technology transfer?**
According to CISA, the 16 critical infrastructure sectors include a wide variety of industries. As more industries shift to more cyber-physical integrated systems, designers in all these industries will be required to implement control systems that can complete complex task while being resilient enough to withstand the bad intentions of varying threat actors.

d. **What is the impact on society beyond science and technology?**
The Cybersecurity of critical infrastructure is perhaps one of the most challenging issues facing governments and society today. Governments must find more effective procedures and methods of insuring individual/commercial data security and information privacy, combating misinformation, uprooting algorithmic bias, and regulating the use of deep fake technology. The political and societal decisions made as result of misguided or misused information can be devastating. Recognition that there is a problem is the first step toward resolving the issue.

7. Changes/Problems:

a. **Changes in approach and reason for change:** Budgetary issues associated second-year funding limited student researcher employment opportunities and hands-on project activities.
b. **Actual or Anticipated problems or delays and actions or plans to resolve them:** No anticipated problems at this point.
c. **Changes that have a significant impact on expenditures:** Partnering institution were able to successful navigate budget allotment issues.

8. Expenditures/Financial Discussion:

Provide information about budget expenditures. A budget sheet may be attached to satisfy this requirement.

Faculty and Staff				Total Spent	%
Position:	**Name**	**Total**			
PI	Dipankar Dasgupta	$67,789.89			
Co-PI	James McGinness/M. Won	$24,586.15			
Investigator	Modh Ali	$17,438.68			
Investigator	Amanda Rockinson-Szapkiw	$11,228.48			
Project Coordinator	tbn	$55,281.48			
Graduate Assistants	tbn (n=2)	$33,755.00			
Undergraduate Workers	tbn (n=3)	$36,789.87			
Module Instructors	tbn (n=2)	$0.00			
Event Coordinator	tbn	$0.00			
Instructional Module Developer	tbn	$0.00			
System Administrator	tbn	$54,006.91			
Total		$300,876.46		$ 326,501.13	109%
Fringe Benefits					
		Total			
PI	Dipankar Dasgupta	$23,899.33			
Co-PI	James McGinnis	$8,650.17			
Investigator	Modh Ali	$6,128.85			
Investigator	Amanda Rockinson-Szapkiw	$3,907.51			
Project Coordinator	tbn	$19,401.06			
Graduate Assistants	tbn (n=2)	$388.73			
Undergraduate Workers	tbn (n=3)	$408.86			
Module Instructors	tbn (n=2)	$0.00			
Event Coordinator	tbn	$0.00			
Instructional Module Developer	tbn	$0.00			
System Administrator	tbn	$3,967.42			
Total		$66,751.94		$ 74,780.93	112%
Other					
Items	**Model/Location**	**Total**			
Equipment		$0.00			
Travel		$8,427.00		$ 4,884.76	
Consultant: Instruction Evaluation		$4,000.00			
Subaward: NCAT		$99,199.20		$ 79,384.98	80%
Subaward: UWF		$226,162.76		$ 205,913.02	91%
Subaward: The Citadel		$109,678.68		$ 30,815.39	28%
Subaward 4		$0.00			
Other: Participant Support: *		$0.00			
Other: Part. Sup - workshops*		$503.00		$ 860.30	
Other: Computing Supplies		$3,387.39		$ 3,387.11	
Other: Annual software licensing fees		$2,000.00		$ 955.75	
Other: Annual Module prod. costs & fees		$1,400.00		$ 1,484.19	
Other: Graduate tuition/fees *		$28,922.00		$ 27,423.00	
Other: Program recruitment and marketing		$695.00			
Other: Printing		$136.30		$ 187.50	
Other: Workshop Audio/Visual Services		$0.00			
Total		$484,511.33		$ 355,296.00	73%
Total Direct Costs					
A+B+C		$853,972.36		$ 756,578.06	89%
F&A					
	Tot. Dir. Costs	**Total**			
Percent Rate	***SEE NOTE***	$161,935.93		$ 144,564.66	89%
TOTAL					
D+E		$1,014,075.66			
		$1,014,075.66		$ 901,142.72	89%

9. Conclusions/Future Activities: This should be brief synopsis of the entire program and where you see it going for your university.

Using the NIST-NICE Cybersecurity Workforce Framework, we will use a work-centered approach for critical infrastructure protection in design, recruitment, development, and retention considering the different categories, specialty areas, and work roles. This inter-disciplinary educational and outreach project focused on enhancing the security and resilience of critical infrastructure systems consistent with Presidential Policy Directive 21 and the National Critical Infrastructure Security and Resilience (CISR) Research and Development Plan. As a matter of fact, a variety of hands-on cybersecurity research projects were conducted with students at the University of Memphis that targeted the transportation sector (i.e., autonomous car security) and the water and wastewater sector (i.e., water pumping stations). Additionally, the University of West Florida conducted a number of training workshops designed for veterans, first responders, and faculty in ICS-RE Threat Intelligence and NERC-CIP Standards & Compliance.

Team members also either conducted or participated in numerous workshops/conferences. Several team members participated in a panel discussion on Critical Infrastructure Protection at the Jack Voltaic Conference on the campus of Citadel College on February 24, 2022. The University of Memphis hosted workshops entitled “Smart Grid Security” and “Cybersecurity for Critical Infrastructure” on March 25, 2023, and April 1, 2023, respectively. The IoT Security Workshop was held at North Carolina A&T State University on September 23, 2022. Five Workforce Development courses (i.e., ICS-RE Security, CMMC, NERC-CIP Standards & Compliance, and ICS-RE Threat Intelligence) have been delivered through the University of West Florida and Indian River Community College. Additionally, workshops entitled “Cybersecurity Education for Critical Infrastructure Protection” and “A Virtual Workshop on AI Enhanced IoT Security” were held at Citadel College on October 19-20, 2023, and North Carolina A&T State University on October 27, 2023, respectively.

The University of Memphis modules on Smart Grid and Zero Trust have been uploaded, reviewed, and released into the CLARK Library. Additionally, a module developed by North Carolina A&T State University entitled “CECIP – IoT Security” was uploaded and submitted for CLARK Committee review on November 7, 2023. The University of West Florida has twenty-one (21) learning objects on IS Security and Threats in association with this grant that have been vetted and released to the Clark Library. They also have ten (10) learning objects on NERC-CIP Compliance, in associated with the CECIP grant, that are being edited and vetted for release to the Clark Library. Finally, the Citadel College is developing a module on Cyber-Physical Systems to be released to Clark Library during Spring 2024.

The University of Memphis led consortium has been approved for its option year. Tentatively, the partnering institutions are planning roughly six (6) workshops designed to reinforce training on zero trust, smart grid security, cyber-physical systems, and IoT security. The University of Memphis is also seeking more student to participate in hands-on projects as well.

Appendix 1

Project Partner Reports

The University of Memphis

Team Report

Two-Year Report for NCAE001-2021 Grant

The University of Memphis

Team:

- Dr. Dipankar Dasgupta (Principal Investigator)
  Hill Professor in Cybersecurity
  Director, Center for Information Assurance
  Department of Computer Science

- Dr. Mohd Hasan Ali (Co-principal Investigator)
  Associate Professor
  Associate Director, Center for Information Assurance
  Department of Electrical/Computer Engineering

- Dr. Myounggyu Won (Co-principal Investigator)
  Assistant Professor
  Associate Director, Center for Information Assurance
  Department of Computer Science

Key Objectives:

- Lead consortium of institutions in the organization of training activities associated with the fulfillment of requirements associated with the NCAE-C-001-2021 grant.
- Organize workshops on cybersecurity education in critical infrastructure protection.
- Engage graduate and undergraduate students in cybersecurity research for critical infrastructure protection.
- Develop cybersecurity training modules in critical infrastructure protection for the Clark library and disseminate of research findings via publications and conferences.

Task Completed:

- Smart Grid Security Workshop was held at the University of Memphis FedEx Institute of Technology on March 25, 2022. There were thirty-seven (37) attendees (i.e., IT professionals, management personnel, teachers, and students).

- Cybersecurity for Critical Infrastructure Protection Workshop was held at the University of Memphis FedEx Institute of Technology on April 1, 2022. A total of seventy-one (71) people registered for the hybrid workshop. Twenty-six (26) of the virtual participants responded to the survey (i.e., IT professionals, management personnel, teachers, and students).
- Cyber Resilient EV Charging Station & Critical Infrastructure Joint Workshop was held at the University of Memphis Herff College of Engineering Auditorium on August 25, 2023. The event had thirty (30) in-person and seven (7) virtual participants.
- Promoted the development of six (6) research projects by graduate and undergraduate student project employees:
    - Autonomous R/C Car Project – Luke Carrington, Douglas Espinoza II, Andrika Cheairs, Ken Schnarrs, Riley Morris, William Richards, Adam Kharsa, and Adam Thieme
    - Dynamic Wireless Charging System Project – Nathan Farar
    - Water Pumping System Project - Hans Siegfried Amelang
    - Hierarchical Multi-factor Authentication – Arturo Perez
    - 5G Math Modeling & Cybersecurity – Tiffany Giestkemper, Allison Plank
    - Autonomous Truck Platoon Security – Luke Carrington
- Several cybersecurity training modules, developed by the University of Memphis, have been released to the Clark Library:
    - The Zero Trust micro-module was released on August 18, 2023.
    - The Smart Grid Security micro-module was released on October 2, 2023.

THE UNIVERSITY OF MEMPHIS | Center for Information Assurance

SMART GRID SECURITY WORKSHOP

Summary Report

March 25, 2022

The Center for Information Assurance (CfIA) successfully hosted the Smart Grid Security workshop on Friday March 25, 2022 on the University of Memphis campus. The hours of the workshop were from 12:00 pm until 5:00 pm. The purpose of the workshop was to cover various cybersecurity issues and their solutions to smart grid and power delivery systems.

A wide variety of topics related to Smart Grid security were represented, including but not limited to: Smart Grid security, Micro-grids, Renewable Energy sources, various cyber-attacks (Device attacks, Data attacks, Privacy attacks, Network Availability attacks, Communication networks, Demand Response, Smart Communication delays and its' mitigation technique, Power Quality, Reliability, Phasor Measurement Unit (PMU), Remote Terminal Unit (RTU) anomaly detection, and security and privacy policies). The workshop organizers offered both in-person and/or virtual attendance options.

The intended audience was IT Professionals, State employees, college students, and all persons interested in Smart Grid Cybersecurity and how to strengthen cyber resiliency. There was participation from various local, state, and federal including transitioning workforce. The participants were engaged for five (5) hours on Smart Grid Cybersecurity topics/ presentations with some real-world case studies, market-ready cyber security knowledge, and skills for career advancements. At the end of each speaker's presentation, there was time set aside for a question-and-answer segment.

The workshop was funded by the Department of Defense (DoD) under the NCAE-C-001-2021 Project Cybersecurity Education for Smart Grid Cybersecurity. All participants who fully participated at the workshop received a completion certificate.

Smart Grid Security Workshop Agenda

Date: March 25, 2022 Time: 12:00 pm to 5:00 pm.

Time:	Event:
12:00 – 12:10 pm	Welcome Remarks – Dr. Dipankar Dasgupta
12:10 – 12:15 pm	Participants Introduction
12:15 – 1:15 pm	Discussion on Smart Grid Cybersecurity – Dr. Hasan Ali
1:15 – 1:30 pm	Break
1:30 – 2:15 pm	Speaker – Dr. Stacy Prowell, Oak Ridge National Laboratory – Title of presentation: *Cautious Optimism.*
2:15 – 2:45 pm	Speaker – Mr. Chip Harris, Cybersecurity Administration at DMI.INC – Title of presentation: *Cybersecurity for Smart Grid Technology for I.T. and O.T.*
2:45 – 3:30 pm	Speaker – Dr. Sandip Roy, Program Director – Computer & Network Systems, NSF – Title of presentation: *Implications-Focused Cybersecurity Research for Power and Transportation Systems.*
3:30 – 3:45 pm	Break
3:45 – 4:15 pm	Presentation by Mr. Nathan Farrar, Undergraduate student, Electrical & Computer Engineering: “Impact Assessment of Cyber-Attacks on Inverter-based Micro-grids”
4:15 – 4:30 pm	Break
4:30 – 4:50 pm	Question and Answer / Discussion Session
4:50 – 5:00 pm	Workshop Closing Remarks – Dr. Dasgupta

An underlying objective for the workshop was “Advance your Career in the Cybersecurity related profession and opportunities at the University of Memphis”. There was a Pre-Survey and a Post-Survey given to all participants. (See Appendix A for a tabulation of responses).

Extracts from the Presentations:

The workshop’s welcoming remarks were given by CfIA Director, Dr. Dipankar Dasgupta. The participants were introduced. Afterwards, Dr. Hasan Ali, workshop organizer, presented on the topic: *“Cyber-Security Issues and Solutions to Distributed Energy Resources”*.

Synopsis: Dr. Ali began his presentation by giving a short description of a conventional power grid, and the issues associated with the grid in its current form. This was followed with the motivation of why smart grids are an important step for the power grid, and what can be accomplished with the adoption of smart grids. Dr. Ali then gave a discussion on distributed energy resources, followed by a visual depiction of how cyber-attacks occur on smart grids and distributed energy resources. Dr. Ali then discussed several different types of attacks that occur on smart grids and hybrid power grids, as well as the implications of the attacks. This was followed by a short discussion of the cyber security issues with Wide Area Measurement Systems (WAMS), including the Phasor Measurement Unit. He then discussed the importance of Photovoltaic (PV) energy in smart grids, as well as the necessity of including a battery storage device in solar networks. He discussed the specific cyber risks related to PV power generation and storage, followed by a control algorithm to detect, and mitigate cyber-attacks on PV systems. Dr. Ali concluded his presentation talk with reiterating that all businesses with an online presence are susceptible to cyber-attacks and that a proactive approach must be taken when managing cyber risk in smart and hybrid power grids.

After a short break, the next speaker was Dr. Stacy Prowell. His topic was: *“Cautious Optimism”*.

Synopsis: Dr. Prowell began his presentation with a recall to the winter storm in Texas that occurred in February 2021. The winter storm knocked out power to millions of customers and caused several hundred deaths in

the area. Thereafter, Dr. Prowell gave a short overview of the petroleum product supply in the gulf coast and east coast regions of the USA. This was followed by an explanation of ransomware, in which he explained how the ransoming is the last part of the cyber kill chain. He then presented an in-depth analysis of what types of firms are targeted by cyberattacks, how vulnerable firms are to cyberattacks, and how the invention of the internet and eventually IoT devices are responsible for the current state of cyber-crimes. He then discussed just how difficult and complex security is in the cyber realm. This was followed with a discussion on the incorrect assumptions coders and consumers make when relating to software and hardware development and utilization. He then finished his discussion by explaining why he is now cautiously optimistic that software and hardware suppliers, as well as consumers are beginning to take cyber security more seriously. Hence, the adoption of modern artificial intelligence algorithms may greatly reduce the risk and aid in prevention and mitigation of cyber-attacks.

The next speaker was Mr. Chip Harris. His presentation topic was: *"Cyber Security for Smart Grid Technology for I.T. and O.T"*.

Synopsis: Mr. Harris began his presentation by showing how much money is spent globally on cyber security from the year 2017 to the year 2026. Mr. Harris then touched on several different cybersecurity tools that when they are implemented effectively, can reduce the occurrence and the effect of cyberattacks. This was followed by a brief explanation of what a smart grid is with respect to IoT devices, and what types of cyber-attacks smart grid networks are facing. Mr. Harris then presented the challenges of a security control framework for identifying, protecting, detecting, responding, and recovering from a cyberattack on a network. This was then followed by a visual representation of the vulnerabilities of smart grids. Mr. Harris concluded his presentation by reiterating the importance of developing and maintaining a strong physical architecture for smart grids and the importance of cyber awareness.

The next speaker for the workshop was Dr. Sandip Roy.
Title of presentation: *"Implications – Focused Cybersecurity Research for Power and Transportation Systems"*.

Synopsis: Dr. Roy began his presentation by giving a brief explanation of his previous and current work experiences in infrastructure autonomy. This was followed by a discussion of why cyber security has become such a big concern in recent years, as well as the challenges to developing a secure system. Dr. Roy then segued into the primary focus of his presentation: the implications, and outcomes of cyberattacks. He used a bulk power system to explain how using physics, one can detect anomalous behavior of the system. A holistic risk approach was then used to detect the cyber risks of air traffic control and management. This was followed by a simulation of different attacks on an air traffic control and management system, as well as the emergency response system tasked with detecting cyberattacks. Dr. Roy concluded his presentation with a display of several axis that represent the challenges for cyber security, which include scale, time, goal, automation, and lifecycle.

After a short coffee break, the final speaker for the workshop was University of Memphis student Nathan Farrar. He presented on *"The Impact Assessment of Cyber-attacks on Inverter-Based Microgrids"*.

Synopsis: Mr. Farrar began his presentation by defining what a microgrid is, and how smart inverters are an integral part of the system. He then went into details of how detrimental a cyber attack could be on microgrid control systems if they should become compromised. Several different detection, prevention, and mitigation strategies were discussed including artificial intelligence, high-speed communication for wireless systems, and limiting "zero day" occurrences. Mr. Farrar concluded with how important it is for every person in the link, from suppliers to consumers, to understand just how important cyber security is, and to take every precaution when dealing with sensitive material.

Workshop Presenter's Biographies:

Dr. Mohd Hasan Ali, University of Memphis: Dr. Ali is currently an Associate Professor with the Electrical and Computer Engineering department at the University of Memphis. He leads the Electric Power and Energy Systems (EPES) Laboratory. His research interests include smart-grid and micro-grid systems, renewable energy systems, energy storage systems, load forecasting in smart buildings, electric vehicles charging

stations, and cybersecurity issues in modern power grids. He serves as the Editor of the IEEE Transactions on Sustainable Energy, IEEE Transactions on Energy Conversion, IEEE Power Engineering Letters, Frontiers in Energy Research, and the IET-Generation, Transmission and Distribution (GTD) Journals. Dr. Ali is a Senior Member of the IEEE Power and Energy Society (PES). He also serves as the Chair of the PES of the IEEE – Memphis Chapter.

Dr. Stacy Prowell, Oak Ridge National Laboratory: Dr. Prowell is a Distinguished Researcher with the Oak Ridge National Laboratory. He is the Chief Cybersecurity Research Scientist in the National Security Sciences Directorate at Oak Ridge National Laboratory. His research focuses on methods to secure the nation's critical infrastructure. He has developed technologies for automated reverse engineering of compiled software to detect vulnerabilities, to detect fileless malware remotely, and to detect attacks and compromises using timing and power side channel information.

Mr. Luther "Chip" Harris, Cybersecurity Administration at DMI.INC: Mr. Harris is the Ethical Hacker, Red Team Leader, Penetration Tester, and a Senior Cyber Security Administrator at DMI.INC. He currently works on network platform-based security technique experience and development of an enterprise IT (Malware Prevention) modernization plan.

Dr. Sandip Roy, Program Director, Computer and Network Systems, National Science Foundation (NSF): Dr. Roy is a Professor in the School of Electrical Engineering and Computer Science at Washington State University. His research is focused on developing secure and resilient autonomy for Cyber-enabled infrastructures. The research has led to tools and software that have been prototyped and deployed in several settings (e.g.: the Western U.S. Power Grid, and the U.S. Air Transportation System's Central Command Center). He is currently on appointment at the National Science Foundation, supporting the Cyber-Physical Systems and

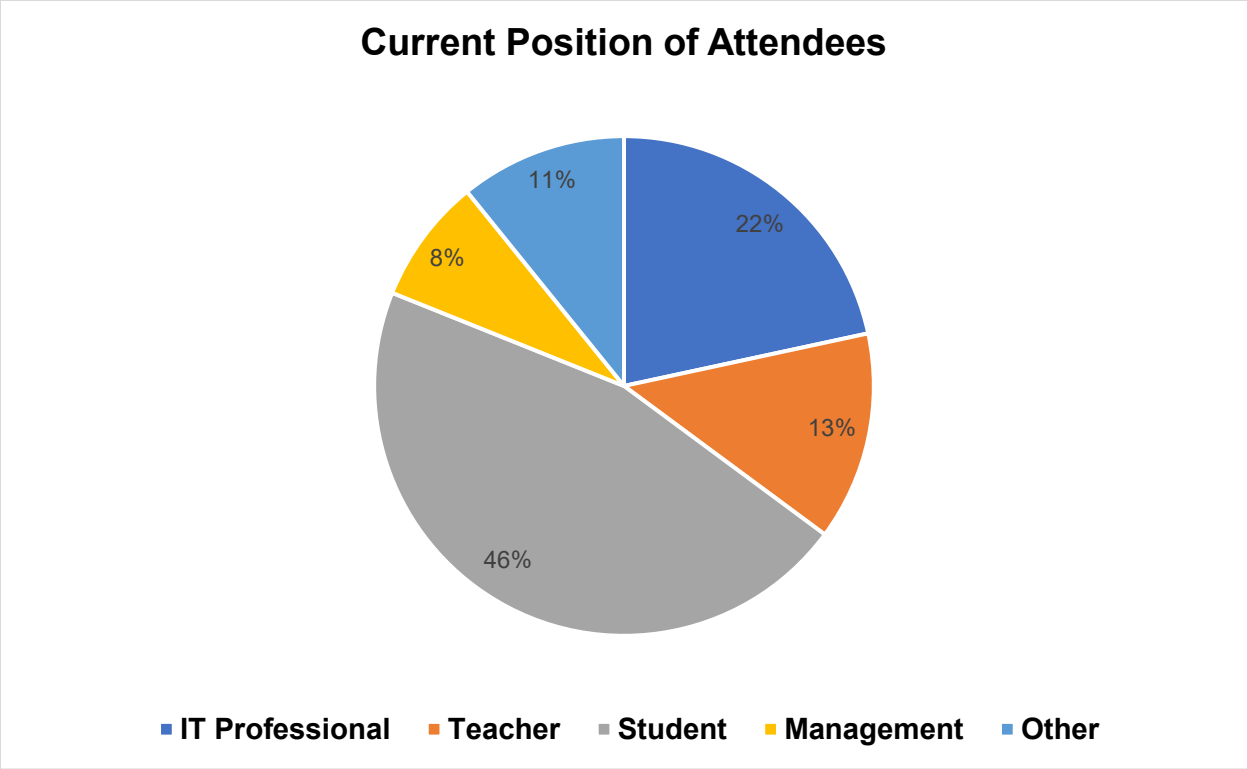
Smart & Connected Communities programs. He also holds a joint appointment at Pacific Northwest National Laboratories.

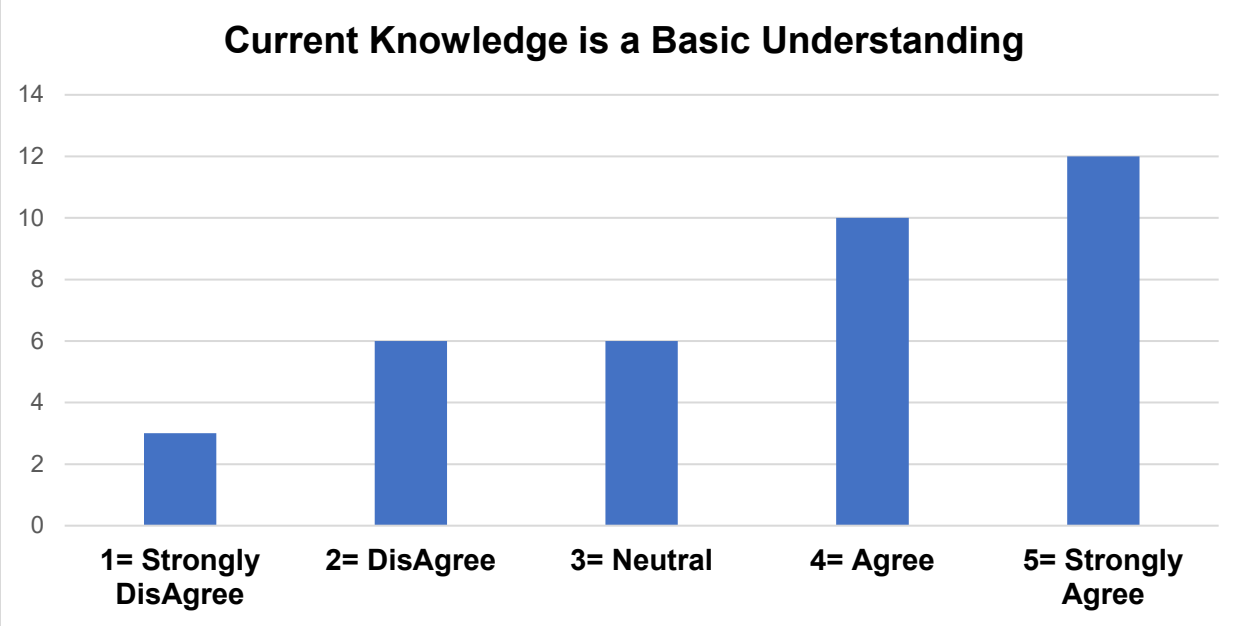
Mr. Nathan Farrar, University of Memphis: Mr. Farrar is an undergraduate student in the Electrical and Computer Engineering department. He will graduate in May 2022 and will start his Master's degree studies during the Fall 2022. His research interests include cybersecurity issues in modern power grid systems, smart grid, microgrid, and renewable energy systems.

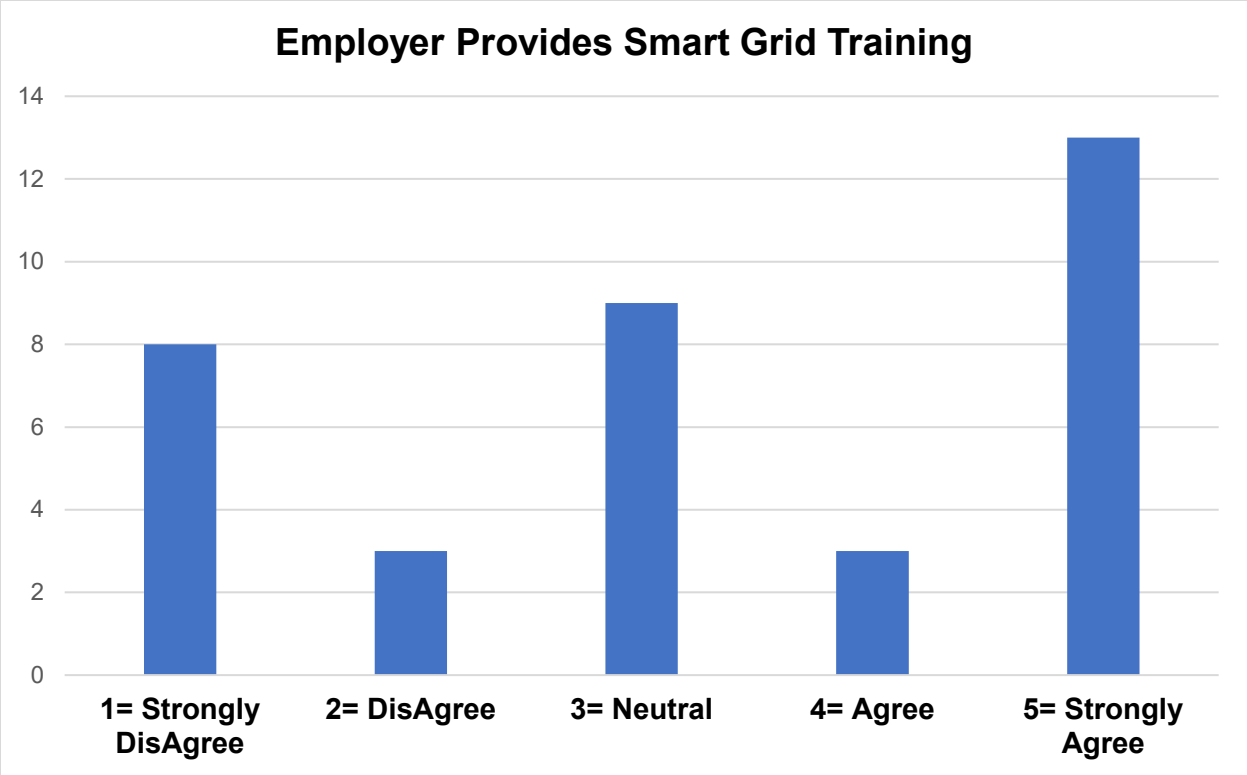
Appendix A: Smart Grid Security Workshop: Participant Data, Workshop Photo, and Feedback Response Charts.

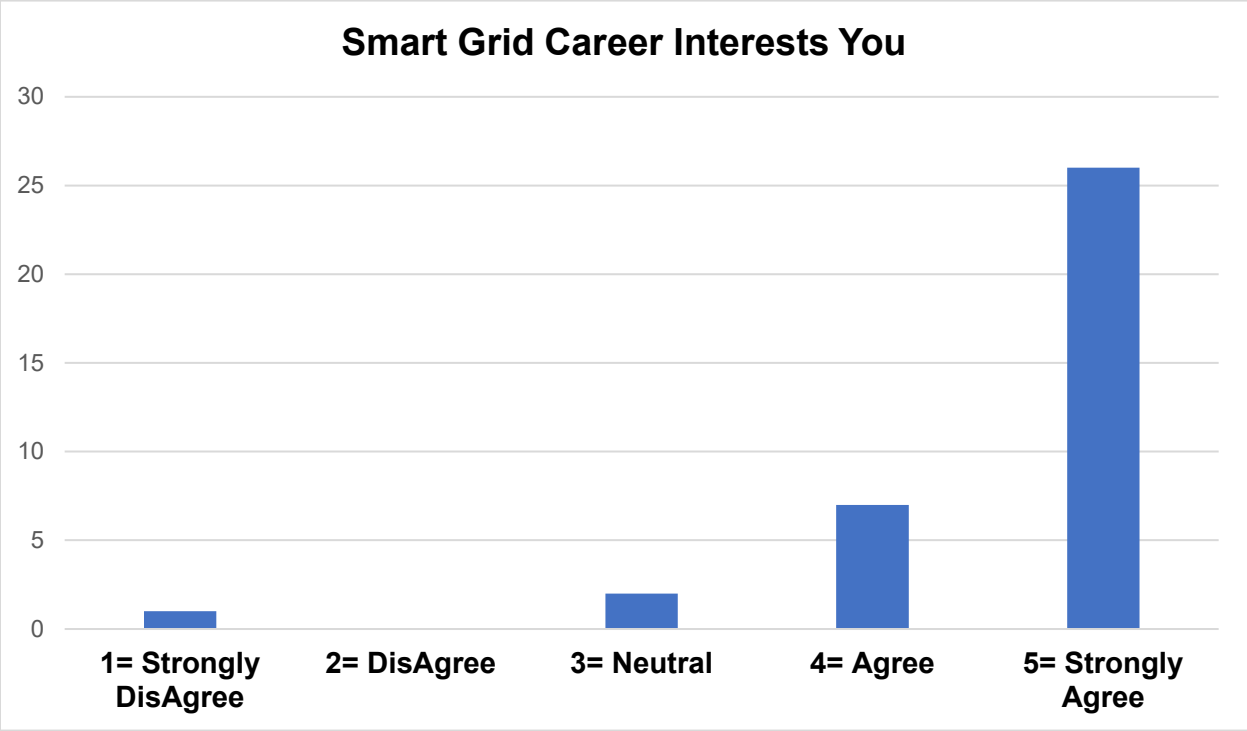
In summary, there were a total of 37 survey respondents (e.g., face to face and virtual).

