THE UNIVERSITY OF MEMPHIS | Center for Information Assurance

# CfIA Annual Report (Full Version)
# Fiscal Year 2017

*Nationally Designated Center of Academic Excellence*

*in*

*Information Assurance/Cyber Defense Education*


**CfIA Director: Dr. Dipankar Dasgupta**

**Professor, Department of Computer Science**

**CfIA Co-Director: Dr. Judith C. Simon**

**Professor, Department of Business Information Technology**

**CfIA Associate Director: Dr. Kan Yang**

**Assistant Professor, Department of Computer Science**

# Table of Contents



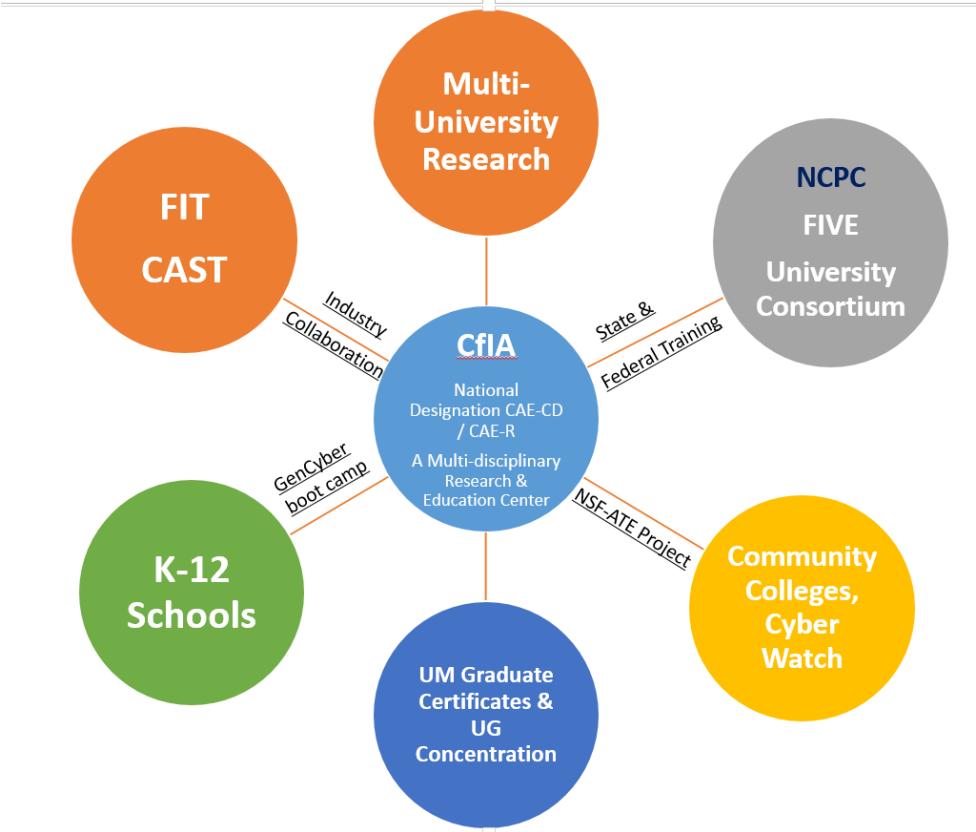
# I. Executive Summary

Fiscal year 2017 is another successful year for the Center for Information Assurance (CfIA). The CfIA continued to expand its activities and maintain high productivity in all areas of academic endeavors. With a new CS faculty member, **Dr. Kan Yang**, who joined the Center as an Associate Director, we are now able to further expand our cyber security activities. In particular, we introduced a new Cyber Security undergraduate concentration during the Fall of 2017.

Research publications and grant funding are increasing alongside our many outreach and training activities. The center also encouraged students to participate in competitions and establish an undergraduate SRO (Student Research Organization) on cyber security education at the University.

The Center faculty expanded their research activities by collaborating with the Center to Advance cyber Security and Testing (CAST) and the Financial Infrastructure Stability and Cyber-security (FICS) Center.

We expect to continue a wide range of activities so that the center can reach the forefront of research, education, and outreach on cyber security in the region and also receive funding in all three areas. The figure below shows the center's activities.



# II. Overview of the Center for Information Assurance

## A. History

The University of Memphis (UM) viewed Cyber and Information Security as a multidisciplinary, campus-wide activity, which led to the establishment of Center for Information Assurance (CfIA) with its charter in October 2004[1]. Since CfIA's inception, the Provost's office has administered and provided various forms of support. Since the CfIA's establishment, the Center 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). This designation is an accomplishment unique to the University of Memphis, since it is the first time that a Tennessee institution has received both of these designations. In addition to the two graduate certificate programs in Information Assurance (via the Department of Computer Science) and Business Information Technology (via the Department of Business Information and Technology (BIT)), the Center has since added a CyberSecurity concentration to the Computer Science Degree program. The CfIA directors have since welcomed Dr. Kan Yang to the Center as Associate Director. Together, the directors manage the programs and monitor students who receive the Department of Defense (DoD) scholarship, which is an initiative led by Dr. Simon.

## B. Goals/ Objectives

"Careers in Information Security Analysis ranks 7th out of 100 best Technology jobs" according to US News and World Report.[2] Over the past 5 years, there has been a 74% increase in job postings, with a 9% increase in salary premiums. Of these postings, 84% require a Bachelor's degree. 83% of these postings require that the applicant have at least 3 years of experience. Individuals seeking Certified Information Systems Security Professional (CISSP) certification, however, will need to have no less than five years of experience prior to taking the test.

That being said, there is still a shortage of Cybersecurity Professionals in the industry. As of October 2017, there were 299,335 unfilled cybersecurity jobs, and these vacancies were projected to increase to 1.5 million by the end of 2019.

The long-term goal is to establish a regional hub for Cybersecurity Education and Research in collaboration with public and private sectors in the State of Tennessee with the goal of making significant impacts on economic development, the provision of public services, citizen privacy and security.

The Center expanded activities in the following directions:

1 Official designation of Center of IA (with its charter) Signed by the President of the University available at: http://cfia.cs.memphis.edu/docs/center-declaration.PDF Dean's (College of Arts and Sciences) letter designating the IA center at the University of Memphis, available at http://cfia.cs.memphis.edu/docs/Dean-Letter.jpg

2 More information about Information Security Analysts can be found at: https://money.usnews.com/careers/best-jobs/information-security-analyst

- Continue expand our research capabilities by collaborating with faculty across campus (from different discipline) and other universities and company partnerships.
- Promote two graduate certificate programs in Information Assurance (via the Department of Computer Science) and Business Information Technology (via the Department of Business Information and Technology (BIT)).
- Develop undergraduate curriculum to educate technically sound cyber defenders and IT professionals (initiated UG concentration in Cyber Security in CS Department and offered an undergraduate course (BIT Department) on using COBIT 5 for standardized procedures in management of various cyber security issues including Audit & Assurance, Risk Management, Information Security, Regulatory and Compliance, and Governance of Enterprise IT). The BIT Department is currently developing an undergraduate concentration on information security management, with a target implementation date of 2018.
- Develop Cyber Corps Program for students from a variety of backgrounds including computer science, mathematics, electrical engineering, chemical engineering, mechanical engineering, law and business (DoD scholarships and others are being explored).
- Expand our cyber security education and awareness activities to community colleges and high schools in the region in partnership (received NSF-ATE grant with Jackson State Community College and NSA-GenCyber Bootcamp for high school and middle school students).
- Established National Cybersecurity Preparedness Consortium (NCPC) to train local, state and federal employees on cyber threats and in critical infrastructure protection (annual report attached).
- Engage in multi-disciplinary research activities in cyber security, spearhead collaborating efforts in new areas of research including cyber ethics, cyber law, secure health informatics, privacy-preserving mobile health, smart grid security and secure supply chain (formation of FIT-CAST).

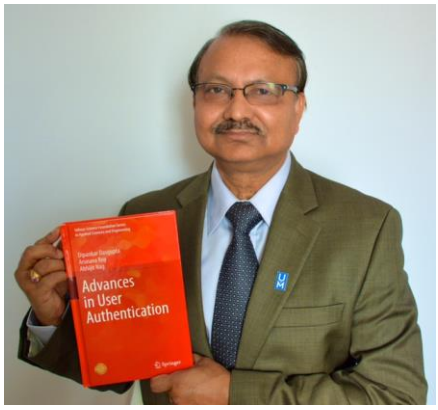
## C. Center Staff

| Name | Affiliation |
|---|---|
| Dr. Andrew Neel | External Researcher |
| Dr. Mike Nolan | External Researcher |
| Dr. Debasish Ghose | External Researcher |
| Dr. Bo Chen | Former Research Assistant Professor (June 2016-June 2017) |
| Dr. German Hernandez | Visiting Scholar (October 2017-December 2017) |
| Kul Prasad Subedi | Current Ph.D Student |
| Daya Ram Budhathoki | Current Ph.D Student |
| Senjuti Dutta | Current Ph. D Student |
| Sajib Sen | Current Ph. D Student (Fall 2017) |
| Kishor Datta Gupta | Current Ph. D Student |

| | |
|---|---|
| Raasi Manasa Annavajjala | Former Ph. D Student (Summer 2017) |
| Subash Poudyal | Current MS Student |
| Ayushi Mehta | Current MS Student |
| Berkeley Willis | Current MS Student |
| John Shrein | Current MS Student and Computer Science Professor |
| Robert Edstrom | Current Undergraduate Student |
| McKittrick Swindle | Current Undergraduate Student |
| Clifford Montjoy | Current Undergraduate Student |
| Peyton Warren | Current Undergraduate Student |
| Jon Walter Cobb | Current Undergraduate Student |
| Carolyn Treadwell-Butler | CyberSecurity Project Coordinator/Staff |
| Shannon Perry | Course Design Specialist/Staff |
| Kelly Freeman | Administrative Staff/Staff |

## III. Achievements/Activities during FY 2017

### A. Research Publications




During 2017 academic year, **Dr. Dasgupta** has published 20 research papers. 10 of these papers were journal articles. His latest book **Advances in User Authentication** [3] was published by Springer Inc. in August 2017. The book provides state-of-art accounts of authentication technologies, which cover not only basic authentication methodologies but also emerging technologies, which are yet to be deployed and adopted by industry. Intended as a graduate-level text, the book covers recent developments in the field, including Prof. Dasgupta's own grant-funded research in the area. The text was co-authored with two of his students, **Arunava Roy** and **Abhijit Nag**.

