THE UNIVERSITY OF MEMPHIS | Center for Information Assurance

CfIA Annual Report (Full Version)

Fiscal Year 2018

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

PERFORMANCE NARRATIVE

1. Primary Goals and Purpose

"Careers in Information Security Analysis ranks 4th out of 10 best Technology jobs" according to US News and World Report. That being said, there is a shortage of Cybersecurity Professionals in the industry. According to Cyberseek, there are over 300,000 cybersecurity job vacancies as of January 2019, and these vacancies are projected to increase to "3.5 million by the end of 2021"[1]. 84% of these postings require a Bachelor's degree, and 83% 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.

Since the Center for Information Assurance (CfIA) established in 2004, 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 continued re-designation is an accomplishment unique to the University of Memphis, since it is the first University in Tennessee to receive both these designations. 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 significant impacts on economic development, the provision of public services, citizen privacy and security.

2. Objectives

To achieve the primary goals, the center has the following objectives:

- 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).

[1] https://cybersecurityventures.com/jobs/

- 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) and FISC (Financial Infrastructure Stability and Cyber-security) .

3. Cybersecurity Activities

3.1 Cybersecurity Research/Education/Training Funding

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 $1.9 million as follows:

Grant Name	Collaborators	Funding Agency	Amount	Date Range
Cyber Security Competitive Training Grant	Norwich University	Lead: NU, Prime: DHS/FEMA II	$325,000	10/1/14-3/31/19
CAE Cyber Security Workforce Development		NSA	$206,085	9/1/17-9/13/19
Mobile Device Security and Privacy	University of Arkansas Little Rock	Lead: UALR Prime: DHS/FEMA III	$473, 218	1/15/16-9/30/19
Cyber Identity and Authentication	University of Texas	Lead: Univ. of TX Prime: DHS/FEMA IV	$503,104	11/1/16-9/30/19
Preparing for Next Generation Cyber Defense		FEMA/DHS	$400,000	9/2017-8/30/20
CAST: PKChain: Decentralized Public-Key Management System Based on Blockchain Technology	Lan Wang	FIT	$15,000	7/1/18-12/31/19
Puzzle-Based Cyber Security Learning	Jackson State University	NSF	$364,864	6/1/14-10/31/18
Adaptive Cybersecurity Training (ACT) Online	University of Texas, San Antonio	FEMA	$207,000 (Multi-University Grant of $800,000)	10/1/13-Present
Realizing Advanced Persistent Threats	Norwich University Applied Research Institute	Lead: NU Prime: DHS/FEMA	(Multi-University Grant of 2.2 million)	9/1/17 -8/31/20

3.2 Cybersecurity Faculty & Staff

Name	Position
Dipankar Dasgupta	CfIA Director/Hill Professor – Computer Science
Judith Simon	CfIA Co-Director/Professor – Business Information Technology
Kan Yang	CfIA Associate Director/Assistant Professor – Computer Science
Xing Gao	Assistant Professor – Computer Science
Myounggyu Won	Assistant Professor – Computer Science
Zahid Akhtar	Research Assistant Professor
Carolyn Treadwell-Butler	Cybersecurity Project Coordinator
Starlett Calhoun	Cybersecurity Course Design Specialist
Erica Boyce	Cybersecurity Workforce Specialist
Terrance Campbell	Manager of Technical Support & Community Engagement
Kelly Freeman	Administrative Support