A total of 84 people registered online for the Smart Grid Security workshop. There was a total of 18 face-to-face and 19 virtual attendees for this event. There were 3 walk-up participants. The following chart provides different categories of the professionals that participated.

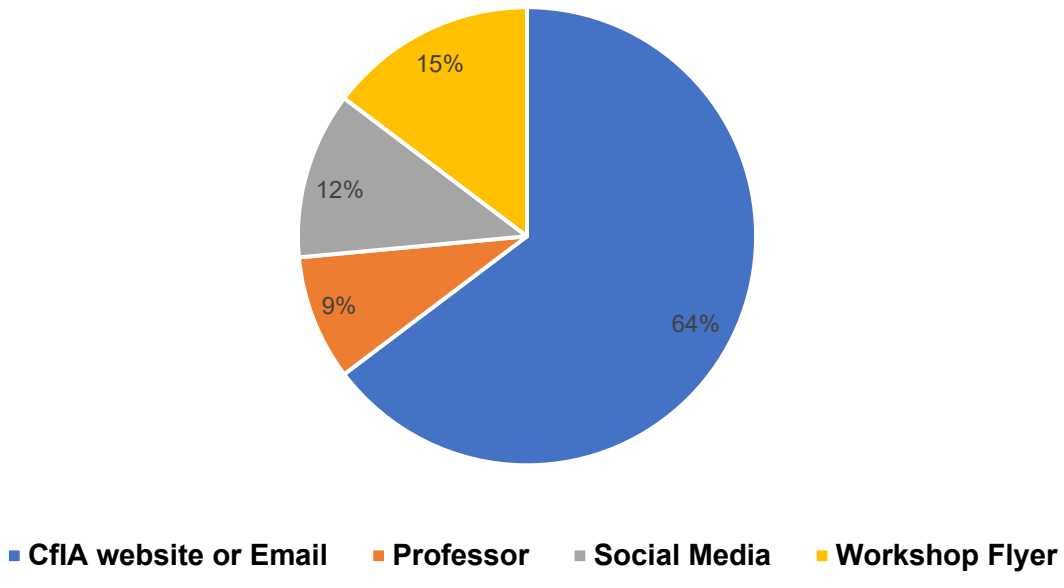

Current Position of Attendees
22%
13%
46%
8%
11%
IT Professional
Teacher
Student
Management
Other


Current Knowledge is a Basic Understanding
14
12
10
8
6
4
2
0
1= Strongly DisAgree
2= DisAgree
3= Neutral
4= Agree
5= Strongly Agree

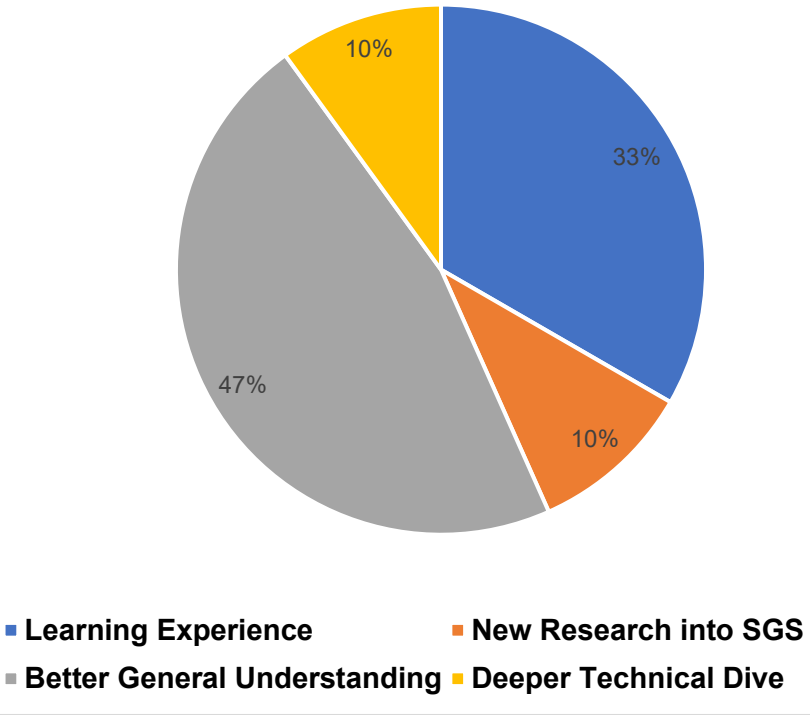

Employer Provides Smart Grid Training
14
12
10
8
6
4
2
0
1= Strongly DisAgree
2= DisAgree
3= Neutral
4= Agree
5= Strongly Agree


Smart Grid Career Interests You
30
25
20
15
10
5
0
1= Strongly DisAgree
2= DisAgree
3= Neutral
4= Agree
5= Strongly Agree

How Did You Hear about this Workshop



Your Expectations of this Workshop



THE UNIVERSITY OF MEMPHIS | Center for Information Assurance

CYBER SECURITY FOR CRITICAL INFRASTRUCTURE WORKSHOP

Summary Report

April, 2022

The Center for Information Assurance (CfIA) successfully hosted the Cybersecurity for Critical Infrastructure workshop on Friday April 1, 2022 on the University of Memphis campus. The hours of the workshop were from 12:00 pm until 5:00 pm. The purpose of the workshop was to highlight the cyber-attacks and other security challenges for emerging information and communication technologies which are continually integrated into national critical infrastructure. A wide variety of topics related to critical infrastructure protection were represented at the workshop which was held both in-person and virtually. The intended audience was state employees, IT professionals, college students, and all persons interested in Cybersecurity within Critical Infrastructures and how to strengthen cyber resiliency. There was participation from various local, state, federal including transitioning workforce. The participants were engaged for five (5) hours on critical infrastructure topics presentations with real-world case studies and market-ready cyber security knowledge, skills for career advancements. At the end of each speaker's presentation, there was time set aside for a question-and-answer segment. The workshop was funded by the Department of Defense (DoD) under the NCAE-C-001-2021 Project Cybersecurity Education for Critical Infrastructure Protection. All participants fully participated at the workshop received completion certificates.

Below is the agenda **of Cybersecurity for Critical Infrastructure Workshop:**

Date: April 1, 2022; 12:00 pm - 5:00 pm

Time	Event
12:00 – 12:10 pm	Welcome Remarks - Dr. Jim McGinnis
	Participants Introduction
12:10 - 12:25 pm	Discussion on Current State of Cybersecurity Dr. Dasgupta
12:25 - 12:50 pm	Cybersecurity Case Studies Review Hampton Roads Sanitation / SolarWinds - (Dr. James McGinnis & Nathan Seymour)
12:50 - 1:00 pm	Break
1:00 – 1:45 pm	Benjamin Denkers, EVP of Operations at CynergisTek. Infrastructure Under Attack: Weaponizing Cyber for Strategic or Tactical Advantage
1:45 – 2:00 pm	Break
2:00 – 3:00 pm	Guest Speaker, Dr Csilla Farkas - U. of South Carolina Cyber-Risk Assessment – a Data-driven View
3:00 – 3:10 pm	Break
3:10 – 3:35 pm	Remote Access Security: Dr. McGinnis Social Engineering, Work from Home.
3:35 – 4:10 pm	Guest Speaker: Jeremy Baker, FBI Memphis Field Office
4:10 – 4:50 pm	Other Security topics & Demo: Defense in Depth - Dr. Dasgupta Zero Trust Model - Nathan Seymour Penetration Testing Demo - Cody Seymour
4:50- 5:00 pm	Questions and Answers / Closing Remarks - Dr. Dasgupta

An underlying objective for the workshop was “Advance your Career in Cybersecurity related profession and opportunities at the University of Memphis”. There was a Pre-Survey, a Post-Survey, and a Post-Survey Assessment given to all participants.

Extracts from the Talks:

The workshop's welcoming remarks were given by the workshop organizer, Dr. James McGinnis. The participants were introduced. Afterwards, Dr. Dipankar Dasgupta conducted an opening talk on 'The Current State of Cybersecurity'. The next presentation segment consisted of case study reviews by Dr. McGinnis and Nathan Seymour. Dr. McGinnis presented information on the Hampton Roads Sanitation ransomware attack. The talk centered on the attack details, the state of the infrastructure, the diagnosis, as well as the remediation and response actions. The presentation was based on research of the Hampton Roads Sanitation District as reported by the podcast '*Ransomware File's* and other related references. Nathan Seymour's presentation centered on the Colonial Pipeline ransomware attack. He also spoke on the SolarWinds and the Kaseya attacks as part of his presentation to the group. In conjunction with the attack incidents, he also presented on research data of key interests points such as: zero trust, zero trust architectures, identity management, access control, and ransomware.

The next segment of the workshop was presented by guest speaker Mr. Benjamin Denkers. The title of the presentation was "Infrastructure Under Attack: Weaponizing Cyber for Strategic or Tactical Advantage". Mr. Denker's presentation focused on the impact cyber security has on critical infrastructures. Disruption as a theme can have an immediate impact as one might imagine; however, the downstream effects of cyber-attacks can be hard to predict and even have worse consequences. Understanding attacker TTPs and how these multipronged attacks evolve, enable organizations to help mature security privacy and security programs to be in the best position to detect and prevent compromises.

After a short break, the next guest speaker was Dr. Csilla Farkas, Professor of Computer Science & Engineering and the Director of Center for Information Assurance Engineering at the University of South Carolina – Columbia. The title of the presentation was "Cyber Risk Assessment – a Data Driven View. The presentation highlights were as follows: Cybersecurity risk assessment methods are hindered by a lack of data availability. Data and information sharing legislation aim to ease this problem. However, the presence of highly sensitive and proprietary data and the lack of mutually trusted entities make such sharing a daunting task. Furthermore, current cyber risk assessment models do not address our nation's

social vulnerability to cyberattacks against critical infrastructures. In this presentation we reviewed secure information sharing approaches that may increase the trust in cybersecurity information sharing practices. The speaker suggested a new view on data collection and analysis that is promising to support a multifaceted risk assessment.

The next workshop segment was presented by Dr. James McGinnis, Professor and workshop organizer with the University of Memphis. The title of the presentation was “Infrastructure: Social Engineering, Remote Access, Working from Home”. The highlights of the presentation were the changing threat landscape involving remote home offices, remote access, and social engineering. The presentation included the growing landscape that has evolved over the last two (2) years, predominately due to the Covid19 pandemic. With more employees working remotely, the threat landscape has increased dramatically due to unprepared businesses and home offices without centralized management and/or monitoring of connections and devices.

The next guest speaker for the workshop was Mr. Jeremy Baker, Special Agent in Charge, FBI Memphis Field Office. The presentation title was “FBI Cyber Program and Cyber Investigations. Mr. Baker spoke on the ongoing efforts of the FBI, not only locally, but nationwide, on the increase in cyber activity and the rigor of the investigative involvement of the FBI in cyber-crimes. Working with academia and corporate entities to stay ahead of cyber criminals and keeping the general population informed and up to date on cyber-crime proves to be a fulltime endeavor, as well as a challenge that constantly changes. The presentation touched on many of the efforts and communication activities that are required to stay adept in a changing cyber world. Immediately after Mr. Baker’s presentation, there were two demonstrations conducted by University of Memphis Graduate Students. First Nathan Seymour talked about the Zero Trust Model. Next Cody Seymour did a demonstration on Penetration Testing for the audience followed by questions and/or comments on the student’s presentations.

The last presentation was delivered by Dr. Dipankar Dasgupta, Professor and Director of the Center for Information Assurance with the University of Memphis. Dr. Dasgupta spoke on the status of the Center for Information Assurance and other cyber security highlights. Professor Dipankar Dasgupta’s talk was entitled

"Emerging Cyber Threats such as Ransomware, Targeted Attacks, and APT's Crypto-jacking". He provided some guidelines and best practices in dealing with such cyberattacks from the user's perspective. His talk also covered the importance of Multi-Factor Authentication and ID Management; the concept of Zero Trust, Endpoint Detection and Response, etc. He also discussed various research and educational opportunities available in Cybersecurity at the University of Memphis.

The Cybersecurity for Critical Infrastructure workshop concluded with a question-and-answer segment, at the end of which Dr. Dasgupta gave the closing remarks and encouraged the attendees to check the University of Memphis CfIA's website frequently for upcoming events and workshops being planned.

Workshop Presenter's Biographies:

Mr. Jeremy Baker, Special Agent in Charge, FBI Memphis Field Office. He is the assistant special agent in charge, Intelligence Partner Engagement, Tech Memphis FBI Field Office. In 2020, Mr. Baker earned his certified information systems security professional designation (CISSP) to complement other cyber security certifications he has earned through the FBI's cyber division, Carnegie Mellon university, and SANS. In August 2020, Mr. Baker began work on a master's degree in Cybersecurity Risk Management through Georgetown University, and in 2021, he became a member of the FBI's Adjunct Faculty program, instructing on behalf of the cyber division.

Mr. Ben Denkers is the EVP of Operations at CynergisTek where he is responsible for supporting growth, ensuring effective and efficient service delivery, and achieving the highest levels of client and employee satisfaction in CynergisTek's security, privacy and compliance services. Mr. Denkers has nearly twenty (20) years of experience in information security and consulting that includes markets such as finance, energy, manufacturing, and healthcare.

Dr. Csilla Farkas is a professor in the department of computer science and engineering at the university of South Carolina (UofSC). She is the founder and director of the center for information assurance engineering. Dr. Farkas' research interests include information security, data inference problems, financial and legal analysis of cybercrime, security and privacy on the Semantic web, and information

warfare. Her early work pioneered the development of semantics-based security models for web data and metadata. Her most recent work addresses security, privacy, and reproducibility of scientific workflow systems and specific security concerns of High-Performance Computing (HPC) systems. She has published over 100 peer-reviewed conference and journal papers. Her research has been funded by the National Science Foundation, National Security Agency, Space and Naval Warfare, IBM, Federal Railroad Administration, and the South Carolina Department of Commerce.

Dr. Dipankar Dasgupta is Hill Professor of Computer Science and the director of the center for information assurance at the University of Memphis. Dr. Dasgupta is a professor of Computer Science and is the founding Director of the Center for Information Assurance (CfIA), (http://cfia.memphis.edu). The Center has been a National Center for Academic Excellence in Information Assurance Education (CAE-CD since 2004) and in Research (CAE-R since 2010). He spearheads the University of Memphis' education, training, and community outreach activities on Cybersecurity and Information Assurance (IA). Dr. Dasgupta's research covers broad areas of computational intelligence (including AI and machine learning) for the design and development of intelligent solutions. He is one of the founding fathers of the field of artificial immune systems, making major contributions in developing tools for digital immunity and survivable systems. Dr. Dasgupta has published several books and edited volumes including Advances in User Authentication (2017), Immunological Computation (2008), Artificial Immune Systems (1999), and another book on genetic algorithms (1996). Dr. Dasgupta has more than 300 publications. A Google search of his name indicates more than 16,500 citations, and an academic search in Microsoft shows that he has collaborated with 106 co-authors, an extraordinary testimony to the broad influence of his contributions within the research community. With an H-index of over 58, he is featured on UCLA's list of prominent computer scientists.

Dr. James McGinnis is an Assistant Professor in the Herff College of Engineering at the University of Memphis. Dr. McGinnis has over twelve (12) years of experience in Academia, and over twenty (20) years of experience in the corporate world. He has been on the front line of Information Technology while serving as an IT Engineer, IT Manager, IT Security Manager, and IT Department director. He has had experience in security policies, Disaster Recovery, Business Continuity and Training.

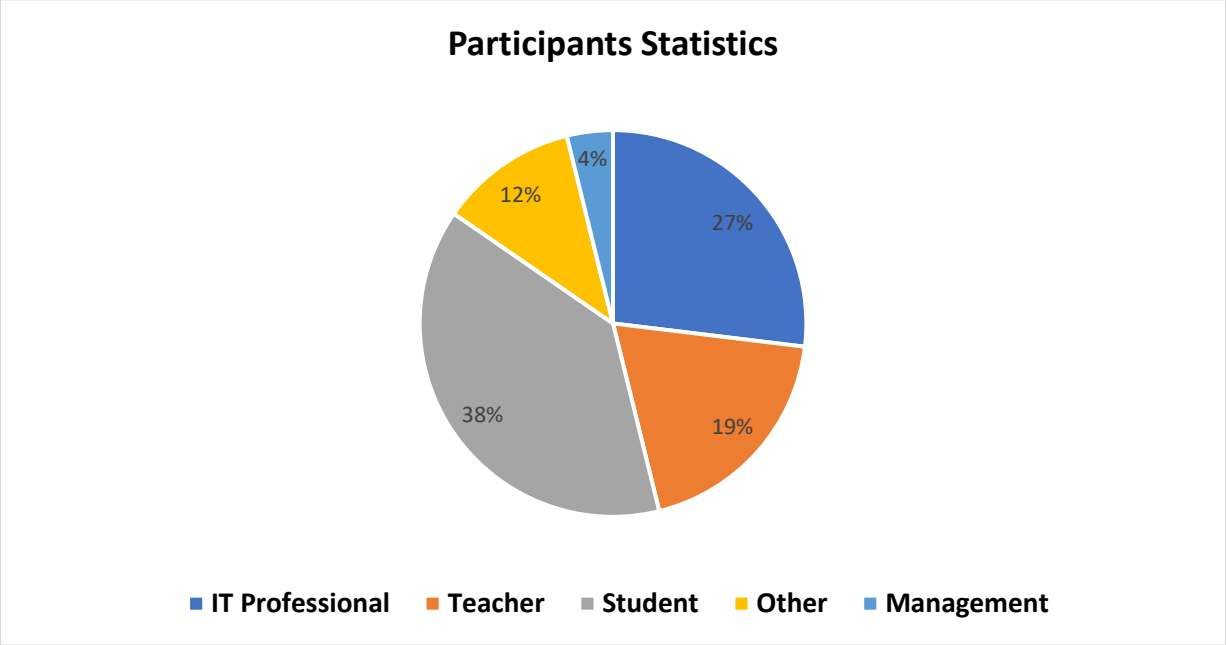
Dr. McGinnis has achieved certifications by ISACA (CISM), Microsoft Server and Workstations, CISCO NetAcademy for the Cisco CCNA series Instructor, and CCNA Cybersecurity. He has extensive training and actual experience in the fields of IT and Security of Information.

Mr. Nathan Seymour is a graduate student in the Computer Science department at the University of Memphis. Currently, he is working under Dr. Dipankar Dasgupta as a graduate research assistant on the Cybersecurity Education for Critical Infrastructure Protection project. Some of his research interests include: Zero Trust, Zero Trust architectures, Identity Management and Access Control, and Ransomware.

Mr. Cody Seymour is an undergraduate student who worked on different security tools and techniques including SNORT intrusion detection system, firewalls, penetration testing and forensic tools.

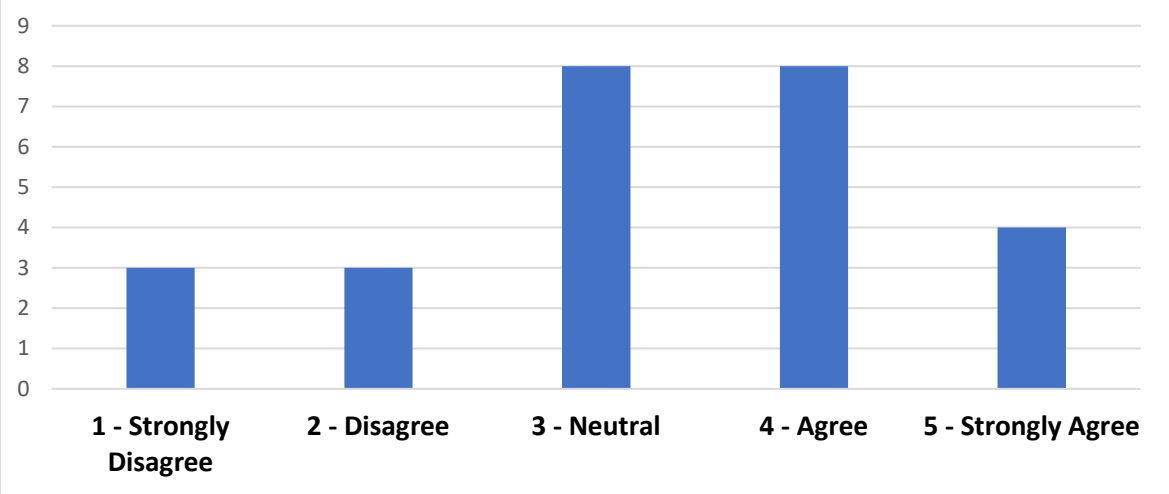
Appendix A: Workshop Participation data and feedbacks.

A total of 71 people registered for the workshop for both face-to-face and virtual event. The following chart depicts the different categories of participating professionals who responded to the survey polls.

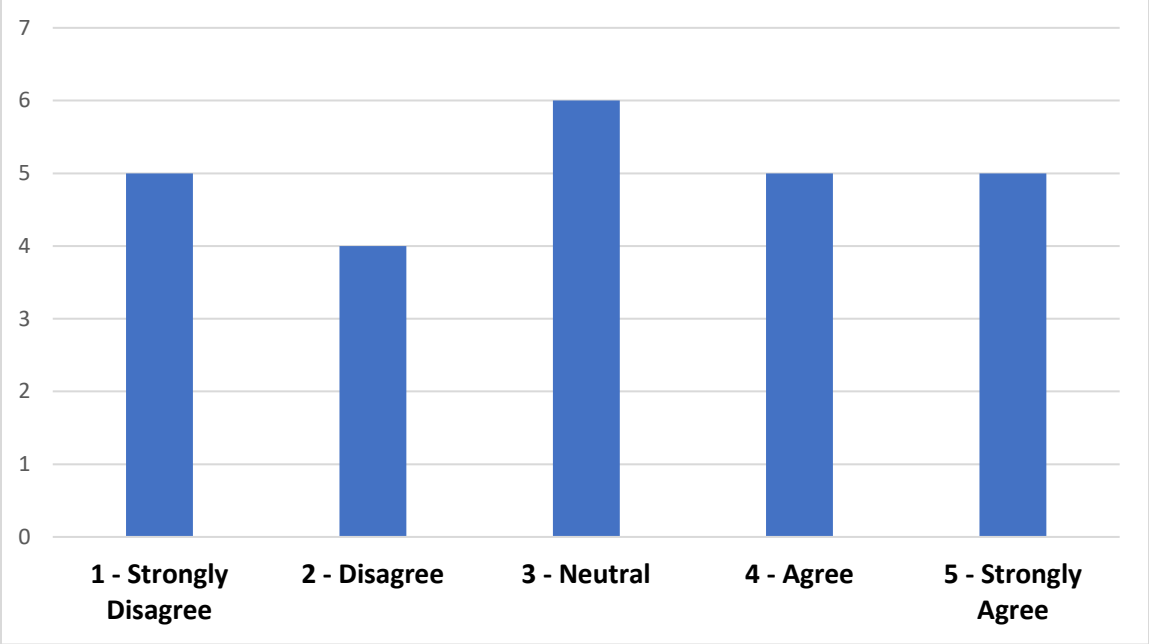


Additional data collected from the attendees as feedback on the workshop and is graphed below:

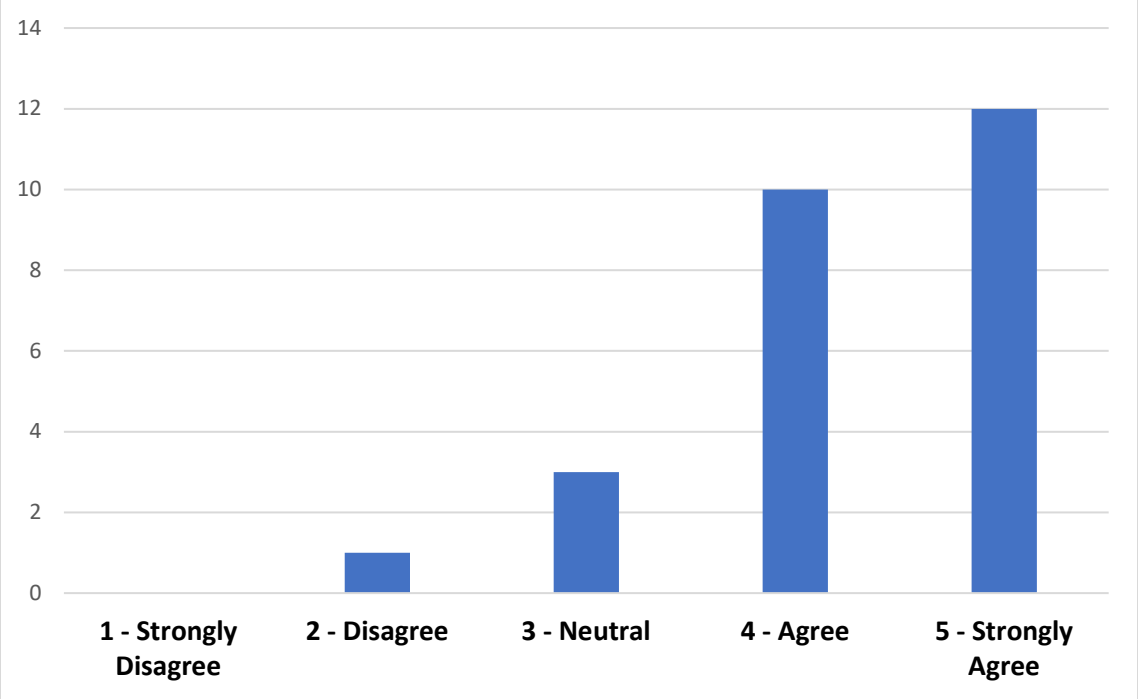
1. The current level of knowledge about cybersecurity for critical infrastructure for the attendees are depicted in the chart below:



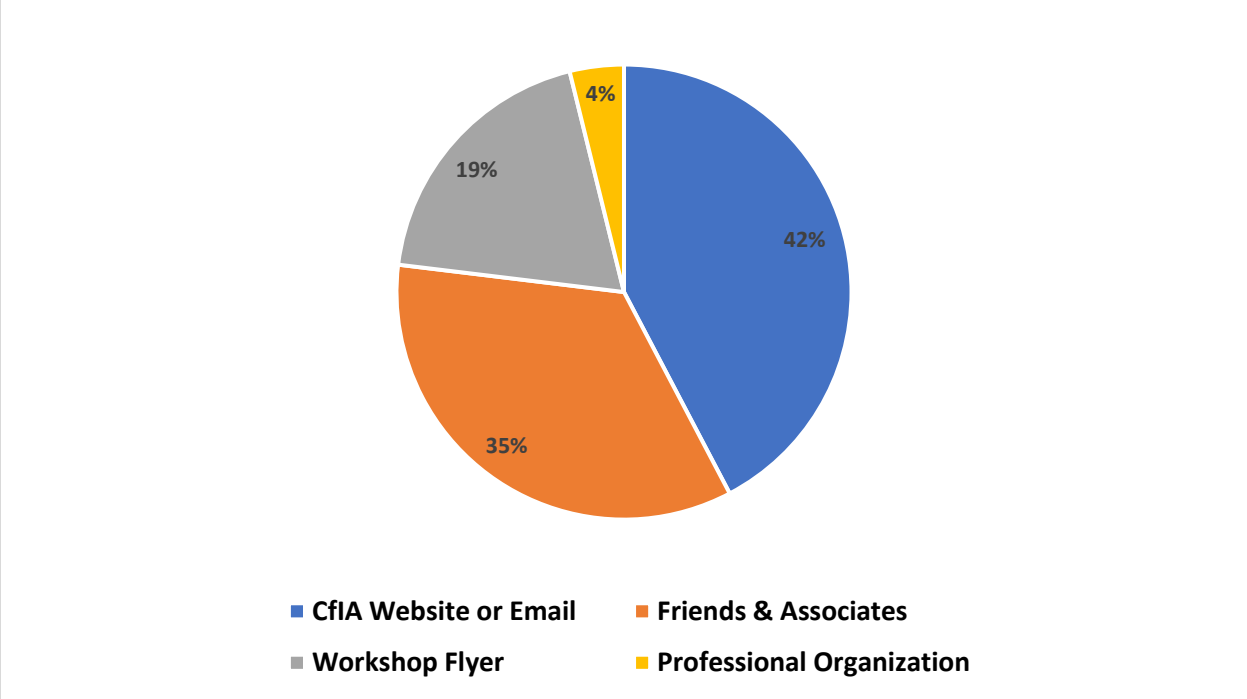
2. Your Employer Provides Critical Infrastructure Training:



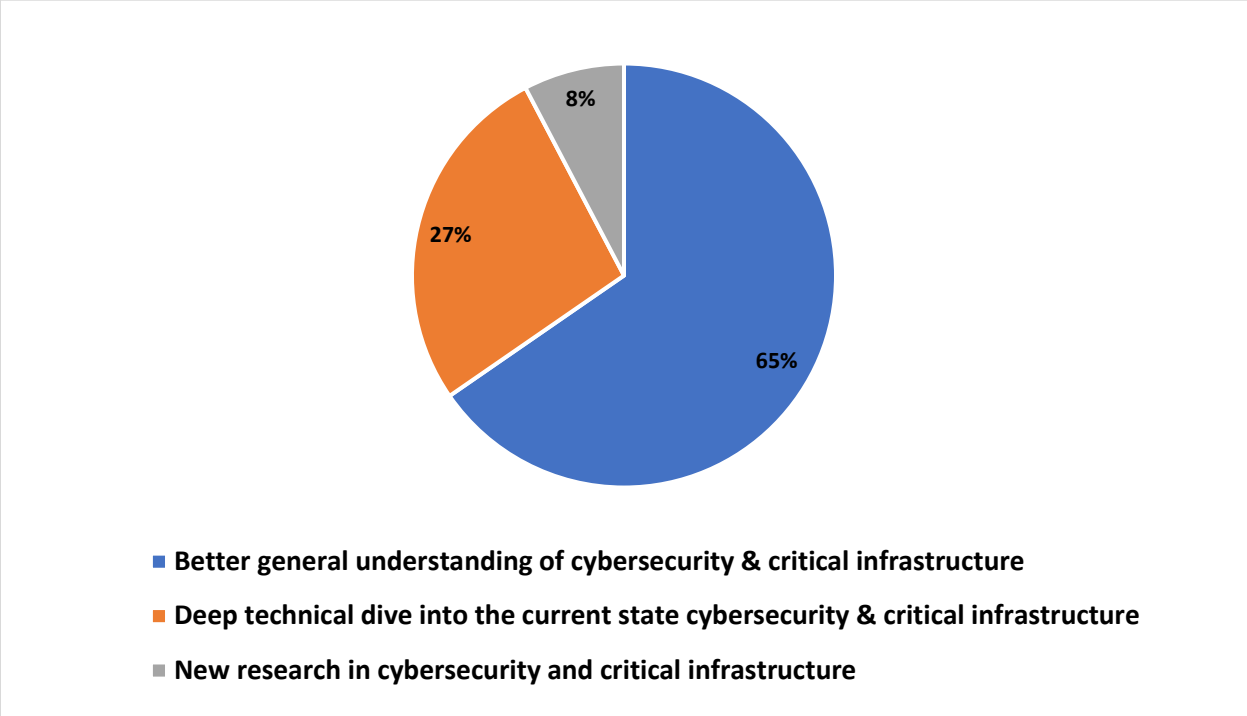
3. A Critical Infrastructure Career Interest You:



4. How did you hear about this Critical Infrastructure Workshop?



5. Your Expectations for this Critical Infrastructure Workshop:



Cyber Resilient EV Charging Station & Critical Infrastructure Workshop

Photo: Workshop in-person attendance for the event

The University of Memphis Center for Information Assurance (CfIA) in conjunction with the Computer Science and Electrical/Computer Engineering Departments hosted the Cyber Resilient EV Charging Station and Critical Infrastructure Workshop. The event was hosted in a hybrid format and had thirty (30) in-person and seven (7) virtual attendees. It was held in the Engineering Auditorium of the Herff College of Engineering on Friday August 25, 2023, from 9am to 5pm CST.

