

NSA/DHS

National Centers of Academic Excellence in Cyber Defense Research 2020 Annual Report

Name of Institution
University of Memphis
Program(s) of Study (add rows if necessary) and Department
<p>Computer Science Department</p> <p>Programs: B.S Cyber Security Concentration • Graduate Certificate in Cyber Security and Information Assurance • Ph.D in computer science with research and dissertation in cyber security</p> <p>Business Information and Technology Department</p> <p>Programs: Graduate Certificate Program in Business Information Assurance • Graduate Certificate Program in Software Testing • Ph.D in BIT with research and dissertation in business information security</p>

Submitters Name	Contact Information
Dr. Dipankar Dasgupta	ddasgupt@memphis.edu

NOTE: Every year, NSA/DHS Centers of Academic Excellence in Cyber Defense Education and Research must submit an annual report containing information regarding student enrollment, number of graduates, student placement, research funding, and a variety of other variables. Submitting this information is a requirement for re-designation.



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

Please submit your information no later than February 15, 2020. If you have questions regarding the CAE Program or the annual report itself, please feel free to contact the CAE Program Office at AskCAEIAE@nsa.gov.



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

I. Contact Information (since last designation))

- a. Provide name and contact information of faculty teaching in the Program of Study
- b. Provide name and contact information for the two levels above Program of Study POC

Current Faculty	Faculty Contact Information
Dr. Dipankar Dasgupta-Center Director	ddasgupt@memphis.edu
Dr. Jim McGinnis-Center Co-Director	jmcgnnis@memphis.edu
Dr. Kan Yang-Center Associate Director	kan.yang@memphis.edu
Dr. Myounggyu Won	mwon@memphis.edu
Dr. Sajjan Shiva	sshiva@memphis.edu
Dr. Zahid Aktar	zmomin@memphis.edu
Dr. Christos Papadopoulos	Christos.Papadopoulos@memphis.edu
Leadership Information (Department Chair, Dean, etc)	Contact Information
Dr. Lan Wang-Department Chair	lanwang@memphis.edu

II. Student Enrollment

Identify the number of students currently enrolled in the programs reflective of the CAE designation for the last academic year – identify any that apply.

Number of students enrolled	
	MA
	MS
	MBA
	PhD
	Other (Graduate Certificate Program in Business Information Assurance)

III. Graduates

Identify the number of students that have graduated from the programs reflective of the CAE designation for the last academic year – identify any that apply.

Number of graduates	
	MA
2	MS
	MBA
3	PhD
	Transfers



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

	Graduate Certificate (Cyber Security Information Assurance)
	Graduate Certificate (Business Information Assurance)

IV. Student Placement

- Identify where M.S. and Ph.D students graduating from the programs reflective of the CAE designation have placed after graduating. This metric should be categorized by the number of students placed into government, industry and academic positions for the last academic year.

NSA	Gov	Industry	Academia	Advanced Degree	Other	Don't collect data
						X

- Identify the number of M.S. graduates in the last year that have elected to continue to an advanced degree program and into which field of study.

#	Field of Study

V. Student Development Opportunities

- “Student development opportunities” that are available to students in your program

First column check yes if offered, second column indicate numbers of students that took advantage of the opportunity		
X		Internships
		Apprenticeships
X		Co-operative education experiences (e.g., technical directors, students & faculty work together)



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

		Other (please specify)
--	--	------------------------

VI. Research Expertise

Since the institution's last designation application:

- Using the Core Area List attached below,* identify your school's current areas of expertise. List in descending order of expertise. (No more than 10)

Core #	Sub-core area
2	Identification and Authentication
2	Authorization and Access Controls
3	Cloud, Grid, distributed computing
2	Wireless, link, and signal security
3	Network models
5	Intrusion detection/analysis/remediation
6	Processes

VII. Publication

Since the institution's last designation application:

- Identify recent publications/papers relevant to the current areas of expertise listed above.