A list of his 2017 publications include:

- Co-Editor of the proceedings as the Chair of IEEE Symposium Series on Computational Intelligence in Cyber Security (CICS), December 2017.
- Mustafa Hajeer and Dipankar Dasgupta. Handling Big Data Using a Data-Aware HDFS and Evolutionary Clustering Technique. Accepted at the Journal IEEE Transactions on Big Data, 2017.

[3] More information about Dr. Dipankar Dasgupta's publications can be found here: https://scholar.google.com/citations?hl=en&user=tMAWoyoAAAAJ&view_op=list_works&sortby=pubdate

- Dipankar Dasgupta, Abhijit Kumar Nag, Denise Ferebee, Sanjib Kumar Saha, Kul Subedi, Alvaro Madero, Abel Sanchez, and John R. Williams, Design and Implementation of Negative Authentication System, published in International Journal of Information Security, Springer-Verlag, pp 1-26, November 2017.
- Dipankar Dasgupta, Arunava Roy and Debashis Ghosh, Multi-user Permission Strategy to Access Sensitive Information, Published in journal of Information Sciences, Elsevier, Volume 423, Pages 24-49 January 2018.
- A Roy, D Dasgupta. A fuzzy decision support system for multifactor authentication. Soft Computing Journal, pp.1-23, Springer-Verlag, May 2017.
- Soumitra Bhuyan, Hyunmin Kim, Oluwaseyi O. Isehunwa, Naveen Kumar, Jay Bhatt, David Wyant, Satish Kedia, Cyril F. Chang, Dipankar Dasgupta Privacy and Security Issues in Mobile Health: Current Research and Future Directions. Elsevier, January 2017.
- Arunava Roy and Dipankar Dasgupta, A Fuzzy Decision Support System for Continuous Multi-Factor Authentication, In Journal of Soft Computing, Springer, pp. 1-23, 2017.
- D Dasgupta, A Roy, A Nag. Biometric Authentication. Book Chapter in Advances in User Authentication, pp.37-84, Publisher: Springer-Verlag, August 2017.
- D Dasgupta, A Roy, A Nag. Pseudo-Passwords and Non-textual Approaches. Book Chapter in Advances in User Authentication, pp.147-183, Publisher: Springer-Verlag, August 2017.
- D Dasgupta, A Roy, A Nag. Continuous Authentication. Book Chapter in Advances in User Authentication, pp.235-279, Publisher: Springer-Verlag, August 2017.
- D Dasgupta, A Roy, A Nag. Adaptive Multi-factor Authentication. Book Chapter in Advances in User Authentication, pp.281-355, Publisher: Springer-Verlag, August 2017.
- D Dasgupta, A Roy, A Nag. Authentication Basics. Book Chapter in Advances in User Authentication, pp.1-36, Publisher: Springer-Verlag, August 2017.
- D Dasgupta, A Roy, A Nag. Negative Authentication Systems. Book Chapter in Advances in User Authentication, pp.85-145, Publisher: Springer-Verlag, August 2017.
- D Dasgupta, A Roy, A Nag. Multi-Factor Authentication. A Book Chapter in Advances in User Authentication, pp.185-233, Publisher: Springer-Verlag, August 2017.
- M. L. Das, B. Roy, D. Dasgupta. Privacy Preserving Proxy Re-encryption with Fine-grained Access Control. In proceeding of 13th International Conference on Information System Security, December 16-20, 2017
- Kul Prasad, Daya Ram Budhathok, Bo Chen, Dipankar Dasgupta. RDS3: Ransomware Defense Strategy by Using Stealthily Spare Space. In the proceedings of IEEE Symposium Series in Computational Intelligence, Dec. 2017.
- A Patent Application#14/968676: Adaptive Multi-Factor Authentication System, patent allowed on November 2017.

**Dr. Simon** worked with PhD students and faculty on research projects that were accepted for AMCIS Conferences in 2016 and 2017; written summaries are available at the AMCIS website. Titles:

- Yao, Shi, Ruby Booth, and Judith Simon. "The Iterative Effect of IT Identity on Employee Cybersecurity Compliance Behaviors."
- Ruby Booth, Sandra Richardson, and Judith Simon. "Security Risks Related to Employee "Extra-Role" Creation of an "Online-persona."

Since 2016, **Dr. Kan Yang** has worked collaboratively with other individuals to publish 3 Conference papers (2017), 13 Journal Papers (2016- 2017) and one books. His most recent book, "Privacy-preserving Data Access Control in the Smart Grid" was published in 2016[4].

A list of his 2017 publications include:

- Q. Xu, Z. Su, Q.Zhao, J. Song, W. Shen, Y. Wang and K. Yang. "QoE Loss Probability Based Game-Theoretic Approach for Spectrum Sharing in Heterogeneous Networks". In Proc. of International Conference on Communications (ICC'17), Paris, France, May, 2017.
- G. Xu, Y. Ren, H. Li, D. Liu, Y. Dai and K. Yang. "CryptMDB: A Practical Encrypted MongoDB over Big Data". In Proc. of International Conference on Communications (ICC'17), Paris, France, May, 2017.
- Z. Yang, K. Zheng, K. Yang and V. C.M. Leung. "A Blockchain-based Reputation System for Data Credibility Assessment in Vehicular Networks". In Proc. of IEEE PIMRC 2017 Special Session SP-05 on "5G Wireless Technologies for V2X Communications", Montreal, QC, Canada, October 8-13, 2017.
- P. Yang, N. Zhang, S. Zhang, K. Yang, L. Yu, and X. Shen. "Identifying the Most Valuable Workers in Fog-Assisted Spatial Crowdsourcing". IEEE Internet of Things Journal, Vol 4, Issue 5, pp. 1193-1203, 2017.
- Q. Xu, Z. Su, and K. Yang. "Optimal Control Theory Based Epidemic Information Spreading Scheme for Mobile Social Users with Energy Constraint". IEEE Access, Vol 5, pp. 14107-14118, 2017.
- G. Xu, H. Li, C. Tan, D. Liu, Y. Dai and K. Yang. "Achieving efficient and privacy-preserving truth discovery in crowd sensing systems". Computers & Security (Elsevier) , Vol 5, pp. 14107-14118, 2017.
- K. Yang, K. Zhang, X. Jia, A. M. Hasan, and X. Shen. "Privacy-Preserving Attribute-Keyword Based Publish-Subscribe Service on Cloud Platforms". Information Sciences(Elsevier) , Vol. 387, Pages 116–131, 2017.
- K. Zhang, J. Ni, K. Yang, X. Liang, and X. Shen. "Security and Privacy in Smart City Applications: Challenges and Solutions". IEEE Communications Magazine, Vol 55, Issue 1, pp. 122-129, 2017.

[4] More information about Dr. Kan Yang's publications can be found here: https://scholar.google.com/citations?user=QqGPbXYAAAAJ&hl=en&oi=ao

- X. Jin, N. Zhang, K. Yang, X. Shen, Z. Xu, C. Zhang, and Z. Jin. "PN Ranging Based on Noncommensurate Sampling: Zero-bias Mitigation Methods"IEEE Trans. on Aerospace and Electronic Systems, Vol 53, Issue 2, pp. 926-940, 2017.
- K. Yang, Q. Han, H. Li, K. Zheng, Z. Su, and X. Shen. "An Efficient and Fine-grained Big Data Access Control Scheme with Privacy-preserving Policy". IEEE Internet of Things Journal, Vol 4, Issue 2, pp. 536-571, 2017.

## B. Director & Co-Directors Activities

FY 2017 has been a busy year for the CfIA's Co-directors. Listed below is a list of their accomplishments during this fiscal year:

- Dr. Dasgupta gave a presentation at the Third annual Community College Cyber Summit (3CS) on July 22-24, 2016 in Pittsburgh.
- Dr. Dasgupta became Program Committee Member of the 1st IEEE International Workshop on Cyber Resiliency Economics (CRE 2016) at Vienna, Austria, August 1-3, 2016.
- Dr. Dasgupta attended the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining on August 15-18, 2016 at San Francisco, CA.
- Dr. Dasgupta attended the GenCyber Fall Meeting on September 15-16, 2016 at Hilton Boston Logan Airport hotel, Boston,MA.
- Dr. Dasgupta attended the Structure Security event on September 27-28, 2016 at San Francisco,CA.
- Dr. Simon served as an editor/reviewer of an extensive online course program on Risk Management in 2016 as part of a grant obtained by Dr. Dasgupta.
- Dr. Kan Yang was invited to serve as a TPC in the 2017 IEEE ICC'17 (Communication and Systems Security Symposium) in October 2016
- Dr. Dasgupta attended the Cyber Seed Competition on October 9-11, 2016 at UConn,CT.
- Dr. Dasgupta gave a presentation and demo at NSF-ATE Conference on October 26-28, 2016 at Washington,DC.
- Dr. Dasgupta attended the 7th Annual National Initiative for Cybersecurity Education (NICE) on November 1-2, 2016 at Kansas City, Mo.
- Dr. Dasgupta was invited to serve as Panelist at Department of Energy Office of Science for Panel Meeting on November 9-10, 2016 at Washington,DC.
- Dr. Dasgupta organized IEEE Symposium on Computational Intelligence in Cyber Security (CICS 2016) at Athens, Greece held from December 6-9, 2016.
- Dr. Dasgupta gave a presentation at DOE/ASCR invited workshop on Smart Networks on December 8-9, 2016 at Rockville,MD.

