A national center of ACADEMIC EXCELLENCE in information assurance

PROTECTING AMERICAS
INFORMATION INFRASTRUCTURE

UNIVERSITY OF MEMPHIS

CENTER FOR INFORMATION ASSURANCE

NEWSLETTER

CYBERSECURITY AWARENESS MONTH
OCTOBER 2022

ABOUT CfIA

The Center for Information Assurance (CfIA) has received millions of dollars in research, and education funds, stands as a nationally-designated Center of Academic Excellence in Cyber Defense Education and Research by the National Security Agency/ Department of Homeland Security. The Cyber Security Center provides a student-centered research environment where both under-graduates and post-graduates get to work on federal-funded projects. Prior students have participated in cyber defense competitions (CANsec), as well as code-breaking (NSA Code-breaking Challenges) and security challenges (CyberSEED 2016), giving them the chance to put their theory knowledge into practice. The center administers two graduate certificates in cyber security, one from the Computer Science Department and the other from the Business Information Technology Department at the University in the midst of the digital age.

Contact for more information: **cfia@memphis.edu**

Greetings From The Center Director

The long-term goal of the Center of Information Assurance (CfIA) at the University of Memphis is to establish a regional hub for Cybersecurity Education and Research in collaboration with public and private sectors in the State of Tennessee with significant impacts on economic development, the provision of public services, citizen privacy and security. Since the center was founded in 2004, it has consistently met the criteria for maintaining its designation as a National Center of Academic Excellence in Information Assurance/Cyber Defense Education (CAE-CD) and Research (CAE-R) by the National Security Agency (NSA and Department of Homeland Security (DHS)). The faculty associated with the center are involved in several funded projects and are engaged with students in their research and education. In 2022, we hosted three cybersecurity workshops and a cyber ambassador bootcamp. A team of undergraduate computer science students associated with the Center for Information Assurance (CfIA), a registered student organization (RSO) called “Cyber Range,” recently participated in the Raymond James Cyber Defense Competition in Tampa, Florida. Among many cyber-related activities, they also participated in the 12th Annual Mid-South Cybersecurity Summit on November 4, 2022.

DIRECTOR

Prof. Dr. Dipankar Dasgupta
Hill Professor of Computer Science,
The University of Memphis

ASSOCIATE DIRECTORS

1. Dr. Myounggyu Won
Assistant Professor
Computer Science

2. Dr. Kan Yang
Assistant Professor
Computer Science

3. Dr. Mohd Hasan Ali
Associate Professor
Electrical Engineering

THE CENTER ACTIVITIES

DURING 2022

Distinguished Lecture by Professor Dipankar Dasgupta at IEEE Day:

On October 4, 2022, Dr. Dasgupta discussed some important uses of AI in research, optimization, prediction and discovery; how algorithmic bias can impact decisions; and how AI can play dual-role and can be applied in many ways with varying intent.

The talk is available on
Youtube: youtu.be/EmMXkwJdgAo

National Cybersecurity Virtual Career Fair:

The 6th annual career fair was held on September 16, 2022. It was sponsored by the National Cybersecurity Training & Education Center (NCyTE) and the Center of Academic Excellence in Cybersecurity (CAE). The career fair brings together students and alumni from over 380 institutions across the nation with employers offering apprenticeships, internships and full-time employment.

IEEE Distinguished Lecture by Professor Dipankar Dasgupta:

On July 21, 2022, Professor Dipankar Dasgupta, gave an invited talk on "Adversarial Machine Learning and Defense Strategies," at **WEITA'22**.

Expansion of Training Opportunities:

On May 12, 2022, UofM Professors Dipankar Dasgupta and James McGinnis worked with the NCPC to create Cybersecurity Legislation. This new law authorized DHS to increase response efforts nationwide. President Biden signed the NCPC Act into law on May 12, 2022. CfIA worked to expand training opportunities under FEMA.

Workshop presented by The Cyber Tigers and CfIA:

On April 28, 2022, a zoom workshop was presented by the Cyber Tigers and CfIA on the UofM campus Student Cyber Security Club. Scott Augenbaum, former FBI Cyber Agent, was the guest speaker.

Approval by the National Security Agency (NSA) for Program of Study (PoS)::

On April 5, 2022, NSA approved the Program of Study (PoS) for Bachelor of Science, with Cybersecurity Concentration of Computer Science. It is validated through the academic year 2027.