Core #	Recent Publications/Papers Relevant to Current Areas of Expertise (Titles only please)
2,3	Multi-user permission strategy to access sensitive information



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

5	A Multi-Level Ransomware Detection Framework using Natural Language Processing and Machine Learning
6	Low Dose Abdominal CT Image Reconstruction: An Unsupervised Learning Based Approach
2	Face Authenticity: An Overview of Face Manipulation Generation, Detection and Recognition
2	A survey of blockchain from security perspective
3	Design and implementation of Negative Authentication System
2	AI vs AI: Viewpoints

VIII. Research Funding

Since the institution's last designation application:

- Identify any significant funding for CD research relevant to the current areas of expertise listed above. Include funding source, amount, and a brief description of research.

Date	Source	Amt	Brief Description
7/1/18-12/31/19	FIT	\$15,000	CAST: PKChain: Decentralized Public-Key Management System Based on Blockchain Technology
9/2017-8/30/20	FEMA/DHS	\$400,000	Preparing for Next Generation Cyber Defense
9/1/17 - 8/31/20	Lead: NU Prime: DHS/FEMA	(Multi-University Grant of 2.2 million)	Realizing Advanced Persistent Threats Norwich University Applied Research Institute
	Department of Defense	\$318,000	Navy ROTC Training Grant

VIII. Institution Successes & Achievements

Since the institution's last designation application:

2020 Annual Report



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

- Describe activities that represent successes and achievements of the program(s) reflective of the CAE designation such as scholarships, outreach, partnerships, awards, conference participation, etc.

Success/Achievements

The Center for Information Assurance welcomed Dr. Christos Papadopoulos and Dr. Sajjan Shiva. These faculty members are teaching cyber-related courses and conducting cybersecurity research.

Dr. Christos Papadopoulos

Dr. Papadopoulos's research interests include Computer networks, network security, multimedia communication, and distributed systems. Dr. Papadopoulos completed 2 publications in 2020 entitled:

Discovering in-network Caching Policies in NDN Networks from a Measurement Perspective

C Fan, S Shannigrahi, C Papadopoulos, C Partridge

Proceedings of the 7th ACM Conference on Information-Centric Networking, 106-116

Delay-based Identification of Internet Block Movement

M Gharaibeh, C Papadopoulos, J Heidemann, C Partridge

Dr. Sajjan Shiva

Dr. Shiva's research interests include software systems and cybersecurity. In 2020, Dr. Shiva completed the following publications:

Network Intrusion Detection using Natural Language Processing and Ensemble Machine Learning

S Das, M Ashrafuzzaman, FT Sheldon, S Shiva

2020 IEEE Symposium Series on Computational Intelligence (SSCI), 829-835

Taxonomy and Survey of Interpretable Machine Learning Method

S Das, N Agarwal, D Venugopal, FT Sheldon, S Shiva

2020 IEEE Symposium Series on Computational Intelligence (SSCI), 670-677

Ads-Guard: Detecting Scammers in Online Classified Ads

S Al-Rousan, A Abuhussein, F Alsubaei, L Collen, S Shiva

2020 IEEE Symposium Series on Computational Intelligence (SSCI), 1492-1498

Ensemble Classifiers for Network Intrusion Detection Using a Novel Network Attack Dataset

A Mahfouz, A Abuhussein, D Venugopal, S Shiva

Future Internet 12 (11), 180

Detecting stealthy false data injection attacks in the smart grid using ensemble-based machine learning

M Ashrafuzzaman, S Das, Y Chakhchoukh, S Shiva, FT Sheldon

Computers & Security 97, 101994

Empirical evaluation of the ensemble framework for feature selection in ddos attack

S Das, D Venugopal, S Shiva, FT Sheldon

2020 7th IEEE International Conference on Cyber Security and Cloud Computing ...



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

Social-Guard: Detecting Scammers in Online Dating

S Al-Rousan, A Abuhussein, F Alsubaei, O Kahveci, H Farra, S Shiva
2020 IEEE International Conference on Electro Information Technology (EIT ...

A holistic approach for detecting ddos attacks by using ensemble unsupervised machine learning

S Das, D Venugopal, S Shiva
Future of Information and Communication Conference, 721-738

Network Intrusion Detection Model Using One-Class Support Vector Machine

AM Mahfouz, A Abuhussein, D Venugopal, SG Shiva
Advances in Machine Learning and Computational Intelligence, 79-86

Toward an effective requirement engineering approach for cloud applications

A Abuhussein, F Alsubaei, S Shiva
Software Engineering in the Era of Cloud Computing, 29-50

Comparative analysis of ML classifiers for network intrusion detection

AM Mahfouz, D Venugopal, SG Shiva
Fourth international congress on information and communication technology ...