The workshop started with a welcome from both Dr. Okenwa Okoli, Dean of the Herff College of Engineering (CoE), and Dr. Stephanie Ivey, Herff CoE Associate Dean for Research. It featured presentations from several noteworthy speakers. Ryan Stanton, Tennessee Valley Authority (TVA), set the tone for the event with his presentation on the "Valley-wide Perspective on Electric Vehicles." Other noteworthy visiting speakers were Dr. Prasad P. Calyam, University of Missouri-Columbia, who presented "A Case for Low Overhead Zero Trust to Protect Critical Edge Infrastructures" and Dr. Anurag K. Srivastava, West Virginia University, who presented on "Enabling Secure and Resilient Cyber-Power Critical Infrastructure." Additionally, Dr. Mohammad Ashiqur Rahman, Florida International University, presented 'Artificial Intelligence-Driven Control-Aware Attack-Resiliency Analytics for Cyber-Physical Systems."

University of Memphis faculty members also presented during the workshop. Dr. Mohd Hasan Ali presented on "Cyber Resilient Electric Vehicle Charging Infrastructure" and Dr. Myounggyu Won made a presentation entitled "Intelligent Adaptive Electric Vehicle Motion Control for Dynamic Wireless Charging."

Finally, University of Memphis graduate students provided update presentations on the status of their research projects. Nathan Farrar's presentation was on "Dynamic Wireless Charging: Cyber Security and the Future of EV Charging" whereas Elijah Durkee made presentation on "Cyber Resilient 5G-Enabled Electric Vehicle Charging Station" on behalf of his research group. Additionally, graduate student Sagar Pathak and staff member Jack O'Meara made a presentation on the National Cybersecurity Preparedness Consortium activities at the University of Memphis.

Dr. David Russomanno, Executive Vice President for Academic Affairs & Provost, and Dr. Dipankar Dasgupta made closing remarks for the event.

Agenda for Cyber Resilient Electric Vehicle Charging Station & Critical Infrastructure Workshop

Location: UofM Engr Admin. Bldg. (Room EA – 203)
Date: Friday August 25, 2023
Time: 9:00 am - 5:00 pm

Time	Event
9:00 -9:30 am	Welcome Remarks (Dr. Okenwa Okoli, Dr. Stephanie Ivey)
9:30 - 9:40 am	Participants Introduction
9:40 - 10:30 am	Speaker- Mr. Ryan Stanton, Tennessee Valley Authority (TVA), Valley-wide Perspective on Electric Vehicles.
10:30 – 10:45 am	Speaker-Dr. Mohd Hasan Ali (UofM), Cyber Resilient Electric Vehicle Charging infrastructure.
10:45 - 11:00 am	Coffee Break
11:00 – 12:00 pm (noon)	Speaker-Dr. Prasad P. Calyam (University of Missouri-Columbia), A Case for Low Overhead Zero Trust to Protect Critical Edge Infrastructures.
12:00 pm - 1:00 pm	Lunch Break
1:00 – 2:00 pm	Speaker-Dr. Anurag K Srivastava (West Virginia University), Enabling Secure and Resilient Cyber-Power Critical Infrastructure.
2:00 – 2:15 pm	Speaker-Dr. Myounggyu Won (UofM), Intelligent Adaptive Electric Vehicle Motion Control for Dynamic Wireless Charging.
2:15 - 3:15 pm	Speaker-Dr. Mohammad Ashiqur Rahman (Florida International University), Artificial Intelligence-Driven Control-Aware Attack-Resiliency Analytics for Cyber-Physical Systems.

3:15 - 3:30 pm	Coffee Break
3:30 - 3:45 pm	Speakers-Elijah Durkee, Allison Plank, Arnab Das, Alexander Martin, and Noah Wargo (UofM), Cyber Resilient 5G-Enabled Electric Vehicle Charging Station.
3:45 - 4:00 pm	Speaker-Nathan Farrar (UofM), Dynamic Wireless Charging: Cyber Security and the Future of EV Charging.
4:00- 4:30 pm	Speakers- Mr. Jack O'Meara and Sagar Pathak (UofM), National Cybersecurity Preparedness Consortium Activities at the UofM.
4:30 – 4:45 pm	Questions and Answers Session
4:45 – 5:00 pm	Closing Remarks (Dr. David Russomanno, Dr. Dipankar Dasgupta)

Guest Speakers Bios:

Dr. Anurag K. Srivastava is a Raymond J. Lane Professor and Chairperson of the Computer Science and Electrical Engineering Department at the West Virginia University. He is also an adjunct professor at the Washington State University and senior scientist at the Pacific Northwest National Lab. He received his Ph.D. degree in electrical engineering from the Illinois Institute of Technology in 2005. His research interest includes data-driven algorithms for power system operation and control including cyber-resiliency analysis. Dr. Srivastava high impact research projects resulted in tools installed at the utility control center supported for more than $50M by US Department of Energy, National Science Foundation, Siemens Corporate Research, Electric Power Research Institute, Schweitzer Engineering Lab, Power System Engineering Research Center, Office of Naval Research and several National Labs. In past years, he has worked in a different capacity at the Réseau de transport d´électricité in France; RWTH Aachen University in Germany; PEAK Reliability Coordinator, Idaho National Laboratory, PJM Interconnection, Schweitzer Engineering Lab (SEL), GE Grid Solutions, Massachusetts Institute of Technology and Mississippi State University. He has delivered 30+ keynotes/ tutorials/ IEEE distinguished

lecture in more than 15 countries. He is an IEEE Fellow, member of several CIGRE WG and the author of more than 350 technical publications including a book on power system security and 3 patents.

Dr. Prasad P. Calyam is the Greg L. Gilliom Professor of Cybersecurity in the Department of Electrical Engineering and Computer Science at University of Missouri-Columbia, and Director of the Center for Cyber Education, Research and Infrastructure (Mizzou CERI). His research and development areas of interest include: Cloud Computing, Machine Learning, Artificial Intelligence, Cyber Security, and Advanced Cyberinfrastructure. He has published over 200 peer-reviewed papers in various conference and journal venues. As the Principal Investigator, he has successfully led teams of graduate, undergraduate and postdoctoral fellows in Federal, State, University and Industry sponsored R&D projects totaling over $30 Million. His research sponsors include: National Science Foundation (NSF), Department of Energy (DOE), National Security Agency (NSA), Department of State (DOS), Army Research Lab (ARL), VMware, Cisco, Raytheon-BBN, Dell, Verizon, IBM and others. His basic research and software on multi-domain network measurement and monitoring has been commercialized as 'Narada Metrics'. He is a Senior Member of IEEE. He currently serves as an Associate Editor for IEEE Transactions on Network and Service Management.

Dr. Mohammad Ashiqur Rahman is an Associate Professor in the Department of Electrical and Computer Engineering and the School of Computing and Information Sciences at Florida International University. He obtained a PhD in computing and information systems from the University of North Carolina at Charlotte (UNC Charlotte) in 2015. Previously, he received BS and MS in computer science and engineering from Bangladesh University of Engineering and Technology (BUET). Dr. Rahman's primary research interests cover a wide area of computer networks and cyber-physical systems (CPS). His research focus primarily includes computer and information security, risk analysis and security hardening, secure and dependable resource allocation, and distributed computing. His research is primarily funded by NSF, DOE, and DOD. He is currently leading multiple grants on CPS security. Dr. Rahman coauthored a book and several book chapters and published over 100 peer-reviewed journal and conference papers. He served on the organization and technical program committees (TPCs) for various IEEE and ACM conferences. He served as the TPC Co-Chair of IEEE/IFIP NOMS 2023.

Mr. Ryan Stanton is the senior project manager for the EV Evolution initiative with the Tennessee Valley Authority (TVA). In this role, Ryan focuses on research, innovation, and strategy for electric transportation, including how TVA can help remove market barriers to adoption of EVs while contributing to TVA's public mission of energy, environment, and economic development. Ryan leads research in the areas of EV adoption forecasting, medium- and heavy-duty fleet electrification, vehicle-to-grid technologies, and

emerging partnership opportunities with stakeholders.

Prior to joining TVA, Ryan led electric vehicle strategy and initiatives for the State of Tennessee's DOE-funded State Energy Office, at the Tennessee Department of Environment and Conservation (TDEC). While at TDEC, Ryan spearheaded new partnerships and initiatives to promote electric transportation for the State, including 1) a first-of-its-kind partnership with EV manufacturer Rivian to install over 100 EV chargers at all 56 Tennessee State Parks, 2) the establishment of Drive Electric TN, and 3) a partnership with TVA to jointly fund a statewide EV fast charging network to triple the State's number of existing DC fast chargers by adding 40 new locations.

Previously, Ryan spent a decade in the private sector working in the fields of software, smart cities, energy efficiency, and microgrids. Originally from the Pacific Northwest, Ryan earned his B.S. in general engineering from Gonzaga University and resides in Nashville.

NC A&T State University

Team Report

North Carolina A&T State University (NCAT)-Semi Annual Report Nov 1

- PIs at NCAT organized a workshop on IoT .

Hybrid IoT Security Workshop

On Friday, September 23, 2022, at 9:00am to 2:30pm, North Carolina A&T State University Center for Cyber Defense (CCD) and the University of Memphis Center for Information Assurance (CfIA) collaboratively hosted a hybrid workshop on IoT Security. The workshop was conducted in-person in the Cyber Defense and AI Lab, room 371, in the Harold L. Martin Sr. Engineering Research & Innovation Complex (ERIC) and broadcasted live on Zoom to the registered virtual audience. The workshop had a combined attendance of 102 participants with 50 in-person attendees and 52 virtual attendees. The Hybrid IoT Security Workshop had the honor of having immaculate and distinguished guest speakers and scholars in attendance. Attendees and registrants of the workshop were local, statewide, and afar from the North Carolina A&T State University, University of Memphis, University of North Carolina Wilmington, Radford University, Fayetteville Technical Community College, University of West Florida, Wallace State Community College, Augusta Technical College, Clark Atlanta University, Talladega College, and Medical University of South Carolina.

Workshop Agenda and Detail Report are attached.

- A graduate student is conducting research on IoT security.

Hybrid IoT Security Workshop Report

North Carolina Agricultural and Technical State University Center for Cyber Defense (CCD)

University of Memphis Center for Information Assurance (CfIA)

Academic Year 2022-2023 | Fall Semester 2022

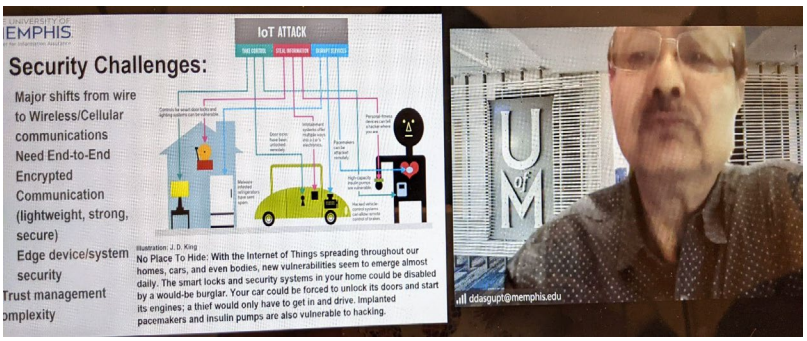
Hybrid IoT Security Workshop Report

On Friday, September 23, 2022, at 9:00am to 2:30pm, North Carolina A&T State University Center for Cyber Defense (CCD) and the University of Memphis Center for Information Assurance (CfIA) collaboratively hosted a hybrid workshop on IoT Security. The workshop was conducted in-person in the Cyber Defense and AI Lab, room 371, in the Harold L. Martin Sr. Engineering Research & Innovation Complex (ERIC) and broadcasted live on Zoom to the registered virtual audience. The workshop had a combined attendance of 102 participants with 50 in-person attendees and 52 virtual attendees. The Hybrid IoT Security Workshop had the honor of having immaculate and distinguished guest speakers and scholars in attendance. Attendees and registrants of the workshop were local, statewide, and afar from the North Carolina A&T State University, University of Memphis, University of North Carolina Wilmington, Radford University, Fayetteville Technical Community College, University of West Florida, Wallace State Community College, Augusta Technical College, Clark Atlanta University, Talladega College, and Medical University of South Carolina.

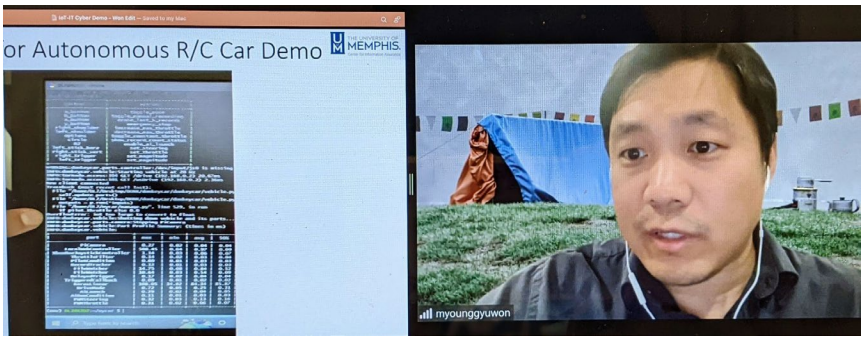
Prior to the day of the Hybrid IoT Security Workshop, flyers were sent out with the registration link and Zoom details to advertise, entice, and garner interest. The workshop was extremely informational and successfully highlighted IoT Security by each presenter and research teams. The workshop's agenda covered opening

remarks, meet and greet, invited talks, hands-on presentations, hands-on tutorial demonstrations, complimentary lunch for in-person attendees, and closing remarks. Starting at 9:00am, Dr. Kaushik Roy, Director of the Center for Cyber Defense and NC A&T Professor and Interim Chair in the Department of Computer Science, opened with welcome remarks. Followed right after, Dr. Salil Desai, NC A&T Distinguished Professor in the Department of Industrial & Systems Engineering, and Director of the Center of Excellence in Product Design and Advanced Manufacturing (CEPDAM), introduced himself and shared remarks to kickstart the meet and greet segment of the workshop.

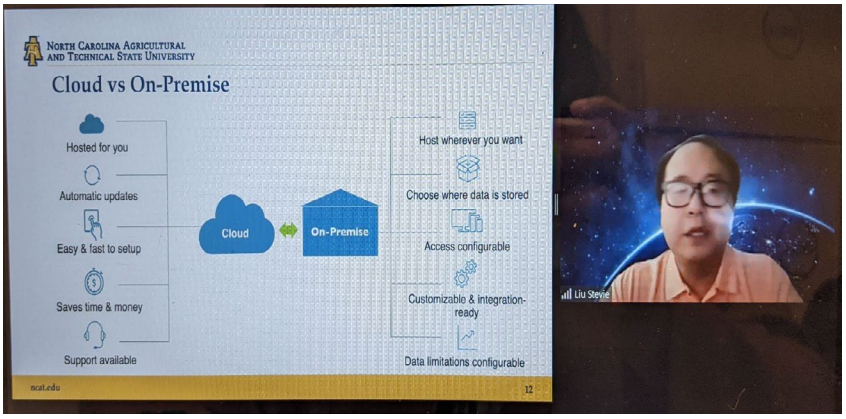
At 9:30am, the first invited talk on IoT Security Issues and Domain-Specific Defense Strategies was given by Dr. Dipankar Dasgupta, Director of the Center for Information Assurance, IEEE Fellow, and Professor of Computer Science at the University of Memphis. Dr. Dasgupta enlightened the audience on the evolution of IoTs, technology integration, IoT security issues, and defense strategies. After his presentation, Dr. Dasgupta listened and answered all the questions posed by some participants. The second invited talk on IoT Cyber Security Programming Project Development, started at 10:00am and was presented by Dr. Myounggyu Won, Director of the Connected Smart Sensor Systems (CS^3) Lab and Assistant Professor in the Department of Computer Science at the University of Memphis. Dr. Won displayed a video demonstration by their IoT Security Project team member, Nathan Farrar, on



Brute Force Password Attack Using Buffer OverFlow on an ESP32 Board Light Controller using Bluetooth Connection. Dr. Won explained what was taking place in the demonstration, provided a close-up of the code on password check, pin checker, and the light controller. Dr. Won also played an Autonomous R/C Car video demonstration and shared a close-up of the cybersecurity code behind it. After presenting, students briefly asked questions, in which Dr. Won happily responded.



At 10:30am, a hands-on presentation on On-Prem and Cloud-Enabled IDS for IoT using Machine Learning was given by Dr. Zhipeng “Nicholas” Liu, a Senior AI/ML Engineer at Fidelity Investments. Dr. Nicholas engagingly informed the audience of escalating cyber threats and threats to user privacy as it relates to IDS for IoT using Machine Learning, the pros, cons, and differences between On-Prem and Cloud-Enabled. He then instructed a live hands-on exercise on Anomaly Detection with Deep Learning Techniques. Both in-person and virtual attendees were able to participate in this hands-on demonstration. Dr. Nicholas, as well, answered questions from the participating audience. After Dr. Nicholas's presentation was concluded at 11:30am, the workshop adjourned for a lunch intermission from 11:30am to 1:00pm. Lunch

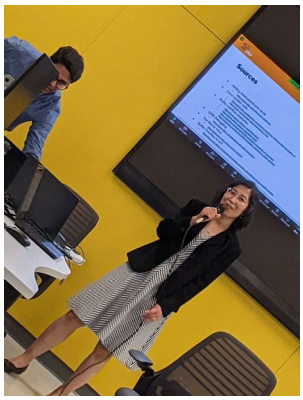


vouchers were handed out to all in-person attendees including students, faculty, and staff. Lunch was served in the conference room.

Once the workshop resumed from lunch at 1:00pm, in-person and virtual participants listened in as Dr. Daniel Limbrick, Director of the Automated Design for Emerging Processing Technologies (ADEPT) Laboratory and Associate Professor in the Electrical and Computer Engineering Department at NC A&T State University introduced his ADEPT Laboratory Research Team of presenters on the Tutorial on How to be an IoT Hacker. The first team member to present was Yohannes Bekele, a 4th Year PhD Student, on How to connect a Raspberry Pi and Arduino to the Internet of Things. Followed by Cebron Williams, a 1st Year Master's Student, on How to run

IoT software on Raspberry Pi and Arduino. Lastly, the final presenting team member, Deriech Cummings, a Senior Undergraduate Student, demonstrated his topic on How to perform a Buffer Overflow on IoT Devices. The ADEPT Research Team answered questions on their presentation and shared insights on related courses to peer participants interested in in-depth learning of their research.

At 2:15pm, all presentations were completed and closing remarks began. Closing remarks and recognitions were given by Dr. Kaushik Roy, and Dr. Xiaohong "Dorothy" Yuan, Professor in the Department of Computer Science at NC A&T State University. Dr. Roy and Dr. Yuan thanked everyone for joining virtually and attending in-person. All participants were thankful to the presenters for the information they gained from the workshop. The workshop successfully concluded at 2:30pm.



Acknowledgements

Special thanks and recognition to everyone involved in making the Hybrid IoT Security Workshop a success! To the speakers and presenters: Dr. Kaushik Roy, Dr. Salil Desai, Dr. Dipankar Dasgupta, Dr. Myounggyu Won, Dr. Nicholas Liu, Dr. Daniel Limbrick, Yohannes Bekele, Cebron Williams, Deriech Cummings, and Dr. Dorothy Yuan. To each research team members who contributed to the research that were presented, the University of Memphis IoT Security Project Team Members: Nathan Farrar, Andrika Cheairs, Hans Amelang, Adam Kharsa, William Richards, Luke Carrington, Tony Pinson, and Ken Schnarrs; and the NC A&T ADEPT Laboratory Research Team Members: Judith Hernandez-Campillo, Dawood Rauf, Deriech Commings, Yohannes Bekele, and Cebron Williams.

To the planning committee and members involved in all the behind the scenes, logistics and coordination of the workshop, Dr. Kaushik Roy, Dr. Salil Desai, Dr. Dorothy Yuan, Dr. Dipankar Dasgupta, Dr. Kelvin Bryant, Associate Professor in the Department of Computer Science at NC A&T State University, Mr. Edmundson Effort, IT Analyst and Adjunct Professor in the Department of Computer Science at the NC A&T State University, Ms. Bianca Govan, Research Associate for the NC A&T State University Center for Cyber Defense, Mr. Tony Pinson, Project Coordinator I for the University of Memphis Center for Information Assurance, and Ms. Rosemary Williams, Administrative Support Specialist & Student Services Coordinator at NC A&T State University.

Comments & Feedbacks

Participants enjoyed, learned, and benefited from this joint effort put together by the CCD and CfIA. Feedbacks to consider for future hybrid events are having or using integrated sound systems. Expressed by some virtual attendees, the sound quality during opening remarks could

have been a bit clearer. Some virtual attendees described the audio of in-person participants, during parts of the morning session of the workshop, as a little muffled. Overall, all attendees were enlightened and engaged. Each presenter provided useful knowledge on IoT Security, their expertise, and the correlation of their experiences within the real world from past to present, and hopeful technological advancements and improvements for the future.

WELCOME

IoT SECURITY HYBRID WORKSHOP

HAROLD L. MARTIN SR. ENGINEERING RESEARCH & INNOVATION COMPLEX

WORKSHOP'S AGENDA

FRIDAY, SEPTEMBER 23, 2022

9:00-9:30AM - Opening Remarks/Meet and Greet

9:30-10:30AM - Invited Talk by Dr. Dipankar Dasgupta
IoT Security Issues and Domain-Specific Defense Strategies

10:30-11:30AM - Hands-On Presentation by Dr. Zhipeng (Nicholas) Liu
On-Prem and Cloud-Enabled IDS for IoT using Machine Learning

11:30-1:00PM - Lunch Break

1:00-2:00PM - Hands-On Tutorial on How to be an IoT Hacker
Student Presentation: Yohannes Bekele, Judith Hernandez-Campillo, Cebron Williams, & Deriech Cummings

2:00-2:30PM - Closing Remarks

A Virtual Workshop on AI-enhanced IoT Security (AI Meets IoT) Report

North Carolina Agricultural and Technical State University Center for Cyber Defense (CCD)

University of Memphis Center for Information Assurance (CfIA)

Academic Year 2023-2024 | Fall Semester 2023

A Virtual Workshop on AI-enhanced IoT Security Report

(AI Meets IoT)

On Friday, October 27th, 2023, from 10:00 am to 2:00 pm, the North Carolina A&T State University (NC A&T) Center for Cyber Defense (CCD) and the University of Memphis (UofM) Center for Information Assurance (CfIA) joined forces to coordinate a virtual workshop on AI-enhanced IoT Security. The virtual workshop was hosted on the Zoom platform, which participants pre-registered to attend. The AI Meets IoT workshop had 53 attendees, of whom were local, statewide, and from far away. The AI-enhanced IoT Security Workshop had the honor of having prestigious guest attendees and registrants from North Carolina A&T State University, the University of Memphis, Piedmont Community College, Blue Ridge Community College, Wake Technical Community College, and Capitol Technology University.

Flyers, email blasts, webpage announcements, department big-screen displays, and word-of-mouth were the different forms of advertisements used to promote the virtual AI-enhanced IoT Security Workshop. All advertisements included the workshop's QR Code and registration link. The workshop was highly enlightening as each speaker highlighted topics related to AI Meets IoT and its securities. The agenda comprised welcome and opening remarks, expert-invited talks, demo-video presentations, student research presentations and results, and closing remarks. Starting promptly at 10:00 am, Dr. Kaushik Roy, Director of the Center for Cyber Defense and NC A&T Professor and Chair of the Department of Computer Science, opened with welcome remarks and the introduction of our speakers. At 10:10 am, the first invited talk on Cyber Threats Early Warning Framework for Operational Technology Systems was given by Dr. Sajad Khasandro, a distinguished NC A&T Assistant Professor of Computer Science. The second invited talk was on the Role of AI in IoT Security by Dr. Dipankar Dasgupta. Dr. Dasgupta is the

Director of the Center for Information Assurance, an IEEE Fellow, and a well-renowned Professor of Computer Science at the University of Memphis.

The third speaker, Dr. Mohd Hasan Ali, a UofM Associate Professor of Electrical and Computer Engineering, gave an invited talk on Cybersecurity Issues and Solutions to Distributed Energy Resources. Following his great presentation was a fourth invited talk by Dr. Myounggyu Won, another adept UofM Assistant Professor of Computer Science. Dr. Won's invited talk was on Cybersecurity Education for High School Students Using Autonomous R/C Cars. Elaborating further on Dr. Won's topic with a demo presentation, was one of his student research assistants, Nathan Farrar. Mr. Farrar is a UofM IoT Security Project Team Member. His presentation and demo video were on Dynamic Wireless Charging: Cyber Security and the Future of EV Charging. From NC A&T Center for Cyber Defense, Steve Chesney was the second student research assistant to present. His presentation was on his research topic entitled Cyber-Attack Analysis for LoRaWAN Smart IoT Networks.

Thirdly, Subhram Dasgupta, an NC A&T Center for Cyber Defense research assistant, gave an in-depth analysis of his presentation on Deepfake Detection. The fourth student research assistant was Camila Gaitan-Cardenas, a member of the NC A&T Center for Cyber Defense. Her presentation was on Explainable Machine Learning-based Intrusion Detection Systems for Cloud and IoT. Likewise, Sesan Akintade, an NC A&T Center for Cyber Defense research assistant, presented his research on Explainable Artificial Intelligence and Features Selection in Cybersecurity. The final speaker of the AI Meets IoT virtual workshop was the revered NC A&T Assistant Professor of Computer Science, Dr. Olusola Odeyomi. He concluded with his invited talk on Differential Privacy from Theory to Practice.

Overall, the workshop was a great success. Each presenter provided useful knowledge on AI-enhanced IoT Security, their expertise, the correlation of their experiences within the real world from past to present, and new research and technological findings for areas of improvement for the future. The workshop's speakers all captivated the audience with their super informative and extensive research on AI in IoT, the evolution of IoTs, explainability, IoT security issues, intrusion detection, cybersecurity defense strategies, and much more. After each presentation, each speaker listened and answered questions posed by inquiring participants. Participants were able to engage and network with each speaker. Lastly, Dr. Roy adjourned the workshop at 2:03 pm after giving the closing remarks and thanking all the speakers and attendees.

Acknowledgments

Special thanks and recognition to everyone involved in making the AI-enhanced IoT Security Workshop a success! To the speakers, research student presenters, and chairperson: Dr. Kaushik Roy, Dr. Sajad Khasandro, Dr. Olusola Odeyomi, Dr. Dipankar Dasgupta, Dr. Mohd Hasan Ali, Dr. Myounggyu Won, Nathan Farrar, Steve Chesney, Subhram Dasgupta, Camila Gaitan-Cardenas, and Sesan Akintade, we thank you for contributing your time and research. To the planning committee and members involved behind the scenes with coordinating the workshop, Dr. Kaushik Roy, Dr. Dipankar Dasgupta, Mr. Tony Pinson, Project Coordinator I for the University of Memphis Center for Information Assurance, Ms. Bianca Govan, Program Manager for the NC A&T State University Center for Cyber Defense, and Ms. Rosemary Williams, Administrative Support Specialist & Student Services Coordinator at NC A&T State University, we thank you for your time and commitment of organizing and distributing flyers for the workshop.