DoD CyberCorps Program Information Seminar:

On March 4, 2022 at Dunn Hall, Rm #123 at 1:00 p.m. the DoD Cyber Scholarship Program (CySP) 2022 – 2023 took place. The Department of Defense was seeking rising junior and senior undergraduates (3rd and 4th year) and graduate/doctoral students who were interested in full-ride scholarships for concentrated studies in information assurance. Students selected for the program will receive full scholarships.

2022 Cyber Ambassador Tech Camp:

The University of Memphis was delighted to host the summer camp again this year in person. This camp introduced high school students to some fundamental concepts of ethical hacking, software patching and coding. Students learned about cybersecurity concepts and embedded programming through a series of lectures and hands-on software coding experiences. Dr. Myounggyu Won was the Tech Camp Organizer.

Re-designation as a National Center of Excellence in Cyber Defense:

The University of Memphis has been re-designated as a National Center of Excellence in Cyber Defense by NSA and U.S. Department of Defense. This re-designation was awarded through the 2027 academic year.

SPONSORED WORKSHOPS

1. October 14, 2022:

Dr. Dipankar Dasgupta (IEEE Distinguished Speaker) gave an invited lecture (virtual) on **Cyber Security and Authentication** at the IEEE Victorian Computational Intelligence Society (CIS) hosted by Dr. Malka N. Halgamuge, RMIT University, Australia.

2. September 28, 2022:

Dr. Dasgupta gave a virtual public lecture 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.

SPONSORED WORKSHOPS

CONTINUED

3. September 23, 2022:

IoT Security Workshop | The University of Memphis Center for Information Assurance and North Carolina A&T State University are collaborating to produce a hybrid workshop on IoT Security. Dr. Dasgupta gave an invited talk on IoT Security at the NCAE workshop.

4. June 21, 2022:

Cybersecurity Research/Training Workshops Funded by Navy ROTC | The University of Memphis, the Center for Information Assurance, and the ROTC Research Students are conducted in-person (hands-on activities) and virtual Cybersecurity Research/Training Workshops in 2022.

5. April 23, 2022:

Cybersecurity Research/Training Workshop on "The Issues and Topics concerning Operational Cybersecurity," led by Dr. James McGinnis.

6. April 1, 2022:

Cybersecurity for Critical Infrastructure Workshop led by Dr. Dipankar Dasgupta.

7. March 25, 2022:

Smart Grid Security Workshop led by Dr. Hasan Ali.

8. March 26, 2022:

Cybersecurity Research/Training Workshop on "The Issues and Topics concerning Operational Cybersecurity," led by Dr. Dipankar Dasgupta

9. February 24, 2022:

Dr. Dasgupta and Dr. Hasan Ali gave invited talks at the Jack Voltaic Conference Series: Cyber Resiliency for Critical Infrastructure. Members of the CfIA project team for the Cybersecurity Education in Critical Infrastructure Protection participated in a panel discussion at the Jack Voltaic Conference Series.

FUNDED PROJECTS
ON CYBERSECURITY

Project No	Project Name	PI/Co-PIs	Agency / Source	Amount	Period
1	NCAE-Research on Cyber Resilient 5G-Enabled Electric Vehicle Charging Infrastructure	PI: Dr. Hasan Ali, Electrical Engineering Co-PI: Dr. Dipankar Dasgupta, Computer Science	NSA	$498K	9.16.2022 - 9.15.2024
2	Context-Aware Authorization Framework for Smart Critical Infrastructure NCAE-C in Cybersecurity Education Research	PI: Dr. Dipankar Dasgupta, Computer Science	NSA	$140K (total $500K Sub-Award from the University of South Carolina)	10.1.2022 - 9.30.2024
3	Zero-Trust Identity & Access Management	PI: Dr. Hasan Ali, Electrical Engineering Co-PI: Dr. Dipankar Dasgupta, Computer Science	DHS/ FEMA	$450K (multi-university grant of $4M)	9.1.2022 - 8.31.2025
4	Developing application-specific shared-trust framework for accessing sensitive information	PI: Dr. Dipankar Dasgupta, Computer Science	DoD/NSA	$500K ($251K awarded yr 1)	8.1.2021 - 7.31.2023
5	Multidisciplinary cybersecurity program for Critical Infrastructure Protection	PI: Dr. Dipankar Dasgupta, Computer Science Co-PI: Dr. Hasan Ali, Electrical Engineering Co-PI: Dr. Myounggyu Won, Computer Science	DoD / NSA	$2M (multi-university, awarded $1M in yr 1)	8.20.2021 - 12.31.2023
6	Cybersecurity Impact Analysis for End Users Security and Privacy	PI: Dr. Hasan Ali, Electrical Engineering, Co-PI: Dr. Dipankar Dasgupta	FEMA/ DHS	$600K (multi-University grant of $4M)	9.1.2021 - 8.31.2024