Security benchmarks for wearable medical things: stakeholders-centric approach

SR Putta, A Abuhussein, F Alsubaei, S Shiva, S Atiewi
Fourth International Congress on Information and Communication Technology ...

Dr. Dipankar Dasgupta

Dr. Dasgupta has completed a myriad of activities in support of the Center for Information Assurance.

- Prof. Dipankar Dasgupta has been awarded U.S. Patent 10,671,747, entitled "Multi-user permission strategy to access sensitive information."
The patent was filed jointly with fellow researchers Arunava Roy and Debasis Ghosh. (#10,671,747) by Dr. Dasgupta on multi-user permission strategy to access sensitive information approved by USPTO on June 2, 2020. For details [click here](#).
- Prof. Dipankar Dasgupta gave an invited talk at INNOVATE IT 2020 Conference hosted by Greater Memphis IT Council on October 8th. Event Agenda at http://www.memphisitcouncil.com/uploads/1/2/8/1/128111718/greater_memphis_it_council_innovate_it_it-program_agenda_-10-8-20_-_revised.pdf. As the top Innovation in Entrepreneurship award, Dr. Dasgupta's Adaptive Multi-Factor Authentication was ranked #1 by the virtual attendees of the event.
- Dr. Dasgupta is organizing a symposium on Computational Intelligence in Cyber Security (CICS) at the IEEE Symposium Series on Computational Intelligence (SSCI) at Canbara, Australia (Virtual) on Dec 1 - 4, 2020.
- Dr. Dasgupta gave an invited talk at the Greater Memphis IT Council (GMITC) Cyber Security Roundtable quarterly meeting of 25 CISOs on July 21, 2020.
- Dr. Dasgupta became a member of IEEE CIS Neural Networks Technical Committee Task Force on Secure Learning.
- Dr. Dasgupta gave a presentation at IEEE World Congress on Computational Intelligence (WCCI) entitled "AI is not Magic—it is Computational Logic" on July 21, 2020. The presentation is available from [YouTube](#).
- Dr. Dasgupta received summer Grant on June 1, 2020 from Idaho National Lab to conduct research on 5G Technology Security.



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

- Dr. Dasgupta received Cybersecurity Training Grant (as Co-PI) on June 1, 2020. For details: [New Cybersecurity Training Grant](#).

Dr. Dasgupta contributed to the following publications for 2020:

AI-Powered Ransomware Detection Framework

S Poudyal, D Dasgupta

(SSCI), Canberra, Australia, 2020, doi: 10.1109/SSCI47803.2020.9308387 ...

Applicability issues of evasion-based adversarial attacks and mitigation techniques

KD Gupta, D Dasgupta, Z Akhtar

2020 IEEE Symposium Series on Computational Intelligence (SSCI), 1506-1515

Adversarial Input Detection Using Image Processing Techniques (IPT)

KD Gupta, D Dasgupta, Z Akhtar

2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile ...

Machine Learning and Feature Selection Based Ransomware Detection Using Hexacodes.

R B.V., K G.J., R V., D D.

Evolution in Computational Intelligence. Advances in Intelligent Systems and ...

Utility of Deep Learning Features for Facial Attributes Manipulation Detection.

Z Akhtar, M Mouree, D Dasgupta

First IEEE International Conference on Humanized Computing and Communication ...

An empirical study on algorithmic bias

S Sen, D Dasgupta, KD Gupta

2020 IEEE 44th Annual Computers, Software, and Applications Conference ...

Determining Sequence of Image Processing Technique (IPT) to Detect Adversarial Attacks

K Datta Gupta, Z Akhtar, D Dasgupta

arXiv e-prints, arXiv: 2007.00337

Multi-user permission strategy to access sensitive information

D Dasgupta, A Roy, D Ghosh

US Patent 10,671,747

Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations

SS Bhuyan, UY Kabir, JM Escareno, K Ector, S Palakodeti, D Wyant, ...