Comments & Feedback

Participants engaged, learned, enjoyed, and benefited from this CCD and CfIA collaboration. Feedback to consider for future virtual events is having or using tools that allow hands-on or interactive demonstrations. Although it was a virtual experience, our goal is to always maintain a space where participants do not feel like they are attending a lecture but are engaged throughout.

University of Memphis

A Virtual Workshop on AI-enhanced IoT Security Agenda
Friday, October 27, 2023

North Carolina A&T State University

TIME	SPEAKER	PRESENTATION TITLE
10 - 10:10AM	Dr. Kaushik Roy, Director of the NC A&T Center for Cyber Defense	Welcome & Open Remarks
10:10 - 10:40	Dr. Sajad Khasandro, NC A&T Assistant Professor of Computer Science	Cyber Threats Early Warning Framework for Operational Technology Systems
10:40 - 11:10	Dr. Dipankar Dasgupta, IEEE Fellow & UofM Professor of Computer Science	Role of AI in IoT Security
11:10 - 11:40	Dr. Mohd Hasan Ali, UofM Associate Professor of Electrical and Computer Engineering	Cybersecurity Issues and Solutions to Distributed Energy Resources
11:40 - 12:10	Dr. Myounggyu Won, UofM Assistant Professor of Computer Science	Cybersecurity Education for High School Students Using Autonomous R/C Cars
12:10 - 12:25	Nathan Farrar, UofM IoT Security Project Team Member	Dynamic Wireless Charging: Cyber Security and the Future of EV Charging
12:25 - 12:40	Steve Chesney, NC A&T Center for Cyber Defense Research Assistant	Cyber-Attack Analysis for LoRaWAN Smart IoT Networks
12:40 - 12:55	Subhram Dasgupta, NC A&T Center for Cyber Defense Research Assistant	Deepfake Detection
12:55 - 1:10	Camila Gaitan-Cardenas, NC A&T Center for Cyber Defense Research Assistant	Explainable Machine Learning-based Intrusion Detection Systems for Cloud and IoT
1:10 - 1:25	Sesan Akintade, NC A&T Center for Cyber Defense Research Assistant	Explainable Artificial Intelligence and Features Selection in Cybersecurity
1:25 - 1:55	Dr. Olusola Odeyomi, NC A&T Assistant Professor of Computer Science	Differential Privacy from Theory to Practice
1:55 - 2PM	Dr. Kaushik Roy, Director of the NC A&T Center for Cyber Defense	Closing Remarks

The Citadel College

Team Report

Quarterly Report for NCAE001-2021

The Citadel

Team:

- Dr. Shankar Banik (Principal Investigator)
  Professor and Head of Department
  Department of Cyber and Computer Sciences

- Dr. Melissa Graves (Co-principal Investigator)
  Assistant Professor
  Department of Intelligence and Security Studies

- Dr. Aleksandra Scalco (Research Associate)
  Adjunct Professor
  Department of Cyber and Computer Sciences

- Ms. Malory Saunders-Gooding (Project Coordinator)
  Project Coordinator
  Department of Cyber and Computer Sciences

Key Objectives:

- Develop Inter-disciplinary course modules for Cyber Protection for Critical Infrastructures.
- Design Case Scenarios for Cyber Tabletop exercises for Critical Infrastructure Protection.
- Organize workshops to share the course modules and run Cyber Tabletop Exercises for Critical Infrastructure Protection.
- Participate in the dissemination of research findings, including publications and conferences.

Task Completed:

- Identified two existing courses and one new course that will be used for including modules on cyber protection for critical infrastructure
  - CSCI 227: Principles and Practices in Cybersecurity
    - Required for all Cyber Operations and Intelligence and Security Studies majors
  - INTL 465: Special Topics in Critical Infrastructure Protection
    - An elective for Intelligence and Security Studies majors
  - CSCI 490/690: Special Topics on Cybersecurity for Industrial Control Systems
    - An elective for undergraduate students
    - An elective for graduate students
- Developed Course Modules for INTL 465

    - Drafted a sample syllabus
    - Developed PPT Slides on different topics
    - Drafted Pre-test and Post-test assessment documents
- Developed a new course on Cyber Physical Systems
    - Cyber Awareness in Control Systems
    - Managing Risks in Cyber Physical Systems
    - Cyber Resiliency for Control Systems
    - Case Scenarios
- Developed Case Scenarios with different sectors of Critical Infrastructures
    - Developed short-term scenarios
    - Developed long-term scenarios
    - Drafted discussion questions for each scenario
- Hosted a Workshop on Cyber Education for Critical Infrastructure Protection (CECIP) on Oct 19-20, 2023
    - Keynote Speakers from Naval Information Warfare Center (NIWC), Cybersecurity and Infrastructure Security Agency, and South Carolina Law Enforcement Divion (SLED)
    - Presentations from faculty on courses that were developed as part of this grant
    - Presentations from students on course projects on Critical Infrastructure Protection
    - Exercise for Case-Scenario based on Cyber Incidents in Critical Infrastructure
    - Fireside Chat to discuss the gaps in Cyber Education for Critical Infrastructure Protection
    - Number of attendees: 40

Work in progress:

- Planning to upload the course modules in CLARK
- Planning to host a Workshop on Cyber Protection for Critical Infrastructure in Fall 2024
- Planning to host a Cyber Table Top Exercises with different sectors of Critical Infrastructure in South Carolina

Cybersecurity Education and Critical Infrastructure Protection Workshop
CECIP at The Citadel Final Report
October 19-20, 2023

Date and Venue:

The Department of Cyber and Computer Sciences at The Citadel was honored to host CECIP Workshop 2023 on October 19-20, 2023, in the Swain Boating Center (The Citadel campus) in Charleston, SC. The CECIP Planning Committee arrived at the venue on October 18, 2023, to run a sound check and to ensure that the room setup was completed properly in the main room and in the conference room. Follow ups with the catering vendor (Sodexo) were performed the week prior to confirm pre-arranged breakfast and lunch would be available for all CECIP guests. *Our team also requested special dietary needs be accommodated by Sodexo as indicated by attendees during the registration phase*.

A discounted hotel room rate was offered to guests traveling to Charleston for the event, and a $1,000.00 travel stipend was offered to out-of-town attendees as well (upon request and based on budget availability).

Summary:

Over the course of 1.5 days, the CECIP Workshop at The Citadel welcomed four keynote speakers from Naval Information Warfare Center (NIWC) Atlantic, Cybersecurity and Infrastructure Security Agency (CISA), Dragos/The Citadel, and South Carolina Law Enforcement Division (SLED). Our team was also proud to introduce eight presentations on topics such as *Cyber Physical Systems, Cyber Protection for Critical Infrastructure, and Cybersecurity Education for High School Students*. The CECIP Workshop also invited 18 Citadel Cyber Cadets to participate in a DECIDE Exercise, which ran parallel to the afternoon session on Day 1 of the workshop. This DECIDE Exercise, hosted by Norwich University Applied Research Institute (NUARI), allowed the student participants to apply their incident response skillset to a real-life cyber case scenario related to Critical Infrastructure. CECIP Workshop attendees were invited to observe the Exercise throughout the afternoon, as the schedule allowed. Finally, the CECIP Planning Committee also coordinated a "Fireside Chat" between Dr. Shankar Banik and Dr. Csilla Farkas regarding *Gaps in Cyber Education for Protecting Critical Infrastructure*. The full workshop agenda can be found in the pages below.

Attendee count*:* Approximately 40

CECIP at The Citadel Planning Committee: Dr. Shankar Banik, Head of Department, Cyber and Computer Sciences, The Citadel and Ms. Malory Saunders-Gooding, Project Coordinator, Department of Cyber and Computer Sciences, The Citadel

Thursday, October 19th: Day 1

The Citadel
Swain Boating Center (11 Hammond Ave.)

7:30 AM to 8:30 AM	**Registration / Continental Breakfast**
8:30 AM to 8:45 AM	**Welcome Address** ***Dr. Shankar Banik, Director, Citadel DoD Cyber Institute Professor and Head of Dept. of Cyber and Computer Sciences, The Citadel*** **Workshop Logistics** ***Ms. Malory Saunders-Gooding, Project Coordinator, Citadel DoD Cyber Institute/Dept. of Cyber and Computer Sciences, The Citadel***
8:45 AM to 9:30 AM	**Keynote Address / Q&A** *(Introduced by Dr. Shankar Banik)* ***Mr. Rich Scalco, MOSAICS CyberSHIELD Technical Manager, Senior Cyber Engineer, Naval Information Warfare Center (NIWC) Atlantic***
9:30 AM to 9:45 AM	**Break**
9:45 AM to 10:30 AM	**Course on Cyber Physical Systems** ***Dr. Aleksandra Scalco, Adjunct Professor, Dept. of Cyber and Computer Sciences, The Citadel***
10:30 AM to 11:15 AM	**Course on Critical Infrastructure** ***Dr. Melissa Graves, Associate Professor and Interim Head of Dept. of Intelligence and Security Studies, The Citadel***
11:15 AM to 12:00 PM	**Hosting a DECIDE Exercise for Case-Scenarios Based on Cyber Incidents** ***Mr. Tom Muehleisen, Director of Exercises, Norwich University Applied Research Institute (NUARI)***
12:00 PM to 1:00 PM	**Lunch and Networking**
***1:00 PM to 4:00 PM**	***NUARI DECIDE Exercise (Swain Boating Conference Room)*** ***Students Only**

1:00 PM to 1:45 PM	**Explainable AI-based Intrusion Detection Systems for Cloud and IoT** *Ms. Maria Camila Gaitan-Cardenas, PhD Computer Science Student, North Carolina A&T University*
1:45 PM to 2:30 PM	**RL-FL Based Intrusion Detection System in an Enterprise Network** *Dr. Pratap Sahu, Assistant Professor, Dept. Math and Computer Science, Claflin University*
2:30 PM to 2:45 PM	**Break**
2:45 PM to 3:30 PM	**Capstone Project: Cyber Protection for Critical Infrastructure** *Cadets William Hall and Zachary Schellinger, The Citadel*
3:30 PM to 4:15 PM	**Keynote Address / Q&A** *(Introduced by Dr. Shankar Banik)* *Mr. Julius Gamble, Regional Director (Region 4), Cybersecurity and Infrastructure Security Agency (CISA)*

Friday, October 20th: Day 2

The Citadel
Swain Boating Center (11 Hammond Ave.)

8:00 AM to 9:00 AM	**Continental Breakfast**
9:00 AM to 9:45 AM	**OT Cyber Risk and Defense Recommendations for the Water & Wastewater Industry** *Dr. Jacob Benjamin, Professor of Practice, Dept. of Cyber and Computer Sciences, The Citadel*
9:45 AM to 10:30 AM	**NERC-CIP Compliance and Auditing** *Dr. Guillermo Francia III, Director, Research and Innovation, University of West Florida Center for Cybersecurity*
10:30 AM to 10:45 AM	**Break**
10:45 AM to 11:30 AM	**Cybersecurity Education for High School Students Using Autonomous R/C Cars** *Dr. Myounggyu Won, Assistant Professor, Dept. of Computer Science, University of Memphis*
11:30 AM to 12:30 PM	**Lunch**

	Fireside Chat: **Gaps in Cyber Education for Protecting Critical Infrastructure** ***Panelists: Dr. Shankar Banik, The Citadel*** ***Dr. Csilla Farkas, University of South Carolina*** ***Moderator: Ms. Malory Saunders-Gooding, The Citadel***
12:30 PM to 1:15 PM	**Keynote Address / Q&A** *(Introduced by Dr. Shankar Banik)* ***Ms. Caitlin Scroggins, Program Coordinator, South Carolina Critical Infrastructure Cybersecurity (SC CIC) Program***
1:15 PM to 1:30 PM	**Concluding Remarks** ***Dr. Shankar Banik, Director, Citadel DoD Cyber Institute*** ***Professor and Head of Dept. of Cyber and Computer Sciences, The Citadel***

University of West Florida

Team Report

University of West Florida
UWF-IRSC CECIP Project
Progress Report
Updates: April 4, 2022, May 15, 2022, November 7, 2022, February 14, 2023, April 30, 2023, July 3, 2023, December 4, 2023

Submitted by: *Dr. Guillermo Francia, III, PI for UWF*
Email: *gfranciaiii@uwf.edu*

Project Objectives

The project objectives are:

1) To design and develop four courses related to the protection of our critical infrastructures. These courses are Industrial Control Systems and Renewable Energy (ICS-RE) Security, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) Compliance, Cybersecurity Maturity model Certification (CMMC) Compliance, and ICS-RE Threat Intelligence;
2) To design and develop tabletop exercises and laboratory hands-on activities to support the four courses;
3) To offer a certificate-based workforce development program consisting of the above four courses with verifiable digital credentials for the specific cybersecurity work roles in critical infrastructures with emphasis on transitioning military personnel, transitioning first responders and other qualified adult learners;
4) To evaluate the effectiveness of the four courses; and
5) To disseminate the course materials for widespread adoption.

Key Outcomes and Major Activities

A. Four workforce development courses are currently being designed and implemented by the project personnel. The courses are described below and offered on the specified dates.

1. ICS-RE Security (at UWF)
Date Offered: May 16-27, 2022
Instructors: Dr. Guillermo Francia, III (UWF)
Dr. Tarek Youssef (UWF)
Dr. Kevin Cooper (IRSC)
Mr. Steven Nicholson (IRSC)
Participants: **15** Veterans, First Responders, Professionals, Adult-learners
Course Content:

- Models and Types of Industrial Control Systems
- Industrial Control Systems Hardware
- Industrial Control Systems Network and Protocols: Modbus, Profibus, DNP3, Ethernet/IP
- Control Logic Software Development: Models, Ladder Logic
- Human Machine Interface Development

- Industrial Control Systems Security: Reconnaissance, Vulnerability Assessment,
- Penetration testing, Intrusion Detection, Firewalls
- Renewable Energy (RE) Systems, Distributed Energy Resources, RE Security

2. Cybersecurity Maturity Model Certification (CMMC) (at UWF)
Date Offered: June 13-24, 2022
Instructors: Guy Garrett (UWF)
Adjunct
Participants: **15** Veterans, First Responders, Professionals, Adult-learners
Course Content:

a. Introduction to CMMC: CUI and FOUO, APTs and FCI, Purpose of the CMMC,
CMMC Models, Levels and Domains, CMMC process Maturity, CMMC capabilities, processes, and practices, Preparation for CMMC

b. CMMC Process Implementation: Addressing the 3 tenets of Security (CIA) and
Safety, Cybersecurity Controls, DFARS, CMMC Requirements, Control Source Mapping: NIST SP800-171, CIS Controls, NIST SP 800-53 Rev 4, UK NCSC Cyber
Essentials, CERT RMM, Establishing the CMMC Team (Internal and External), CMMC Evidence Collection, Readiness Assessment, Security in Depth

c. CMMC Domain details: Access Control, Asset Management, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Recovery, Risk Management, Security Assessment, Situational Awareness, System and Communication Protection, System and Information Integrity

d. Hands-on exercises, case studies, and quizzes on CMMC

3. NERC-CIP Standards and Compliance (at UWF)
Date Offered: August 01-12, 2022
Instructors: Dr. Guillermo Francia, III (UWF)
Dr. Kevin Cooper (IRSC)
Mr. Steven Nicholson (IRSC)
Participants: Veterans, First Responders, Professionals, Adult-learners
Course Content:

A. CIP Standards

- BES (Bulk Electric System) Cyber System Categorization
- Security Management Controls
- Personnel and Training
- Electronic Security Perimeters
- Physical Security of BES Cyber Systems

- System Security Management
- Incident Reporting and Response Planning
- Recovery Plans for BES Cyber Systems
- Configuration Change Management and Vulnerability Assessment
- Information Protection
- Supply Chain Risk Management
- Physical Security

B. **Model**

NERC Functional Model

C. Hands-on exercises, case studies, and quizzes on NERC-CIP

4. ICS-RE Threat Intelligence (at UWF)

Date offered: August 22-26, 2022
Instructors: Dr. Tirthankar Ghosh (UWF)
Dr. Guillermo Francia, III (UWF)
Participants: **15** Veterans, First Responders, Professionals, Adult-learners
Course Content:

- Fundamentals of Threat Intelligence (TI) and Threat Modelling (TM)
- Threat Intelligence Sources
- Open-Source Threat Intelligence Tools
- Consuming Threat Intelligence
- Threat Intelligence at the Strategic, Operational, and Tactical levels
- Threat Intelligence Applied to ICS and Renewable Energy Security
- Hands-on exercises, case studies, and quizzes on TI and TM on ICS and RE Security

5. ICS-RE Security (at UWF)

Date Offered: October 22-November 6, 2022
Instructor: Dr. Guillermo Francia, III (UWF)

Participants: **9** Veterans, First Responders, Professionals, Adult-learners
Course Content:

- Models and Types of Industrial Control Systems
- Industrial Control Systems Hardware
- Industrial Control Systems Network and Protocols: Modbus, Profibus, DNP3, Ethernet/IP
- Control Logic Software Development: Models, Ladder Logic
- Human Machine Interface Development
- Industrial Control Systems Security: Reconnaissance, Vulnerability Assessment,
- Penetration testing, Intrusion Detection, Firewalls
- Renewable Energy (RE) Systems, Distributed Energy Resources, RE Security

B. Faculty Development Workshop (at UWF)
B.1 Date Offered: June 28-30, 2022
Participants: **21** College Faculty from across the USA

B.2 Date Offered: August 15-17, 2022
Participants: **9** College Faculty from across the USA

Completed the 2nd and 3rd Faculty Development workshops on Cybersecurity Scenario building. Introduced the use of Docker containers to build a simulated ICS-SCADA system for system reconnaissance and penetration testing. Covered the ICS MITRE ATT&CK Framework. There were 21 Faculty members from across the USA who participated.

C. Dr. Kevin Cooper (IRSC) presented a talk titled "The Convergence of Cyber Curriculum Across All Disciplines: The Critical Infrastructure Study."
Date: September 7, 2022
Participants: 20 Faculty + Students

The talk covered the importance of the NERC-CIP Standards and hosted by NCyTE.

D. Five academic courses were impacted through the infusion of the learning modules from the four workforce development courses. Each of these impacted courses are described below.

1. ETI 1701 Industrial Safety (at IRSC)
Date offered: Summer 2022
Instructors: Dr. Kevin Cooper (IRSC)
Participants: College Students

2. ETP 2930 Special Topics in Power Plant Technology (at IRSC)
Date offered: Summer 2022
Instructors: Dr. Kevin Cooper (IRSC)
Participants: College Students

3. ETS 2530 Process Control Technology (at IRSC)
Date offered: Spring 2023
Instructors: Dr. Kevin Cooper (IRSC)
Participants: College Students

4. EEL 4276/EEL 5277 Cyber Security of Industrial Control Systems (at UWF)
Date offered: Fall 2022
Instructors: Dr. Tarek Youssef (UWF)
Participants: College Students (30 Undergraduate + 3 Graduate)

5. CIS 4385 Ethical Hacking and Penetration Testing (at UWF)
Date offered: Fall 2022
Instructors: Anthony Pinto (UWF)

Participants: College Students (40)

6. ETP 2410 Solar Photovoltaic Systems (at IRSCC)
Date offered: Spring 2023 (2/7/2023)
Instructors: Kevin Cooper
Participants: College Students (10)

7. CIS 4221 Ethical Hacking course (at UWF)—ICS Security
Date offered: Spring 2023 (4/24/2023)
Instructors: Guillermo Francia
Participants: College Students (40)

E. Credentialing in form of digital badges and certificates are awarded to each participant who successfully completed the courses offered by UWF. It is a major component of the workforce development activities. The system is built on the Badgr system that was adopted by an earlier workforce development project.

Media and Products Results
Course learning modules such as lectures, scenarios, and hands-on exercises are currently prepared to be disseminated to the CAE community using the CLARK course repository.

Project Personnel

Dr. Guillermo Francia, III	Project PI at UWF
Dr. Kevin Cooper	Project PI at IRSC
Dr. Eman El-Sheikh	Project co-PI at UWF
Dr. Tarek Youssef	Associate Professor at UWF
Guy Garret	Instructor at UWF
Anthony Pinto	Instructor at UWF
Steven Nicholson	Instructor at IRSC

F. Curriculum materials were submitted to the CLARK repository (Clark.center). Twenty-one (21) learning objects on ICS Security and Threats were vetted and released for public dissemination (see Table 1). Ten (10) learning objects on NERC-CIP Compliance are currently being edited and vetted for public release (see Table2).

Table 1. Released Learning Objects on ICS Security and Threats

Learning Object Name	Type	Date
Industrial Control Systems (ICS)-Renewable Energy (RE) Security	Course	December 2, 2023
Industrial Control Systems (ICS) Threat Intelligence	Unit	October 13, 2023
Fundamentals of Threat Intelligence (TI) and Threat Modeling (Module 1)	Module	October 13, 2023

Threat Intelligence Sources (Module 2)	Module	October 13, 2023
Open-Source Threat Intelligence Tools (Module 3)	Module	October 13, 2023
Threats in ICS Environment (Module 4)	Module	October 13, 2023
Threat Sharing (Module 5)	Module	October 13, 2023
Models and Types	Module	December 1, 2023
ICS Hardware	Module	December 1, 2023
ICS Net Protocols	Module	December 1, 2023
ICS Software	Module	December 1, 2023
HMI	Module	December 2, 2023
ICS Security Arch	Module	December 2, 2023
ICS Recon Pentest VA	Module	December 2, 2023
Fundamentals of Renewable Energy	Module	December 2, 2023
Control Systems RE	Module	December 2, 2023
RE Security	Module	December 2, 2023
ICS Threat Intel	Module	December 2, 2023
ICS Incident Response	Module	December 2, 2023
Security Auditing	Module	December 2, 2023
Compliance	Module	December 2, 2023

Table 2. Draft Learning Objects on NERC-CIP Compliance

Learning Object Name	Type	Date
NERC-CIP Compliance	Unit	October 24, 2023
NERC-CIP Module 1: Standards and Compliance	Module	October 24, 2023
NERC-CIP Module 2: CIP-004-6 and CIP-005-6	Module	October 24, 2023
NERC-CIP Module 3: CIP-006-6 and CIP-007-6	Module	October 24, 2023
NERC-CIP Module 4: CIP-008-6 and CIP-009-6	Module	October 24, 2023
NERC-CIP Module 5: CIP-010-3 and CIP-011-2	Module	October 24, 2023
NERC-CIP Module 6: CIP-012-3, CIP-013-1, and CIP-014-2	Module	October 24, 2023
NERC-CIP Module 7: Reliability Functional Model	Module	October 24, 2023
NERC-CIP Module 8: Standards Compliance	Module	October 24, 2023
NERC-CIP Module 9: NERC-NIST Cybersecurity Framework Mapping	Module	October 24, 2023

Appendix 2

UofM Hands-On Project Minutes

CFIA-Project Team Meeting

07/14/2022
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	**Type of meeting:**	Project Team
Facilitator:	Dr. Myounggyu Won	**Note taker:**	Debera Pittman
Called to Order:	12:30:00 pm	**Adjourned:**	1:00 pm

Attendees: Dr. Won, Dr. Dasgupta; Tony Pinson; Debera Pittman; Andrika Cheairs; Ken Schnarrs.

Minutes

Discussion:

Meeting Minutes – Did not have a meeting for July 7, 2022. CFIA (Center for Information Assurance) had an Ambassadors Tech Camp, on that day for high school students.

Discussion: Dr. Dasgupta discussed researchers being present at the meetings. This is very important to attend the meetings, so the researchers can explain their projects and give updates.

General Discussion – Dr. Won explained how Luke and Douglas have significantly improved the autonomous driving model. Now the R/C car can autonomously avoid obstacles (the cones) no matter where they are placed on the racing track. Luke and Douglas will work on running two R/C cars autonomously running simultaneously on the track.

Luke and Douglas will start brainstorming cybersecurity threats against the autonomous driving module and solutions (as cybersecurity projects for high school students) to defend against those threats. Ken arrived late in the meeting and had a discussion with the team.

Dr. Won reviewed the buffer overflow project that Ken suggested. Ken and Nathan will produce cybersecurity problems that affect the operation of the hardware components (such as LEDs, motors, Wi-Fi/Bluetooth modules) of the Arduino-based IoT system. Tony Pinson talked about a workshop that will be held in North Carolina at North Carolina A &T.

New Business:

Dr. Won would like Andrika and Ken to work on projects together. Dr. Won will have project ideas set up in the next meeting. The implementation of the projects will be started from there.

The meeting was adjourned at 1:00pm.

CFIA-Project Team Meeting

8/4/2022
12:00pm
Room 120
Dunn Hall- U of M

Meeting called by:	Debera Pittman	Type of meeting:	Project Team
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:10 pm	Adjourned:	1:00 pm

Attendees: Dr. Dasgupta, Dr. Won, Debera Pittman, Riley Morris, Andrika Cheairs, Tony Pinson, Hans Amelang, Nathan Farrar, Luke Carrington, Ken Schnarrs.

Minutes

Discussion:

The Project Team welcomed the new students, Riley Morris, and Hans Amelang.

General Discussion – Dr. Dasgupta discussed why there is the project meeting, so you can report to the team on how the projects are coming along. Dr. Won explained the two projects that the students are working on.

(1) Luke and Douglas have successfully confirmed that the buffer overflow attack can crash the autonomous R/C car software. They will extend this to develop cybersecurity programming projects.

(2) Ken, Nathan, and Andrika had difficulty in utilizing the Wi-Fi module. It was not able to connect to the University Wi-Fi network with the unauthorized Wi-Fi module. Therefore, we discussed some ideas to use either the local area network or a Bluetooth module instead of the Wi-Fi module.

(3) Ken, Nathan, and Andrika, after the discussion, talked about purchasing the Bluetooth module. They will also try using the local area network using a router available in the lab. They will report the progress next Thursday.

(4) Andrika expressed her interest in leading a cybersecurity project.

(5) Hans and Riley joined the project. They were briefed on the projects that our teams have worked on. They will be provided with basic materials on Arduino programming to build background to join our team.

New Business:

There will be updates on the projects.

The meeting was adjourned at 1:00pm.

CFIA – Project Team Meeting

08/11/2022

12:00pm

Room 120 Dunn Hall- UofM

Meeting called by:	Debera Pittman	**Type of meeting:**	CIFA- Project Team
Facilitator:	Dr. Myounggyu	**Note taker:**	Debera Pittman
Called to Order:	12:10pm	**Adjourned:**	1:00pm

Attendees: Dr. Won; Tony Pinson; Debera Pittman; Nathan Farrar; Riley Morris; Hans Amelang; Ken Schnarrs; Luke Carrington; Douglas Espinoza II.

Minutes

Discussion:

Meeting Minutes – The meeting minutes from the meeting held on August 4, 2022, were reviewed, and approved, as written.

General Discussion: Each project team shared information on their projects. Dr. Won discussed how the teams have made progress on their projects.

The R/C car team was successful in crashing the R/C car with the buffer overflow attack.

Dr. Won asked the R/C car team to draft manuals on (1) how to set the development environment in terms of both hardware and software, and (2) how to use the buffer overflow attack project to educate high school students on cybersecurity concepts.

The Arduino team is attempting to apply the buffer overflow attack example to a traffic light application.

The Arduino team successfully integrated a WI-FI module and can provide the user input wirelessly to the Arduino board via the Bluetooth interface.

The Arduino team is exploring another project related to hacking the WI-FI password and encryption/decryption techniques.

Tony Pinson attended workshop entitled: NCyTE Faculty Development Academy on Automobile Security - Pen Testing
The location and date: Mall of America in Minneapolis/St. Paul, MN area, the month of August 2022.

Synopsis: Workshop focused on using Raspberri PI and Kali-Linux Platform Tools to launch attacks against normal internal combustion engine automobile operation.

New Business:

There will be weekly updates on the projects.

Meeting was adjourned at 1:00 pm. Motion by Debera Pittman and seconded by Nathan Farrar.

CFIA-Project Team Meeting

09/01/2022
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	**Type of meeting:**	Project Team
Facilitator:	Dr. Myounggyu Won	**Note taker:**	Debera Pittman
Called to Order:	12:10:00 pm	**Adjourned:**	1:00 pm

Attendees: Dr. Myounggyu Won; Dr. Dipankar Dasgupta; Tony Pinson; Debera Pittman; Luke Carrington; Hans Amelang.

Minutes

Discussion:

Meeting Minutes – The meeting minutes from the meeting held on September 1, 2022, were reviewed, and approved, as written.

General Discussion –

The teams gave Dr. Won updates on their projects and how they are progressing.

Hans is building a replica of the traffic signal application using a ESP32 microprocessor, which is like an Arduino but has built in WIFI and Bluetooth capabilities. Hans is also working on the programming of the unit for the light cycle and its web functionality.

Nathan has started recording the video of the traffic application that Dr. Dasgupta requested and has completed the initial version.

Luke is working on the username/password crack project. He found a tool called Hydra and is learning about it.

Douglas is working on the Wed-UI-based buffer overflow attack project.

Dr. Dasgupta briefly discussed about two more projects maybe being funded, that will have something doing with the health care.

New Business:

There will be updates on the projects.

The meeting was adjourned at 1:00pm.

CFIA-Project Team Meeting

09/09/2022
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Team
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	**12:10:00 pm**	Adjourned:	**1:00 pm**

Attendees: Dr. Myounggyu Won, Dr. Dipankar Dasgupta; Tony Pinson; Debera Pittman; Hans Amelang; Luke Carrington; William Richards; Adam Kharsa.

Minutes

Discussion:

Meeting Minutes – The meeting minutes from the meeting held on September 1, 2022, are shared, and reviewed, as written.

Discussion: Dr. Dasgupta discussed researchers being present at the meeting and working on their projects. This is very important to attend the meetings, so the researchers can explain their projects and give updates to Dr. Won.

General Discussion – Dr. Won had a brief discussion with the Project Teams, to get and ideal how they are coming along on their projects.

Luke got the password cracking tool (Hydra) working. He is working on the documentation of the password cracking project for the R/C car.

Nathan has made the final edits to his video recording for demonstrating the traffic light application.

Hans is working on integrating the water pump module with the Arduino board.