3.3 Cybersecurity Students 2018-2019

Name	Level	Status
Daya Ram Budhathoki	Graduate	Graduated
Jon Walter Cobb	Undergraduate	Graduated – Employed (St. Jude Children's Hospital)
Robert Edstrom	Undergraduate	Employed (Discover)
Kishor datta Gupta	Graduate	In Progress
Sajib Sen	Graduate	In Progress
Peyton Warren	Undergraduate	In Progress – Employed (Discover)
Berkeley Willis	Undergraduate	Graduated – Employed (Discover)
Carrie Atkins	Undergraduate	In Progress
Clifford Montjoy	Undergraduate	Graduated - Employed
Coby Glass	Undergraduate	Graduated - Employed (Boeing)
Subash Poudyal	Graduate	In Progress
Senjuti Dutta	Graduate	In Progress
McKittrick Swindle	Undergraduate	Graduated – Employed (St. Jude Children's Hospital)
Ayushi Mehta	Graduate	In Progress
Johnathon Hardin	Undergraduate	Employed (Discover)
Marcus Kelly	Undergraduate	In Progress
Saurabh Pahun	Graduate	In Progress
Raavi Pavan Venkat	Graduate	In Progress
Manish Kasu	Graduate	In Progress
Pradeep Sanbu	Graduate	In Progress
Sharmin Afroz	Graduate	In Progress
George Thaiparambil Thomas	Graduate	In Progress
Kul Prasad Subedi	Graduate	Graduated – Dissertation Success
Jamal Mosakheil	Graduate	In Progress
Lei Yan	Graduate	In Progress
John Shrein	Graduate	In Progress
Jobin J. Sunny	Graduate	Employed (St. Jude Cloud)
Benjamin Borstad	Undergraduate	In Progress – Employed (St Jude Children's Hospital)

3.4 Cybersecurity Research Publications

a.) Dr. Dipankar Dasgupta

In 2018 academic year, **Dr. Dasgupta** has published 10 research papers. Of these research papers, 2 were Journal Articles, 6 were Conference Papers, and 1 was a Patent. Some of his publications include:

1.) D. Dasgupta, A. Roy, D. Ghosh. "Multi-User Permission Strategy to Access Sensitive Information" Information Sciences, Vol. 423, pp. 24-49, 2018
2.) D. Dasgupta. "Thermal Vein Signatures, DNA and EEG Brainprint in Biometric User Authentication" Applied Computer Sciences in Engineering, Vol. 915, p. 30, 2018
3.) D. Dasgupta, AK. Nag, A. Roy (2018) *U.S. Patent No. 9,912,657.* Washington, DC: U.S. Patent and Trademark Office
4.) KP Subedi, DR. Budhathoki, D. Dasgupta. "Forensic Analysis of Ransomware Families using Static and Dynamic Analysis" 2018 IEEE Security and Privacy Workshops (SPW), pp. 180-185, 2018
5.) DR. Budhathoki, D. Dasgupta, P. Jain. "Big Data Framework for Finding Patterns in Multi-market Trading Data" International Conference on Big Data, pp. 237-250, 2018.
6.) D. Dasgupta. "Biometrics and its use: Viewpoint" Biostatistics and Biometrics –Open Access Journal (ISSN; 2573-2633), Vol. 7, Iss. 3, pp. 1-3, 2018
7.) DR Budhathoki, D. Dasgupta, P. Jain "Analysis of Multi-Market Stock data to find Exchange Dominance" 8th Annual International Conference on Accounting and Finance (AF), Singapore, pp. 23-24, 2018.
8.) S. Ghosh, MH. Ali, D. Dasgupta "Effects of Cyber-Attacks on the Energy Storage in a Hybrid Power System" Proceedings of the IEEE PES General Meeting, Portland, OR, USA, ISS. 978-1-5386-7703-2/18, 2018
9.) C. Cabrera, G. Hernandez, LF Nino, D. Dasgupta "Thermal Vein Signatures, DNA and EEG Brainprint in Biometric User Authentication" International Workshop on Experimental and Efficient Algorithms, pp. 30-41, 2018
10.) KD Gupta, D. Dasgupta, S. Sen "Smart Crowdsourcing Based Content Review System (SCCRS): An Approach to Improve Trustworthiness of Online Contents" International Conference on Computational Social Networks, pp. 523-535, 2018
11.) Subash Poudyal, Kul Prasad Subedi, D. Dasgupta "A Framework for Analyzing Ransomware using Machine Learning" IEEE Symposium Series on Computational Intelligence, Bengaluru, India, Nov 2018

b.) Dr. Kan Yang

In 2018, **Dr. Kan Yang** has worked collaboratively with other individuals to publish 12 Journal Articles.