Journal of medical systems 44 (5), 1-9

5G Enabled Energy Innovation: Advanced Wireless Networks for Science, Workshop Report

P Beckman, C Catlett, M Ahmed, M Alawad, L Bai, P Balaprakash, ...

USDOE Office of Science (SC)(United States)

Adaptive multi-factor authentication system with multi-user permission strategy to access sensitive information

D Dasgupta, A Roy, D Ghosh, AK Nag

US Patent App. 16/387,839



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

Shamir's Secret Sharing for Authentication without Reconstructing Password

KD Gupta, ML Rahman, D Dasgupta, S Poudyal

2020 10th Annual Computing and Communication Workshop and Conference (CCWC ...

Machine learning in cybersecurity: a comprehensive survey

D Dasgupta, Z Akhtar, S Sen

The Journal of Defense Modeling and Simulation, 1548512920951275

Dr. James McGinnis

Dr. McGinnis serves as the center co director and PI of the new ROTC Training Grant awarded to the Center for Information Assurance. Dr. McGinnis was featured in the June 2020 Research and Innovation newsletter and named as a Committee member for curriculum development on the National Cybersecurity Preparedness Consortium. Dr. McGinnis additionally attended the National Cybersecurity Preparedness Consortium 508 Course Design Compliance Review Training.

Dr. Won

Dr. Won's research interests consists of cyber physical systems, mobile computing, intelligent transportation systems. Dr. Won's 2020 accomplishments and publications include:

- [08/2020] Our paper is accepted to GLOBECOM'20.
- [08/2020] Dr. Won was invited to serve on TPCs of WCNC and IPCCC.
- [05/2020] Dr. Won was invited to serve on TPCs of MASS and WiMob.
- [04/2020] Our paper is accepted to IEEE Access!
- [03/2020] Our paper is accepted to IEEE Access!
- [01/2020] Our paper is accepted to ICRA'20!
- [01/2020] Dr. Won was invited to serve as a guest editor for MDPI Electronics journal.

[GLOBECOM'20] B. Karki, and M. Won, "Characterizing Power Consumption of Dual-Frequency GNSS of a Smartphone".

[Access'20a] M. Won, "Intelligent Traffic Monitoring Systems for Vehicle Classification: A Survey".

[Access'20b] M. Won, A. Shrestha, K. Park, Y. Eun, "SaferCross: Enhancing Pedestrian Safety Using Embedded Sensors of Smartphone".

[ICRA'20] M. Won, "UBAT: On Jointly Optimizing UAV Trajectories and Placement of Battery Swap Stations".

Dr. Akhtar

Dr. Akhtar contributed to the following publications in 2020:

Contactless Multi-biometric System Using Fingerprint and Palmprint Selfies

A Herbadji, N Guermat, L Ziet, Z Akhtar, M Cheniti, D Herbadji

Traitement du Signal 37 (6), 889-897

Applicability issues of evasion-based adversarial attacks and mitigation techniques

KD Gupta, D Dasgupta, Z Akhtar

2020 IEEE Symposium Series on Computational Intelligence (SSCI), 1506-1515

Directional Neighborhood Topologies based Multi-scale Quinary Pattern for Texture Classification

E Rachdi, Y El Merabet, Z Akhtar, R Messoussi

IEEE Access



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

Feature-level fusion of major and minor dorsal finger knuckle patterns for person authentication

A Attia, Z Akhtar, Y Chahir

Signal, Image and Video Processing, 1-9

Deep rule-based classifier for finger knuckle pattern recognition system

A Attia, Z Akhtar, NE Chalabi, S Maza, Y Chahir

Evolving Systems, 1-15

Accelerating deep reinforcement learning model for game strategy

Y Li, Y Fang, Z Akhtar

Neurocomputing 408, 157-168

3D Palmprint recognition using Tan and Triggs normalization technique and GIST descriptors

M Chaa, Z Akhtar

Multimedia Tools and Applications, 1-15

Determining Sequence of Image Processing Technique (IPT) to Detect Adversarial Attacks

K Datta Gupta, Z Akhtar, D Dasgupta

arXiv, arXiv: 2007.00337

Combining Multiple Biometric Traits Using Asymmetric Aggregation Operators for Improved Person Recognition

A Herbadji, Z Akhtar, K Siddique, N Guermat, L Ziet, M Cheniti, ...