William and Adam are new students participating in the R/C car cybersecurity project.

Luke gave learning materials to them to build background in the R/C car.

Douglas is working on modifying the WebUI of the donkey car platform to use it for the buff overflow project.

Dr. Won will order floor mats to rebuild the racing track.

Dr. Dasgupta would like for Hans Amelang to work on the lift project.

Tony Pinson talked about the IoT workshop with North Carolina AT&T/University of Memphis, that will be held on September 23, 2022. This will be a virtual workshop and registration is still available.

Dr. Dasgupta briefly gave information about the Capstone Project.

New Business:

Dr. Won introduced the new students to the Project Team Meeting and what project they will be working on.

The meeting was adjourned at 1:00pm.

CFIA-Project Team Meeting

09/15/2022
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Team
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:10:00 pm	Adjourned:	1:00 pm

Attendees: Dr. Myounggyu Won, Debera Pittman; Tony Pinson; Nathan Farrar; Hans Amelang; Luke Carrington; William Richards; Adam Kharsa.

Minutes

Discussion:

Meeting Minutes – The meeting minutes from the meeting held on September 8, 2022, are shared, and reviewed, as written.

Discussion: Dr. Won had a brief discussion with the Project Teams.

General Discussion –

1. Luke has finalized the password cracking project. Luke is documenting the Chapter 5 of the R/C car cybersecurity project manual (upload on the shared drive). Luke is expected to finish Chapter 5 of the manual.
2. Adam and William reviewed the donkey car tutorial and have tested autonomous driving of the donkey car in a simulated environment. Luke has shown them how to train and operate the R/C car. Adam and William are expected to start hands-on programming work.
3. Nathan proposed an idea of extending his traffic light application with the Raspberry Pi and he also express his interests in a Smart Home project. I will review some papers on Smart Home Security and come up with a research project to work with him.
4. Hans mentioned some combability issue regarding integration of the “water pump” hardware module with the Arduino board. Hans is considering an alternative device that can be hooked with the board. He is expected to send the links for those devices for my review.
5. Tony mentioned the cybersecurity workshop and encouraged students to register.
6. Floor mats for rebuilding the racing track are on the way. It will arrive this Sunday. I will put them in the lab on Monday so students can start working on it.

New Business:

Dr. Won will be assigning the new team members their assignments for their projects.

The meeting was adjourned at 1:00pm.

CFIA-Project Team Meeting

09/22/2022
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Team
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:10:00 pm	Adjourned:	1:00 pm

Attendees: Dr. Myounggyu Won, Debera Pittman; Tony Pinson; Hans Amelang; Luke Carrington; William Richards; Adam Kharsa.

Minutes

Discussion:

Meeting Minutes – The minutes from the meeting held on September 22, 2022, are shared, and reviewed, as written.

Discussion: Dr. Won had a brief discussion with the Project Teams.

General Discussion –

1. Nathan has fixed his video demo, getting it ready to be presented at the workshop.
2. Hans is investigating a water pump project. He has found hardware/software resources on an industrial IoT (Internet of Things) water pump application built with the Arduino platform. He will order hardware parts to build the water pump system. After building the hardware system, he will investigate potential cybersecurity problems related to industrial IoT that can be applied to the water pump system.
3. Luke has completed Chapter 5 of the Autonomous R/C car cybersecurity project document. He will send the document to Dr. Won for review.
4. Luke, William, and Adam have produced a new cybersecurity idea for their R/C car project and added an intentional delay to the camera feed to cause the car to behave unexpectedly. It would be interesting to demonstrate the impact of the "delay attack." They will also investigate potential prevention techniques as well as attack detection methods.
5. Tony will add William and Adam to the group list to allow them to access the shared drive.
6. Dr. Won has talked with the R/C car team and confirmed that the floor mat works and has ordered additional floor mats to create a bigger "portable" track.
7. Dr. Won is looking into the image processing module of the R/C car software.
8. Dr. Won will investigate industrial IoT security which can apply to the IoT team's water pump system.

New Business:

Dr. Won will be discussing Industrial IoT security next week with the project teams.

The meeting was adjourned at 1:00pm.

CFIA-Project Team Meeting

09/29/2022
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Team
Facilitator:	Dr. Dipankar Dasgupta	Note taker:	Debera Pittman
Called to Order:	12:10:00 pm	Adjourned:	1:00 pm

Attendees: Dr. Dasgupta; Debera Pittman; Tony Pinson; Hans Amelang; Luke Carrington; William Richards; Douglas Espinoza.

Minutes

Discussion:

Meeting Minutes – The minutes from the meeting that was held on September 22, 2022, are on One Drive, shared and written.

Discussion: Dr. Dasgupta had a brief discussion with the Project Teams.

General Discussion –

1. Hans Amelang discussed with Dr. Dasgupta and the project team, about building the water station. When the parts arrive Hans and Nathan will begin Phase I construction, working on the infrastructure of the project. Hans and Nathan had a meeting about the automated conveyor transferring systems.
2. Dr. Dasgupta would like Dr. Mohd Hasan Ali to attend the next Hands-on Project Meeting on October 6, 2022.
3. Dr. Ali is involved in the project with Nathan Farrar about the Smart Grid Cybersecurity.
4. Dr. Dasgupta said in Germany the autonomous car is making progress and gave some insight about the charging station for the Autonomous R/C car. He explained there is a charging station in Chicago, Illinois.
5. Luke Carrington wanted to know if the charging elevates the performance of the car.

New Business:

Students need to send updates to Dr. Won.

The meeting was adjourned at 1:00pm.

CFIA-Project Team Meeting

10/06/2022
12:30pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Team
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:30:00 pm	Adjourned:	1:00 pm

Attendees: Dr. Myounggyu Won; Dr. Mohd Hasan Ali; Debera Pittman; Tony Pinson; Hans Amelang; Luke Carrington; William Richards; Nathan Farrar; William Richards; Adam Kharsa.

Minutes

Discussion:

Meeting Minutes – The minutes from the meeting that was held on September 29, 2022, are on the One Drive, shared and written.

General Discussion –

- Hans
    1. Is waiting on the parts for his water pump project that was ordered on Monday.
    2. Hans is strongly suggested to work with Nathan. Hans's expertise in coding and Nathan's expertise in the hardware system will be creating a synergistic effect.
    3. Hans started to read the paper about the Industrial IoT security that suggested by Dr. Won.
    4. Hans will check the price of the student-version simulator mentioned in the Industrial IoT security paper.
    5. Hans will work on the water pump project as soon as the parts arrives, next week.
    6. Hans will let us know if he would like to pursue the Industrial IoT security project. If he is busy with the water pump project, he will let Dr. Won know so another student can work on the IoT security project.
- R/C car team
    1. The team has worked on resolving the software issue related to the front camera of the R/C car. To save some time used to address the software issue, a quick solution of buying a new R/C car will be attempted. Although some R/C cars recommended by the donkey car website are out of stock, the team will try with a different car from the same vendor. Dr. Won will place the order today.
    2. The team has set up the new, "portable" R/C car racing track using the new floormats.
    3. The team will address the software issue. The team will also demonstrate if the software issue can be resolved with a new car that they will receive on Wednesday.
    4. The team installed new lane marking for the racing track.
- Nathan
    1. Nathan reviewed the paper on dynamic wireless charging that Dr. Won suggested.
    2. Nathan will come up with a rough plan for building a prototype dynamic EV charging system.
    3. Nathan will work closely with Hans on this project.
    4. Dr. Won will provide mor information on how to build the prototype EV charging system. Nathan will review the information.
- Tony
    1. Tony mentioned a report regarding the workshop hosted by North Carolina A&T University.
    2. Tony also mentioned the Cybersecurity Summit.

New Business:

The teams will give weekly updates to Dr. Won.

The motion for the meeting be adjourned by Debera Pittman and seconded Hans Amelang.

CFIA-Project Team Meeting

10/13/2022
12:30pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:30:00 pm	Adjourned:	1:30 pm

Attendees: Dr. Myounggyu Won; Dr. Mohd Hasan Ali; Debera Pittman; Tony Pinson; Hans Amelang; Luke Carrington; William Richards; Nathan Farrar; William Richards; Adam Kharsa.

Minutes

Discussion:

Meeting Minutes – The minutes from the meeting that was held on October 06, 2022, are on One Drive, shared and written.

General Discussion –

- Dr. Mohd Ali has joined the team for the meetings. Dr. Ali introduced himself and talked about his recent project on 5G-enabled EV charging system.
- Hans
    1. Hans is willing to conduct research on both the IoT (Internet of Things) water pump project and the industrial IoT project in collaboration with Nathan.
    2. Hans will reach out to the power factory software company to ask for a quote for their student-version simulation software today.
    3. Nathan and Hans are exploring potential security breaches for the Arduino platform which they think is quite robust and secure.
    4. Hans will check the cost for the student-version grid system simulation software.
    5. Hans will continue reading the industrial IoT paper and get ready to discuss it with Dr. Won.
    6. Hans will be able to explain the water pump system to the team.

- R/C Car Team
    1. The team took off the old tape and got new tape to finish the racetrack with better lane markings.
    2. The team reset the configuration file and obtained the necessary background to start training R/C car. This can be done as soon as the new cars arrive.
    3. The two cars that Dr. Won ordered will arrive on Monday. Dr. Won will deliver the cars to the lab.
    4. The R/C car team is expected to finish the racing track, to show new lane markings.
    5. The R/C team start training with the two new cars.

- Douglas
    1. Douglas has been working with Tareq who is working on his honors project under the supervision of Dr. Won.
    2. Tareq has a good background in JavaScript, so Douglas thinks that Tareq will be able to complete the WebUI-based buffer overflow attack project.
    3. Douglas would like to see a new project recommendation from Dr. Won. Dr. Won identified a new project for GenCyber program for him.

- Tony
    1. Tony mentioned a faculty training session that will be in the Spring. He will provide more information to the team about the event.
    2. Tony explained the 2022 CSForAll Summit for the students (attached in this email). He encouraged students to participate in this event if interested.
- Nathan
    1. Nathan has finished reading the Industrial IoT paper that Dr. Won suggested.
    2. Nathan will read a paper about building a prototype dynamic wireless charging system.

New Business:

The teams will give weekly updates to Dr. Won.

The motion for the meeting be adjourned by Debera Pittman and seconded William Richards.

CFIA-Project Team Meeting

10/20/2022
12:30pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:30:00 pm	Adjourned:	1:30 pm

Attendees: Dr. Dipankar Dasgupta; Dr. Myounggyu Won; Debera Pittman; Douglas Espinoza; Hans Amelang; Luke Carrington; William Richards; Nathan Farrar; William Richards; Adam Kharsa.

Minutes

Discussion:

Meeting Minutes – The minutes from the meeting that was held on October 13, 2022, are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Dr. Dasgupta and Douglas Espinoza discussed the R/C Car. Dr. Dasgupta also talked with Hans Amelang about the Water Pump Project.
- Each team gave Dr. Won updates on their projects.

  Douglas

  1. Read an article about V2X that Dr. Won sent to him.
  2. An idea was discussed about sending a fake image from one car to another via V2X.
  3. Douglas will coordinate with Dr. Won to work on a V2X security project.
- Hans
  1. The parts for the Water Pump Project have arrived.
  2. A discussion about the hardware parts being assembled.
  3. Hans will focus on the Water Pump Project. The Cybersecurity Project for a grid system has been postponed since Hans will concentrate on the Water Pump Project.
  4. Hans will complete assembly of the parts, so he can show a minimum demo of the project next week.
- R/C Car
  1. Documented the process of building the racing track using floor mats.
  2. Tested the new cars, and unfortunately the new cars did not work.
  3. The team will demonstrate autonomous driving on the new racing track and get ready to implement the delay attack scenario.
- Nathan
  1. Has reviewed the paper that Dr. Won sent about implementation of dynamic wireless charging.
  2. Nathan will start working on creating the hardware platform for dynamic wireless charging.

- Dr. Won worked along with the students on the R/C car, to help figure out what was wrong with the relay.

New Business:

The teams will give weekly updates to Dr. Won.

The motion for the meeting be adjourned 1:30 pm.

CFIA-Project Team Meeting

10/27/2022
12:30pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:30:00 pm	Adjourned:	1:30 pm

Attendees: Dr. Dipankar Dasgupta; Dr. Myounggyu Won; Dr. Mohd Ali; Debera Pittman; Hans Amelang; Luke Carrington; William Richards; Nathan Farrar; William Richards; Adam Kharsa.

Minutes

Discussion:

Meeting Minutes – The minutes from the meeting that was held on October 20, 2022, are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Each team gave Dr. Won updates on their projects.

- Hans
    1. Hans has completed the design part for the water pump project. He also created a diagram that illustrates his plan to build the system. Hans explained the diagram in the meeting.
    2. The goal of this project was discussed with faculty.
    3. Hans will begin the assembly of the project.
- AV Team
    1. The AV Team addressed the battery issue of the old car.
    2. The team did a test with the old model but still had some issues. They also tried the new model and autonomous driving began to work.
    3. The team demonstrated to the faculty of the autonomous driving of the R/C car on the racing track.
    4. The team will try Douglas's R/C car, to see what results they will receive.
    5. The team will send Dr. Won a document that summarizes the image processing operation of the R/C car.
    6. The team is getting prepared to implement an image disruption attack scenario.
- Nathan
    1. Nathan produced a circuit design of the prototype dynamic wireless charging system.
    2. Nathan discussed a diagram with faculty members.
    3. It also discussed measurement methods on how to measure power transfer efficiency.
    4. Purchasing parts are needed to implement this project, for the building of the hardware prototype system.

- Douglas
    1. Douglas has begun working on a V2X cybersecurity project.
    2. It is challenging because the team does not have a V2X module installed on the R/C car.
    3. A simulation-based method could be used.
    4. Dr. Won will have a discussion with Douglas and produce a concrete plan.

New Business:

The teams will give weekly updates to Dr. Won.

The meeting was not adjourned until 1:30 pm.

CFIA-Project Team Meeting

11/03/2022
12:30pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:30:00 pm	Adjourned:	1:30 pm

Attendees: Dr. Dipankar Dasgupta; Dr. Myounggyu Won; Dr. Mohd Ali; Ms. Debera Pittman; Hans Amelang; Luke Carrington; William Richards; Nathan Farrar; William Richards; Adam Kharsa: Douglas Espinoza.

Minutes

Discussion:

Meeting Minutes – The minutes from the meeting that was held on October 27, 2022, are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Each team gave Dr. Won updates on their projects.

- Hans
    1. Hans has built the first version of the hardware platform for the water pump project.
    2. He is addressing wiring challenges.
    3. The goal is to make it as simple as possible using commonly available parts so we can use this platform for educational projects.
    4. Arduino programming should be done next week-aiming to finish on Monday or Tuesday.
- AV Team
    1. AV Team has completed implementing two attack scenarios. Implementation of another attack scenario are in progress.
    2. Scenario 1: Delay the rate of the image feeding.
    3. Scenario 2: Make a camera take a phone with some delay-working on a issue and aims to address this issue next week.
    4. Scenario 3: Hack the Boolean variable used to flip the camera, i.e., manipulate this variable to intentionally flip the camera.
    5. The completed attack scenarios are ready to be demonstrated in the capstone project class.
    6. Dr. Won will address the issue related to the attack scenario in scenario 2.
    7. Dr. Won will think about turning these attack scenarios into educational projects.
- Nathan
    1. Nathan did research on parts needed to create a hardware platform for DWC system.
    2. There will be a decision on parts to purchase.
    3. Nathan will start building a prototype system.

- Douglas
    1. Douglas is working on V2X attack scenarios.
    2. He is also working on the Wormhole attack. He will come up with an idea of the attack scenario as well as counter measure.
    3. He will continue to investigate the wormhole attack scenario. Fina a open-source resource to implement the wormhole attack scenario.

New Business:

The teams will give weekly updates to Dr. Won.

The meeting was adjourned at 1:30 pm.

CFIA-Project Team Meeting

11/10/2022
12:30pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:30:00 pm	Adjourned:	1:30 pm

Attendees: Dr. Dipankar Dasgupta; Dr. Myounggyu Won; Dr. Mohd Ali; Debera Pittman; Hans Amelang; Luke Carrington; William Richards; Nathan Farrar; William Richards; Adam Kharsa; Tony Pinson.

Minutes

Discussion:

Meeting Minutes – The minutes from the meeting that was held on November 3, 2022, are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- A tour of our lab was offered to the students from the Management Information Systems (MIS) Department.

- Hans
    1. Hans has completed the first version of the program and tested it.
    2. Dr. Dasgupta suggested to put the water pump system in an acrylic box for better with some LEDs for demonstration.
    3. Hans will read the NIST paper that Dr. Dasgupta suggested. The paper is about cybersecurity scenarios for a water pump system.
    4. Hans will keep working on the software part.
    5. Once the basic operation of the water pump is implemented, we will think about cybersecurity scenarios.
- AV Team
    1. AV Team has completed a demonstration successfully in the capstone project. The class was very intrigued.
    2. AV Team has started working on the implementation of the delay attack.
    3. AV Team drafted a document that explains the details of the attack scenarios and the mitigation methods.
    4. AV Team implement the delay attack scenario.
- Nathan
    1. Nathan has found a part for the dynamic wireless charging project.
    2. Dr. Won confirmed that the part can certainly be used to implement the prototype wireless dynamic charging system.
    3. The parts for the prototype system are being purchased, so developing can start.

- Douglas
    1. Douglas is working on the worm-hole attack scenario.
    2. Douglas will find available source code the implements the worm-hole attack scenario. Adapt the code for our R/C car application.

New Business:

The teams will give weekly updates to Dr. Won.

The meeting was adjourned at 1:30 pm.

CFIA-Project Team Meeting

12/01/2022
12:30pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:30:00 pm	Adjourned:	1:30 pm
Attendees:	Dr. Dipankar Dasgupta; Dr. Myounggyu Won; Dr. Mohd Ali; Debera Pittman; Doris Allen; Hans Amelang; Luke Carrington; Nathan Farrar; William Richards; Adam Kharsa; Tony Pinson.		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on November 24, 2022, are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
    1. Hans does not have much update this week.

- AV Team
    1. AV Team created a promo video like a truck commercial and they will share the video.
    2. AV Team created a power-point slides for the capstone project demo.
    3. Wrap up the document that summarizes everything.
    4. Record video demonstrations of normal driving and attack/counter-attack scenarios.

- Nathan
    1. Nathan is waiting on parts and will start to build the prototype DWC system once the parts arrive.

- Douglas
    1. Looking at available source code on worm hole attack.

- Tony
    1. Subaward 502-seeking volunteers who will work an hour or two to act as a mentor for high school students on the Discord server.

New Business:
The teams will give weekly updates to Dr. Won.

The meeting was adjourned at 1:30 pm.

CFIA-Project Team Meeting

12/15/2022
12:30pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:30:00 pm	Adjourned:	1:30 pm
Attendees:	Dr. Myounggyu Won; Dr. Mohd Hasan Ali; Debera Pittman; Hans Amelang; Luke Carrington; Nathan Farrar; Tony Pinson.		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on December 1, 2022, are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
    1. Hans collaborated with Nathan and made the water pump system working.
    2. Hans recorded a video of the working water pump system.
    3. Hans will continue to work on it aiming to demonstrate a working system in the next meeting.

- Luke
    1. Luke has successfully completed the capstone project.
    2. Luke has started working on a survey paper on authentications methods for intelligent vehicle communication and control.
    3. A more specific topic will be determined in consultation with Dr. Dasgupta.

- Nathan
    1. The new parts arrived for Nathan.
    2. Nathan designed a hardware configuration of the DWC system.
    3. Nathan will perform a proof-of-concept testing of the coils.
    4. Nathan is expected to report some preliminary test results in the next meeting.

- Douglas
    1. Did not attend the meeting.

- Tony
    1. Discussed the 502 subaward.
    2. Dr. Won will send a draft budget.

New Business:
At the next meeting the team will give updates and receive new meeting time and date for the new year.

The meeting was adjourned at 1:00 pm.

CFIA-Project Team Meeting

01/18/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12::00 pm	Adjourned:	1:10 pm
Attendees:	Dr. Dipankar Dasgupta: Dr. Myounggyu Won; Dr. Mohd Hasan Ali; Debera Pittman; Luke Carrington; Nathan Farrar; Tony Pinson.		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on December 15, 2022, are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans

  Hans was not present.

- Luke
  1. Luke is exploring a research project topic.
  2. Dr. Dasgupta suggested a research project related to block chain.
  3. Dr. Won asked if Dr. Dasgupta agrees that Luke works on a survey paper on cybersecurity platooning.
  4. Dr. Won is looking into state-of-the-art survey works.

- Nathan
  1. Nathan has done a final testing of his proof -of-concept dynamic wireless charging system.
  2. Nathan has created video recordings for Dr. Won's review.
  3. Dr. Dasgupta suggested investigating the effect of different dielectric properties.

New Business:
Hands-on-Project Meeting will be every Wednesday at 12:00 pm until 1:00pm.

The meeting was adjourned at 1:10pm.

CFIA-Project Team Meeting

01/25/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12::00 pm	Adjourned:	1:10 pm
Attendees:	Dr. Dipankar Dasgupta: Dr. Myounggyu Won; Dr. Mohd Hasan Ali; Debera Pittman; Luke Carrington; Doris Allen; Nathan Farrar; Tiffany Geistkemper Tony Pinson; Hans Amelang.		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting on January 18, 2023, are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
    1. Hans got a new contract
    2. A prototype for the water pump system is nearly completed. Only some refinement is remaining.
    3. Dr. Dasgupta: planning a workshop here at Memphis. The water pump project is expected to be used as a hands-on project for the workshop.
    4. Expect to see the water pump working in the next two weeks or so.

- Nathan
    1. Created a video demonstrating some proof-of-concept results for the dynamic wireless charging system.
    2. Will investigate the effect of the ground materials on the charging efficiency.
    3. Discovered that the height (i.e., the vertical distance between the receiver and the transmitter) seems to affect the charging efficiency.
    4. But if the height is exceedingly small, the impact of the receiver location seems minimal. Nathan said consistent, but what does that consistency exactly mean?
    5. Dr. Dasgupta: Investigate the impact of material.
    6. Dr. Dasgupta: Also mentions some security issues such as stealing energy from the wireless charging system.
    7. Curious to find out what happens if voltage setting is increased?
    8. Possibility leading to a new problem of a 3D motion control rather than the lateral motion control.

- Dr. Dasgupta
    1. Citadel will hold a workshop (early May).
    2. They want us to give a presentation and demo.

- Tiffany
    1. Fourier series PowerPoint presentation
    2. Dr. Dasgupta wants to explore the 5G spectrum research.
    3. She worked on a 5G toolbox to visualize the 5G spectrum.
    4. Understanding the math model of 5G technology.

- Luke
    1. Working on block chain and encryption techniques.
    2. Proposed an idea of using meta data for a new encryption process.
    3. Luke is waiting for input for research papers to review.
    4. Dr. Dasgupta mentions the onion routing (tor). Suggested to read the tor paper.

New Business:

Dr. Dasgupta will discuss with Dr. Won about attending the workshop and have two of the students participate with Dr. Won.

The meeting was adjourned at 1:10pm.

CECIP-Project Team Meeting

2/08/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Mohd Hasan Ali; Debera Pittman; Hans Amelang; Tiffany Geistkemper; Luke Carrington; Nathan Farrar; Tony Pinson; Brayden Pusser; Adam Thieme.		

Minutes

Discussion:
Meeting Minutes – Due to inclement weather the meeting was cancelled on February 1, 2023.

General Discussion –

- Hans
    1. Hans ordered more parts to complete the project. Waiting on the parts to arrive.
    2. Read the IoT network layer paper that Dr. Dasgupta suggested and will share with Dr. Won.
    3. Dr. Ali: The goal of this project is to demonstrate the effect of the cyber-attack on the water pump system.
    4. What will be done in the next week, A prototype of water pump system in the next week.

- Nathan
    1. The receiver coil larger than the current one is needed to better demonstrate the power transfer efficiency effect depending on the horizontal position of the receiver coil.
    2. Planning to test with different materials.

- Tiffany
    1. Conducted a wave form analysis for 5G.
    2. Studying the Fourier analysis.
    3. Prepared a power point presentation about complex Fourier series, Fourier transform analysis.

- Luke
    1. Read the whole survey paper.
    2. Preparing for a presentation of the paper.

- Capstone
    1. Building background on the R/C car.

- Tony
    1. Tony mentioned the Citadel workshop and update on 502 projects.

New Business:
The teams will give updates at the next CECIP meeting.
.

The meeting was adjourned at 1:00 pm.

CECIP-Project Team Meeting

2/15/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Mohd Hasan Ali; Dr. Dipankar Dasgupta; Debera Pittman; Hans Amelang; Tiffany Geistkemper; Luke Carrington; Nathan Farrar; Tony Pinson; Doris Allen; Adam Thieme.		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on February 8, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
    1. Worked on model refining. Some refinement is needed. Coding issues need to be fixed.
    2. Need to talk to Dr. Won or Dr. Dasgupta about the final form factor.
    3. Will share the paper that Dr. Dasgupta suggested to read with Dr. Won.
    4. Next Week: Prepare a working prototype and demonstrate to the group.
- Nathan
    1. Parts ordered. Larger receiver coils, AC/DC converter, and voltage regulator.
    2. Dr. Dasgupta: The funding for these parts should come from the DWC project. Dr. Ali agreed.
    3. Dr. Dasgupta mentions the public network cybersecurity education tool developed by Cisco and suggests exploring the use of the tool.
    4. NEXT WEEK: Research on how to run a machine learning model on the IoT platform.
- Tiffany
    1. Studied two topics: (1) how to model OFDM symbols (wave form of 5G) – found an article about this topic explaining the details about that as well as some related filter techniques; (2) In-depth study on the topic of Fourier transform, and related math techniques about 5G (reading a book) and found an article about this topic.
- Luke
    1. Read the review paper.
    2. Brief the findings that Luke learned from the paper.
    3. Dr. Dasgupta: prepare a presentation. See if you can use Cisco's packet tracer. Mentions some potential implementation methods (e.g., denial of service attack) for software demonstration, specifically based on client-server environment.
    4. Dr. Dasgupta clarified some issues related to the encryption technique presented in the paper (i.e., private key used by sender and the public key used by the receiver, is this the correct method?) His answer was that it can be used either way.
    5. NEXT WEEK: prepare a short presentation (15mins) about the review paper.
- Tony
    1. Ready to kick off the 502 Project. 2.
    2. Project activity presentations at a STEM conference, this Saturday.
- Capstone
    1. Building background on the donkey car platform.

New Business:

Hands-on-Project Updates every Wednesday meeting. The meeting adjourned at 1:15 pm.

CECIP-Project Team Meeting

2/22/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Debera Pittman; Doris Allen; Hans Amelang; Tiffany Geistkemper; Luke Carrington; Nathan Farrar; Tony Pinson; Adam Thieme.		

Minutes

Discussion:
Meeting Minutes – The meeting minutes from the meeting held on February 15, 2023, were reviewed, and approved, as written.
General Discussion –

- Hans
  - Prepared a working prototype and demonstrated it.
  - An issue was found. The tubing is too large resulting in water leakage. It should be fixed.
  - Should develop cybersecurity components for the water pump project.
  - NEXT WEEK: presentation of the paper that Dr. Dasgupta suggested to read.
  - Dr. Dasgupta: Some timeline should be determined. After the spring break, we should be able to release the demo (in a classroom setting). Make a video of the demo (as a contingency plan if the system does not work).
  - Dr. Ali: More specific information about the attack is needed, e.g., uploading adversary code via the USB port, or we can consider a network attack via Wi-Fi.
- Nathan
  - Parts will arrive tomorrow.
  - Discussed the idea of adding a motion sensor to switch on off automatically. This is a promising idea for a demonstration purpose.
  - NEXT WEEK: the complete system will be built and shown to the lab members.
- Tiffany
  - Read an article about the OFDM signal and the mathematical model. Building background on the impulse response filter.
  - Covered YouTube lecture series (U of Alabama) about complex analysis, differential equation.
  - Reading chapter 6 of the book mentioned in the previous week.
  - Dr. Ali: suggest learning MATLAB simulation
  - NEXT WEEK: Will learn about the MATLAB simulation. Will post all files in the shared folder.
- Luke
  - Install the Cisco packet analyzer. Learning the analyzer.
  - NEXT WEEK: Prepare a short presentation (15 minutes).
- Tony
  - Participated STEM conference supported by national African American engineers' association.
  - Update on 502 Project.
- Capstone
  - Ready to work with an actual hardware platform.
  -

New Business:

There will be updates on the projects.

The meeting was adjourned at 1:00pm.

CECIP-Project Team Meeting

3/15/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Dipankar Dasgupta; Dr. Hansan Ali; Debera Pittman; Doris Allen; Hans Amelang; Tiffany Geistkemper; Luke Carrington; Nathan Farrar; Tony Pinson; Arturo Perez		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on March 15, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
    1. The video showing his water pump system's operation was created and uploaded on the shared folder.
    2. He will work on the project write-up.
    3. Dr. Ali suggested that the introduction/purpose part of the video should go first before the demonstration.
    4. Tony commented that a diagram illustrating the structure of the system would be helpful.
- Nathan
    1. The video demonstrating the operation of his dynamic wireless charging system has been created and uploaded on the shared folder.
    2. Discuss the funding needs for the next stage of the project.
    3. Dr. Ali suggested that the system introduction part of the video should be up front before the demonstration of the system.
- Tiffany
    1. Studied about the simulation of FFT on MATLAB
    2. Met with a graduate student Dr. Ali suggested and learned about the tool.
    3. Working on OFDM signals and 5G toolbox.
- Luke
    1. Started working on implementing simulation of a platoon of trucks.
- Tony
    1. Mentioned the annual report.
    2. Asked for official grant numbers for active reports.
    3. Mentioned event scheduling for the 502 projects.
- Perez
    1. Welcomed a new member with the team.
    2. Interested in a multi-factor authentication project.

New Business:

Give Hands-on-Project updates at every Wednesday meeting.

The meeting adjourned at 1:00 pm.

