A national center of ACADEMIC EXCELLENCE in information assurance

PROTECTING AMERICAS
INFORMATION INFRASTRUCTURE

UNIVERSITY OF MEMPHIS

CENTER FOR INFORMATION ASSURANCE

NEWSLETTER

2023

GREETINGS FROM THE CENTER DIRECTOR:

"The University of Memphis serves as the National Security Agency (NSA) Centers of Academic Excellence in Cyber Defense (CAE-CD) Regional Hub for Cyber Security Education and Research efforts in collaboration with private and public sectors in Tennessee. As a CAE-CD designated institution, the CfIA is recognized for its significant contributions to meeting the national demand for Information Assurance and Cyber Defense education by developing a growing number of professionals with cybersecurity expertise in various disciplines, who will ultimately contribute to the protection of the National Information Infrastructures. As such, the Center for Information Assurance leads efforts to advance cybersecurity education, research, and workforce development. The faculty directors are currently involved in several grant-funded projects which engage university students in their Cybersecurity education and research.

For more information regarding these projects, please refer to our webpage at Memphis.edu/cfia. A list of a few current projects include: the “Traffic Light Project: the “Tree Parity Machine” (TPM), and Identity Management Capability Powered by AI to Transform the way User Access privileges are Managed, Monitored, and Controlled. The CfIA builds a strong cybersecurity community by hosting workshops throughout the year, faculty development events, student competitions, and facilitating high school outreach efforts, as well as collaborations with other CAE institutions and military partners across the region. The University of Memphis has demonstrated leadership as the regional resource center since 2004. Welcome to this edition of the CfIA newsletter. We look forward to any collaboration opportunities you are considering.

CfIA's ACTIVITIES

1. On September 28, 2022, Dr. Dasgupta gave a public lecture (virtual) at Purdue University on Secure User Authentication and Identity Management based on his patented work on AMFA and how AMFA can provide Zero-trust capabilities to authentication.
2. On November 16, Professor Dipankar Dasgupta attended the DoD University Consortium for Cybersecurity (UC2) Research Workshop hosted by National Defense University at Fort McNair, Washington DC. In response to the DoD-UC2 Request for Information (RFI), Dr. Dasgupta formed a team of faculty experts from 15 Universities (which include Purdue, MIT, Penn-State, and others) and submitted a whitepaper.
   on implementing zero trust at the tactical warfighting edge. This research paper ranked first position by reviewers among all submissions from the national academic community. As the team lead, Dr. Dasgupta was invited to present and was well-received by attendees from different federal agencies. "This engagement and collaboration on cybersecurity will open the door for furthering our research and education" according to Dr. Dasgupta, Director Center for Information Assurance at the University of Memphis.
3. On December 4, Dr. Dasgupta gave a tutorial with Dr. Roy and K. Gupta on 'ML Applications, Adversarial Attacks, and Mitigation Strategies" at the IEEE Symposium Series on CI (SSCI), held in Singapore.
4. On December 5 & 6, 'Chair Sessions' held at the Computational Intelligence in Cybersecurity Symposium at the IEEE-SSCI, held in Singapore.
5. On December 7, Prof. Dasgupta gave an invited talk at the University of Malaya, Kaula Lumpur under IEEE CIS Distinguished Lecturer Program on Adaptive Multi-Factor Authentication and Cyber Identity – vTools Events.
6. On December 8, Dr. Dasgupta gave a talk at 'A*STAR' Nanyang Technological University in Singapore; he was invited as an IEEE Distinguished Lecturer. His topic: "Adversarial ML and Defense Strategies".
7. On December 14, Dr. Dasgupta was selected as a prestigious National Academy of Inventors (NAI) Fellow for the Class of 2022.
8. On December 21, Dr. Dasgupta was the Keynote Speaker; his talk topic was: "Adaptive Multi-Factor Authentication & Cyber Identity". Held at the 2nd International Conference on Advanced Network Technologies and Intelligent Computing (ANTIC-2022), BHU in Varanasi, India.

CfIA NEWS & EVENTS

Dr. Dasgupta was awarded the Arthur C. Graesser Presidential Award for Lifetime Achievement in Research | April 7, 2023

The honor, which is the highest level of research recognition available to UofM faculty, is given to a full professor who has made significant contributions to UofM's research enterprise and reputation through an exemplary and sustained record of academic scholarship, research collaboration, mentoring, and university citizenship.