Symmetry 12 (3), 444

Weighted quasi-arithmetic mean based score level fusion for multi-biometric systems

H Abderrahmane, G Noubel, Z Lahcene, Z Akhtar, D Dasgupta

IET Biometrics 9 (3), 91-99

A Survey on Machine and Deep Learning for Detection of Diabetic Retinopathy

A Attia, Z Akhtar, S Akhrouf, S Maza

ICTACT journal on image and video processing 11 (02), 2337-2344

Adversarial Input Detection Using Image Processing Techniques (IPT)

KD Gupta, D Dasgupta, Z Akhtar

Utility of Deep Learning Features for Facial Attributes Manipulation Detection

Z Akhtar, MR Mouree, D Dasgupta

IEEE International Conference on Humanized Computing and Communication with ...

Machine learning in cybersecurity: a comprehensive survey

D Dasgupta, Z Akhtar, S Sen

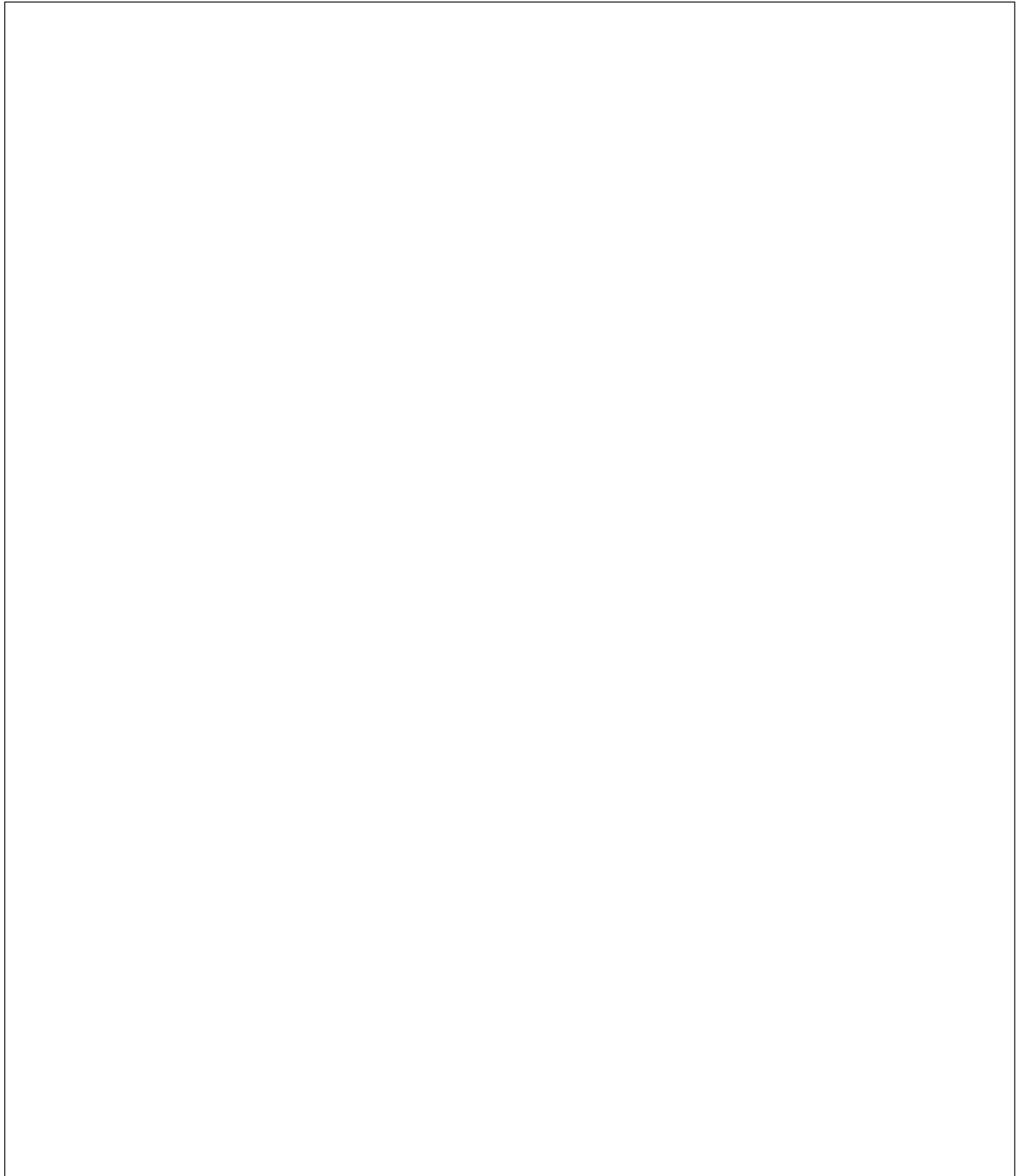
The Journal of Defense Modeling and Simulation, 1548512920951275