FUNDED PROJECTS

ON CYBERSECURITY

CONTINUED

Project No	Project Name	PI/Co-PIs	Agency / Source	Amount	Period
7	Examining Advanced Persistent Threats	PI: Dr. Dipankar Dasgupta, Computer Science Co-PI: Dr. James McGinnis, Engineering Technology	FEMA/ DHS	$331,000 (multi-University grant of $2M)	10.1.2017 - 3.31.2022
8	Navy ROTC Cybersecurity Training Program	PI: James McGinnis, Engineering Technology Co- PI: Dr. Dipankar Dasgupta, Computer Science	DoD	$318K	5.1.2020 - 7.31.2022
9	Scholarship for Services (SFS)	PI: Dr. Kan Yang, Computer Science Co-PI: Dr. Myounggyu Won, Computer Science Co- PI: Dr. Dipankar Dasgupta, Computer Science, Co- PI: Dr. Amy Cook, Computer Science	NSF	$3.8M	2.1.2022 - 1.31.2027
10	GenCyber Summer Boot Camp for High School Students	PI: Dr. Myounggyu Won, Computer Science PI: Dr. Dipankar Dasgupta, Computer Science	NSA	$100K	3.01.2022 - 2.28.2023
11	Designing Machine Learning-based Solutions for APT Detection	PI: Dr. Kan Yang, Computer Science Co-PI: Dr. Xiaofei Zhang, Computer Science	FedEx	$397K	8.1.2022 - 7.31.2025

Project Details

Project 01: NCAE-Research on Cyber Resilient 5G-Enabled Electric Vehicle Charging Infrastructure

The project's overall goal is to explore related technologies to develop a secure and trustworthy approach for 5G-enabled electric vehicle charging station (EVCS) and its charging system. This project will significantly impact industry, academia, and society at large. In military bases, the proposed 5G-based EVCS can play a significant role in charging vehicles securely and successfully. The PIs will also engage in outreach and educational activities designed to expose diverse populations, including women, minorities and undergraduate students, to 5G-enabled EVCS and cybersecurity science. This project is affiliated to the Center for Information Assurance (CfIA) of the University of Memphis and Dr Ali is an Associate Director of the Center.

Project 02: Context-Aware Authorization Framework for Smart Critical Infrastructure NCAE-C in Cybersecurity Education Research

The University of South Carolina (lead institute), the University of Memphis, and The Citadel propose a joint research project to develop a secure authorization framework for critical infrastructure components. International conflicts make the United States of America a prime target for state sponsored cyber-attacks. As cybersecurity threats against critical infrastructure components increase, novel solutions that can adapt to the rapidly changing environment are in high demand.

Project 03: Zero-Trust Identity & Access Management

The goal of this project is to increase the understanding of Zero Trust methodology, principles and implementation and also to prepare organizations to face existing threats and adapt to new threats in the future. CfIA will develop a new 5-hour web-based course titled, Zero Trust: Identity & Access Management, to serve approximately 400 individuals and help state, local, tribal and territorial governments and private industry administrative and IT personnel implement organizational policies, procedures and operational strategies that will better enable their organizations to protect the public and our critical IT infrastructure through Zero Trust Access Control.

Project 04: Developing Application-specific Shared-trust Framework for Accessing Sensitive Information

Center for Information Assurance director Professor Dipankar Dasgupta received a $251K grant from the National Centers of Academic Excellence in Cybersecurity for “Developing application-specific shared-trust framework for accessing sensitive information.”