Dr. Kan Yang is the leading guest editor of a Special Issue on "Recent Advances of Security, Privacy, and Trust in Mobile Crowdsourcing" on IEEE Internet of Things Journal

Students Win 1st Place at Technology against Tornado Competition

Doctoral students Meiying Zhang and Suravi Regmi were awarded 1st place at the inaugural technology against Tornado Student Competition and Expo, held at the University of TN Martin on April 21, 2023. Their work on ML- based tornado prediction, mentored by Dr. Kan Yang.

.

Dr. Dasgupta’s Singapore Conference at SSCI 2023

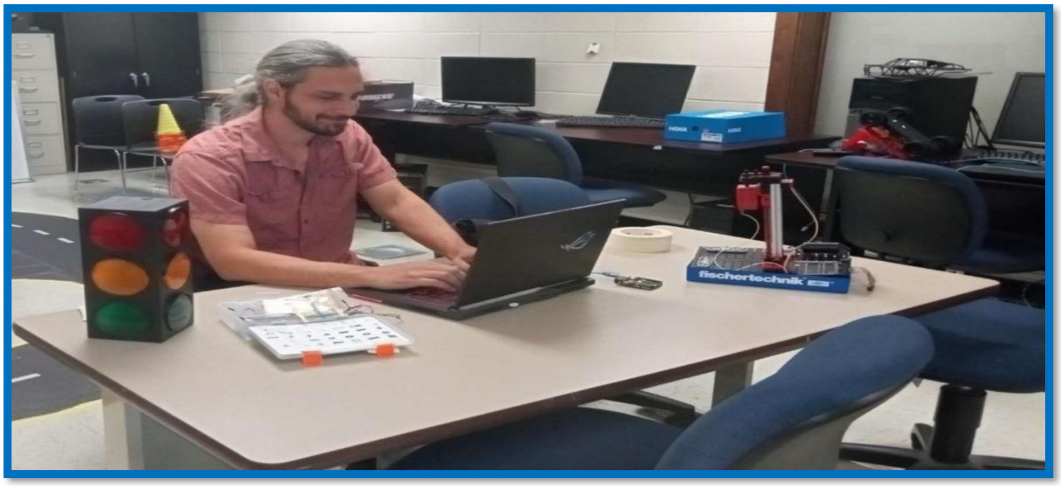
The professors are from the Computer Science Department and Engineering Department. They are building the cyber security program with interesting projects and along with challenges, within the technology of today. Students are working on various projects, keeping data safe, being aware of cyber trends, AI and Machine Learning, and Zero- Trust. Some of the projects: Water Pump Project, EV Charging, an Open-Source Worm Attack, an AV Car Team, and an Insider Threat Detection and Prevention Protocol. The lab has enquiring minds that would like to know what happened and how it can be resolved. Research is being done by Graduate and Undergraduate students. They have an opportunity to work hands-on, with different projects. There is a demand for Cyber Security in global companies.

Dr. Dipankar Dasgupta, Dr. Mohd Hasan Ali and Dr. Myounggyu Won (left to right)