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

IX. Designation Return on Investment

- Identify any opportunities, successes and/or achievements specifically resulting from the institution’s designation as a CAE.

ROI

The Center for Information Assurance’s (CfIA) CAE designation has opened opportunities for the center to act as a HUB for educational institutions, government agencies, and local businesses on Cybersecurity initiatives. We have had the opportunity to work with other universities that have received the CAE-CD and/or CAE-CD & CAE-R designation as a founding member of the National Cybersecurity Preparedness Consortium (NCPC) on research that has produced cutting edge research and created multiple training opportunities. The University of Memphis is proud to announce that formal agreements have been made with the following schools for shared curriculums, lectures, and teaching materials. We hope that this is the first step of many towards significantly greater exposure and recognition for the Information Technology capabilities of the participating schools and surrounding businesses. We hope that continued interest will be maintained by the Mid-South area and our efforts can encourage the growth of not only the students but also the private sector as a result of a supply of NSA certified graduates entering the job market.

Online Cybersecurity Courses Available

Two new online courses concerning Cybersecurity have been developed and are available for access online. These courses are funded by DHS/FEMA and are offered to the public at no charge.

The first course is titled “Understanding Social Engineering Attacks” and covers some of the techniques and tools used in social engineering. The course also offers insight to equip learners with a better understanding of how attackers use people as a “weakest” link to compromise a targeted organization. Please see the attached flyer for more information and to share with persons within your organization. This course is hosted on a FEMA funded site by the University of Texas A&M Engineering Extension Service at <https://teex.org/class/AWR367/>

The second course is titled “Mobile Device Security and Privacy”. This course is designed to assist individuals to better understand security and privacy issues with mobile devices and infrastructure. Using scenarios, thought challenges and exercises as a framework, students will learn about:

- The purpose of Enterprise Mobile Management platforms
- Elements that make mobile networks and operating systems different
- Mobile malware classifications and detection strategies
- Mobile architecture data leakage detection and prevention strategies.

Silicon Valley Startup Licenses Patent for Adaptive Multi-Factor Authentication System

The University of Memphis Research Foundation has signed an agreement to license a U.S. patent for an Adaptive Multi-factor Authentication System invented and developed by a team led by Dr. Dipankar Dasgupta, professor of Computer Science and director of the Center for Information Assurance. The patent is licensed to i2Chain, a San Francisco-area cybersecurity startup, which plans to evolve adaptive authentication for its own applications as well as offer the technology as a service to other identity providers.



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

Professor Dasgupta receives Innovation Award 2020

Dr. Dipankar Dasgupta, UofM Hill Professor of Cybersecurity and director of the Center for Information Assurance, was honored by the Greater Memphis IT Council at its annual INNOVATE IT conference for his development of the patent for the Adaptive Multi-Factor Authentication solution in cybersecurity.

"We conducted a live poll to select the top Innovation in Entrepreneurship and the University of Memphis Adaptive Multi-Factor Authentication was ranked #1 by the attendees. We are very proud to extend our first innovation award to Dr. Dasgupta and the University of Memphis for this outstanding application." – Regina Whitley, IT Council Executive Director.