- Dr. Dasgupta gave an invited talk at CSA Dept (Computer Science & Automation) of Indian Institute of Science (IISc) Bangalore, India on Dec 15, 2016. (Host: Mr. K. Gopinath, Dept. Chair)
- Dr. Dasgupta gave an invited talk at the Indian Statistical Institute on December 16, 2016 at Bangalore,India.
- Dr. Dasgupta gave an invited talk at the Computer Science Dept. of Jadavpur University, Kolkata, West Bengal, India on Dec 22, 2016 (Host: Mr. Ujjwal Maulik)
- Dr. Dasgupta gave a keynote speech at the Seminar on Cyber Security at iLead | Institute of Leadership Entrepreneurship & Development, Kolkata, West Bengal, India on Dec 23, 2016. (Host: Mr. Pradip Chopra, iLEAD Chairman)
- Dr. Dasgupta gave a lecture at the Cyber Security Training at Nashville, TN on Jan 13, 2017.
- Dr. Dipankar Dasgupta was featured in an interview with Dr. David Fogel, former president of the IEEE Computational Intelligence Society and current co-general chair of IEEE SSCI 2017.
- Dr. Simon was a guest speaker at the BIT Colloquium on February 10, 2017. The topic of this colloquium was The Iterative Effect of IT Identity on Employee Compliance Behaviors.
- Dr. Dipankar Dasgupta gave a presentation to the TN Senate Education Committee on the University of Memphis Cyber Security Initiatives at Nashville, Feb 15, 2017.
- Dr. Dasgupta gave a talk on the A-MFA patent at IP Parade as the inventor at the Memphis Scipreneur Challenge at Memphis Bioworks, February 23, 2017.
- Dr. Dasgupta gave a Talk on Cyber security integration into PAL3 at a Navy Visit to Institute of Intelligent Systems (IIS) at FIT 405, February 27, 2017.
- Dr. Dasgupta co-hosted the CAST (Cluster to Advance Cyber Security and Testing) Lightning talk at FIT on February 28 at 5-7 pm.
- Article on the cyber security concentration at Study International second editorial launch - University of Memphis on March 3, 2017.
- Dr. Dipankar Dasgupta attended and gave a demo of PBL Project at ACM SIGCSE, Seattle, WA on March 8-11, 2017.
- Dr. Simon was selected in Spring 2017 to serve on the National CyberWatch Center Curriculum Standards Panel Board (NCC-CSP), which will involve several years of development.
- Dr. Simon supported the development of the Women in Cybersecurity (WiCyS) event from March 31-April 1, 2017.
- Dr. Simon served as a moderator for NCUR students visiting the University of Memphis on April 7, 2017.

- Dr. Simon gave a presentation on April 7, 2017, to the BIT Department Advisory Board regarding IoT (Internet of Things).
- Dr. Dasgupta gave an invited talk at the Summer School on Cyber Physical Systems at the Dhirubhai Ambani Institute of Information and Communication Technology (DA-IICT) Gandhinagar, Gujarat, India on April 10, 2017.
- Dr. Dasgupta gave an ACM Distinguished Speaker Talk on An Adaptive Multi-Factor Authentication (A-MFA) Methodology at the Computer Science and Engineering Department of IIT Gandhinagar, India on April 11, 2017.
- Dr. Dasgupta gave an invited talk on Internet Safety and Privacy at the Tigers Tech Expedition Camp for Middle School Students on April 22, 2017.
- Dr. Simon developed, administered, and graded PhD examinations for two students completing the program in April 2017.
- Dr. Dasgupta gave an invited talk on Cyber Security initiatives at the University of Memphis Brief at The 2017 Cybersecurity Conference on June 6, 2017 at the Cook Convention Center, Memphis, TN.
- Dr. Dasgupta attended the National Cyber Security Summit (NCS) on 07-08 June 2017, Huntsville, AL.
- Dr. Dasgupta organized and hosted two week-long GenCyber Bootcamps (for Middle and High School students) at the University of Memphis during June 11-16 and June 19-23, 2017 respectively.
- Dr. Dasgupta attended the National Cyber Preparedness Consortium (NCPC) core members meeting at Washington DC on June 19, 2017.
- Dr. Dasgupta gave an invited talk on Adaptive Multi-Factor System at the Applied Cyber Security Seminar, at Massachusetts Institute of Technology (MIT) on June 20, 2017.
- Dr. Kan Yang was invited to serve as a TPC in the 10$^{th}$ IEEE International Conference on Cyber, Physical and Social Computing (CPSCom'17), Exeter, England, UK, 21-23 June 2017.
- Dr. Kan Yang was invited to serve as a TPC in the 10$^{th}$ IEEE Globecom'17 (Communication and Information Systems Security Symposium)
- Dr. Kan Yang was invited to be a guest speaker for CityU-CS Research Student Workshop to be held from June 21-23, 2017 in Hong Kong
- Dr. Kan Yang was invited to serve as a TPC in the IEEE ICC'18 (Communication and Information Systems Security Symposium)
- Dr. Dasgupta offered a session on Online Social Networks and Privacy issues for School Students at the Lausanne Summer Conference organized for teachers for Middle School STEM program under Engaging Students in Technology Enhanced Project-Based Learning LLI 17 1:1 NEXT CONFERENCE at Memphis, TN on July 17, 2017 (Host: Dr. Stephanie S. Ivy).

## C. Grant-Funded Projects

The Center continues to be actively involved in IA-related projects, and has received federal funding to support multiple projects and initiatives. Collaboratively, they are working on external grants that total over $2.3 million, and are listed as follows (Received by Prof. Dasgupta as PI):

| Grant Name | Collaborators | Funding Agency | Amount | Date Range |
|---|---|---|---|---|
| Adaptive Cybersecurity Training (ACT) Online | University of Texas, San Antonio | FEMA | $207,000 (Multi-University Grant of $800,000) | 10/1/13-1/31/18 |
| Puzzle-Based Cyber Security Learning | Jackson State University | NSF | $364,864 | 6/1/14-5/31/18 |
| Cyber Security Competitive Training Grant | Norwich University | Lead: NU Prime: DHS/FEMA II | $325,000 (Multi-University Grant of $2.3 million) | 10/1/14-9/30/18 |
| CAST Funding | FedEx Institute of Technology | UM Foundation/FIT | $40,000 | 11/1/15-12/31/17 |
| Mobile Device Security and Privacy | University of Arkansas Little Rock | Lead: UALR Prime: DHS/FEMA III | $473,218 (Multi-University Grant of $3 million) | 1/15/16-12/31/18 |
| GenCyber Summer Camps | | NSA | $174,359 | 3/1/16-4/30/18 |
| Cyber Identity and Authentication | University of Texas, San Antonio | Lead: Univ. of Texas Prime: DHS/FEMA IV | $503,104 | 11/1/16-10/30/19 |
| CAE Cyber Security Workforce Development | | NSA | $206,085 | 9/1/17-8/31/18 |
| Preparing for Next Generation Cyber Defense Workforce | Norwich University | FEMA/DHS | $400,000 | 9/2017-8/30/20 |

### Adaptive Cybersecurity Training (ACT) Online

The Adaptive Cyber-security Training (ACT) project is in collaboration with Vanderbilt University and Sparta Corporation and is involved in the development and delivery of a multi-level, multi-track cyber security training curriculum. It uses state-of-the-art online learning technology and employs a dynamic, interactive, scenario-based problem solving environment. The goal of the project is to train a large number of Computer Users, IT professionals, First responders and defenders on various information assurance tools, techniques and best practices so that they can reduce threats and vulnerabilities and protect our national information infrastructure. Several ACT Online courses are available and all nine courses will be available soon. For more information visit the web site: https://www.act-online.net

### Puzzle-Based Cyber Security Learning

The goal of this project is to improve the effectiveness of cyber security education through puzzle-based learning (PBL), expanding student knowledge and problem solving skills through the stimulation of their cognitive abilities. PBL has already proven effective in many STEM learning environments including mathematics, physics, and computer science as an interesting and effective way of learning complex logic and abstract concepts. Cyber security has increasingly become important due to the escalating sophistication and frequency of online attacks, as well as the consequences of these attacks for various organizations and their infrastructures. This PBL project utilizes various approaches (simulations, interactive graphics, games, etc.) to improve defensive skills that will not only teach students how to protect specific systems, but also how to protect entire classes of systems that provide similar services, but with differing hardware/software components and architectures.

### Cyber Security Competitive Training Grant

In partnership with the Norwich University Applied Research Institutes (NUARI), Criminal Justice Institute of the University of Arkansas System, the Texas A&M Engineering Extension Service, and the Center for Infrastructure Assurance & Security at the University of Texas at San Antonio, the CfIA plans to develop cybersecurity training materials over the course of this grant.[5]

### DHS/FEMA Funded Cyber Security Training Programs

For 2017, the Center was able to develop research-based extensive online cyber security training programs in multiple tracks through their Adaptive Cyber-Security Training (ACT) Online website. The following courses were offered through this platform: Understanding Social Engineering Attacks (USEA) and Mobile Device Security & Privacy (MSP). They are currently working on the development of another web course entitled Cyber Identity and Authentication (CIAA).

[5]More information about this grant can be found at: http://oc.norwich.edu/blog/norwich-university-wins-2-3m-fema-cybersecurity-grant/

## Mobile Device Security and Privacy

The Federal Emergency Management Agency (FEMA) awarded a 2015 Continuing Training Grant of $3 million for cyber security training to the National Cybersecurity Preparedness Consortium (NCPC). The project is led by the University of Arkansas Criminal Justice Institute; the Center for Information Assurance (CfIA) has collaborated on the project as a core member of the consortium.

This Homeland Security National Training Program (HSNTP) will provide FEMA-certified training to first responders, emergency managers, technical specialists, and local government and community leaders, preparing them for all types of cyber emergencies.

The University of Memphis is at the forefront of information security research, education, and outreach in the region, according to Dr. Dipankar Dasgupta, founding director of CfIA, which is a National Center for Academic Excellence in Information Assurance. "The center will receive $474,000 from the consortium, and though this grant we will be developing an online training course on mobile device security and privacy issues. The course will make it safer for everyone browsing the Internet," he said.

The 36-month program focuses on four areas: cyber security, hazardous materials, countering violent extremism and rural preparedness. Rural preparedness includes school-based incidents, mass fatality planning and response, the development of emergency operation plans, rail car safety, media engagement strategies for first responders, agro-terrorism, food and animal safety, and hazardous materials.

## Cyber Identity and Authentication

The Center for Information Assurance (CfIA) at the University of Memphis will share a $3 million grant from the Department of Homeland Security and Federal Emergency Management Association with four other universities.

On Sept. 23, 2016, the DHS/FEMA awarded a Cyber Security Grant (CTG) to the National Cybersecurity Preparedness Consortium (NCPC), in which CfIA is a core member. The other partner universities are the University of Texas at San Antonio (UTSA), Texas A&M University, Norwich University (Vermont) and the University of Arkansas.