CECIP-Project Team Meeting

3/22/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Hansan Ali; Debera Pittman; Doris Allen; Hans Amelang; Tiffany Geistkemper; Luke Carrington; Tony Pinson; Arturo Perez; Adam Thieke		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on March 15, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
    1. Will prepare a write-up on background and description of the water pump system.
    2. Wireless setup for the Arduino.
        - Wireless updating -> need access to IoT cloud (based on their cloud app). Examine tokens exchanged.
    3. Will work on a webapp-based attack scenario (similar to the traffic light system).
    4. Also looking at security issues related to USB injection.
        - A physical attack when updating the device via the USB port.
- Tiffany
    1. Worked on simulations of OFDM using MATLAB. Testing to see if the output is correct.
    2. Implementing FFT
        - Three examples were implemented. Encountered some issues in implementing it and investigated them.
    3. Dr. Ali. mentioned the difference between Fourier Series and FFT. Asked if they are distinguished in the implementation. Tiffany said yes.
    4. Reading the paper that Dr. Dasgupta suggested.
- Luke
    1. Worked on the simulation of truck platoon.
    2. Working on automating the attacking procedure using Wire-shark.
    3. NEXT WEEK: provide a list of good/latest papers on cybersecurity for truck platooning. Dr. Won will suggest one or two papers. Luke will read them.
- Tony
    1. Dr. Dasgupta encouraged to attend the CAE symposium in Seattle.
    2. Preparing presentation for the meeting.
    3. Need a paragraph explaining each project.
    4. Dr. Ali mentioned one or two slides to explain an individual project would be better.
- Perez
    1. Working on multi-user authentication.
    2. Working on Rails and Flask – python-based web server. Found libraries that can be used for implementing multi-ser authentication.
- Capstone (Adam)
    1. Looked into the basics of wormhole attack scenarios.
    2. Dr. Won will develop a plan for the wormhole attack scenario and let the team know.

New Business:

Give Hands-on-Project updates at every Wednesday meeting.

The meeting adjourned at 1:00 pm.

CECIP-Project Team Meeting

3/29/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Dipankar Dasgupta; Debera Pittman; Hans Amelang; Tiffany Geistkemper; Luke Carrington; Nathan Farrar; Tony Pinson; Doris Allen; Adam Thieme; Allison Plank.		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on March 22, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans

    1. Water pump – project description and base device done (documentation in OneDrive folder) – currently researching Bluetooth capability to design a basic wireless attack.
    2. Cisco PacketTrace – going through an introduction to Cisco Packet Trace training through SkillsForAll.com to evaluate as a learning tool for networking and security for the University, new project from Dr Dasgupta. I can provide more details via email or at our meeting Wednesday if you would like.

- Nathan
    1. Currently waiting for the approval to go ahead and get the parts ordered for the DWC project. Debera reached out to Dr Dasgupta yesterday, but we still haven't received any feedback.
    2. Working on an algorithm to control the actuators based on Faraday's Laws of Voltage Induction of a coil in motion and Ampere's Laws of Magnetic fields.
    3. Hoping to simulate the system at least statistically before the parts come in so that we can be ready to implement it asap.
- Tiffany
    1. Working on the EV wireless charging station project under Dr. Dasgupta and Dr. Al.
    2. Currently studying the simulation processes needed to simulate cybersecurity attacks in Simulink and MATLAB.3
    3. Also studying Fourier analysis to analyze data from CP-OFDM signals used in 5G to simulate the wireless (5G) cyberattacks, derive the mathematical equations that represent these attacks, write code to prevent these attacks, and integrate this code with the rest of the code in the project.
- Luke
    1. Completed reading the "Secure Content Delivery for Connected and Autonomous Trucks: A Coalition Formation Game Approach" paper we agreed upon.
- Arturo
    1. Met with the 2 graduate students who have been working on this project before me and are currently working the project.
    2. Learning the current environment and language we are working in and the status of the project. Also learning React.js to look over the current code and understand it.
    3. Will learn MongoDB as we are transitioning the project's database from SQL to Mongo.

New Business:

Hands-on-Project Updates every Wednesday meeting. The meeting adjourned at 1:15 pm.

CECIP-Project Team Meeting

4/05/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Hansan Ali; Debera Pittman; Doris Allen; Hans Amelang; Luke Carrington; Nathan Farrar; Tony Pinson; Arturo Perez		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on March 29, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
    1. Working on Bluetooth connectivity and potential attack scenarios for the Arduino-based water pump system.
    2. Met with Sagar, studying the Cisco packet tracer.
    3. Next week: Continue to work on the water pump project focusing on development of the cyber security attack scenario related to Bluetooth connectivity.

1. Nathan
    1. Waiting for approval for the research item purchase.
    2. Ran MATLAB simulation on dynamic wireless charging.
    3. Next week: Begin learning about reinforcement learning.

- Tiffany
    1. Conference in Orlando Florida.
- Luke
    1. Finished reading a paper related to platooning security.
    2. Next week: Luke will read more papers on platooning security. Dr. Won will send related papers.

- Tony
    1. Mentioned the CAE tech talk and encouraged to attend.

- Perez
    1. Working on MongoDB and related tools (e.g., Java Script).
    2. Also read one or two papers related to this.
    3. Next week: Continue to work on MongoDB.

New Business:

Give Hands-on-Project updates at every Wednesday meeting.

The meeting adjourned at 1:00 pm.

CFIA-Project Team Meeting

04/12/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	**Type of meeting:**	Project Team
Facilitator:	Dr. Myounggyu Won	**Note taker:**	Debera Pittman
Called to Order:	12:00:00 pm	**Adjourned:**	1:00 pm

Attendees: Dr. Myounggyu Won; Dr. Dipankar Dasgupta; Dr. Mohd Hansan Ali; Tony Pinson; Debera Pittman; Tiffany Geistkemper: Luke Carrington; Hans Amelang; Adam Thieme

Minutes

Discussion:

Meeting Minutes – The meeting minutes from the meeting held on April 2023, were reviewed, and approved, as written.

- Hans
    - worked on the Cisco packet tracer.
    - Dr. Dasgupta mentioned that the Packet tracer could be used as a class exercise.
    - Dr. Dasgupta requested to create a 10min video about the Cisco packet tracer
    - Dr. Dasgupta mentioned holding a workshop that presents hands-on projects.
    - Dr. Dasgupta mentioned the Cisco visit.
    - Worked on the Bluetooth/WiFi part of the Arduino project for cybersecurity attack scenario development.
- Nathan
    - Did research on AI and ML for the DWC project.
    - Dr. Dasgupta suggested studying the genetic algorithm. Explained an example application of a genetic algorithm for the Ford Motor company.
    - Identified some practical issues regarding deployment of the dynamic wireless charging system.
    - No funding for purchasing the requested items. The budget must be adjusted and may have to wait a few months.
- Tiffany
    - Went to a conference last week.
    - Noah introduced a paper about a layered approach for 5G cyber security attack. MATLAB code is available based on SimuLink.
    - Writing a paper about 5G cyber security.
    - Dr. Dasgupta mentioned creating a shared folder for her project.
- Luke
    - Dr. Won sent some papers.

    - Luke is reading the papers. One of them is about the spring stability and impact of the sensor anomaly.
    - Next Week: Dr. Won will work on the structure of the journal paper, and Luke will read all the 10-12 papers that Dr. Won suggested.
- Tony
    - Mentioned the CAE-R annual report.
- Perez
    - Perez is basically exploring various topics for his research.
    - Read three papers (about various aspects of intrusion detection systems, related theory).
    - Dr. Dasgupta explained the scope of the project, e.g., start with a survey work. Suggested some resources to look at.
- Capstone (Adam)
    - Man in the middle proxy server running.
    - Successfully captured packets between the R/C car and the web server.

New Business:

There will be updates on the projects.

The meeting was adjourned at 1:00pm.

CECIP-Project Team Meeting

4/19/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Debera Pittman; Hans Amelang; Tiffany Geistkemper; Luke Carrington; Nathan Farrar; Tony Pinson; Doris Allen; Adam Thieme		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on April 12, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
    1. Did not attend.
- Nathan
    1. An algorithm for moving the coils left and right in cm was developed using Google co-lab.
        - The objective is to migrate the code to the designated hardware platform when the requested research items have been required.
    2. Started looking at genetic algorithms that Dr. Dasgupta mentioned.
- Tiffany
    1. Dr. Ali suggested taking an on-line course to build CS background on 5G.
        - e.g., Tennessee Southeast Community College, Cisco.
    2. Tony mentioned some cybersecurity courses developed in collaboration with FEMA. Doris will forward the information. (e.g., mobile device security 5G).
- Luke
    1. Reviewing papers on cybersecurity for platooning.
    2. Discussed into more details on papers that they are worth to read.
    3. Dr. Won will continue to work on preparing the template survey paper so Luke can add his summaries in that document.
- Tony
    1. Preliminary information submitted to University of West Florida for subaward about workforce development.
- Perez
    1. Did not attend.

New Business:

Hands-on-Project Updates every Wednesday meeting. The meeting adjourned at 1:15 pm.

CECIP-Project Team Meeting

5/17/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Mohd Hasan Ali; Debera Pittman; Arturo Perez; Nathan Farrar; Tony Pinson; Doris Allen; John Jack O'Meara		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on May 3, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

John J O'Meara attended the meeting. He took over Brian's position. He is in the administrative office and Room 117.

Perez:

Finished reading "A Review of Insider Threat Detection: Classification, Machine Learning Techniques, Datasets, Open Challenges, and Recommendations."

a. This work is from June of 2020 and aimed to be a survey of over 100 recent insider threat publications to review what the current trends in research show.
b. Covered topics such as paths to entry.
c. Different ways to categorize insiders.
d. Methodology of attack
e. Motivation for attack

Started another paper which I am working through. Once finished with this 2nd paper. Will begin working solely on the MUAC project to understand the way it works with React, MongoDB, Node, and its adjacent libraries its currently utilizing. Worked with Sagar the graduate student and got the web application and phone application working. I was not seeding or connecting a database.

Nathan:

Research on Zero Trust power system principle and walk through and check for each layer. Also working on physical demonstration on charging system, have a network simulation going on and will implement AI. Will write a research paper on Zero Trust and will communicate with Dr. Won for the name of the paper.

Tony:

The University of Memphis is designated for studies with CAE. He will be going to a workshop on May 24-25., San Antonio, TX. He will attend CAE Symposium in June 7-9, in Seattle WA.
He explained about the July 7, 2023, workshop on campus.

Hans:

Did not attend.

Luke:

Did not attend.

New Business:
Updates on Hands-on-Project.

CECIP-Project Team Meeting

5/24/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Dipankar Dasgupta; Debera Pittman; Arturo Perez; Allison Plank; Doris Allen; John Jack O'Meara		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on May 17, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

Allison:
- 5G Charging System Internet
- A research paper on security communication for 5G that will increase with guidelines, that Allison read about.
- There are more vulnerable ways to attack the 5G.

Perez:
- PowerPoint shown on Outsider/Insider Threat Detection.
- Current and Past Research.
- Ex-employees are threats.
- It showed how a low-level National Guardsman was able to access classified documents.
- Researched Edward Snowden the whistle blower 2013.
- Researched Airman Jack Teixeira the IT Specialist that passed classified documents.
- PowerPoint is on the lab exercise One Drive in the Zoom Meeting.

Nathan:
- Did not attend.

Hans:
- Did not attend.

Tony:
- Did not attend.

New Business:
Updates on Hands-on-Project.

CECIP-Project Team Meeting

5/31/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Dipankar Dasgupta; Debera Pittman; Doris Allen; Tony Pinson; Nathan Farrar; Dr. Mohd Hasan Alii; Arturo Perez;		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on May 24, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Allison
  - Is working on the EV project.
  - I have studied 5G waveform, OFDM, and MIMO.
  - I also studied the MATLAB 5G toolbox by watching instructional videos focusing on 5G waveform generation.
  - Next week: continue to learn about 5G. Work with Tiffany.
  - Dr. Dasgupta suggested that a regular progress report should be submitted and uploaded on the shared folder.
- Arturo
  - Presented PowerPoint presentation about the negative authentication system.
  - Created a PowerPoint presentation on the paper that Dr. Dasgupta suggested about insider threat detection/access control focusing on how to detect unauthorized access to sensitive documents.
  - The PowerPoint slides have been uploaded on the shared folder.
  - Dr. Dasgupta requested a presentation at the Friday meeting. Students are welcome to attend the Friday meeting.
- Nathan
  - Implemented an AI (Artificial Intelligence) algorithm for coil alignment on MATLAB.
  - Also worked on the Zero trust power system.
  - Dr. Dasgupta suggested demonstrating this project at the July 7 workshop. Nathan said that he would join the workshop via Zoom.
  - Next week: implement the machine learning algorithm on the Raspberry Pi platform.
- Hans
  - Not attended. Should continue his research on secure water systems as part of his MS thesis.
- Dr. Dasgupta
  - Asked Tony to create a registration page for the workshop. Tony is expected to work with Jack and Sagar on this.
  - Asked Doris to advertise the workshop in the university newsletter.
  - Dr. Ali will advertise the event on the IEEE chapter.
  - It is mentioned that CAE would like to see graduating students (where they are going e.g., government jobs), research papers, etc. must be included in the annual report. Attending CAE-R conferences is required.
- Tony
  - Worked on new requirements related to center redesignation.
  - Will submit lectures on CLARK.
  - Attended the CAE workshop at San Antonio about pin testing.

- **New Business:**

Give Hands-on-Project updates at every Wednesday meeting.

The meeting adjourned at 1:00 pm.

CECIP-Project Team Meeting

6/07/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Nathan Farrar; Jack O'Meara; Doris Allen		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on May 31, 2023., are on One Drive, shared and written. The meeting was called to order by Doris Allen.

General Discussion –

- Hans
  1. Not attended
- Arturo
  1. Not attended
- Allison
  1. Not attended
- Nathan
  1. Worked on an ML (Machine Learning) algorithm for the DWC project.
  2. Found that the STD algorithm was overkill for the project.
  3. Tried the DDPG algorithm and ANN algorithm instead.
  4. Explained a plan for building a prototype hardware for DWC.
  5. Next week: will implement the prototype hardware system for DWC.
- Jack
  1. Worked on the module for FEMA course.
  2. A course on End user security and privacy.
  3. New course on zero trust.
  4. Editing exiting course on mobile device security and privacy. Trimming it down to smaller size.

New Business:

Hands-on-Project Updates every Wednesday meeting. The meeting adjourned at 1:00 pm.

CECIP-Project Team Meeting

6/14/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Dipankar Dasgupta; Dr. Mohd Hansan Ali; Debera Pittman; Doris Allen; Nathan Farrar; Tony Pinson; Arturo Perez; Allison Plank; Jack O'Meara		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on June 07, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
  - Not Attended
- Nathan
  - Integrating the AL on the RPI.
  - Will have all the bugs fixed by the next meeting.
  - Working on a live demo for the 7/7 demo.
- Allison
  - Read a paper on OFDM system analysis, specifically for OFDM systems with high bandwidth.
  - Discussed the channel leakage problem.
  - Next week: Learn about MATLAB 5G simulation.
- Arturo
  - Met with Dr. Dasgupta.
  - Demonstrated the front-end app for uploading and displaying files.
  - Explained the code of the App.
  - This app will be used to implement and evaluate the insider threat detection/access control methods.
  - Next Week: integrate with the Mongo DB and add users.
- Tony
  - The discord server for the 502-project registration issue was addressed.
  - Attended the CAE-Symposium held in Seattle, June 7-9.

New Business:

Give Hands-on-Project updates at every Wednesday meeting.

The meeting adjourned at 1:00 pm.

CECIP-Project Team Meeting

6/21/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Mohd Hasan Ali	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm

Attendees: Dr. Dipankar Dasgupta; Debera Pittman; Doris Allen; Tony Pinson; Nathan Farrar; Dr. Mohd Hasan Ali; Arturo Perez; Allison Plank; Jack O'Meara

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on June 14, 2023. are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
  - Did not attend.
- Arturo
  - Shows the data to put in the database, shown his PowerPoint test users.
  - JavaScript servers, application.
  - 4 Steps CRUB, RBAC, MUAC, Test.Users.
- Nathan
  - Building Raspberry Phi to show physical model using sensor cord.
  - Agent Autonomous Driving prototype
  - Submitting paper to Dr. Won.
- Allison
  - Understanding Mathematic Lab, how the 5G system works.
- Jack
  - Developing coursework for FEMA for Remote Home Office. University of Memphis, along with 5 different colleges receiving portion of grant funding.
- Tony
  - Cyber Resilient EV Charging Station & Critical Infrastructure Workshop is being reschedule on August 25, 2023.

New Business:

Hands-on-Project Updates every Wednesday meeting. The meeting adjourned at 1:00 pm.

CECIP-Project Team Meeting

7/19/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Allison Plank; Debera Pittman; Doris Allen; Nathan Farrar; Tony Pinson; Jack O'Meara.		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on July 19, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
    - Not attended.
- Nathan
    - Completed building a proof-of-concept DWC system.
    - Demonstrated the working of the prototype system.
    - Discussed the extension of the accepted ITSC paper for submission to the T-ITS journal.
    - Will work on drafting a document on the proof-of-concept implementation details to be included in a journal paper.
- Allison
    - Presented a paper about cybersecurity for EV charging systems.
    - Discussed various cybersecurity vulnerabilities of EV charging systems.
    - Will talk to Dr. Ali to find a specific topic on cybersecurity for EV charging systems to go into more details.
    - Will find if there is any paper on cybersecurity for EV charging appeared in top-tier CS cybersecurity conferences.
- Arturo
    - Note attended.
- Tony
    - Will give a presentation on the Discord server for the 502 projects.

New Business:

Hands-on-Project Updates every Wednesday meeting. The meeting adjourned at 1:00 pm.

CECIP-Project Team Meeting

7/26/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Debera Pittman; Nathan Farrar; Allison Plank; Doris Allen; John Jack O'Meara; Tony Pinson.		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on July 19, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
  - Not attended.
- Nathan
  - Presented results in terms of the prediction accuracy of the proof-0f-concept system.
  - Next week: will present an entire demonstration: will work on the writeup for the journal paper extension.
- Allison
  - Delivered a presentation on a paper that detailed various vulnerabilities within the Electric Vehicle Charging System Management System (EVCSMS).
  - The paper not only outlined potential threats of using the EVCS against power grid systems, but also provided an in-depth analysis of reverse engineering techniques applied to the firmware, application, and web application of the EVCSMS.
  - Next Step: Dr. Won will identify cybersecurity research papers on actual attacks against real-world Electric Vehicle Charging Systems (EVCS), with a preference for those presented at computer science conferences.
- Jack
  - Reported an update on course development.
- Arturo
  - Not attended.
- Tony
  - Will complete the preliminary draft for the NIST proposal; will send the draft this afternoon to Dr. Dasgupta.
  - Gave a presentation for 502 projects.

New Business:
Updates on Hands-on-Project.

CECIP-Project Team Meeting

8/2/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm
Attendees:	Dr. Myounggyu Won; Dr. Mohd Ali;; Nathan Farrar; Allison Plank; Doris Allen; John Jack O'Meara; Tony Pinson.		

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on July 26, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
  Not attended
- Nathan
  - Nathan has completed building the prototype charging system.
  - There was a minor technical issue in demonstrating the system.
  - Nathan will shoot a video and share the video with everyone.
- Allison
  - Presented a paper about EV charger pen testing.
  - Next Week: will read one of the papers that Dr. Won suggested and prepare a presentation about that paper.
- Jack
  - Worked on a remote home office course-web based training course. Submitted to FEMA. Received comments from them.
- Arturo
  - Not attended.
- Tony
  - Discussed issues on the 2033 Cyber Resilient EV Charging Station and Critical Infrastructure Workshop.

New Business:
Updates on Hands-on-Project.

CECIP-Project Team Meeting

8/09/2023
12:00pm
Room 120 Dunn Hall -UofM

Meeting called by:	Debera Pittman	Type of meeting:	Project Teams (Hands-on-Meeting)
Facilitator:	Dr. Myounggyu Won	Note taker:	Debera Pittman
Called to Order:	12:00:00 pm	Adjourned:	1:00 pm

Attendees: Dr. Myounggyu Won; Nathan Farrar; Allison Plank; Debera Pittman; John Jack O'Meara; Tony Pinson.

Minutes

Discussion:
Meeting Minutes – The minutes from the meeting that was held on August 2, 2023., are on One Drive, shared and written. The meeting was called to order by Debera Pittman.

General Discussion –

- Hans
  Not attended
- Nathan
  - Nathan demonstrated the prototype DWC system.
  - Nathan is ready to incorporate the actuator with the system.
- Allison
  - Allison presented two papers about cybersecurity for an EV charging system that Dr. Won suggested.
- Jack
  - Worked on the CTG course.
  - Worked with Sagar on the cyber resilience workshop presentation.
- Arturo
  - Not attended.
- Tony
  - Worked on the quarterly report.
  - Worked on the preparation for the Cyber resilience workshop.
  - Talked with Dr. Dasgupta about event preparation.

New Business:
Updates on Hands-on-Project.

Appendix 3

UofM Internal Team Minutes

CFIA - NCAE CI Project Team Meeting

04/05/2022
4:00pm
UofM Zoom

Meeting called by:	Dr. Dipankar Dasgupta	**Type of meeting:**	NCAE CI Project Team
Facilitator:	Tony Pinson	**Note taker:**	Doris Allen
Called to Order:	4:07 pm	**Adjourned:**	4:44 pm

Attendees: Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Dr. Amanda Rockinson; Nathan Farrar, Nathan Seymour; Tony Pinson; Doris Allen.

Minutes

Discussion:

Minutes – The meeting minutes from March 22, 2022 are approved as written. There was a motion by Dr. Dasgupta and a second by Nathan Seymour.

Old Business:

Smart Grid Security Workshop: The workshop was held on the campus of the University of Memphis. The building location was FIT – Fishbowl (Room 203/205). The date was Friday, March 25, 2022 as scheduled. A summary report of the workshop will be compiled by Dr. Hasan Ali. It is expected to be completed within the next 2 weeks.

Cybersecurity for Critical Infrastructure Workshop: The workshop was held on the campus of the University of Memphis. The building location was the Fogelman College of Business & Economics (Room 119). The date was Friday, April 1, 2022 as scheduled. (There was a last minute room change from Room 118.) A summary report of the workshop will be compiled by Nathan Seymour. It is expected to be completed within the next 2 weeks.

New Business:

The NCAE Semi-Annual Report: The target completion date for the semi-annual performance report for the NCAE-C-001-2021 grant is April 8, 2022. The report is being developed by Tony Pinson. The report should incorporate information / data provided by the partner institutions. Doris Allen is to provide input for Section 3g. Tony Pinson is to develop a paragraph for each workshop for Section 4a. Corinne O'Connor is to provide a summary report of the expenditures (e.g., though mid-March 2022) for Section 8.

Meeting was adjourned at 4:44 pm.

CFIA - NCAE CI Project Team Meeting

04/19/2022
4:00 pm
UofM

Meeting called by:	Dr. Dipankar Dasgupta	**Type of meeting:**	NCAE CI Project Team
Facilitator:	Tony Pinson	**Note taker:**	Doris Allen
Called to Order:	4:02 pm	**Adjourned:**	4:40 pm

Attendees: Dr. Dipankar Dasgupta; Dr. James McGinnis; Dr. Mohd Hasan Ali; Nathan Seymour; Nathan Farrar; Tony Pinson; Doris Allen.

Minutes

Discussion:

Minutes – The meeting minutes are approved as corrected. (The correction involved adding Dr. McGinnis' name along with Nathan Seymour to work on compiling the workshop report). A motion was made by Dr. Dasgupta and seconded by Dr. James McGinnis.

Dr. Dasgupta has suggested that starting with the May 3rd meeting, the time can be moved to 3:00 pm going forward.

Open Items:

Smart Grid Security Workshop – A summary report of the workshop event will be developed by Dr. Hasan Ali. It will be presented at the next CECIP Internal team meeting.

Cybersecurity for Critical Infrastructure Workshop – A summary report of the workshop event will be developed by Dr. James McGinnis and Nathan Seymour. It will be presented at the next CECIP Internal team meeting.

Semi-Annual Report – The semi-annual performance report for the NCAE-C-001-2021 grant was sent in, received by the organization, and accepted by the submission deadline date as required. (Date of submission: April 18, 2022).

New Business:

Grant Project Checklist – Dr. Hasan Ali will develop course materials for the Smart Grid Security classroom modules during the 2022 summer months. Dr. McGinnis and Nathan Seymour will develop course materials for the Cybersecurity for Critical Infrastructure classroom modules. The CECIP Internal team has set a target date of September 2022 to host a Competition/Tabletop Exercise Conference.

Grant Funding – Stephanie Thompson should be attending during the next scheduled CECIP Partners Meeting to discuss current year invoicing and second year funding for the NCAE-C-001-2021 grant.

Regarding the Project Checklist: the things to be uploaded to CLARK are classroom content, videos, & quizzes.

The meeting was adjourned at 4:40 pm.

CFIA - NCAE CI Project Team Meeting

05/03/2022
3:00pm
UofM

Meeting called by:	Dr. Dipankar Dasgupta	**Type of meeting:**	NCAE CI Project Team
Facilitator:	Tony Pinson	**Note taker:**	Doris Allen
Called to Order:	3:07 pm	**Adjourned:**	3:38 pm

Attendees: Dr. Dipankar Dasgupta; Dr. James McGinnis; Dr. Mohd Hasan Ali; Debera Pittman; Doris Allen; Tony Pinson.

Minutes

Discussion:

Meeting Minutes – The meeting minutes from April 19, 2022 were reviewed and approved as written.

Old Business:

Discussion

Smart Grid Security Workshop – Dr. Hasan Ali requested another week for the submission of the Smart Grid Security Report. He also indicated that a preliminary report had been emailed to Dr. Dasgupta.

Cybersecurity for Critical Infrastructure Workshop – Dr. McGinnis indicated that the Cyber Security for Critical Infrastructure summary report is almost complete.

Semi – Annual Report – The semi-annual performance report for the NCAE-C-001-2021 grant was sent, received, and accepted by the submission deadline.

Grant Project Checklist – Dr. Dasgupta indicated that the project modules will be based upon the various case studies from the workshop. He also stated that we are not in a good position to host a competition/tabletop event. Lastly, a general discussion was held regarding identifying the best subject matter expert for the review of the project modules.

General Discussion – Dr. Dasgupta indicated that students and the student workers should be encouraged to attend and to document attendance of webinars & competitions. Debera Pittman will collect information from Spencer (i.e. Cyber Tiger President). He encouraged members (i.e. Tony Pinson) to document their attendance of the CAE TechTalks series and other webinars as well.

New Business:

No new business.

Meeting was adjourned at 3:38 pm.

CFIA - NCAE CI Project Team Meeting

05/17/2022
3:00pm
UofM-FIT 324

Meeting called by:	Dr. Dipankar Dasgupta	**Type of meeting:**	NCAE CI Project Team
Facilitator:	Tony Pinson	**Note taker:**	Debera Pittman
Called to Order:	3:06 pm	**Adjourned:**	3:45 pm

Attendees: Dr. Dipankar Dasgupta; Dr. James McGinnis; Dr. Mohd Hasan Ali; Debera Pittman; Doris Allen; Tony Pinson.

Minutes

Discussion:

Meeting Minutes – The meeting minutes were reviewed and approved as written.

Old Business:

Discussion

Smart Grid Security Workshop – Dr. Ali has submitted his final workshop report to Dr. Dasgupta. The data should be double checked for total number of registered participants, via virtual and in person.

Cybersecurity for Critical Infrastructure Workshop – Dr. McGinnis has submitted his final report to Dr. Dasgupta. Doris is working to have the final report ready by the next meeting. Tony will then have the final report uploaded to the website.

NCAE-C-001-2021 Grant Project Checklist – Prepare content on SGS content for review. Selecting a subject matter expert to review the content (Smart Grid Security), possibly Mr. Chip Harris, was discussed.

General Discussion – Prepare course content for upload to CLARK website.

New Business:

Dr. Dasgupta would like to have the teams plans for the summer months. We will continue having our internal meetings every two weeks during the summer. Dr. McGinnis will be on campus Tuesdays and Thursdays. Dr. Ali is available all summer with exception of one family trip planned.

A motion to adjourn by Dr. McGinnis; and seconded by Dr. Ali.

Meeting was adjourned at 3:45 pm.

CFIA - NCAE CI Project Team Meeting

05/31/2022
3:00pm
UofM

Meeting called by:	Dr. Dipankar Dasgupta	**Type of meeting:**	NCAE CI Project Team
Facilitator:	Tony Pinson	**Note taker:**	Doris Allen / Debera Pittman
Called to Order:	3:12 pm	**Adjourned:**	3:48 pm

Attendees: Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Debera Pittman; Doris Allen; Tony Pinson; Nathan Farrar.

Minutes

Discussion:

Meeting Minutes – The meeting minutes from May 17, 2022, were reviewed and corrections are to be made before the approval at the next scheduled meeting. The correction is regarding the CLARK content / course numbers.

Old Business:

General Discussion – The team will hire Mr. Chip Harris as the subject matter expert (SME) reviewer. Three courses are to be developed and subsequently reviewed by him. After the review, they will then be posted to CLARK.

The Smart Grid workshop report is on schedule to be finalized on/before June 3rd.

Dr. Ali and Nathan Farrar are working on a hands-on a training / presentation PowerPoint. It will be delivered to CLARK by the end of the summer.

It was noted that Dr. Kevin Bryant of NCA&T State University indicated that the IoT Workshop scheduled for June 2022 has been postponed and set for September 2022.

New Business:

What other partner institutions are doing during the summer months is to be added to the CECIP Internal Meeting agenda.

Tony Pinson is to maintain an up-to-date project team checklist of deliverables. He is also assisting Dr. Ali and Nathan Farrar with preparation of the SGS materials for upload to the Clark website.

Dr. Won's Cyber Ambassador summer camp is tentatively scheduled for the first week in July 2022. The CfIA staff will be available to assist as needed.

A motion to adjourn was made by Dr. D. Dasgupta. It was seconded by Doris Allen.

The meeting was adjourned at 3:38 pm.