The Center for Information Assurance Traffic Light Project

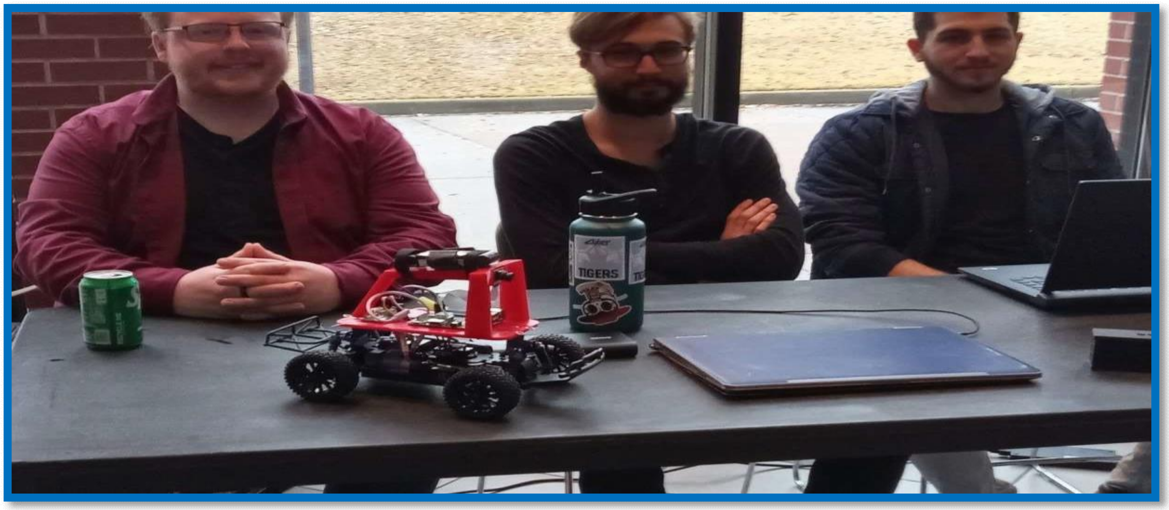
Nathan Farrar and his team under Dr. Myounggyu Won worked on a buffer overflow attack simulation last fall utilizing an ESP32 Wi-Fi and Bluetooth-enabled chip and a traffic light signal. The simulation showed how the Bluetooth on the ESP32 could be hacked and used to change the operational mode of the traffic light, using a password brute force technique that overflowed the buffer on the ESP32.

This was successfully demonstrated with a password and a pin key. Future goals for the project are to use the traffic light to simulate an intersection with the autonomous donkey car project and show how hacking different components, such as the traffic light or the donkey car itself, can cause major traffic flow problems as well as a safety issue for the public.



Center for Information Assurance Cyber Security Spotlight "DEMO DAY ON CAMPUS" December 12, 2022

UofM displayed a Demo Day on Campus, under the supervision of Dr. Amy Cook, Capstone Instructor. There were students that participated from the Center for Information Assurance Lab, William Richards, Luke Carrington, and Adam Karsha. These students were the AV Team, and they demonstrated the RC Car or Autonomous Car (a self-driving car, the driverless car, or robotic car, is a car that can travel without human input). In their demonstration, they talked about Cyber Risks and Liabilities such as hacking, software, and the make-up of the RC Car. Technology always has something new to explore.



Dr. Dasgupta's IEEE CIS Meeting at Kolkata | January 10, 2023

On January 10, 2023, Prof. Dasgupta led a high-level technology research meeting with 8 leading universities which was hosted by TCS-Research Kolkata, India. The event was organized under the IEEE Computational Intelligence Society (Kolkata Chapter) in hybrid attendance mode and was attended by 25 invited experts working in variety of AI/ML applications. The discussion started with the fundamentals of AI techniques and the best ways to use these practice (topics included data collection, validation, explain-ability, etc..); one focus area was the use of trustworthy AI/ML technologies in medical applications. This interactive session generated interest among the participating institutes and to explore academia-industry collaboration in their areas of interest.

Hands-On-Lab Project Update | January 30, 2023

- Center for Information Assurance student DONTE MITCHELL researched "Insider Threat Detection and Prevention Protocol: ITDP (2021)" under Dr. Dipankar Dasgupta.
- ITDP is a protocol utilized by authenticating a user's security questions to authenticate the user.
- Based on information on security questions, clock-in/out times, answering times, etc. Accuracy: 98.3% (500 iterations)
- Reduce account access from unauthorized users.

New Student, Arturo Perez, Is Working on These Projects:

- Working on multi-user authentication.
- Working on Rails and Flask – python-based web server. Found libraries that can be used for implementing multi-user authentication.

From left to right: Allison Plank, Adam Thieme, Luke Carrington, Tiffany Geist Kemper, Arturo Perez, Tony Pinson, and Dr. Dipankar Dasgupta.

Tiffany Geistkemper Works on Her 5G Research Project

- Working on the EV wireless charging station project under Dr. Dasgupta and Dr. Ali.

- Currently studying the simulation processes needed to simulate cybersecurity attacks in Simulink and MATLAB

- 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 cyberattacks, write code to prevent these attacks, and integrate this code with the rest of the code in the project.