Administered by FEMA, the CTG is a competitive grant awarded annually to entities that play an important role in the implementation of the National Preparedness System by supporting the building, sustainment and delivery of core capabilities essential to achieving the national preparedness goal of a secure and resilient nation. FEMA provides the funding via cooperative agreements to partners like UTSA to develop and deliver training to prepare communities to prevent, protect against, mitigate, respond to, and recover from acts of terrorism and natural, man-made and technological hazards.

This collaborative project will be led by UTSA; CfIA will receive a sub-award of $503,000 for three years to develop research based best practices for cyber identity and authentication. The project will deliver a unique and innovative approach with "tabletop" scenarios supplementing online training to demonstrate participants' knowledge and skill sets to protect and defend systems with different authentication tools and techniques. The online training will assist state and federal jurisdictions with coordination and management of response efforts between emergency response organizations and critical infrastructure IT personnel necessary to prevent cyber incidents.

On May 16, the U.S. House of Representatives passed Rep. Joaquin Castro's bill that was inspired by National Cybersecurity Preparedness Consortium, The National Cybersecurity Preparedness Consortium Act (H.R. 4743), which allows nonprofits, including universities, to work more closely[1] with DHS to address cyber security risks and incidents at the state and local level. Earlier this month, Sen. John Cornyn introduced companion legislation for consideration in the U.S. Senate.

Dr. Dipankar Dasgupta, CfIA director, said, "Because of the center's multi-faceted activities, the University of Memphis is at the forefront of the research, education and outreach on cyber security in the region, and has continually maintained its designation as a National Center for Academic Excellence in Information Assurance/Cyber Defense Education (CAE-CD) and in Research (CAE-R) by the National Security Agency and the Department of Homeland Security."

## D. Presentation/Talks

### a. Events

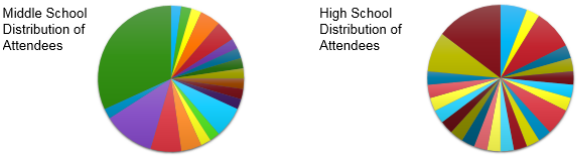
#### i. GenCyber Summer Bootcamp

The University of Memphis hosted two, one week, GenCyber summer camps for middle and high school students in 2017. The Middle school camp was hosted June 12th through June 16th and the High school camp was hosted from June 19th through June 23rd. Our theme for the camp was Cybersecurity Awareness with the objective of introducing the GenCyber 1st principles to students who had little or no knowledge about the concepts. Our target audience was from the middle and high school student population in Shelby County. Since Shelby County is served by one large county school system (approximately 116,000 students) and six small city districts, it provided the best opportunity to reach out to the economically disadvantaged students.

Our GenCyber 2016 camp survey indicated that 44% of the participants were new to cybersecurity and an additional 30% may have had some knowledge. GenCyber 2016 proved to be successful in piquing the interest of the participants, as approximately 65% stated they enjoyed learning about cybersecurity. The enrollment goal for the two 2017 summer camps was a 50/50 ratio of males to females and a minimum of 65% non-white students, with at least 90% of those students representing under-represented groups such

as African American and Hispanic/Latino students. Target enrollment for each camp was 50 students with an increase in student workers. The chart below showcases the number of students as of the last day of camp.

| | Middle School Camp | High School Camp |
|---|---|---|
| Attendees/ Available Spaces | 45 / 50 | 35 / 50 |
| Returning from 2016 Camps | 8 | 7 |
| Number of Unique Schools | 20 | 24 |




Our scope for the 2017 GenCyber camp was two-fold; we wanted to introduce students to the world of cybersecurity and include an outreach component that will allow the sustainability of the GenCyber program at the University of Memphis. Since the curriculum proved to be a success from the previous year, it was not changed significantly. Our GenCyber camp was designed to introduce or expand the student's knowledge of cybersecurity and help students gain practical programming skills. The learning objectives and outcomes were aligned to Computer Science Standards for Cybersecurity. Our learning activities were learner-centered with a focus on personal information security, password effectiveness, encryption, and fingerprint scanning.

The outreach component included face-to-face contact with school administrators, parents, civic organizations and the establishment of an advisory board. Each camp incorporated lesson plans and activities that brought awareness to the GenCyber 1st principles. Various games, activities and lessons were designed with these principles as a central theme.

The following steps were considered during the planning stage of this camp:

1. After reviewing the comments from 2016 participants and evaluators, we thought that it was important to add some time for group activities to allow the participants more time to get their project completed. There also seemed to have been some downtime that contributed to some classroom management issues. The changes we made to address this issue involved having more activities available so that we could keep students engaged in between the planned lessons. This change was successful for us because it included both inside and outside activities that were designed to just have fun. However, it did not solve

classroom management issues with the middle school campers because we still had visible challenges. Classroom management was not stated as an issue for the 2016 high school camp and it certainly was not an issue with the 2017 high school campers.

2. The other changes we proposed involved adding additional staff to assist with the participants. Our reason for adding more staff was due to the previous year's report that indicated that there was not enough staff to help out with the different activities. Also, in discussion with past camp staff the problem was the lack of staff. We were able to do what we envisioned with the additional staff. The goal was to have dedicated leaders that would be over teams. We also reached out to LeMoyne-Owen College for Cybersecurity students that could assist with activities and managing the students. One of the students had previous experience working with middle school students and was instrumental in providing guidance in the training.

3. We also proposed to be more proactive in our recruitment of students. Our goal was to contact school administrators and community groups to get student referrals. Our staff started early in contacting schools and civic organizers to talk about the GenCyber program. This was a great success for us. We were able to start an e-mail campaign to schools and organization within a 20 mile radius. This resulted in face to face interviews that allowed us to discuss the program with School administrators. This also paved the way for a relationship with the schools indicated in the image below. These schools do not have cybersecurity programs or activities and want to use the University of Memphis as an educational resource to get programs started.


4. We established GenCyber Advisory Board that consisted of 8 members. The board is comprised of secondary educators, entrepreneurs, administrators and UM staff.

| Members | Affiliation |
|---|---|
| Dr. Denise Ferebee | Director of the Center for Cyber Defense, Assistant Professor of Computer Science at Lemoyne-Owen College |
| Erica Boyce | Administrative Associate II at the School of Public Health at the University of Memphis |
| Iris Myers | Science and Social Studies Teacher at Peabody Elementary |
| Karen Bell | System Analyst of Information Technology Services at the University of Memphis |
| Meka Egwuekwe | Executive Director of CodeCrew |
| Pamela Mashburn | Retired MidSouth Math teacher |
| Sonya L. Boyce | Science Lab Teacher at Springdale & Vollentine Elementary, STEM Fellow 2016 |
| Tiffany Sanders Jones | Board member for Memphis Academy of Science & Engineering and member of the Shelby County Headstart Pre-K Advisory Committee |

The purpose of the GenCyber board was to assist us with coming up with ideas that we could use to make the GenCyber experience great for everyone. Having a board with a diverse background of experience was instrumental in providing us with leaders, innovative ideas, disciplinary knowledge and best practices. We were able to have 2 meetings prior to the start of the 1st GenCyber camp. These meetings yielded ideas that helped improve the GenCyber experience.

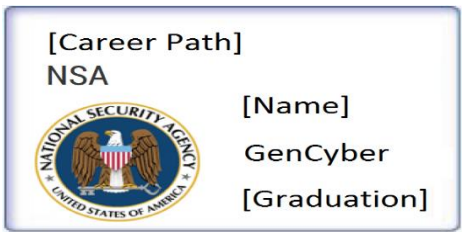
The Advisory Board was also invited to attend the camp at different times. One of our board members was a presenter at our camp. They also participated in the closing ceremonies.

**Changes from 2016**

Earlier in the year, we were invited to talk about GenCyber at an event sponsored by a College Readiness program entitled Empowering Students Universally, Scholars Inc. (ESU Scholars) by Dr. Jada Meeks. She asked if she could speak to our GenCyber High School group. We also added a college fair to our camp, where U of M students provided discussion on programs offered in Cybersecurity. Our graduate students displayed interactive projects that allowed the students to be engaged. Dr. Jada Meeks was added as a Presenter and she also participated in the college fair. LeMoyne-Owen College and other Computer Science programs were invited. Parents were invited to attend the college fair and Dr. Meeks presentation. This addition will be something that we want to continue in future camps for high school students. It was a success because it links the GenCyber and the Center for Information Assurance (CfIA) goals to increase interest in cybersecurity education, careers and diversity in the cybersecurity workforce.

We added a new process to the NSA for A Day activity. We wanted the campers to leave with the thought that they are a Cybersecurity professional. So, based on the outcome of their online journey, we created Identification Cards with their name and specializations. It was added to the Certificate of Completion. As each child's name was called during our closing ceremony, we addressed them by their specialization.

The template for the NSA for a Day card can be seen below:




**Program Outcomes**

Both Camps Learning Outcome:

1. GenCyber 1st First (10) Principles- Introduced in Opening Sessions and reinforced through demonstrations, challenge and activities.
    - Middle School
        - Jeopardy Game
        - Card Game
        - Passport Completion Challenge
        - Crossword Activity
        - Kahoot Activity
    - High School
        - Kahoot Activity
        - Virtual Scavenger Hunt
        - Ransomware Demonstration
        - Crossword Activity
        - Cryptogram Challenge
2. Simple Encryption – Introduced and Reinforced in Online Security Demo & Practice.
    - High School
        - Caesar Cipher Lesson - they were given the cipher wheel. The learning outcome was demonstrated in the Online Security Game.
3. Online Privacy, Security, and Safe Browsing – Introduced steps to identify and create a secure password.
    - Both Camps demonstrated learning with
        - Puzzle activity
        - Passport Book
4. Java Script programming – Introduced & executed in Final Projects

- Middle School
  - Scratch App
- High School
  - Greenfoot

Each of the learning outcomes described above were hands-on activities. To add an element of fun to these activities, we made them competitions. We believed healthy competition would inspire them to do their best. We had both individual and group competitions. It was evident when the students knew they were competing; they became more inquisitive and worked together. The evidence we have of this are the finished projects that were reviewed by an Expert Panel. Awards were given accordingly. The project that the campers made the decision on what they wanted to feature in their final projects. Projects from both camps used elements they had previously learned during the camp sessions. Here are a few of the topics covered:

- Hacking
- Password Security
- Cyber Bullying

After the camp ended, one student stated that they have already used the knowledge gained from our GenCyber camp to mentor other youths in a science camp that they are teaching this summer.