INNOVATE IT (October 6, 2020)Event LINK: <https://www.btsvirtualevents.com/innovateit>

Online Cybersecurity Courses Available

Two new online courses concerning Cybersecurity have been developed and are available for access online. These courses are funded by DHS/FEMA and are offered to the public at no charge.

The first course is titled "Understanding Social Engineering Attacks" and covers some of the techniques and tools used in social engineering. The course also offers insight to equip learners with a better understanding of how attackers use people as a "weakest" link to compromise a targeted organization. Please see the attached flyer for more information and to share with persons within your organization. This course is hosted on a FEMA funded site by the University of Texas A&M Engineering Extension Service at <https://teex.org/class/AWR367/>

The second course is titled "Mobile Device Security and Privacy". This course is designed to assist individuals to better understand security and privacy issues with mobile devices and infrastructure. Using scenarios, thought challenges and exercises as a framework, students will learn about:

- The purpose of Enterprise Mobile Management platforms
- Elements that make mobile networks and operating systems different
- Mobile malware classifications and detection strategies
- Mobile architecture data leakage detection and prevention strategies.

Currently Engaged Schools

Arkansas State University
Mid-South Community College
LeMoyne-Owen College
Christian Brothers University
Rhodes College
Rust College

In an effort to expand the influence of the program we are trying to involve as many schools as possible. Each school in the program has the potential to collaborate with the University of Memphis in future proposals and grants.



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

In addition, the University of Memphis will share teaching materials with partners, offer video-lectures, investigate articulation, and promote the continuation of undergraduate and graduate students to pursue a B.S., M.S., or Ph.D. degree with available scholarships in IA. LeMoyne-Owen College, one of the nation's historically black four-year institutions, has applied for their CAE designation and has entered a mentoring relationship with us. We continue to work collaboratively with their Director of Cyber Defense to provide them guidance through this process.

Scholarship

Since our designation as a CAE, we have been awarded several internal grants from the University of Memphis and external grants from government agencies for both research and education. Students have expressed a desire to participate with our institution due to the cutting edge research that we have been able to study thanks to these grants, and have ultimately allowed us to offer scholarship opportunities to both undergraduate students and graduate students.

<https://www.memphis.edu/cfia/scholarships/index.php>

ROTC Training Program

The CAE designation has given us the opportunity to develop a program for ROTC Research in conjunction with U of M ROTC, Arkansas State University and Arkansas State University ROTC. This will allow us to create additional opportunities to students. In 2020, the Center for Information Assurance was awarded \$318,000 to develop a cybersecurity ROTC Training Program. With this grant, we have been able to form additional partnerships with our campus ROTC departments as well as develop student publications and a cybersecurity workshop.

CAE Tech Talk

The Center for Information Assurance supports The Centers of Academic Excellence (CAE) in Cybersecurity Community Tech Talk feature presentations. We encourage students to expand their knowledge by attending additional workshops and presentations. Details are given below.

Time: 1:00 - 1:50pm EST

Topic: Secure Container for Data Protection in Transit and at Rest with Leakage Detection

Location: <https://captechu.zoom.us/j/664120328>

Time: 2:00 - 2:50pm EST

Topic: Reverse Engineering Malware (REM)

Location: <https://captechu.zoom.us/j/664120328>

Fall 2020 Cybersecurity competition

ServiceMaster hosted a virtual Capture The Flag for Terminix on Friday, July 31, 2020. This jeopardy-style hacking competition pits teams against each other, solving a variety of tasks in categories such as web exploitation, network forensics, and reverse engineering while finding flags and scoring points. There were three participants from The University of Memphis. The participants were Subash Poudyal, Benjamin Michael Borstad and Tony Gregory Pinson. The team scored a total of 3700 points securing the 19th position among 157 teams.

Prof. Dasgupta Awarded New U.S. Patent

Prof. Dipankar Dasgupta has been awarded U.S. Patent 10,671,747, entitled "Multi-user permission strategy to access sensitive information."