CFIA - NCAE CI Project Team Meeting

06/14/2022
3:00pm
UofM-FIT 324

Meeting called by:	Dr. Dipankar Dasgupta	**Type of meeting:**	NCAE CI Project Team
Facilitator:	Tony Pinson	**Note taker:**	Debera Pittman / Doris Allen
Called to Order:	3:08 pm	**Adjourned:**	3:42 pm

Attendees: Dr. Dipankar Dasgupta; Dr. James McGinnis; Dr. Myounggyu Won; Debera Pittman; Doris Allen; Tony Pinson; Mikhelle Taylor; Nathan Farrar.

Minutes

Discussion:

Meeting Minutes – The meeting minutes for the May 17th meeting were reviewed and approved as corrected.

The meeting minutes for the May 31st meeting were reviewed and approved as corrected.

Old Business:

Dr. Dasgupta indicated that to help reduce corrections, Debera will take the minutes for the CECIP Internal meetings and Doris will take the minutes for CECIP Partners' meetings. Final changes before distribution will be completed by Tony Pinson.

Dr. James McGinnis will get in touch with Mr. Chip Harris, cybersecurity SME, within the next few days to determine if he would agree to review our smart grid and critical infrastructure security module content. Team members should have module content ready for review by early July. We should plan to have Chip Harris' contract ready by the first week of July.

A project student worker, Ken Schnarrs, will be working with Dr. McGinnis on the cybersecurity for critical infrastructure module content. The goal is to have all the modules completed by the end of August 2022.

Dr. Won is working with student workers to develop hands-on activities for the Cyber Ambassador technical camp. The camp is scheduled to be held during the first week of July.

Dr. Dasgupta said that it would be good if someone wanted to volunteer for the summer camp. He also stated that it would be okay to invite an undergraduate research student from an institution like Rhodes college. Doris will handle getting the appropriate volunteer waiver forms in place and signed as needed. Dr. Won has sent an email to a potential volunteer student and is waiting to hear back.

Dr. Won will add a folder to OneDrive to archive the Cyber Ambassador tech camp activities that are cybersecurity related. At the next meeting, Tony Pinson will display an example of how some universities are submitting modules for posting to the Clark website.

New Business:

Dr. Dasgupta would like for the team to continue reporting updates at each team meeting.

Mikhelle Taylor is working on budget modifications and Corinne O'Conner will be giving her a statement next week.

Dr. Dasgupta stated that all cyber security activities should be reported to the CfIA, even if they are not directly related to a specific project. The University of Memphis has been redesignated as a Center for Academic Excellence in Cyber Defense through 2027.

Dr. Won, Andrika Cheairs, Ken Schnarrs, and other student workers are working on an autonomous race car project. The presentation slides will be ready by the end of August.

Nathan Farrar is working on a forensics training report. Tony Pinson will look up previous documents and share with Nathan and Ken.

Dr. Dasgupta stated that our students should attend the internal CECIP meetings because they are a part of the grant funding. Debera will change the weekly project meetings in DH-120 to a day in which the student workers are all available. He also stated that the conference in Atlanta, GA went very well. There are lots of cyber security opportunities for good jobs in both industry and government agencies. He checked for a CLARK document submission. There are no CLARK document standards yet.

Dr. Dasgupta made the motion for adjournment. Dr. Won seconded it.

The meeting adjourned at 3:42 pm.

CFIA - NCAE CI Project Team Meeting

06/28/2022
3:00pm
FIT 324 - UofM

Meeting called by:	Dr. Mohd Ali	**Type of meeting:**	NCAE CI Project Team
Facilitator:	Tony Pinson	**Note taker:**	Debera Pittman / Doris Allen
Called to Order:	3:11 pm	**Adjourned:**	3:54 pm

Attendees: Dr. James McGinnis; Dr. Mohd Ali; Dr. Myounggyu Won; Tony Pinson; Mikhelle Taylor; Debera Pittman; Doris Allen; Nathan Farrar; Andrika Cheairs.

Minutes

Discussion:

The minutes for the June 14th meeting of the CECIP Internal team were approved as written. Debera Pittman made the motion: Doris Allen seconded it.

Old Business:

Mikhelle Taylor provided a report on the grant funding status. She indicated that a copy of the budget overview, received from Corinne O'Conner, was sent to Tony Pinson and Dr. Dasgupta.

Tony reports that UWF is the only partner institution that is conducting summer CECIP training courses. He indicated that UWF has conducted or will conduct the following project training courses: (1) ICS-RE Security Course: May 16-27, 2022, (2) Cybersecurity Maturity Model Certification Course: June 13-24, 2022, (3) NERC-CIP Standards & Compliance: August 1-12, 2022, (4) ICS-RE Threat Intelligence: August 22-26, 2022. UWF are offering two-course modules also: ETI 1701 and ETP 2930. The other partner institutions have workshops planned for Fall 2022.

After briefly reviewing a generic Clark guideline document that he created, Tony walked through an example of a course module from the Clark website. Dr. McGinnis inquired as to the process for uploading/submitting our work to the Clark websites. Tony will find out this information and report his findings back to the group at the next scheduled meeting.

Dr. McGinnis stated that he has been in touch with Mr. Chip Harris regarding the SME opportunity for the CECIP Smart Grid Security and Cybersecurity for Critical Infrastructure modules. They have a meeting scheduled for Friday July 1st. Dr. McGinnis also provided an update on the Cybersecurity for Critical Infrastructure module. It is 65-70% completed. The slides for the module look good but needs rearranging. He is investigating whether this course should be considered a module or a nano module.

Dr. Ali indicated that the Smart Grid Security module is on track for completion.

New Business:

Dr. Won sent the tentative agenda for the Cyber Ambassador Tech Camp to volunteer staff team members. The slides have been created and sent to the students before the camp. He is monitoring the camp registration and is expecting thirty-five students to attend. He also indicated that the lab (Dunn Hall – 118) has been reserved for the 3-day tech camp (i.e., July 5-7).

Dr. Won indicated that all team members have read and signed the required policy/form entitled "Minors on Campus." All staff and volunteer background checks have been completed. He will be sending out the finalized agenda by tomorrow to all team members.

Dr. Won will be getting an update on the Track/Autonomous Cars project on Thursday during the weekly team meeting.

Dr. Ali indicated that Nathan Farrar is reviewing the Digital Forensic Professional Development report information for IoT digital forensic ideas. Nathan will seek more input from Dr. Dasgupta regarding the detailed requirements for the assignment.

The meeting at 3:54 PM. Dr. Ali made the motion: it seconded by Nathan Farrar.

CFIA - NCAE CI Project Team Meeting

07/12/2022
3:00pm
FIT #324 - UofM

Meeting called by:	Tony Pinson	**Type of meeting:**	NCAE CI Project Team
Facilitator:	Tony Pinson	**Note taker:**	Doris Allen / Debera Pittman
Called to Order:	3:05 pm	**Adjourned:**	3:45 pm

Attendees: Dr. Dipankar Dasgupta; Dr. James McGinnis, Dr. Mohd Hasan Ali; Dr. Myounggyu Won; Debera Pittman; Doris Allen; Tony Pinson; Nathan Farrar.

Minutes

Discussion:

Meeting Minutes – The minutes from the meeting held on June 28, 2022, were reviewed and approved as written. Dr. James McGinnis made the motion to approve. Debera Pittman seconded it.

Old Business:

General Discussion

Dr. Won gave an update on the two (2) Lab Exercise Projects.

Project #1. The student workers have created a new model for the autonomous car project that is accurate. They are making nice progress. The RC car can avoid obstacles and can drive autonomously very nicely. But the objective and focus is to develop cyber security for autonomous driving. Dr. Won indicated that he is researching the literature to find out if there are any prototypes and how best to integrate them.

Project #2. Ken Schnarrs and Andrika Cheairs are working on this project. Andrika is learning how to use the Arduino Uno toolkit and the C programming language for the project. Ken Schnarrs' primary responsibility is C programming for the project. Dr. Won will create a PowerPoint presentation incorporating Arduino Uno introductory slides along with more technical details and depth for the IoT Security projects. Dr. Dasgupta mentioned that a weekly project activity plan should be made for Nathan Farrar (Electrical Engineering student) and Ken. Nathan joined the project group on Thursday July 7th and indicated that Arduino Uno security can be compromised using buffer overflow or stack access, if the device had a Wi-Fi (Blue Tooth) component. He is willing to pursue whichever method the group decides on. The group will collaborate with Dr. Won to complete the coding for the project. Dr. Won will also brainstorm some IoT Arduino security issues incorporating Wi-Fi (Blue Tooth) for the project. Dr. Dasgupta indicated that we should have a better idea as to the lab portion of the IoT Security Workshop by next week. This project is slated to be incorporated into the NCA&T IoT Workshop in September 2022.

Development of the two curriculum courses (i.e., Smart Grid Security, Cybersecurity for Critical Infrastructure Protection) are 80-90% complete. Debera will make sure Ken and Andrika are present for the CECIP internal meetings going forward. Dr. James McGinnis asked a question regarding who will be doing the SME reviews. Dr. Dasgupta suggests contacting Dr. Andrew Neal. Otherwise, we will have to look at other universities. The UofM project curriculum materials will be shared with our partners before submission to the CLARK website. Dr. Dasgupta indicated that curriculum materials were used in classroom courses during the Spring 2022 semester. It should be noted in our progress reports to the government. He recommended that the course title and number specified as well. Smart Grid Security topics were incorporated in the EECE 4205/6205 (Modern Grid with Renewables) course.

Tony Pinson gave an update on submitting materials to the CLARK website. He stated that there is a provision for adding curriculum to the website. The curriculum materials will have to go to a review committee first. He will present the required steps for this process during the next meeting for adding a course / module to CLARK.

New Business:

No new business.

The meeting adjourned at 3:45 pm. Dr. Dasgupta made the motion. Doris Allen seconded it.

CFIA - NCAE CI Project Team Meeting

07/26/2022
3:00pm
FIT 324 - UofM

Meeting called by:	Dr. Dasgupta	**Type of meeting:**	NCAE CI Project Team
Facilitator:	Tony Pinson	**Note taker:**	Debera Pittman/Doris Allen
Called to Order:	3:05 pm	**Adjourned:**	3:43 pm

Attendees: Dr. Dasgupta; Dr. McGinnis; Doris Allen; Tony Pinson; Debera Pittman; Nathan Farrar; Andrika Cheairs.

Minutes

Discussion:

The meeting was called to order by Tony Pinson. The minutes from the CECIP Internal Team meeting held on July 12, 2022, were reviewed and approved with a minor correction: Dr. McGinnis' name was added to the list of attendees. Dr. Dasgupta made the motion to approve the minutes. Dr. McGinnis seconded the motion.

Old Business:

General Discussion: Dr. Ali is attending a workshop/conference in Gulfport, Mississippi. Dr. Won is overseeing the summer projects. He reminded everyone that there is only one month remaining to finish the summer lab projects. Nathan indicated that he thought the project was doable despite the timeframe. On August 1,2022, a new student named Hans Amelang is scheduled to join the project group.

Dr. Andrew Neel has been hired as the subject matter expert for the CECIP Internal team course modules. Tentatively, Dr. Neel will be scheduled to review the Smart Grid Security, Cybersecurity for Critical Infrastructure, and Zero Trust course modules, respectively. Dr. Dasgupta indicated that he will be adding roughly 36 slides to the Zero Trust course module that Nathan initially worked on. Dr. Won provided two reports for reviewed by the group. The reports were on the Autonomous Race Car and the Arduino IoT projects, respectively. Thereafter, Dr. Won provided a project update on the students.

(1). Autonomous R/C Project

Luke and Douglas have made substantial progress improving the accuracy of the autonomous driving model. They have obtained good understanding of the Autonomous R/C car software, stack, server platform, and machine learning framework. They are ready to transition to implement cybersecurity projects with the Autonomous R/C car. Dr. Won requested them to brainstorm potential cybersecurity projects given the limited timeframe. Dr. Won suggested a couple of cybersecurity ideas for the Autonomous Race Car project to them and indicated that he is reviewing literature on automotive security. He will discuss the ideas in more detail during the next project meeting.

(2). IoT Cybersecurity Project

After the meeting last Thursday, Ken and Nathan have made good progress on the project. They have successfully verified that our approach for the buffer overflow attack can actually "break" the Arduino. This is good news because we can apply this buffer overflow attack to various IoT projects that we used for Cyber Ambassadors Tech Camp and real-world applications such as the light control system that Nathan has suggested to make the project aesthetically pleasing. I view that Ken and Nathan are on track and will be able to complete the cybersecurity project development by the end of August. The group viewed the video of the car on the track.

Regarding the hands-on-projects, Dr. Dasgupta mentioned that the cybersecurity components should be added to the projects next. He also indicated the Corinne is reviewing the CECIP project's budget and although we have only received funding for one year of the proposed budget, it will have to be spread out over the second year period.

New Business:

No new business.

The meeting adjourned at 3:45pm. Dr. Dasgupta made the motion. Doris Allen seconded it.

Appendix 4

CECIP Partners Team Minutes

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

April 4, 2022

I. Call to order

The meeting was called to order at 3:35 pm.

II. Roll call

The following persons were present: Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Dr. Guillermo Francia; Dr. James McGinnis; Dr. Kelvin Bryant; Dr. Yuan; Mr. Tony Pinson; and Ms. Doris Allen.

Minutes:
The meeting minutes from the last meeting were approved as written. The motion was made by Dr. Guillermo Francia and a second by Dr. Hasan Ali.

III. Principal Investigator Reports:

University of West Florida – Dr. Francia gave the report. He indicated that a workshop between UWF and Indian River Community College (IRCC) is tentatively being scheduled for the first or second week of June 2022. A second workshop is being planned for Pensacola, FL in the Fall of 2022. He also indicated that they have become the recipients of new equipment for renewable energy programming and security (e.g. SCADA System). It will become a part of the university's Cyber Range.

University of Memphis – Dr. Hasan Ali gave the report. He indicated that the U of M (CFIA) team has fulfilled its' successful implementation of the Smart Grid Security and also the Cybersecurity for Critical Infrastructure workshops.

North Carolina A&T University – Dr. Bryant and Dr. Yuan collaborated to provide their team's report. An IoT module has been added to one of the university's Spring 2022 courses. An IoT Workshop is being planned for 2022.

New Business / General Discussion: Dr. James McGinnis suggested that the team should put together a schedule of events for the project moving forward.

Adjournment:

The meeting was adjourned at 3:55 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

May 02, 2022

I. Call to order

The meeting was called to order at 3:34 pm.

II. Roll call

The following persons were present: Dr. Dipankar Dasgupta, Dr. James McGinnis, Dr. Kelvin Bryant, Dr. Guillermo Francia, Dr. Shankar Banik, Mikhelle Taylor, Tony Pinson, Debera Pittman, and Doris Allen.

Minutes: The meeting minutes for the last meeting were reviewed and approved as written. The motion was made by Dr. Dasgupta and seconded by Dr. Francia.

III. Principal Investigator Reports:

University of West Florida – Dr. Francia gave the report. He indicated that they have reviewed and updated the generic project timeline provided for their institution to reflect their project activities more accurately. He also indicated that quarterly reports and an aggregate final report will be developed outlining the number of students impacted by their workshops/courses.

University of Memphis – Dr. Dasgupta and Dr. McGinnis collaborated to give the report. They indicated that the University of Memphis team is working on comprehensive reports, based upon case studies, for the Smart Grid Security as well as the Cybersecurity for Critical Infrastructure workshops. Recommendations for improvements and classroom modules are forthcoming. Dr. Dasgupta also indicated that the hybrid workshop format was beneficial from an attendance standpoint.

Citadel - Dr. Banik gave the report. He indicated that his team has identified three (3) classes for which they are designing modules. The classes are CSCI 227, INTL 465, and CSCI 490. He and his co-PI's are designing the modules for CSCI 227 and INTL 465. The professor who was to teach the CSCI 490 course has resigned. They may seek out a subject matter expert (SME) to assist with designing the modules for the CSCI 490 course. He also indicated that their cyber tabletop exercises took place, in conjunction with the South Carolina National Guard, during the February 2022 Jack Voltaic Conference. Finally, a cybersecurity workshop is being planned for the Fall semester of 2022. It should last for one to one and a half days.

North Carolina A&T University – Dr. Bryant provided the team report. He reviewed the schedule. He indicated that IoT Security modules are being developed for their summer GenCyber workshops. IoT Security modules for professionals are forthcoming as well.

New Business / General Discussion: It was decided that the necessary discussion regarding the project budget and invoice submissions will be postponed until the next scheduled meeting. Additionally, a suggestion was made to provide due dates for the quarterly written reports for each institution. The suggestion was acceptable to the team members present. The due dates for the quarterly reports are to be incorporated into the timeline.

IV. Adjournment:

The meeting was adjourned at 3:55 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

June 06, 2022

I. Call to order

The meeting was called to order at 3:35 pm.

II. Roll call

The following persons were present: Dr. Dipankar Dasgupta, Dr. James McGinnis, Dr. Kelvin Bryant, Dr. Guillermo Francia, Dr. Shankar Banik, Mikhelle Taylor, Stephanie Thompson, Tony Pinson, Debera Pittman, and Doris Allen.

Minutes: The meeting minutes from the May 2, 2022, meeting were reviewed, corrects were made, after which they were subsequently approved as corrected. The motion for approval was made by Dr. Francia and seconded by Dr. Bryant.

III. Principal Investigator Reports:

University of West Florida – Dr. Francia gave the report. He indicated that IRSC had 18 participants for the NERC CIP course, UWF had 15 workshop participants for the ICS-RE course, and UWF is planning a face-to-face Faculty Development Workshop for roughly 30 faculty members the last week of June. He states that all summer workshops will be completed by August. He will be sending in the summary reports once all workshops are completed. There will be a total of three reports.

University of Memphis – Dr. McGinnis gave the report. He indicated that he is working on the first draft of the Cybersecurity for Critical Infrastructure case studies by the end of the June. Dr. Dasgupta also indicated that some Arduino projects are being considered for hands-on activities associated with the CECIP project.

Citadel - Dr. Banik gave the report. He indicated that his team is developing course modules. They have a subject matter expert for their CSCI 490 class. They are planning a workshop for Fall 2022. They are also designing some tabletop exercises for Fall 2022.

North Carolina A&T University – Dr. Bryant gave the report. He indicated that the IoT Workshop proposed for their 2022 GenCyber Summer Camp was not adequate for the CECIP grant. He also stated that the dates for the Fall 2022 CECIP IoT Workshop, tentatively scheduled for September, will be solidified after a discussion with Dr. Roy. Dr. Dasgupta offered to help them with planning and promotion for the event. Dr.

Dasgupta also indicated that a flyer should be created to help with advertising for the event.

New Business / General Discussion: Stephanie Thompson gave a report on the CECIP grant funding status. She indicated that all subawards are fully executed and encouraged all partner institutions to submit their invoices accordingly. She also indicated that the budget is on track and that partner institutions should connected with their grant officers assess their grant budget information. She indicated that we are currently implementing a two-year project under a one-year base budget, unless the option year funding issue can be resolved, until 12/31/2023. She also stated that she has been in contact with the grant officer and is working with the sponsor to correct the budgeting issue.

Mikhelle Taylor stated that funding issued was caused by a misunderstanding associated with base year and option year funding in the new grant form. Mikhelle also indicated that the error has been corrected on the updated form.

Tony Pinson has developed a check list for all the partner institutions to utilize. He also displayed some of the summary reports that were developed for the UofM CECIP workshops. Dr. Dasgupta encouraged the partner institutions to create similar reports and send them in for the grant final report.

IV. Adjournment:

The meeting was adjourned at roughly 4:28 pm. Motion was made by Dr. Francia, a second was made by Dr. Banik.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday - July 11, 2022 – 3:30pm

I. Call to order

The meeting was called to order at 3:32 pm by Dr. Dipankar Dasgupta.

II. Roll call

The following persons were present: Dr. Dipankar Dasgupta; Dr. James McGinnis; Dr. Hasan Ali; Dr. Guillermo Francia; Dr. Shankar Banik; Dr. Kaushik Roy; Mikhelle Taylor; Tony Pinson; Debera Pittman; and Doris Allen.

Minutes: The meeting minutes from the June 6, 2022, meeting were reviewed. Minor corrections were made. They were approved with corrections. Dr. Dasgupta made the motion for approval. Dr. Francia seconded it.

III. Principal Investigator Reports:

University of West Florida – Dr. Francia gave the report. He indicated that he will be updating the existing project activities report as opposed to sending three reports. Additionally, he indicated that they completed the Cybersecurity Maturity Model Compliance course, where they had 15 participants, and the Faculty Development workshop, where 21 faculty members from across the country attended. They anticipated having 30 in attendance, but some of them had travel problems. Future UWF CECIP project activities are outlined in the planned activities section of their report. During the 2nd year, they will be embedding the module information into their classroom courses. IRSC will be conducting 3 of the classroom courses, whereas UWF will be conducting 2.

Citadel - Dr. Banik gave the report. He indicated that a subject matter expert has been found for their CSCI 490 course. He also indicated that his team is developing modules for a special topics course to be held during Fall 2023. They are working on Tabletop modules. They have not finalized the date for the Fall Workshop but will forward to the group once it has been established. The target date is in October 2022. Tony Pinson developed a generic guideline, based upon existing courses posted to Clark, that will be shared with CECIP team.

University of Memphis – Dr. McGinnis gave the report. He gave an update on the case study that was being developed for the Cybersecurity for Critical Infrastructure module for the Clark website. He indicated that he had received first-hand information from a

corporate representative associated with the victimized company. The new information should permit them to go into more detail about the cybersecurity breach. The module should be available for subject matter expert review in a couple weeks. Dr. Dasgupta indicated that the UofM CECIP modules will be shared with the partnering institution teams before being submitted to the Clark website. Dr. Ali indicated that progress is being made on the slides for the Smart Grid Security module. He indicated that it be done soon. Dr. Dasgupta indicated that Zero Trust module is also being developed. He also indicated that some work is being done on IoT (i.e., Arduino Uno activities).

North Carolina A&T University – Dr. Roy gave the report. He indicated that although a date has not been set, the IoT Security Workshop will likely be held around the end of September 2022. IoT Security module information was implemented into their Spring 2022 classes, and they plan to incorporate the material into their Fall 2022 classes as well. Dr. Dasgupta indicated that the course title, course number, and the number of students impacted should be documented and shared. Dr. Roy indicated that Dr. Bryant will be the primary agent in conducting the IoT workshop for NCA&T State University. They are planning to advertise the workshop with flyers. Dr. Bryant and a Master of Science Student are developing modules for IoT (i.e., Workshop on IoT: Explainable AI). They plan to submit the module to the Clark website during the spring. Dr. Roy will share the IoT slides with Tony Pinson.

New Business / General Discussion:

Mikhelle Taylor met with Alice in July. Alice indicated that there is no additional funding for the 2nd year. Each institution will have to rework its' budget, include justifications for the changes, and send it to her for the 2nd year. She will compile the principal investigator changes, change in sponsor's budget, and send to the project sponsor for approval. In summary, the money that we have received is all that will be available for the project (per Dr. Dasgupta). Mikhelle indicated that any changes would probably be easiest to do through their internal budget forms.

IV. Adjournment:

The meeting was adjourned at 4:12 pm. Motion was made by Tony Pinson, a second was made by Dr. Dasgupta.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday. August 01, 2022

I. Call to order

The meeting was called to order at 3:34 pm.

II. Roll call

The following individuals were present: Dr. Dipankar Dasgupta; Dr. Guillermo Francia; Dr. Kaushik Roy; Tony Pinson; Debera Pittman; and Doris Allen.

Minutes: Tony Pinson reviewed the July 11, 2022, CECIP Partners Meeting minutes. The minutes were approved as written. Dr. Francia made the motion for approval: Dr. Roy seconded it.

III. Principal Investigator Reports:

University of West Florida – Dr. Francia gave the report. He indicated that they were in session with their 3rd course associated with the project entitled NERC CIP Compliance. He also stated that in 2 weeks they will be conducting a Faculty Development Workshop on ICS Security. They are anticipating having their 4th and final agreed upon project course during the 3rd week in August entitled "ICS Threat Intelligence." The remaining money from their project budget will be used to conduct a small course on ICS Security in November or December 2022.

University of Memphis – Dr. Dasgupta gave the report. He stated that the students at UofM are working to complete their summer lab projects. He also indicated that they have hired a subject matter expert (SME) to review their CLARK course modules. The UofM will share the course modules with the partners once they have been completed.

Citadel – Not available.

North Carolina A&T State University – Dr. Roy gave the report. He stated that their Masters' students are continuing to work on the slides and the lab exercises for the IoT Security Workshop. The tentative agenda for the workshop was sent to Dr. Bryant. The hybrid workshop is tentatively scheduled for September 23rd from 9:00AM - 2:30PM EST. Dr. Dasgupta indicated that he is available to be physically present on the date of the workshop. He committed to being a face-to-face participant. Dr. Roy indicated that he sent the IoT Security slides to Tony Pinson. The updated Fall 2022 slides will also be

sent to Tony once they are completed. Bianca will contact Tony about the workshop flyer. Dr. Dasgupta stated that the UofM project students are working on IoT activities in the lab and can share their exercises with the NCAT students. He indicated that the students should set up a zoom meeting to share ideas. Additionally, he stipulated that the UofM students could demonstrate their buffer overflow attack during the IoT Security Workshop. Dr. Roy indicated that Dr. Lindrick, former NC A&T State University student, will be conducting demonstrations focused on IoT hardware. Dr. Dasgupta indicated that as soon as Tony receives the flyer, he can set up the registration for the IoT Security Workshop. The goal is to have the flyer and registration link available so that the other partner institutions can help advertise the event.

New Business / General Discussion: Tony Pinson states that all institutions should get their budget revisions/changes in to Mikhelle Taylor.

IV. Adjournment:

The meeting adjourned at 4:08 pm. Dr. Francia made the motion. Dr. Dasgupta seconded it.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

September 12, 2022

I. Call to order

Dr. Dipankar Dasgupta called to order the regular meeting of the CECIP Partner Meeting at 3:40 pm on 09/12/2022 via U of M hosting Zoom.

II. Roll call

The following persons were present: Dr. Dipankar Dasgupta; Dr. Guillermo Francia; Dr. Myounggyu Won; Dr. Melissa Graves; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

The August 1 meeting minutes were approved as written. Dr. Dasgupta made the motion and Doris Allen seconded it.

III. Project Timeline P.I. Reports:

NCA&T State University:

Dr. Dasgupta gave the report for Dr. Roy. He noted that Dr. Roy will not attend the meeting because he tested positive for covid 19. He also indicated that the U.S Government First Lady, Dr. Jill Biden, is visiting NCA&T State University today. As a result, their faculty is relatively preoccupied. Additionally, Dr. Dasgupta suggested that The Citadel and the University of West Florida should invite their students to join the IoT Security workshop. He requested that the project coordinator, Tony Pinson, send them the web links to the IoT Security flyer and registration page for advertising. He would like to have at least 5 or 6 participants from each partner institution in attendance.

University of Memphis:

Dr. Dasgupta gave the report. He stated that webpage links for the IoT Security Workshop registration and flyer have been created. As of August 1, 2022, forty individuals had registered for the event. About half of the individuals registered for the virtual option. Dr. Won spoke about the two project teams. One student team is working on an autonomous car project. The other student team is working on an IoT attack project for the upcoming IoT Security Workshop. Nathan Farrar is creating a video demonstration of the Buffer Overflow Attack to be shown during the IoT

Security Workshop. The second team is also working on some Arduino project ideas for future summer camps. The project coordinator, Tony Pinson, will be sending the links to the other institutions for the workshop flyer and registration for advertising purposes. Dr. Dasgupta indicated that Dr. Andrew Neel is under contract until the end of September. Dr. Neel should be sent the Zero Trust Module by September 15. Additionally, the Smart Grid Security Module's status should be checked and forwarded to Dr. Neel as soon as possible to ensure that all reviews are completed by the end of September 2022.

Citadel College:

Dr. Melissa Graves gave Citadel College's report. She is continuing to design a critical infrastructure course. She worked on it this past summer and is teaching modules from it in the classroom this Fall. She indicated that KBSI, a contractor, designed a software product (e.g., SIP IP) that enables students to calculate security risk. Students in their classes have access to the software through KBSI's cloud network. The hope is that in the future that instead of having colleges & universities charging students a lab fee, KBSI will make available to the public through its cloud network. She also indicated that they are awaiting approval from DHS and final approval from Office of Director of National Intelligence (ODNI) for the release of tabletop exercise they have written. Finally, Dr. Banik is working with a subject matter expert from the Naval Information Warfare Center on a course on "Cyber-Physical Systems." It will be the subject of a course that will be offered in Spring 2023. They are planning a faculty development workshop for Spring 2023.

University of West Florida:

Dr. Guillermo Francia delivered the report. They have completed their last two proposed courses: NERC CIP Compliance & ICS Threat Intelligence course. They held the third faculty development workshop on Cybersecurity Scenario Workshop. They had nine participants to attend virtually. The goal was to trained faculty to develop virtual ICS on docker containers to deploy in ICS environments. Students would then program PLCs and develop HMI upon which to conduct penetration testing. They will be including this workshop as one of the artifacts for their contribution to the project. They are planning their last course on ICS Security for Oct. 24 – Nov. 16, 2022. The goal of the course is to have students be able to deploy a virtual environment to run virtual/physical PLCs to conduct security exercises on ICS systems.

IV. Adjournment:

The meeting was adjourned at 4:15 pm. Dr. Francia made the motion and Dr. Dasgupta seconded it.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday - October 03, 2022

I. Call to order

The meeting was called to order at 3:34 pm.

II. Roll call

The following persons were present: Dr. Dipankar Dasgupta; Dr. Myounggyu Won; Dr. Shankar Banik; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

The meeting minutes from 9/12/2022, were reviewed and approved with minor corrections. Dr. Dasgupta made the motion for approval. Dr. Banik seconded it.

III. Principal Investigator Reports:

University of West Florida – There was no representative available during the meeting.

NCA&T State University – There was no representative available during the meeting.

Citadel College – Dr. Banik gave the report. He stated that the KBSI software from Dr. Graves critical infrastructure course will be available free of charge through Citadel College's cloud platform. It will make it available through one of their CECIP project modules. Dr. Graves is also working on case scenario exercises with DHS. Once approved, they will be shared with the CECIP partnering institutions' faculty for use. The course on cyber-physical systems is on schedule to be offered during Spring 2023 term. The faculty workshop date has not been finalized. It should be determined by the next CECIP Partners meeting. It will be offered in a hybrid format.