Project 05: Multidisciplinary Cybersecurity Program for Critical Infrastructure Protection

The overall project goal is to design and develop a multi-disciplinary critical infrastructure cybersecurity program addressing the technical needs of public utility operations and emergency decision-makers. A successful outcome of this project will create a strong southeast regional coalition, leveraging the NCAE’s expertise in cybersecurity to assist NCAE-C students (the future workforce), state and local government and critical infrastructure industry partners in contending with evolving threats. CfIA Co-Directors Dr. Dipankar Dasgupta (Computer Sc) and Dr. James McGinnis (Engineering Tech), along with faculty members Dr. Mohd Hasan Ali (Electrical) and Dr. Amanda Rockinson-Szapkiw (Education), will be leading initiatives on behalf of the University of Memphis.

Project 06: Cybersecurity Impact Analysis for End Users Security and Privacy

The Center for Information Assurance received a $600K grant from DHS/FEMA to develop cybersecurity training courses on Remote Home Office (RHO) security and End Users Security and Privacy (ESP). The UofM portion of the DHS/FEMA grant is led by Professor James McGinnis (Engineering Technology), and the grant is part of a multi-university $4M project spearheaded by the University of Arkansas Criminal Justice Institute.

Project 07: Examining Advanced Persistent Threats

This course was developed by the University of Memphis through the DHS/FEMA Homeland Security National Training Program. IT provides an overview of similarities and differences between traditional systems attacks and APT attacks. At the end of this course, participants should possess a fundamental understanding of the most common attack path for various advanced persistent threats (APTs). The course covers the cyber kill chain model, APT cases and attack techniques and tools and common APT defense strategies.

Project 08: Navy ROTC Cybersecurity Training Program

This program is for building a team consisting of students capable of effectively conducting research studies in cybersecurity, pairing a variety of skills with organization and leadership to enhance research outcomes in the ROTC program. The goal of this grant is to develop a technically sound ROTC program through the introduction of cybersecurity in the existing curriculum. The project will design and develop hands-on exercises based on the latest threats and social engineering attacks and introduce those in workshops and research papers, enhance the capabilities of students to detect and predict evolving threats whereby they can deploy the latest defense strategies and countermeasures in their workplace, and provide a support network in order to retain diverse and minority students within the program through advising, mentoring, networking, internships and workforce connections, tutoring, soft skills building, collegiality, etc. The project will be led by principal investigator Dr. James McGinnis, assistant professor in Engineering Technology, and co-PI Dr. Dipankar Dasgupta from Computer Science, Hill Professor in Cybersecurity, both of whom are directors of the CfIA. This grant is a part of the center's mission on education and outreach in cybersecurity.

Project 09: Scholarship for Services (SFS)

A $3.8 million Cybersecurity Education Grant from National Science Foundation (NSF). The five-year project, titled "CyberCorps Scholarship for Service: Developing the Cybersecurity Workforce in West Tennessee, Mississippi, and Arkansas" will recruit four cohorts of scholars from the Department of Computer Science, Department of Business Information Technology, College of Engineering, Department of Criminal Justice and other UofM units. Priority will be given to underrepresented students such as women, minorities and veterans. The grant is given under the NSF's Cybercops Scholarship for Service (SFS) program, which will provide full scholarships to individuals who agree to work in the cybersecurity sector for the government after graduation.

Project 10: GenCyber Summer Boot Camp for High School Students

The Department has received a new one-year, $100K cybersecurity education grant from the National Security Agency. Part of the NSA's GenCyber program, the project will create an integrated curriculum, in consultation with a K–12 pedagogical expert, focused on incorporating fundamental cybersecurity concepts with their applications to solve practical cybersecurity problems using autonomous R/C cars as a cyber-physical system platform. PI is Professor Myounggyu Won.

Project 11: Designing Machine Learning-based Solutions for APT Detection

UofM's Dr. Kan Yang (PI) and Dr. Xiaofei Zhang (Co-PI), two assistant professors in the Department of Computer Sciences, have been awarded funding from FedEx Service Inc. to develop advanced machine learning-based solutions to enhance the enterprise cyber analytic defense ecosystem. The project, entitled "Designing Machine Learning-based Solutions for APT Detection," will explore the recent advancement of machine learning techniques to detect Advance Persistent Threat (APT) attacks, which are used by experienced, state-sponsored attackers to steal data and perform disruptive operations on cyberinfrastructure.