Our recruitment efforts for middle and high school camp have created interest in the field. This has opened an opportunity for the University of Memphis to partner with Manassas High School in creating a 4 year Cybersecurity Curriculum track.

We hosted a 4-hour workshop on August 3, 2017 that was entitled “Cyber Safety Professional Development Workshop for Teachers”. It was designed to provide local teachers with basic fundamental knowledge of Cyber Security principles.

**Reflections**

The Final projects for both of our groups were phenomenal. The process of getting them there from beginning to end was filled with numerous activities. We had them form two different groups and they identified well with the idea of having a main group and a project group. We introduced different activities to create or jump-start the project development process. The campers formed a bond and produced a quality projects that they were all proud to present.

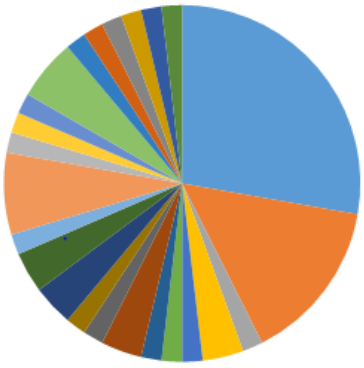
We learned that it’s going to take a village. It is going to take collaboration, communication and the joining of forces among parents, teachers and the student community. There is noticeable gap between what we are able to do in a week and what the children need to continue on this path of learning. It is a great opportunity to build a

Cybersecurity community. It is going to take educators, parents and professionals working together to prepare our children for this specialization.

It would be ideal to offer the GenCyber program to everyone who applies. However, if we host another camp, we will limit the number of applicants to 20-25 motivated students. Our goal, as well as GenCyber's goal, is to increase interest in the cyber security field, so we want to be able to do that in an environment conducive to learning and mentoring. Which is why we would like to make sure that our next camp is more hands-on and project driven. We also want to consider offering a camp for beginners and a camp for more advanced students. The advanced camp will require a vetting process to determine the level of skill.

**Summary Report**

The Center for Information Assurance (CfIA) successfully hosted its annual GenCyber Boot Camps for two consecutive weeks during the month of June. More than 80 Middle and High school students, from different places, came to the University of Memphis to learn more about cyber safety and best practices. The chart below shows that campers came from 24 different schools (indicated by different colors) across the mid-south region (with a few coming from other parts of the country). The highest number of middle school applicants came from White Station, and the second highest number came from Schilling Farms.



Relative Distribution of Participant Schools

Each camp officially started with a welcome from the Dean of Arts & Sciences, Dr. Thomas J. Nenon. The week-long camp was divided into multiple sessions that allowed students to be engaged in activities that included digital fingerprinting, online safety, privacy and more! The main theme of the camp, however, centered on the Cyber Security First Principles. These principles were illustrated with real-world examples by security experts. This rigorous training also had week-long group projects where the students were tasked with developing cyber security related stories/games. Each group presented their projects to a panel of industry professionals on the last day of the camp. The

campers also toured different campus facilities including Data Center, University Library and FedEx Institute of Technology while they attended the camp. The security professionals who shared their experiences with the campers included Ms. Karen Bell (U of M Systems Analyst), Dr. Dipankar Dasgupta (CfIA Director and GenCyber Program Director), Mr. Tim Marsh (FBI Agent), Dr. Lan Wang (Computer Science Department Chair), Mr. Meka Egwuekwe (CodeCrew Director), and Mr. James Cotter (Department of TN Homeland Security). The Director of ESU Scholars, Dr. Jada Meeks, also spoke to the High School campers on the importance of early preparation for college. The University of Memphis provost, Dr. Karen Weddle-West, addressed the audience at the closing ceremony on June 23rd. She also participated in a panel discussion and highlighted the important role that the University is playing in the region.

The two weeks of GenCyber were filled with education and fun. When asked about their experience, one of the campers, Walter Valentine, had this to say "I actually enjoyed the camp, it was very interesting." Another student, Maddie Dowd, had this to say: "I thoroughly enjoyed my experience with the instructors and other students; I found everyone very welcoming. I have already used my new-found knowledge at a volunteer youth science camp at which I am teaching this summer." Her mother, Dawn Decker, shared similar sentiments "The Gen Cyber camp is a treasure for students. A wonderful experience in a critical field for all of our futures."


**Additional Information**

More information about our camp can be found here.

The following links can be used for Individual Information

- Parent Orientation Summary

**Middle School GenCyber Boot Camp**

- Event video
- Some activities from June 12-16 Middle School Camp
- Middle School Awards

**High School GenCyber Boot Camp**

- Event video
- Some activities from June 19-23 High School Camp
- High School Awards

**GenCyber Personnel**

**Staff**

- Dr. Dipankar Dasgupta, Program Director
- Kriangsiri "Top" Malasri, Lead Instructor
- Carolyn Treadwell-Butler, Project Coordinator
- Kelly Freeman, Project Assistant
- Karen Bell, Systems Analyst
- Kendra Tillis, Business Officer
- Lyndsey Rush, Administrative Secretary

**Student Assistants**

- Anika Boyce
- Cletus Hatten
- Meg Homeyer
- Trakeisha Millbrook
- Terrika Muhammad
- Shashwat Patra
- Taylun Smith
- Rhythm Syed

**Student Volunteers:** Robert Edstrom, McKittrick Swindle, Irfan Rahman, Berkeley Willis, Ayushi Mehta, Raasi Manasa Annavajjala, Subash Poudyal, Peyton Warren, John Shrein, Daya Ram Budhathoki, Vamsi Krishna Polam

## Middle School Agenda

### Monday, June 12

| Time Slot | Activities |
|---|---|
| 8:30-9:15 | Breakfast/Registration – FIT Lobby |
| 9:15 -9:30 | Pre-survey –DH 118 (Online) |
| 9:30-9:45 | Welcome by the A & S Dean, U of M |
| 9:45-11:15 | Icebreaker<br>Cyber Security First Principles<br>Lab activity: Image EXIF Forensics |
| 11: 15-11: 30 | Break |
| 11:30-12:00 | Cyber Code of Conduct & University Network Access Policy (Guest Speaker) |
| 12:00-1:30 | Lunch (Team Naming Ceremony to take place afterward) |
| 1:30-2:30 | Online Privacy, Security, and Safe Browsing (Guest Speaker) |
| 2:30-2:45 | Break |
| 2:45-4:15 | Why Is a Strong Password Needed? (Lecture/Lab) |
| 4:15-4:30 | Debrief |

### Tuesday, June 13

| | |
|---|---|
| 8:30-9:30 | Breakfast – Psychology Auditorium Lobby |
| 9:30-11:00 | Cyber Security First Principles<br>Lab activity: Fingerprinting |
| 11:00-11:15 | Break |
| 11:15-12:00 | Introduce Group Project |

| | |
|---|---|
| | Distribute project instruction sheets |
| 12:00-1:30 | Lunch |
| 1:30-2:30 | NSA Day of Cyber: Session 1/Card Game |
| 2:30-2:45 | Break |
| 2:45-3:30 | Guest Speaker |
| 3:30-4:15 | Campus Tour: U of M Data Center |
| 4:15-4:30 | Debrief |

**Wednesday, June 14**

| | |
|---|---|
| 8:30-9:00 | Breakfast – Psychology Auditorium Lobby |
| 9:00-9:30 | NSA Day of Cyber: Session 2 |
| 9:30-11:00 | Cyber Security First Principles<br>Lab activity: Jeopardy Game |
| 11:00-11:15 | Break |
| 11:15-12:00 | Online Security Game Demo |
| 12:00-1:30 | Lunch |
| 1:30-2:30 | Card Game/NSA Day of Cyber: Session 1 |
| 2:30-2:45 | Break |
| 2:45-3:30 | Continue Project Activities |
| 3:30-4:15 | Campus Tour: FedEx Institute of Technology (FIT) |
| 4:15-4:30 | Debrief |

**Thursday, June 15**

| | |
|---|---|
| 8:30-9:00 | Breakfast – Psychology Auditorium Lobby |
| 9:00-9:30 | NSA Day of Cyber: Session 2 |

| | |
|---|---|
| 9:30-11:00 | Lab Activities:<br>Review of Cyber Security First Principles (Lab) – use of Kahoot<br>(Break as necessary) |
| 11:00-12:00 | Tallest Standing Structure contest |
| 12:00-1:30 | Lunch |
| 1:30-4:15 | Team project work<br>Breaks as needed |
| 4:15-4:30 | Debrief (Meeting to Discuss HS Activities) |

**Friday, June 16**

| | |
|---|---|
| 8:30-9:30 | Breakfast – Psychology Auditorium Lobby |
| 9:30-11:00 | Complete team projects, prepare presentations |
| 11:00-11:15 | GenCyber Bootcamp Post-survey (Online) |
| 11:15-11:30 | Break |
| 11:30-12:00 | Importance of Computer Science & Cyber Education (Guest Speaker) |
| 12:00-1:30 | Lunch |
| 1:30-2:30 | Campus Tour: McWherter Library |
| 2:30-2:45 | Break |
| 2:45-4:00 | Team Project Presentations (parents are welcome) – Psychology Auditorium |
| 4:00-4:30 | Award Ceremony and Closing –Psychology Auditorium |

## High School Agenda

**Monday, June 19**

| **Times** | **Activities** |
|---|---|

| | |
|---|---|
| 8:30-9:00 | Breakfast/Registration – FIT Lobby |
| 9:00 -9:15 | Welcome by the Dean Arts & Sciences-DH 118 |
| 9:15-9:45 | Address by the Chair Computer Science, U of M |
| 9:45-10:00 | Pre-Survey—DH 118 (Online) |
| 10:00-10:15 | Icebreaker |
| 10:15-11:00 | Cyber Security First Principles<br>Lab activity: Image EXIF Forensics |
| 11:00-11:15 | Break |
| 11:15-11:45 | Cyber Code of Conduct & University Network Access Policy (Guest Speaker) |
| 12:00-1:30 | Lunch |
| 1:30-2:30 | Code Crew Programming Initiatives (Guest Speaker) |
| 2:30-2:45 | Break |
| 2:45-4:15 | Why Is a Strong Password Needed? |
| 4:15-4:30 | Reminder: All Students need to bring earphones for PC computer. |