University of Memphis – Dr. Dasgupta gave the report. He indicated that Dr. Won is working on security exercises in two different domains: autonomous vehicle security and water pumping station security. He also indicated that the two UofM CECIP project modules that will be released to CLARK have been reviewed by a subject matter expert (SME). The modules will be released to the partners soon. The UofM project team is seeking opportunities to present the modules to the CAE community.

Dr. Won indicated that Mr. Hans Amelang has started working on an industry IoT project. He has reviewed some very interesting papers on the subject. One of the papers focuses on a SCADA simulation system and there is a possibility of obtaining a student

version of SCADA system upon which to simulate attacks. Speculation is that the student version of the SCADA simulation software is free. Nathan is developing a prototype for an EV charging system. The autonomous car project team is waiting on the delivery of race car track floor mats. They are also looking into the image processing capabilities of the software for vulnerabilities. The overall project timeline is a little behind schedule due to the amount of time required for in depth research on the topic.

IV. Adjournment:

The meeting adjourned at 4:05 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday - November 07, 2022

I. Call to order

The meeting was called to order at 3:39 pm.

II. Roll call

The following people were present: Dr. Dipankar Dasgupta; Dr. Guillermo Francia; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

The minutes from last month's meeting (October) will be approved during the next scheduled meeting.

III. Principal Investigator Reports:

University of West Florida – Dr. Francia gave the report. He indicated that the ICS RE course modules will be available to students in the future through a UWF course. He had nine students to attend. UWF will wrap up their project activities during Spring 2023. The completed modules have met the objectives that were set for the project. He will send the modules to Tony Pinson to be included in the annual report.

NC A&T State University – There were no representatives available during the meeting.

Citadel College – There were no representatives available during the meeting.

University of Memphis – Dr. Dasgupta did not give a report this week. He will instead schedule a meeting with Tony to finalize the UofM report.

IV. Adjournment:

The meeting was adjourned at 3:44 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday - December 05, 2022

I. Call to order

The meeting was called to order at 3:32 pm.

II. Roll call

The following persons were present: Dr. Myounggyu Won; Dr. Kelvin Bryant; Dr. Guillermo Francia; Dr. Melissa Graves; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

Minutes: The minutes were reviewed for the November 7th and October 3rd meetings. Dr. Francia indicated that corrections need to be made to his November 7th meeting report. Tony Pinson will make the corrections. Dr. Francia made the motion to approve the minutes for November 7th meeting as corrected. Dr. Won seconded the motion.

The minutes for the October 3rd meeting were approved as written. Dr. Won made the motion to approve the minutes. Dr. Francia seconded the motion.

III. Principal Investigator Reports:

University of West Florida – Dr. Francia gave the report. They are wrapping up their part of the project. They are preparing to submit the modules to Clark. He invited colleagues to submit a paper for the Advances in Computing Research workshop which will take place in Orlando, Florida on May 8 – 10, 2023. The submission deadline for papers is January 15, 2023. A notification of acceptance will be given by February 15, 2023. Registration will officially open on March 15, 2023. He will be sending the flyer for the workshop to other partner institutions.

NC A&T State University – Dr. Bryant gave the report. He stated that Dr. Roy has completed and submitted the IoT workshop report. They have a graduate student who is working on an IoT research paper which will be submitted in January 2023.

Citadel College – Dr. Graves gave the report on behalf of Dr. Banik. She indicated that they identified two existing courses and one new course that will be using modules on cyber protection/critical infrastructure. The courses identified are CS 227 (Principles & Practices in Cybersecurity), Intel 465 (Special Topics in Critical Infrastructure Protection), and CS 490/690 (Special Topics on Cybersecurity for Industrial Control

Systems). Case scenarios, pre-tests, and post-tests are being developed for the courses. They are attempting to make the courses accessible to the consortium. They are planning a workshop which has a tentative date of May 15, 2023. She will notify partner institutions if the workshop will be offered in a hybrid format after consulting with Dr. Banik.

University of Memphis – Dr. Won gave the report. He indicated that there are three groups of students developing modules. Hans Amelang is working on a cybersecurity water pump project. Once the project prototype is complete, cybersecurity exercises will be developed. The team will document and create the modules. The second team is working on an autonomous vehicle cybersecurity project. They have upgraded the track and developed two different cyber scenarios for the autonomous vehicle platform. A video will be recorded documenting the cyber-attack scenarios. The remediation methods for the cyber-attacks will be included in the documentation. Nathan Farrar is working on a wireless charging system for electric vehicles. He is awaiting the delivery of the hardware parts necessary to build the system. A module will be developed for this hands-on project as well.

IV. Adjournment:

The meeting adjourned at 4:00 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – January 23, 2023

I. Call to order

The meeting called to order at 3:32 pm.

II. Roll call

The following individuals were present: Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Dr. Shankar Banik; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

Minutes: The minutes were reviewed for the December 5, 2023, meeting. Dr. Dasgupta made a motion to approve the minutes as written. Dr. Banik seconded the motion.

III. Principal Investigator Reports:

University of West Florida – A Principal Investigator was not available to give a report for UWF.

NC A&T State University – A Principal Investigator was not available to give a report for NCA&T.

Citadel College – Dr. Banik presented the report. His team, including Dr. Graves, is investigating whether the workshop will be 1 day or 1-1/2 days. The tentative date is set for Monday, May 15, 2023. The Citadel Marketing Department is working to finalize the flyer. The workshop will be face to face/in-person. He will be sending out a call for presentations. All the Citadel's CECIP content will be included in their CLARK artifacts. Dr. Dasgupta inquired as to whether provisions could be made for Dr. Won and several students to attend and present their hands-on project at the workshop. Dr. Dasgupta also inquired as to whether a live remote link for listening could be offered to the partnering institutions. Dr. Banik indicated that a remote link for listening would be provided for virtual attendees. Dr. Banik also indicated that he would inform Tony Pinson of their availability of travel funds for guest speakers and provide him with the workshop flyer. The topic for the workshop is Cyber Security for Critical Infrastructure Education. The workshop will also feature a presentation/panel discussion from SLED (i.e., South Carolina Law Enforcement Division) as part of the workshop agenda. The event will be posted on the University of Memphis CfIA website.

University of Memphis – Dr. Dasgupta and Tony Pinson gave the report. Tony indicated that he has sent the module on Zero Trust to the principal investigators. He plans to submit the module to CLARK once all of reviews and revisions are complete. He is asking all principals to look at the modules and provide feedback. Dr. Banik asked if the module will be submitted to CLARK as a mini, micro, or nano-module. Dr. Dasgupta would like to get some feedback from the partners. Dr. Dasgupta indicated that he plans to give a presentation on Zero Trust during a CAE Tech Talk meeting. Tony has requested a time slot date from the CAE. Tony will also evaluate the course module level based upon its size (i.e., approx. sixty-eight slides).

Dr. Dasgupta stated that Dr. Won's hands-on projects are going well. Dr. Won submits weekly progress reports to Debera Pittman. As a final note, Dr. Dasgupta also stated that we should submit a CECIP progress report to NSA by the end of the month. Tony will submit it as an interim report, incorporating the meeting minutes through December 2022.

IV. Adjournment:

The meeting adjourned at 4:00 pm. Dr. Dasgupta made a motion to adjourn, while Dr. Banik seconded the motion.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – February 6, 2023

I. Call to order

The meeting called to order at 3:34 pm.

II. Roll call

The following individuals were present: Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Dr. Shankar Banik; Dr. Myounggyu Won; Dr. Guillermo Francia; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

Minutes: The CECIP Partner's minutes was reviewed for the January 23rd meeting. Dr. Dasgupta motioned to approve the minutes as written, while Dr. Banik provided the second.

III. Principal Investigator Reports:

Citadel College – Dr. Banik provided the report for Citadel College. He indicated that they have a firm date for the workshop conference (i.e., May 15, 2023). He also indicated that he would send the flyer to the partner institutions soon. He stated that travel support for CECIP faculty members presenting during the conference is available. The chief of SLED will present at the workshop.

University of Memphis – Dr. Dasgupta and Dr. Won gave the report for the University of Memphis. Dr. Dasgupta indicated that Tony would send out a meeting reminder notice the Friday before the meeting date, in the future, as a courtesy to all partner representatives. He also stated that the University of Memphis has obtained a slot to give a presentation at an upcoming CAE tech talk. He would like the partner institutions to participate, if possible, Tony will be sending out a calendar invite to the team members. Tony will also check on the status of a CECIP interim progress report that was circulated to the UofM research office for feedback before being sent to the NCAE PMO.

Dr. Won provided a report on the CECIP lab projects underway at the university. He stated that several undergraduate students are working on content/projects for the upcoming summer camp. The CECIP lab projects include a water pumping system model and an autonomous RC car platform. The water pumping system model is nearing completion and will have a series of cybersecurity exercises designed for it. Additionally, cybersecurity exercises are being further refined and explored for the autonomous RC car

platform. Finally, a prototype for a wireless charging system is being investigated. Once the model is complete, cybersecurity exercises will be developed for it as well.

NC A&T State University – A principal investigator was not available to give a report for NCA&T.

University of West Florida – Dr. Francia provided the report for the University of West Florida. He stated that the university team will have the final versions of their materials ready in about 4 weeks for submission to CLARK.

The meeting adjourned at: 3:53 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – March 13, 2023

I. Call to order

The meeting was called to order at 3:32 pm.

II. Roll call

The following individuals were present: Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Dr. Shankar Banik; Dr. Myounggyu Won; Dr. Guillermo Francia; Dr. Kaushik Roy; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

Minutes: The minutes from the February 6th CECIP Partners Meeting were reviewed and unanimously approved. Dr. Francia made the motion for approval. Dr. Banik seconded it.

III. Principal Investigator Reports:

Citadel College – Dr. Banik gave the report. He indicated that they have made travel support provisions for twenty faculty members to attend and/or present at the "Cybersecurity Education for Critical Infrastructure Protection" conference on May 15-16, 2023. The flyer for the event was displayed during the zoom meeting showing the QR code for registration. Faculty desiring travel support should specify during registration. Additionally, he indicated that he is preparing the conference agenda so CECIP faculty members should let him know if they plan to present as soon as possible. The chief of SLED (i.e., South Carolina Law Enforcement Division) will be presenting at the workshop. If you have questions about the conference, please let them know.

NCA&T State University – Dr. Roy gave the report. He indicated that they sent in their CECIP quarterly report and sent a review of the UofM Clark Module (i.e., Zero Trust Module) to Tony Pinson. He also indicated that they have a graduate research student working on IoT security sponsored by the CECIP grant. The student plans to defend her master's thesis in summer two. Her thesis is on "Comprehensive Analysis of RT Data Using Explainable AI for Intrusion Detection."

University of Memphis – Dr. Dasgupta and Dr. Won gave the report. Dr. Dasgupta will be giving a presentation at the CAE-CD Tech Talk in April 2023. He requested that Tony share the specific date with the CECIP Partner institutions. He also requested that

provisions be made for some of the undergraduate research students to attend the conference in Charleston, South Carolina.

Dr. Won reported on the CfIA lab projects. He indicated that progress was being made on the "Water Pumping System" and "5G Wireless Charging System" projects. The researchers are waiting on materials for both projects. He also indicated that students are conducting research on the design for cyber-attacks against platooning vehicles and the theoretical aspects of 5G communications for mitigation of attacks against wireless charging system. Finally, he indicated that he plans to attend the conference at Citadel College with several researching students.

Dr. Banik indicated that he needs the names of the students planning to attend the conference with Dr. Won along with their project synopses. Dr. Dasgupta indicated that it is important to collect statistics of the impact/exposure of the grant workshops and materials shared in courses. Tony Pinson requested the assistance of team in collecting the information.

University of West Florida – Dr. Francia gave the report. He stated that the university's team members have almost finalized the materials being prepared for submission to CLARK. He also indicated that Dr. Kevin presented a talk on "Security for Photovoltaic Cells" in one of his courses. Additionally, he will be lecturing in an upcoming course on "Ethical Hacking" at UWF. Finally, Dr. Francia indicated that he was interested in attending the conference at Citadel College in May and that he will present on NERC CIP Compliance, if he is able to attend.

.

The meeting was adjourned at: 4:00 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – May 8, 2023

I. Call to order

The meeting was called to order at 3:39 pm.

II. Roll call

The following persons were present: Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Dr. Shankar Banik; Dr. Myounggyu Won; Dr. Kaushik Roy; Ms. Mallory S. Gooding; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

Minutes: The meeting minutes were reviewed for the March 13, 2023, Partners meeting. The minutes for the March 13th meeting were approved as written. There was a motion by Dr. Banik, the second was offered by Dr. Dasgupta. It should be noted that the April 2023 CECIP Partners Meeting was canceled due to project quorum requirements for principal investigators.

III. Principal Investigator Reports:

University of West Florida – A representative was not in attendance.

Citadel College – Dr. Banik gave the report. He stated that they will be moving the date for their workshop to the Fall 2023 semester to obtain maximum participation. There have been very few registrations to date due to conflicts with other conferences, plus everyone is winding down for summer break. The goal is to schedule the workshop in October since it is Cybersecurity Awareness Month. If there is an issue, they will consider holding the conference in September. They are working on a revised schedule/flyer and will send it to all partners once completed. He would like for all the partner institutions to participate in the workshop. The date will be checked for end of CECIP grant and the possibility for a grant zero-cost extension.

University of Memphis – Dr. Won gave the report. He reported on the progress of the three lab projects being conducted at the CfIA. His project reports included updates on: Water Pump system, Wireless Charging system for electric vehicles, RC car platform, platooning vehicles project, and password cracking.

NCA&T State University – Dr. Roy gave the report. He indicated that he would not have been able to attend the conference at Citadel College in May due to conflicts. He also indicated that one of their graduate students, associated with the CECIP project, had her paper accepted for publication. The same student's work was accepted as a student poster for the 2023 CAE Symposium. Additionally, she will be defending her masters' thesis during the Summer 2023 term. Dr. Roy will present the student poster at the CAE Symposium.

NCA&T State University does not have any workshops planned for Summer 2023. They have sent in their comments on the UofM Zero Trust Micro-Module Clark materials. NC A&T State University plans to submit Clark website materials in Fall 2023.

The meeting was adjourned at: 4:05 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – June 5, 2023

I. Call to order

The meeting was called to order at 3:40 pm. This meeting was classified as unofficial due to a failure to achieve quorum for partner institution representation.

II. Roll call

The following individuals were present: Dr. Guillermo Francia; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

III. **Minutes**

The meeting minutes were reviewed from the CECIP Partners Meeting on May 8, 2023.

IV. Principal Investigator Reports:

University of West Florida – Dr. Francia gave the report. He stated that he delivered a three-hour lecture for one course. He also stated that he is interested in attending the University of Memphis workshop being planned for July 7, 2023.

NCA&T State University – There was not a representative in attendance.

Citadel College – There was not a representative in attendance.

University of Memphis – There was not a representative in attendance.

The meeting was adjourned at: 4:00 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – July 10, 2023

I. Call to order

The meeting was called to orderat 3:35 pm.

II. Roll call

The following people were present: Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Malory Saunders-Gooding; Dr. Myounggyu Won; Dr. Guillermo Francia; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen

III. Minutes

The meeting minutes were reviewed and approved from the May 8, 2023, Partners meeting. Dr. Francia moved for the approval of the minutes and Dr. Dasgupta seconded the motion.

IV. Principal Investigator Reports

Citadel College – Malory Saunders-Gooding gave the report. She said the workshop on Critical Infrastructure Security was supposed to have been held in May 2023, but did not take place due to low participation and bad timing. Consequently, the workshop has been rescheduled for October 19-20, 2023, on the campus of Citadel College in Charleston, S. Carolina.

The workshop will be about the curriculum for Critical Infrastructure Protection and IOT Security. It will include tabletop exercises and a case study, for the students, which will be on campus. Additionally, Citadel College is inviting students from the University of Memphis and the other partnering institutions. They are considering making the tabletop exercise involving students virtual. However, the workshop is in-person only currently due to budget constraints.

If any faculty would like to attend or participate, Citadel College has funding budgeted for travel. Dr. Francia will be one of the speakers at the workshop. Citadel is still seeking presenters and speakers. Malory stated that Cyber Awareness Month will be around the time of the workshop.

Dr. Dasgupta asked Dr. Roy about attending the workshop.

University of Memphis – Dr. Won gave the report about the Cyber Ambassador Tech Camp that was held by the University of Memphis on June 28- 30, 2023. The goal for the camp was to introduce the high school students to basic programming and cybersecurity concepts. The university received forty (40) applications for the camp, but twenty (20) were chosen due to limited resources. The students were divided into four (4) groups with their own RC cars, racing track, and laptop. They worked on a variety of project activities associated with the RC car such as Password Cracking, Buffer Overflow, and Man-in-the-Middle attacks. The students learned how to set up the racing track and enjoyed the 3-day event. Data was collected from a pre-experience and post-experience survey. The survey data will be used as a basis for a data research paper on RC cars and cyber security education. The event is an annual event.

Tony explained that the Zero Trust micro-module was uploaded to the Clark website. It is pending review from CLARK staff members. A micro-module on Smart Grid Security is also being prepared for upload to CLARK as well.

Dr. Ali stated that a workshop on Cyber Resilient EV Charging Station and Critical Infrastructure will be held on Friday August 25, 2023, at the University of Memphis.

NC A&T State University - Dr. Roy indicated that he presented his graduate student's poster at the CAE Symposium. Graduate student successfully defended her master's thesis. He indicated that he hopes that she will return as a PhD student in the fall. Also, she is planning to present a paper at an international conference in Hawaii in later this month.

University of West Florida – Dr. Francia indicated they have completed all of their project commitments. Their project report updates have been shared to the University of Memphis OneDrive. Additionally, they are planning to submit project materials to Clark on the ICS-RE curriculum. Dr. Francia also had several classroom lectures on CECIP materials recently. Dr. Francia asked Tony to send a new link to the UofM OneDrive so that he could make updates.

The meeting was adjourned at: 4:30 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – August 14, 2023

I. Call to order

The meeting was called to order at 3:32 pm.

II. Roll call

The following individuals were in attendance: Dr. Mohd Hasan Ali; Dr. Shankar Banik; Dr. Myounggyu Won; Dr. Guillermo Francia; Ms. Malory S. Gooding; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

Minutes: The meeting minutes were reviewed from the July 10, 2023, CECIP Partners meeting. The minutes for the July meeting were approved as written, pending minor corrections. There was a motion by Dr. Francia, the second was offered by Dr. Won.

III. Principal Investigator Reports:

University of West Florida – Dr. Francia gave the report. They have completed all their commitments associated with the project. By September or October, they are planning to submit their project materials to CLARK. He wanted to reiterate his commitment to joining the Citadel workshop in October. He will be making a presentation on "Compliance & Auditing in ICS Security" that will include case studies and tabletop exercises.

NC A&T State University – There was not a representative in attendance.

Citadel College – Dr. Banik gave the report. He indicated that they are seeking presenters/speakers for their workshop at the Citadel College on October 19-20, 2023. He also indicated that they have funds available for travel support. The availability of the funds is on a first-come-first-serve basis. The workshop flyer has a QR code for registration and a link to information regarding lodging for the event.

University of Memphis – Dr. Won gave the report. He reported on the progress of the student's projects. He indicated that one student has worked on a prototype development for a dynamic wireless charging system. The student's paper on dynamic wireless charging systems was accepted by the International Conference on Intelligence Transportation Systems. Another student, Allison, has been reviewing papers on cyber security threat models for EV Charging Systems. Regarding the summer camp held in

June, Dr. Won indicated thar he is drafting a paper to be submitted to a computer science education conference.

Tony Pinson reported that the Zero Trust micro-module (https://clark.center/details/tgpinson/492686fc-cec2-4d47-813a-727fac98feaa) has been uploaded to CLARK. A second micro-module on Smart Grid Security is also being submitted. Tony also indicated that we need to get everyone who participated in the development of modules for the CLARK website to registering on the site. He also indicated that he is in the process of attempting to upload the IOT security module from NC A&T State University.

Dr. Ali encouraged everyone to register for the upcoming UofM workshop in August on Cyber Resilient EV Charging Stations and Critical Infrastructure.

The meeting was adjourned at: 3:54 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – September 11, 2023

I. Call to order

The meeting was called to orderat 3:36 pm.

II. Roll call

The following individuals were present: Dr. Dipankar Dasgupta; Dr. Shankar Banik; Dr. Myounggyu Won; Dr. Guillermo Francia; Ms. Malory S. Gooding; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

Minutes: The minutes from the August 14, 2023, CECIP Partners meeting were reviewed. The minutes were approved as written, pending minor corrections. The motion for approval was made by Dr. Dasgupta and seconded by Dr. Banik.

III. Principal Investigator Reports:

Citadel College – Dr. Banik provided the report. He stated that they are seeking presenters/ speakers from each of the partner institutions to participate in their upcoming workshop which will be held October 19th and 20th. The agenda for the event is being finalized this week. Three speakers have been scheduled from Citadel College. He requested that each speaker from a partner institution send their name and the title of their presentation. He also indicated that he had gotten a commitment from Dr. Francia at West Florida. Dr. Francia requested a Friday slot for his presentation. Dr. Won agreed to present at the workshop as well. The title of Dr. Won's 30-minute presentation is forthcoming. The Citadel College Workshop flyer has a QR code for registration. Also, there is a link in the Eventbrite link for requesting funding for faculty travel support.

University of Memphis – Tony Pinson provided an update on the CLARK course/module submissions. He indicated that the Zero-Trust micro-module had been released to the CLARK curriculum and that Smart Grid micro-module is under review by CLARK's Review Committee. He also stated that the workshop held on August 25th at the UofM Herff College of Engineering was a success. The workshop had approximately thirty in-person attendees and seven virtual participants. The workshop featured speakers from TVA, Florida International University, the University of Missouri – Columbia, West Virginia University, and the University of Memphis. Dr. Dasgupta indicated that we should get all activities associated with this project finished. He also indicated that we

should make a commitment to send in our course/module training materials to CLARK. He also inquired if the Citadel College or the University of West Florida will be releasing course modules under this project initiative. Dr. Banik indicated that the Citadel College will be submitting a new course to CLARK entitled Cyber-Physical Systems. Dr. Francia indicated that the University of West Florida has already sent a full course on ICS Renewable Energy Security to CLARK. The course has been used four times so far, twice for workforce development and twice for faculty development. They have trained thirty faculty members across the nation using the course. Dr. Francia also indicated that they have two other courses that are undergoing formatting before being submitted to CLARK. Tony was requested to place the released CLARK course links in the CECIP minutes and on our website. Dr. Won will post his lecture presentation being held at the Citadel in October as a course link on CLARK.

NCA&T State University – There was no representative in attendance.

University of West Florida – Dr. Francia provided the report. He stated that they have completed all their project commitments. He indicated that the ICS Renewable Energy Security course had been submitted to CLARK but is in the review stage.

The meeting was adjourned at: 4:06 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – October 2, 2023

I. Call to order:

The meeting was called to order at 4:02 pm.

II. Roll call

The following individuals were present: Dr. Dipankar Dasgupta; Dr. Shankar Banik; Dr. Myounggyu Won; Dr. Guillermo Francia; Ms. Bianca Govan; Ms. Malory S. Gooding; Mr. Tony Pinson; Ms. Debera Pittman; and Ms. Doris Allen.

Minutes: The CECIP Partners minutes were reviewed for the September 11 meeting. The minutes were approved as written. The motion for approval was made by Dr. Dasgupta and seconded by Dr. Won.

III. Principal Investigator Reports:

Citadel College – Dr. Banik provided the report. He shared the tentative agenda for the upcoming Cybersecurity Education for Critical Infrastructure Protection workshop on October 19 – 20, 2023. He indicated that everyone should have received an email from Malory regarding the lodging information and that a reduced rate is available for individuals interested in staying at the Marriott Hotel. Additionally, he reviewed the details for the workshop's tentative agenda.

University of Memphis – Tony Pinson provided an update on the CECIP CLARK website submissions. He indicated that the "Zero-Trust" micro-module and the "Smart-Grid Security" micro-module were released to the CLARK library on August 18, 2023, and October 2, 2023, respectively. It was noted that Dr. Hasan Ali and Dr. Dipankar Dasgupta are both planning to make virtual presentations at the NC A&T State University workshop. Ms. Bianca Govan plans to send Tony the workshop link with the flyer/registration information. Ms. Doris Allen will send the link out to U of M students who will be speaking at the workshop.

NCA&T State University – Ms. Bianca Govan provided the report. She indicated that she would provide a link for registration for the upcoming "A Virtual AI Enhanced IoT Security Workshop." The workshop is scheduled for Friday October 27, 2023. Dr. Won indicated that some University of Memphis student demo videos can be presented at the

workshop. Ms. Govan indicated that she would like to get a list of the presenting students as soon as possible to add their names to the agenda.

University of West Florida – Dr. Francia provided the project update. He indicated that they have completed all their project commitments. They have sent their course modules to CLARK and are waiting feedback. Dr. Francia will send the CLARK Library links of the released course modules to Tony Pinson, for posting to the CfIA website once they become available.

The meeting was adjourned at: 4:25 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – November 6, 2023

I. Call to order:

The meeting was called to order at 4:05 pm.

II. Roll call

The following individuals were present: Dr. Shankar Banik; Dr. Myounggyu Won; Dr. Guillermo Francia; Ms. Malory S. Gooding; Mr. Tony Pinson; and Ms. Doris Allen.

Minutes: The minutes were reviewed for the October 2, 2023, CECIP Partners meeting. They were approved as written after a correction. Dr. Francia made the motion for approval. The motion was seconded by Dr. Won.

III. Principal Investigator Reports:

Citadel College – Dr. Banik provided the report. He indicated that their workshop was successful. He thanked partner institution faculty members for presenting their research during the workshop conference. He also noted that the conference had several keynote speakers site exercises conducted for the students. He plans to share the presentation slides with the workshop attendees once approval is received from the presenters. The Citadel's Cyber-Physical Systems course, being offered this Fall, will be posted to CLARK during the Spring 2024 term. A summary report of the workshop will be sent to Tony Pinson.

NCA&T State University – No representative in attendance. Their workshop was successful per an email update from Dr. Roy. Tony Pinson provided the email update. Additionally, Tony indicated that NC A&T State University's IoT Security materials have been submitted to CLARK for review on October 17, 2023.

University of West Florida – Dr. Francia provided the report. One course is completely reviewed and ready to be released. He also indicated that they have two other courses being reviewed by CLARK. They have completed all activities for the project and are ready to close the books. They are waiting for the final invoice from the Indian River state college.

University of Memphis – Dr. Won provided the report. He indicated that Dr. Dasgupta, Dr. Ali, and he presented their research work during the "Getting to Know your Fellow

CAE-R" event. Dr. Won also indicated that he attended the "Cybersecurity Education for Critical Infrastructure" workshop hosted by the Citadel. Finally, he noted that Dr. Dasgupta, Dr. Ali, Nathan Farrar, and he attended the "A virtual workshop on AI Security" hosted by the NCA&T State University.

The meeting was adjourned at: 4:25 pm.

Center for Information Assurance / University of Memphis
CECIP Partners Meeting Minutes

Monday – December 4, 2023

I. Call to order:

The meeting was called to order at 4:00 pm.

II. Roll call

The following persons were present: Dr. Dipankar Dasgupta; Dr. Mohd Hasan Ali; Dr. Shankar Banik; Dr. Myounggyu Won; Dr. Guillermo Francia; Ms. Malory S. Gooding; Ms. Bianca Govan; Mr. Tony Pinson; and Ms. Debera Pittman.

Minutes: The meeting minutes were reviewed from the November 6, 2023, CECIP Partners meeting. The minutes for the November meeting were approved as written pending grammatical corrections. The motion for approval of the minutes was made by Dr. Dasgupta. The motion was seconded by Dr. Francia.

III. Principal Investigator Reports:

Citadel College – Dr. Banik gave the report. He indicated that he submitted the workshop report before the Thanksgiving break in November. The course on Cyber Physical Systems, being taught during the Fall 2023 semester, will be upload and submitted to the Clark Library during Spring 2024. He also stated that the presentation slides from the workshop will be shared with attendees once they have received approval from the presenters.

University of West Florida – Dr. Francia gave the report. He stated that twenty-one (21) learning objectives were released. There is a total of thirty-one (31) learning objectives ready to be disseminated publicly. He expects the final ten (10) learning objectives to be released soon. At present, you can only find the courses on the Clark site by typing his last name (i.e., Francia) in the search box. Sharing his screen with the group, he showed learning objectives which had been released in Clark and those that are still in the draft/review phase. He indicated that some of the learning objectives have already been downloaded for use by visitors to the site. Their final financial report is forthcoming by the end of December.

NCA&T State University – Ms. Govan gave the report. She states that they hosted a virtual workshop on Friday, October 27th, it was a success. The title was "A Virtual Workshop on AI – Enhanced IoT Security – AI meets IoT". They had a total attendance

of 53 persons, with 36 being students ranging from post-doctoral, masters, PhD, as well as undergraduates.

University of Memphis – Dr. Dasgupta provided the report. He stated that the University of Memphis participated in the Citadel College workshop. He also had some good news: the optional year for the CECIP Grant has been awarded to the consortium. Dr. Dasgupta received a document from NSA which extends the grant for one year until December 2024. He stated that each university should be able to continue working with any money associated with their budget allocation. Dr. Banik stated that he is waiting to hear back from Alice regarding a budget modification that he submitted. Dr. Dasgupta stated that he did not think that it would be a problem, but that he had discuss it with the University of Memphis Research Office. He also indicated that next year he would like for the consortium to plan a workshop every two months to be hosted by one of the partners. His goal is to have a total of six (6) workshops for the year. Finally, he would like for the University of West Florida to involve the other partners more in their project activities. Dr. Francia states that he can't commit right now. UWF is overbooked with other grant-related work at this time. He will know more by the January meeting. It is conceivable that the university may not be able to participate in optional year for the project.

Dr. Won indicated that two papers are being published in association with the project. Dr. Dasgupta encouraged all the partnering institutions to include any publications associated with the CECIP project in their respective reports.

The meeting was adjourned at: 4:28 pm.