PUBLISHED RESEARCH ARTICLES

1. Kishor Datta Gupta, and Dipankar Dasgupta. “Adversarial Attacks and Defenses for Deployed AI Models.” *IT Professional* 24.4 (2022): 37-41.

2. Arunava Roy, and Dipankar Dasgupta. “A Robust Framework for Adaptive Selection of Filter Ensembles to Detect Adversarial Inputs.” *2022 52nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*. IEEE, 2022.

3. Kishor Datta Gupta and Dipankar Dasgupta, “Negative selection algorithm research and applications in the last decade: a review.” *IEEE Transactions on Artificial Intelligence*, vol. 3, no. 2, pp. 110-128, 2022

4. Dipankar Dasgupta, and Kishor Datta Gupta. “Dual-filtering (DF) schemes for learning systems to prevent adversarial attacks.” *Complex & Intelligent Systems*: 1-22, 2022.

5. Dipankar Dasgupta, Zahid Akhtar, and Sajib Sen. “Machine learning in cybersecurity: a comprehensive survey.” The Journal of Defense Modeling and Simulation 19.1: 57-106, 2022

6. Mario Hyman, and Mohd Hasan Ali. “A Novel Model for Wind Turbines on Trains.” *Energies* 15.20: 7629, 2022.

7. Mohammad Ashraf Hossain Sadi, Dongbo Zhao, Tianqi Hong, and Mohd Hasan Ali. “Time Sequence Machine Learning-Based Data Intrusion Detection for Smart Voltage Source Converter-Enabled Power Grid.” *IEEE Systems Journal*, 2022.

8. Manoj Basnet, and Mohd Hasan Ali. “Multi-Agent Deep Reinforcement Learning-Driven Mitigation of Adverse Effects of Cyber-Attacks on Electric Vehicle Charging Station.” arXiv preprint arXiv:2207.07041, 2022.

9. Xingmiao Wang, Kai Fan, Kan Yang, Xiaochun Cheng, Qingkuan Dong, Hui Li, and Yintang Yang. “A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living.” *Computer Communications* 186: 121-132, 2022

10. Michael Villarreal, Bibek Poudel, Ryan Wickman, Yu Shen, and Weizi Li. “AutoJoin: Efficient Adversarial Training for Robust Maneuvering via Denoising Autoencoder and Joint Learning.” arXiv preprint arXiv:2205.10933, 2022.

11. Zachariah Threet, Christos Papadopoulos, William Lambert, Proyash Podder, Spiros Thanasoulas, Alex Afanasyev, Sheikh Ghafoor, and Susmit Shannigrahi. “Securing automotive architectures with named data networking”, 2022.

12. K Bhargavi, and Sajjan G Shiva. “Uncertainty Aware T2SS Based Dyna-Q-Learning Framework for Task Scheduling in Grid Computing” *Cybernetics and Information Technologies*, vol.22, no.3, 2022, pp.48-67.

13. K Bhargavi, and Sajjan G Shiva, “Man-in-the-Middle attack Explainer for Fog computing using Soft Actor Critic Q-Learning Approach,” 2022 *IEEE World AI IoT Congress (AIIoT)*, pp. 100-105 , 2022

14. Philipp Moll, Varun Patil, Lan Wang, and Lixia Zhang. “SoK: The evolution of distributed dataset synchronization solutions in NDN.” *Proceedings of the 9th ACM Conference on Information-Centric Networking*. 2022.

15. Navid Mohammad Imran, and Myounggyu Won, “Reducing Operation Cost of LPWAN Roadside Sensors Using Cross Technology Communication,” *IEEE Transactions on Intelligent Transportation Systems (T-ITS)*, 2022.

16. Myounggyu Won, “L-Platooning: A Protocol for Managing a Long Platoon with DSRC,” *IEEE Transactions on Intelligent Transportation Systems (T-ITS)*, 2022.