**Tuesday, June 20**

| | |
|---|---|
| 8:30-9:30 | Sign In-FedEx Institute of Technology/Breakfast-Psychology Auditorium Lobby |
| 9:30-11:00 | Cyber Security First Principles<br>Lab activity: Fingerprinting / Possibly encryption and programming as well |
| 11:00-11:15 | Break |
| 11:15-12:00 | Introduce Group Project<br>Distribute project instruction sheets |
| 12:00-1:30 | Lunch |
| 1:30-2:30 | NSA Day of Cyber: Session 1 |

| | |
|---|---|
| 2:30-2:45 | Break |
| 2:45-3:30 | Securing the National Cyberspace - Guest Speaker |
| 3:30-4:15 | Campus Tour: U of M Data Center |
| 4:15-4:30 | Debrief |

**Wednesday, June 21**

| | |
|---|---|
| 8:30-9:30 | Sign In-FedEx Institute of Technology/Breakfast-Psychology Auditorium Lobby |
| 9:30-11:00 | Cyber Security First Principles<br>Team project work |
| 11:00-11:15 | Break |
| 11:15-12:00 | Virtual Scavenger Hunt |
| 12:00-1:30 | Lunch |
| 1:30-2:30 | NSA Day of Cyber: Session 2 |
| 2:30-2:45 | Break |
| 2:45-3:45 | Online Privacy, Security, and Safe Browsing (Guest Speaker) |
| 3:45-4:15 | Campus Tour: FedEx Institute of Technology (FIT) |
| 4:15-4:30 | Debrief |

**Thursday, June 22**

| | |
|---|---|
| 8:30-9:30 | Sign In-FedEx Institute of Technology/Breakfast-Psychology Auditorium Lobby |
| 9:30-12:00 | Team project work<br>Breaks as needed |
| 12:00-1:30 | Lunch |
| 1:30-2:30 | Online Security Game Demo |

| | |
|---|---|
| | Ransomware Demonstration |
| 2:30-3:30 | Forensic Exercises |
| 3:30-3:45 | Break |
| 3:45-4:30 | Web form validation exercises<br>Multi-factor authentication demo<br>Cryptogram Challenge |
| 4:15-4:30 | Debrief |

**Friday, June 23**

| | |
|---|---|
| 8:30-9:30 | Sign In-FedEx Institute of Technology/Breakfast-Psychology Auditorium Lobby |
| 9:30-11:00 | Complete team projects, prepare presentations |
| 11:00-11:15 | Post-survey (Online) |
| 11:15-11:30 | Break |
| 11:30-12:00 | Security Analysis (Guest Speaker) |
| 12:00-1:30 | Lunch |
| 1:30-2:00 | Cyber Security College Fair-FIT Lobby |
| 2:00-2:30 | College Readiness-Empowering Students Universally Scholars, Inc. – FIT The Zone. |
| 2:30 – 2:45 | Break |
| 2:45-3:00 | Address by the Provost, U of M – FIT The Zone |
| 3:00-4:30 | Team Project Presentations (parents are welcome) – FIT The Zone |
| 4:30-5:00 | Award Ceremony and Closing – FIT The Zone |

**Downtime Activities**

- **GenCyber Passport Booklet**

  Students are encouraged to complete the puzzles inside of the GenCyber Passport Booklet (a booklet that was originally designed by Dakota State University).

- **Team Naming Ceremony**

  Students will work together to create a name that represents their team. They will decorate a poster that will represent themselves and showcase it at our closing ceremony.

- **Cybermon GO!**

  5 teams will embark on a challenge to find "Cybermon". In order to find these Cybermon, the students will need to solve multiple riddles. Some of these riddles involve Caesar Cipher, while others are pictorial. Each team will have their own locations and riddles. The teaching assistants/student workers will have all the answers to the activities, and verify whether or not the students have correctly solved all the riddles.

- **Graphite Activity**

  Students will draw a picture using a Number 2 pencil, then use a 9 Volt Battery to cause a LED light to light up.

- **Magnetic Slime**

  Students will create magnetic slime. They will use liquid starch, elmer's glue, Iron Oxide powder, disposable bowls and neodymium magnets.

- **Binary Code Jewelry**

  Students will use an ASCII chart to create binary code jewelry. One color will represent 1 and another color will represent 0. A third color will represent the spaces

- **Secret Code Number Cipher**

  This Activity teaches them the basic level of cryptography, which is also an aspect of cybersecurity. Will potentially utilize the following types of ciphers:

  - Atbash Cipher (reversed alphabet)
  - Polybius Square (translate letters into numbers)
  - Rail Fence Cipher (Rails of an imaginary fence)

- **Hula Hoop Activity**

  Students stand in a large circle while holding hands. The Hula Hoop is held by two students, and then transferred around the circle without breaking the circle. This is a team building activity

- **GenCyber MadLibs**

  Teaching assistants have created scenarios, with blank spaces involved, so that the students can fill in the blank. Usually, these result in humorous stories once the students have added all the requested words.

- **Crafting**

  Students will use Pipe Cleaners to construct multiple items. They will either engage in a tower building contest or create little figures.

- **Coding Games (dependent on the coding level of students)**

  Students will play the following coding games in their free time (suggested for beginner level coders):

  - Play Code Monkey Game
    - This website is made for beginner level coders. The purpose of this game is to creatively drill students on coding.

  - Code Combat
    - This game is set up like the scratch coding site

  - Lightbot
    - It is a game where children can solve puzzles using programming logic. Lightbot is fun and it allows children to learning basic and complex principles of programming in a fun and interactive way. It allows children to learn loops, if-then statements and etc., all without coding.

  Students will play the following coding games in their free time (suggested for advanced level coders):

  - Coding Game

- This website is pure coding. The user can choose which language to code in to complete the game. This game is an outer space meteor mission that requires that the user shoot all of the meteors.

- Untrusted
  - This coding game engages the student into using code to break the "@" out of a maze. The code being used is java. The game also gives hints on how to solve it. There are many levels to this game.

### ii. Cyber Security Summit

The Center for Information Assurance (CfIA) successfully hosted its 10th annual Cybersecurity Summit on October 12, 2017 at the FedEx Institute of Technology on the University of Memphis campus. Dr. Dipankar Dasgupta and Dr. Judith Simon, Co-Directors and Dr. Kan Yang, the Associate Director of the Center, were involved in hosting of this year's summit and welcomed professionals from multiple areas in the Cybersecurity industry and students.

The Summit started with a presentation from Thomas Davis, who is the Director of Information Security, Compliance and Risk at ServiceMaster. He emphasized the importance of having security built in from the start of any project. Both servers and code age poorly, so frequent testing becomes more important as time passes. Davis concluded his presentation with a discussion of tools that both organizations and average users can utilize to help find compromises in their systems.

The next presenter was the CfIA's own Co-Director, Dr. Judy Simon who has been associated with the center since its formation in 2004. Recently, Dr. Simon received the high honor of being selected as a member of the National CyberWatch Center's Curriculum Standards Panel (NCC-CSP). According to Dr. Simon, this panel will identify the learning objectives, concepts, procedures, situational judgments and intellectual abilities needed to develop capability and maturity in cybersecurity foundation principles and protocols. There are two different models for education: Outcome-Based and Competency-Based. Outcome-Based education focuses on the results, while Competency-Based focuses on a student's rate of improvement. The panel has determined that the Outcome-Based method is a better fit for this wide-ranging curriculum proposal. After determining which of these two educational models is most effective, this panel hopes to develop a new model so that they can provide continuing education for IT professionals and develop/provide 2 and 4-year programs.

After a networking break, the attendees then listened to a presentation from Bob Sydow, who is the Principal and Americas Cybersecurity Leader of Ernst & Young in Cincinnati, Ohio. After graduating from the University of Memphis in 1981, he has since become a leader in the Americas division of the global company Ernst & Young, which includes over 2000 people in North and South America. Sydow's presentation focused on Cyber Economics, which is a data-driven experience that looks at the open

source data that is available in addition to risk analysis to understand the economic impact of cyber threats. With Cyber Economics, it is important to understand *how, who and why* someone is targeting you. Understanding these three items will help a business understand how to better implement additional controls and where to target their spending. At the end of his presentation, he stressed the importance of training more individuals in analytics and information, since the future of cybersecurity cannot be sustained with just coders and programmers.


Pictured (l-r): Bob Sydow, Dr. Judith Simon

After lunch, Steve Crocker, the Director of Information Security & Information Security Officer at Methodist LeBonheur Healthcare, gave a presentation on the current state of cybersecurity in the Healthcare field. Prior to working with Methodist LeBonheur Healthcare, Crocker was the CIO for Magna Bank for 14 years. During his presentation, Crocker emphasized the importance of healthcare industries doing more to improve their security. Weak security, combined with the value of the data that is stored in healthcare establishments, makes this field a relatively large target for cyber criminals. Crocker stated that he believed that a combination of the focus on compliance (as opposed to risk) and the lack of quick action with regard to government regulation led to the current state of cybersecurity in the healthcare field. To improve cybersecurity, he emphasized the importance of changing the process for mitigating cyber attacks, documenting everything, updating systems, and segmenting the network. He concluded his presentation with a prediction that healthcare will continue to be a massive target, but that he believed that it was possible for the field to eventually be a leader in cybersecurity innovation.

The next speaker was Ron Cundiff, who is a manager at Vanick, a software development and integration solutions company. Cundiff has 23 years of experience in IT and has worked in multiple positions. In his presentation, Cundiff focused on the importance of increasing security awareness. During a cyber attack, people can be considered the

weakest link. 81% of breaches are due to stolen and/or weak passwords, and 1 in 14 people fall victim to phishing attacks. These statistics, combined with the fact that attackers are becoming more advanced, are reasons why it is important for people to become more aware. Towards the end of his presentation, Cundiff suggested the following tips for staying safe online: identify potential weaknesses (like weak passwords), perform routine risk assessments and reinforce best practices amongst yourself and fellow employees.