2020 Annual Report

NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

CAE VIRTUAL CAREER FAIR 2020

The Centers of Academic Excellence (CAE) in Cybersecurity Community hosted the fourth annual CAE Virtual Career Fair (VCF), sponsored by the National Cybersecurity Training and Education (NCyTE) Center and the National Science Foundation (NSF), on September 4, 2020, from 9:00 am-1:00 pm. Students and cybersecurity enthusiasts were encouraged to attend to learn more about the growing field and it's facilitators.

Rust College
process.

X. CAE Community Contributions

- Check all that apply to the institution's specific contributions to the CAE Community such as attendance at CAE Community Meetings, participation in working groups, Tech Talk contributor, participation in KU development and refinement, etc.

Community Contributions	
X	Attendance at CAE Community Meetings
X	Participation in CAE Working Groups
X	CAE Research Collaborations
X	Assistance to other institutions seeking CAE designation (e.g.; reviewers, advisors, mentors)
	Tech Talk/CAE Forum speaker
	CAE Regional Resource Center (CCRC) or CAE National Resource Center (CNRC)
	KU Development/Refinement
	Other (Please specify)

XI. Additional Information

- Institution may use this section to provide any additional information not previously mentioned in this report pertinent to the CAE program.

Additional Info



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

- During the 2020 academic year, a global pandemic caused many delays and cancellations of many activities, conferences and gatherings in order to assure the safety of faculty, staff and students.
- Our Center's students have experienced a lot of success over the course of the past year. While working with our Center, students have completed internships, placements and other co-operative experiences to further facilitate student development opportunities. While working with the Center, these students have received both academic and moral support from our faculty and staff. 2020 Computer Science Graduates include the following students with cybersecurity related research:
 - **PhD**
 - Faisal Alsubaei (advisor: Prof. Sajjan Shiva)
Thesis: "Security Assessment Framework for the Internet of Medical Things Solutions"
 - MdMaminur Islam (advisor: Prof. Deepak Venugopal)
Thesis: "Advances in Improving Scalability and Accuracy of MLNS using Symmetries"
 - Nazir Saleheen (advisor: Prof. Santosh Kumar)
Thesis: "Behavioral Privacy Risks and Mitigation Approaches in Sharing of Wearable Inertial Sensor Data"
 - **MS**
 - Senjuti Dutta (advisor: Prof. Kan Yang)
Thesis: "Enabling Efficient and Privacy-Preserving Task Matching For Cloud-Based Crowdsourcing"
 - Laqin Fan (advisor: Prof. Lan Wang)
Thesis: "Secure Sharing of Spatio-Temporal Data through Name-based Access Control"

One new course "Secure Coding and Testing" will be added to the 2020 Spring semester with the help of the Center's faculty and students. Before launching, Dr. Dasgupta tested and prepared the course materials with his graduate students and researcher Dr. Andrew Neel.



NSA/DHS National Centers of Academic Excellence in Cyber Defense Research

*Core Area List

1. Principles

- Domains and domain separation
- Resources and resource isolation
- Privileges and least privilege
- Layering
- Application of principles to function, component and system levels
- Composition

2. Security Mechanisms / Functionality

- Cryptography
- Identification and Authentication
- Authorization and Access Controls
- OS/DBMS/Network mechanisms
- Trusted processes (what are they, when are they needed)
- Virtualization
- Biometrics
- Audit, monitoring, anomaly detection, DLP
- Wireless, link, and signal security

3. Architectures

- Network models
- OS/DBMS/Network architectures
- OS/DBMS/Network subjects and objects (active entities and data containers)
- Cloud, Grid, distributed computing
- Custom/specialized architectures (e.g., Ad-hoc networks, SCADA)
- Interconnectivity and routing
- Privilege and separation issues
- Components vs. Solutions vs. Systems
- Critical infrastructure security

4. Assurance

- Software
- Hardware
- Testing (functional, penetration, black box, white box, measurement, etc.)
- Modeling and Formal methods (must focus on feasibility, applicability, strengths/weaknesses)

5. Operations

- Configuration
- Security automation
- Intrusion detection/analysis/remediation

6. Analysis

- Cryptanalysis
- Malware analysis
- Forensics
- Data mining
- Process
- Audit
- Certification and accreditation

7. Non-technical CD Issues

- Legal issues
- Policy issues
- Privacy
- Business Case / Economics
- Awareness
- Supply Chain