17. Pradeep Sambu, and Myounggyu Won, “An Experimental Study on Direction Finding of Bluetooth 5.1: Indoor vs Outdoor,” *IEEE Wireless Communications and Networking Conference (WCNC)*, 2022

18. Navid Mohammad Imran, Sabya Mishra, and Myounggyu Won, “Towards Fully Autonomous Drone-Based Last-mile Delivery,” *IEEE Transactions on Intelligent Transportation Systems (T-ITS)*, 2022. (under revision)

19. Jibran Ali Abbasi, Navid Mohammad Imran, and Myounggyu Won, “WatchPed: Pedestrian Crossing Intention Prediction Using Embedded Sensors of Smartwatch,” *Association for the Advancement of Artificial Intelligence (AAAI)*, 2022. (under review)

20. Lokesh Chandra Das, Dipankar Dasgupta and, Myounggyu Won, “LSTM-Based Adaptive Vehicle Position Control for Dynamic Wireless Charging,” *International Conference on Robotics and Automation (ICRA)*, 2022 (under review)

21. K. Yang, J. Shu, and R. Xie. “Efficient and Provably Secure Data Selective Sharing and Acquisition in Cloud-based Systems”. To appear on *IEEE Transactions on Information Forensics and Security*, 2022.

22. Xingmiao Wang, Kai Fan, Kan Yang, Xiaochun Cheng, Qingkuan Dong, Hui Li, and Yintang Yang, “A new RFID ultra-lightweight authentication protocol for medical privacy protection in smart living”. *Computer Communications*, Elsevier, Feb. 2022.

23. Anjia Yang, Jian Weng, Kan Yang, Cheng Huang, and Xuemin Shen, “Delegating Authentication to Edge: A Decentralized Authentication Architecture for Vehicular Networks”. *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 2, pp: 1284-1298, 2022.

24. Lei Yan, Kan Yang, and Shouyi Yang, “Reputation-based Truth Discovery with Long-term Quality of Source in Internet of Things”. *IEEE Internet of Things Journal*, Vol. 9, no.7, pp. 5410-5421, 2022.

NEWS & EVENTS

Left to Right: Dylan Hensley, Luke Carrington, Spencer Tartera (Team Captain), Chase Rumfelt, and Cody Seymour.

2022 Raymond James CTF Competition:

The University of Memphis Cyber Tigers participated in a Capture the Flag competition at Raymond James Headquarters in Tampa, Florida on October 22, 2022. Participants competed not only for team cash prizes, but also the opportunity to participate in Raymond James' Cybersecurity Summer Internship and Accelerated Development Programs. The 1st, 2nd, and 3rd place teams received $10,000, $5,000, and $2,500, respectively, along with the opportunity to dine at the table of a variety of Raymond James executives. Unfortunately, the UofM Cyber Tigers fell a little short of the desired goal. Members of the Cyber Tigers' competition team for this event were as follows: Spencer Tartera (Team Captain), Dylan Hensley, Chase Rumfelt, Luke Carrington, and Cody Seymour. Tony Pinson served as the University of Memphis team advisor for the event. Non-Floridian participants were provided air travel, hotel lodging, and shuttle service to and from Tampa International Airport.

2. On September 27, 2022. Sajib Sen accepted a position with Intel Corporation in the department of AI Ethics. He completed his MS degree and was co-author along with Dr. Dasgupta of the paper: *An Empirical Study of Algorithmic Bias. 2022.*

3. Walt Williams, an undergraduate student in the Computer Science department, was accepted into Google's Computer Science Research Mentorship program and was Research Scientist Intern with Adobe Research in the summer of 2022.. While working in the CfIA, he published a research paper discussing the latest trends in social engineering attacks and how Machine Learning (ML) can be used to mitigate and prevent cyber-attacks.

4. Subash Poudyal is a recent PhD graduate who worked on Cyber Security issues with Dr. Dasgupta. Mr. Subash recently worked on ransomware and possible AI-based countermeasures which were featured in Analytics India Magazine.

UPCOMING
EVENTS/WORKSHOPS

12TH ANNUAL MID-SOUTH CYBERSECURITY SUMMIT 2022

Friday Nov 4, 2022 | This annual summit aims to provide a platform for companies and institutions in the Mid-South Region to learn, discuss, and exchange knowledge and technologies about Cyber Security. The theme this year is “When AI meets Cybersecurity.” Registration link is forthcoming soon.

THE UNIVERSITY OF MEMPHIS®

University of Memphis | Center for Information Assurance | Memphis, TN 38152-3115 | cfia.memphis.edu