The summit's last speaker was Dr. Gerry Dozier, who is both a professor and the Director of the ID Research Lab at Auburn University. His presentation focused on Identity Science, which is the understanding of the dynamic nature of the 'self' interacting with the environment. As Dr. Dozier said, "Since you leave behind digital exhaust when you go online, it is possible for someone else to track the information that is left behind with the proper tools." In particular, Dr. Dozier expressed his interest in reducing the number of de-anonymization attacks, which can uncover a machine's personal writing style. While not a perfect solution, he has discovered that utilizing Iterative Language Translations helps mitigate de-anonymization attacks, albeit while leaving behind digital fingerprints. Some Iterative Language Translations include Adversarial Stylometry, which has a 9-feature set, and Adversarial Authorship, which has a table with a set of actions and a cluster of writing styles. In addition to using Iterative Language Translations, he also utilizes a tool that will morph text well enough to fool Identification Systems

The afternoon highlight was the traditional panel discussion, with this year's topic focusing on cybersecurity in the healthcare industry. Prof. Dasgupta moderated the panel focusing on the latest cybersecurity issues and how these are impacting the healthcare industry and how to avoid cyber incidents. The panelists, who each had a wide range of expertise in healthcare, IT security, and public health, participated in discussion. The panelists pictured below are: Lynette Larkin and (St. Jude Children's Hospital), Steve Crocker (Methodist Le Bonheur Healthcare), Dr. Soumitra Bhuyan (University of Memphis), and Brian Elrod (St. Jude Children's Hospital). The discussion covered recent cybersecurity incidents in the news, hardware vulnerabilities, FDA regulations and more. The panelists concluded the discussion by providing potential solutions to the lack of cybersecurity in the healthcare field. There was a particular emphasis on individuals and organizations learning from past mistakes and looking for trends to prevent future mistakes. It was particularly apparent to the panelists that healthcare providers needed to learn how to not only protect patient data, but all data. After the panel ended, Dr. Dasgupta and Dr. Simon concluded the Summit with a farewell address.


Pictured (l-r): Lynette Larkin, Steve Crocker, Dr. Dipankar Dasgupta, Soumitra Bhuyan, Brian Elrod

The event was a great success, and received many positive comments from attendees and speakers. Listed below are just a few of the comments that we received from attendees:

> "I want to commend and thank both of you, and your technical team, for a well-organized Cyber Security Summit. I thoroughly enjoyed it. It was a day well spent."
>
> "It was a pleasure. I had a great time doing it. I respect what the University is doing and I will support you in any way that I can."
>
> "Thanks again for the opportunity to speak at the Cyber Security Summit. I really appreciate having the chance to engage with the community in order to improve the state of cyber security overall. Keep me in mind for future events, as I'd love to help in any way possible."
>
> "I enjoyed the cybersecurity panel last Thursday and I hope the symposium was a successful one. Again, thank you for the invitation."

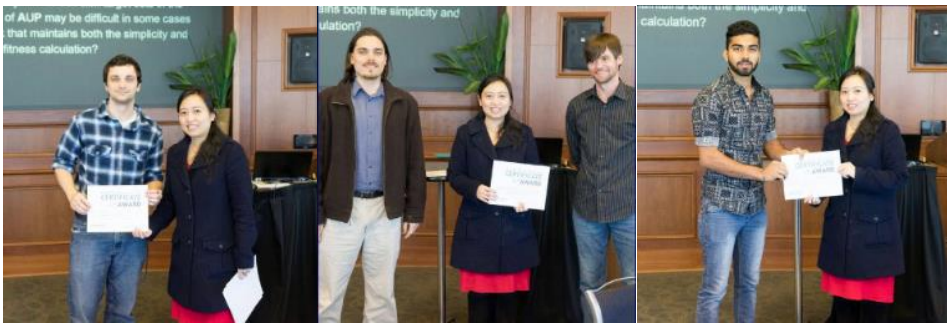
**b. Student Activities**

**University of Memphis Student Research Forum**

**McKittrick Swindle** won 1st place in the University of Memphis' 29th Annual Student Research Forum, which was hosted on March 27, 2017, for his presentation on *Adaptive Multi-Factor Authentication*. **Berkeley Willis** and **Robert Edstrom** teamed up to give a presentation on *Puzzle Based Learning*, and won 2nd Place in this event.

**Computer Science Research Day**

During the 13th Annual Computer Science Research Day event, four CfIA students placed in both the Oral and Poster Presentations. **McKittrick Swindle** (pictured on the far left next to Computer Science chair, Dr. Lan Wang) won 3rd place during the Oral Presentation portion of the event with a presentation *Linux Encrypted Containers: Implementing Data at Rest*. Both **Robert Edstrom** and **Berkeley Willis** (pictured in the center photograph) teamed up to work on a project entitled *Understanding Social Engineering Attacks through Simulated Cyber Environment – PBL II*. They won 2nd Place during the Poster Presentation portion. **Adithya Murthy** (pictured on the far right) won 3rd Place during the Poster Presentation portion of the event with his presentation on *Big Data Analysis using Hadoop & Spark*



## Cyber Cup Competition

**Robert Edstrom** and **Jon Walter Cobb** both participated in the 2nd Annual Cyber Cup Competition that was hosted in the Von Braun Civic Center in Huntsville, Alabama from June 7-8, 2017. The Cyber Cup competition is a Capture the Flag event. More information about this event can be found here.

## CfIA Students form RSO

A group of students from the Center for Information Assurance formed a Registered Student Organization that was open to all University of Memphis students. This RSO, called Nu11t3s3r, has since competed in Cyber Defense competitions and offered classes. Their cabinet members are as follows: **Berkeley Willis** (Graduate Student, President), **Robert Edstrom** (Undergraduate Student, Vice-President), **Jon Walter Cobb** (Undergraduate student, Treasurer).

## CANSec Cyber Defense Competition

A team of students from Nu11t3st3r (pronounced "Nulltester") won 1st place in the CANSec Student Cyber-Defense Competition on October 29, 2017 at the Missouri University of Science and Technology in Rolla, Missouri. The team from Nu11t3st3r, who named themselves Johnson & Johnson, was comprised of six Computer Science majors (**Berkeley Willis**, **McKittrick Swindle**, **Jon Walter Cobb**, **Robert Edstrom**, **Carrie Atkins** and **Craig Miller**). While the core members have participated in several competitions in the past, this is their first year competing as an official RSO.

This competition focused on cyber defense and was divided into three major stages. In the first stage, which can be described as the Preparation Stage, each team was given a one-hour time limit and a vulnerable virtual machine. Within the given time frame, each team was tasked with repairing as many weaknesses as they could find and reactivating services. Once the initial time limit expired, the competition moved into its second stage.

During this stage, which could be described as an Active Defense/Offense Stage, teams were allowed to continue working on the defense of their machines; however, a new element called the Red Team was added to the competition. The Red Team was essentially a team of hackers who attempted to breach each of the competing team's defenses in an effort to "Capture the Flag." Flags, which are akin to unique files, are hidden within the services that the competing teams are defending. Losing flags meant that a hacker had accessed a high enough privilege that they could disrupt services or steal sensitive information, which would ultimately result in the loss of points. The red team remained active until the end of the competition.

The final stage began during the final 30 minutes of the competition. At this point, teams were allowed to attack each other in what can only be described as a free-for-all. Competing teams were tasked with not only fending off the attacks of their fellow competitors, but also the attacks of the previously mentioned Red Team. In addition, each team could only attack another team once they received permission to do so from their CEO, who was assigned to them from amongst the University's staff. By this point, Johnson & Johnson had received a lot of points for both completing extra anomaly challenges and maintaining their service connections, so they were target number one for the other teams. Unfortunately for one opposing team, one of our observant students noticed that they had made the fatal error of having their username and password posted as their image. Johnson & Johnson was able to use this login information to later delete the other team's virtual machines. Maintaining their services led Johnson & Johnson to the win, with a combined score of 597 points, leaving their next closest competitor, the Louisiana Hot Snakes, behind with a score of 582.5, a result of only having a few of their services running throughout the competition.

### CodeBreaker Challenge

The NSA CodeBreaker Challenge is a national competition that is open to both students and professors. This competition tests the reverse engineering and low level code analysis skills of each participant. For the 2016 NSA CodeBreaker Challenge, a team of students (comprised of both Undergraduate and Graduate students) from the CfIA managed to place 11th nationwide. They competed against more than 200 universities. The 2017 CodeBreaker Challenge has since started, and some of the Center's students have started to take on the challenge.

## E. Collaboration/Consortium

### a. Collaborations with FIT-CAST

In following President M. David Rudd's new vision for the FedEx Institute which included emphasizing a stronger technology focus (on March 2015), the Center for Information Assurance (CfIA), in partnership with the Systems Testing Excellence Program (STEP) and the FedEx Institute of Technology (FIT), established the Cluster to Advance cyber Security & Testing (CAST). CAST is an actively expanding collaborative effort of experts and the CfIA has had strong research collaborations with FIT-CAST in the following research projects:

### Research Projects

1. *Collaborative Monitoring of Moving Target Defense Mechanisms for Cloud Computing* (Sajjan Shiva)
2. *Investigation and Testing of Cyber Security in Protective Relay System of Smart Power Distribution Grid* (Mohd Hasan Ali, Dipankar Dasgupta)
3. *Exploring Cyber Security Issues and Solution for Energy Storage at Smart Microgrid System* (Mohd Hasan Ali, Dipankar Dasgupta)
4. *Mitigating Ransomware Attacks by Leveraging Isolation Techniques* (Bo Chen, Dipankar Dasgupta)
5. *Protecting Data Security in Smart Internet-of-Things (IoT) Environments* (Lan Wang)
6. *Impact of Privacy Data Events on Consumer* (George Deitz, Mehdi Amini, Subhash Jha)
7. *Design of Gamification for Information Security Awareness and Compliance: An Empirical Study in the Context of Phishing Emails* (William Kettinger, Jong Lee, Chen Zhang)
8. *Corporate Governance Effectiveness and Cyber Security Risk Assessment and Management* (Zabi Rezaee, Joseph Zhang)
9. *Senior Hospital Administrators' Challenges on Emerging Cyber Security in Healthcare: An Exploratory Study using Q-Methodology* (Soumitra Bhuyan, Marian Levy, Dipankar Dasgupta)

10. *Securing Online Review Platforms: An Anomaly Detection Framework Using Advanced Machine-Learning (*Naveen Kumar, Deepak Venugopal*)*

**Activities/Events**

- **February 28, 2017: CAST Lightning Talks:** Brief talks and a reception as the 2017 research fellows present their recently awarded projects.
- **May 5, 2017: CAST Conversations:** CAST is a collaborative effort of experts who lead research, education and technology transfer at the FedEx Institute of Technology. This event allowed attendees to discuss current cyber security efforts led by UofM researchers

**b. Collaboration with Financial Infrastructure Stability and Cyber-security (FISC) Center**

Funded through the University Research Foundation, another multi-disciplinary initiative has been undertaken with the Finance Department of the University of Memphis. The Goal of the Financial Infrastructure Stability and Cyber-security (FISC) Center is to identify systemic threats to financial infrastructure stability and market resiliency by applying big data analytics and advanced statistical techniques to financial data. Information and activities of FISC is available at http://www.memphis.edu/finance/research/fisc.php.