Pictured Above: Tiffany

Fuzzing | A Method to Test Software

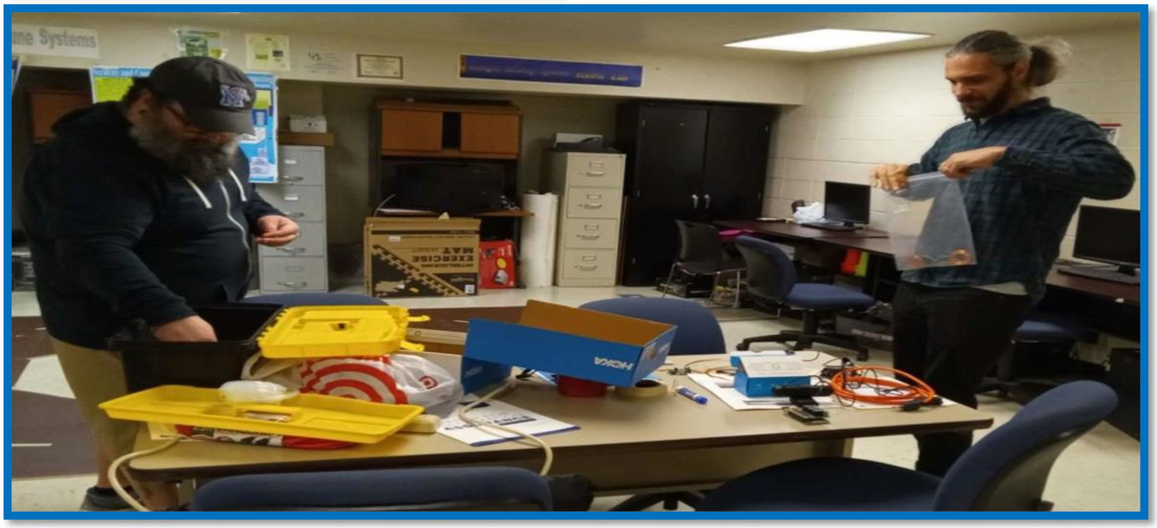
Center for Information Assurance student Hans Amelang, along with Max Hagemann, Mohammed Shami. The main idea behind their project was fuzzing SocketCan in Linux. Fuzzing is a way to automatically test software. The fuzzer provides lots of invalid random inputs into the program. The test tries to cause crashes, errors, memory leaks and so. The SocketCan package is an implementation of CAN protocols (Controller Area Network) for Linux. Can is a networking technology which has widespread use automation, embedded services, and automotive fields.

CfIA Teams are Inventing & Developing Under the Supervision of Dr. Dipankar Dasgupta, Dr. Myouggyu Won and Dr. Mohd Hasan Ali:

Hands-On-Lab Project News | November 17, 2022

In the lab, about 5-6 students are participating in Hands-On Projects. One student has completed the first version of the program for the water pump project and is testing it. They plan to put the water pump system in an acrylic box with LEDs for demonstration and are reading papers on cybersecurity scenarios for a water pump system. The AV Team has completed a demonstration in the capstone project and is working on the implementation of a delay attack, along with drafting a document explaining attack scenarios and mitigation methods. Another student has found a part of the dynamic wireless charging project and confirmed its usability, while a third student is working on adapting source code for a worm-hole attack scenario to our R/C car application.

Pictured below: Hans Amelang and Nathan Farrar, assembling their Hands-on projects: Water pump and DWC wireless charging projects.



CENTER FOR INFORMATION ASSURANCE

CFIA.MEMPHIS.EDU

CfIA Staff

CfIA Project Coordinator:
Tony Pinson
tgpinson@memphis.edu

Administrative Staff:
Doris Allen
djallen3@memphis.edu

Debera R. Pittman
drpttman@memphis.edu

CyberCorps Program Coordinator:
Rhonda K. Smothers
rsmothrs@memphis.edu

Course Design Specialist:
Jack O'Meara
jjomeara@memphis.edu

Workforce/System Specialist:
Chinita S. Holmes
csholmes@memphis.edu

THE UNIVERSITY OF MEMPHIS®

The University of Memphis is an Equal Opportunity/Affirmative Action University. It is committed to the education of a non-racially identifiable student body. UOM016-FY2324