**Dr. German Hernandez** and **Daya Ram Budhathoki** are currently working in collaboration with FICS. FICS hopes to identify systemic threats to financial infrastructure stability and market resiliency by applying big data analytics and advanced statistical techniques to financial data.

Financial infrastructure stability is critical to proper functioning of the US economy on Wall Street, Main Street businesses, and in individual investors' savings portfolios. Market integrity failure, counterparty risks, position exposure, risk spillover from interconnected markets, liquidity mismatch, loss of investor confidence, excessive public and private sector leverage, malfunctioning algorithms, hardware and software failures, and cyber-attacks are just some threats that endanger the stability of financial infrastructure.

The Department of Finance, Insurance, and Real Estate has excellent data for the study of the microstructure of financial markets. The Daily Trade and Quote (DTAQ) data purchased from the New York Stock Exchange comprises all trades and quotes and their associated sizes for exchanges and dark pools in the U.S. time stamped to the millisecond. Quotes outnumber trades by a factor of 100 to 1. The ITCH data from the National Association of Securities Dealers is time stamped to the nanosecond and comprises all messages (trades, quotes, and cancellations and their sizes). The Department also subscribes to a number of other datasets, including CRSP, Compustat, and NEEDS data. The department maintains two servers dedicated to the processing and analysis of transactions data. The Cook Lab is a state-of-the-art computer lab used for teaching and research. The Lab has 11 Bloomberg Terminals, which provide real-time data on financial markets worldwide. Additional TAQ

data and University wide Bloomberg licenses are required to expand our research and teaching missions[6]

### c. National Cyber Security Preparedness Consortium (NCPC)

As a founding member of a National Cybersecurity Preparedness Consortium (NCPC)[7] with partner universities University of Texas at San Antonio, Texas A&M University, Norwich University (Vermont), and the University of Arkansas, the CfIA continues to work together to update and extend the distribution (through FEMA) of our pioneering ACT Online cybersecurity training and awareness curriculum to first responders and security personnel across the nation. This group of universities has been cooperating under the Community Cyber Security Maturity Model, and has either conducted training/exercises in numerous communities and states around the country, or become involved in cybersecurity research. The consortium does the following:

1. Provides training to State and local first responders and officials specifically for preparing and responding to cybersecurity attacks
2. Develops and updates a curriculum and training model for state and local first responders and officials
3. Provides technical assistance services to build and sustain capabilities in support of cybersecurity preparedness and response
4. Conducts cybersecurity training and simulation exercises to respond to cyber attacks
5. Serves as a single focal point for states and communities seeking assistance on cybersecurity issues
6. Works with federal agencies to tie state and community efforts into existing national programs and initiatives
7. Conducts research to enhance the ability of states and communities to prevent, detect, respond to, and recover from cyber events

The members of the proposed consortium have informally come together to organize around the CCSMM to ensure a coordinated approach to help train individuals in states and communities.

## F. Other Associations (CAE Community)

In an effort to remain connected with the other Centers of Academic Excellence (CAE), the CfIA has become more active on the CAE in Cyber Security Community website. This website links other Centers of Academic Excellence by sharing important news, events and resources.

CfIA also established research collaborations with Oak Ridge National Laboratory and several leading universities.

[6] More information about FICS can be found at: http://www.memphis.edu/finance/research/fisc.php
[7] More information about the NCPC can be found at: http://nationalcpc.org/

## G. Outreach

In an effort to educate more individuals about the importance of Cyber Security, the Center reached out to multiple schools and organizations in the Mid-South area. **Carolyn Butler** and **Kelly Freeman** visited the following schools and organizations:

- Havenview Middle School (1481 Hester Rd.)
- Memphis Ambassador's Program (315 S. Hollywood St.)
- Benjamin Hooks Library (3030 Poplar Avenue)
- Reach Memphis (4646 Poplar, Suite 327)
- Sherwood Middle School (3840 Rhodes Ave.)
- Ridgeway Middle School (6333 Quince Road)
- Booker T. Washington (715 S. Lauderdale St.)
- Treadwell Middle School (920 N. Highland)
- Craigmont High School (3333 Covington Pike)
- Kingsbury High School (1270 N. Graham St.)
- Manassas High School (1111 N. Manassas St.)
- YMCA (6373 N. Quail Hollow)

These visits resulted in the Center forming a partnership with Manassas High School, which is currently trying to develop a Cyber Security Track for their students. The Memphis Ambassador's program has also expressed an interest in creating a Cyber Security Day/Week/Month for their students.

Due to the Center's connection with other individuals in the industry, the following professionals have spoken at past events hosted by the CfIA:

1. Tim Marsh - Special Agent for the FBI (GenCyber, Cyber Summit)
2. Meka Egwuekwe – CodeCrew (GenCyber)
3. Dr. Deon Garrett – Autozone (GenCyber)
4. Dr. Aregahegn S. Negatu – St. Jude Children's Research (GenCyber)
5. Dr. Andrew Neel – Discover (GenCyber)
6. Kay Cooper – FedEx (GenCyber)
7. Laury Garrett – Vaco (GenCyber)
8. Thomas Davis – ServiceMaster (Cyber Summit)
9. Ron Cundiff – Vanick (Cyber Summit)
10. Steve Crocker – Methodist LeBonheur Healthcare (Cyber Summit)

11. Brian Elrod – St Jude Children's Hospital (Cyber Summit)
12. Lynette Larkin – St. Jude Children's Hospital (Cyber Summit)
13. Bob Sydow – Ernst & Young LLP Cincinnati (Cyber Summit)
14. Dr. Gerry Dozier – Auburn University (Cyber Summit)
15. Dr. Jada Meeks – Empowering Students Universally (ESU) Scholars (GenCyber)

## IV. Media Exposure

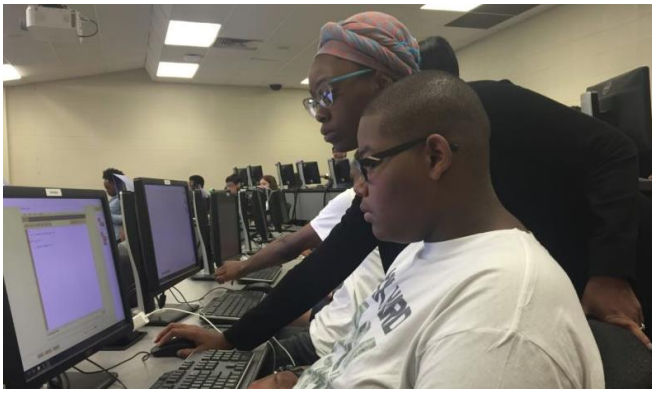
The CfIA has had a productive year. Multiple individuals have been interviewed by news outlets and newspapers. Below is a list of the CfIA's appearances in the media:

- *Patients Concerned After Medical Records Hacked at Memphis Doctor's Office*: An interview with Local 24 News. Dr. Dasgupta and Berkeley Willis (Graduate Student) provided their input on the compromise of patient data from an East Memphis medical practice. This interview can be viewed here.


- *Is Big Brother Watching? How Hackers Can Use Your Electronics to Spy On You*: An interview with Local 24 News. Dr. Dasgupta weighed in on Internet-Connected Devices and potential risks they pose. This interview can be viewed here.
- *UofM free web-based course overview*: An interview with WMC News Channel 5. Carolyn Butler (Project Coordinator for Cyber Security) discussed the Understanding Social Engineering Attacks course that was available on the ACT Online website. This interview can be viewed here.


- *University of Memphis: Enhance your career with a degree in Cyber Security*: A news article written by Study International. This article details the University of Memphis' new Undergraduate Cyber Security degree program that was offered Fall 2017. This story can be read here.
- *University of Memphis NSA Codebreaker Challenge interview*: An interview with WMC News Channel 5. Dr. Dasgupta and Berkeley Willis (Graduate Student) discussed the results of the 2016 CodeBreaker Challenge. This interview can be viewed here.


- *2017 IEEE Symposium Series on Computational Intelligence: Interview with Prof. Dipankar Dasgupta*: An interview between Dr. Dasgupta (Chair of the 2017 IEEE Symposium on Computational Intelligence in Cybersecurity) and Dr. David Fogel (Co-Chair of the 2017 IEEE Symposium on Computational Intelligence in Cybersecurity). Dr. Dasgupta discussed how computational intelligence relates to cyber security. This interview can be read here.
- *At GenCyber camp, Memphis Students get lessons in coding – and exposure to hot careers*: A news story on the GenCyber BootCamp by ChalkBeat. The article details the events that transpired during the High School session of GenCyber. This story can be read here.



- *Summer camp teaching kids to stay cyber secure*: A news story on the GenCyber Boot Camp by WMC News Channel 5. This story details the events that transpired during the Middle School session of GenCyber. This story can be viewed here.


- *CfIA Successfully Concludes 10th Annual Cyber Security Summit*: A news story that briefly covers the events that occurred during the Cyber Security Summit that was hosted in the FedEx Institute of Technology at the University of Memphis. This story can be viewed here.

## V. Report Summary

Directed by the Co-Directors, the Center conducts research, develops educational tools, programs and training for the Mid-South. By offering information assurance graduate and undergraduate course and hosting workshops for the students and professionals, the CfIA is working to create a future of secure online commerce and a safe computing environment. The Center also contributes to the community by training local educators at all levels to serve their students better. The center not only motivates students to break through in academic research but also continues to challenge them to advance their grasp on cyber security that they so passionately dedicate themselves.

The Center's motto is to explore all aspects of cyber security work through various research projects, to offer new avenues for innovative security research, and establish linkage with state's security need at different levels. In addition, the Center will serve as the state and national resources and provide educational and outreach activities for next-generation workforce development. Research and outreach activities at the center are attracting bright minds to the University of Memphis. For several years now, students who acquired research experiences by working at the center were offered high-valued jobs and are now in great demand in the job market. An outside view of this center's

successful goal oriented structure really reconfirms the University of Memphis's slogan "Driven by doing", and doing in collaboration is something the CfIA does beyond comparison.