Journal Articles:

1) J. Shu, X Jia, K. Yang, H. wang. "Privacy-Preserving Task Recommendation Services for Crowdsourcing". IEEE Transactions on Services Computing, 2018.
2) H. Ren, H. Li, Y Dai, K. Yang, X Lin. "Querying in Internet of Things with Privacy Preserving: Challenges, Solutions and Opportunities". IEEE Network, Issue 99, pp. 1-8, 2018.
3) J. Shu, X. Liu, X. Jia, K. Yang, R. Deng. "Anonymous Privacy-Preserving Task Matching in Crowdsourcing". IEEE Internet of Things Journal, 2018
4) Y. Zhang, C. Xu, H. Li, K. Yang, J. Zhou, X. Lin. "HealthDep: An Efficient and Secure Deduplication Scheme for Cloud-Assisted eHealth Systems". IEEE Transactions on Industrial Informatics, 2018
5) Z. Yang, K. Yang, L. Lei, K. Zheng, VCM Leung. "Blockchain-based Decentralized Trust Management in Vehicular Networks". IEEE Internet of Things Journal, 2018

6) Y. Zhang, RH. Deng, J. Shu, K. Yang, D. Zheng. “TKSE: Trustworthy Keyword Search over Encrypted Data with Two-side Verifiability via Blockchain” IEEE Access, 2018.
7) K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, Y. Yang. “Blockchain-based Secure Time Protection Scheme in IoT”. IEEE Internet of Things Journal, 2018
8) J. Shu, K. Yang, X. Jia, X. Liu, C. Wang, R. Deng. “Proxy-Free Privacy-Preserving Task Matching with Efficient Revocation in Crowdsourcing” IEEE Transactions on Dependable and Secure Computing, 2018.
9) J. Shu, X. Liu, K. Yang, Y. Zhang, X. Jia, R. Deng. “SybSub: Privacy-Preserving Expressive Task Subscription with Sybil Detection in Crowdsourcing” IEEE Internet of Things Journal, 2018
10) Z. Su, Q. Xu, Q. Zhao, J. Song, W. Shen, Y. Wang, K. Yang. “Experience Blocking Ratio Based Game Theoretic Approach for Spectrum Sharing in Heterogeneous Networks” IEEE Transactions on Network Science and Engineering, 2018
11) K. Fan, C. Zhang, K. Yang, H. Li, Y. Yang. “Lightweight NFC Protocol for Privacy Protection in Mobile IoT”. Applied Sciences, Vol. 8, Issue 12, p. 2506, 2018
12) G. Xu, H. Li, Y. Dai, K. Yang, X. Lin. “Enabling Efficient and Geometric Range Query With Access Control Over Encrypted Spatial Data” IEEE Transactions on Information Forensics and Security, Vol. 14, Issue 4, p. 870-885, 2019 (to be published in April)

c.) Dr. Xing Gao

In 2018, **Dr. Xing Gao** joined the Center and published the following:

1.) X. Gao, Z. Xu, H. Wang, L. Li, X. Wang. “Reduced cooling redundancy: A new security vulnerability in a hot data center” Proceedings of the network and distributed system security symposium, 2018
2.) S. Deng, X. Gao, Z. Lu, X. Gao. “Packet Injection Attack and Its Defense in Software-Defined Networks” IEEE Transactions on Information Forensics and Security, Vol. 13, Iss. 3, pp. 695-705, 2018
3.) X. Gao, B. Steenkamer, Z. Gu, M. Kayaalp, D. Pendarakis, H. Wang “A Study on the Security Implications of Information Leakages in Container Clouds” IEEE Transactions on Dependable and Secure Computing, 2018
4.) S. Deng, X. Gao, Z. Lu, Z. Li, X. Gao “DoS vulnerabilities and mitigation strategies in software-defined networks”Journal of Network and Computer Applications, Vol. 125, pp. 209-219, 2019

d.) Dr. Myounggyu Won

In 2018, **Dr. Myounggyu Won** joined the Center and published the following:

1.) M. Won, “A Review on V2V Communication for Traffic Jam Management” Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communications: A Technical Approach, p. 1, 2018
2.) M. Won, A. Shrestha, Y. Eun “Enabling WiFi P2P-Based Pedestrian Safety App” arXiv preprint arXiv: 1805.00442, 2018
3.) A. Shrestha, M. Won, “DeepWalking: Enabling Smartphone-based Walking Speed Estimation Using Deep Learning” arXiv preprint arXiv: 1805.03368, 2018
4.) M. Won, Y. Zhang, X. Jin, Y. Eun “Wiparkfind: Finding empty parking slots using wifi” 2018 IEEE International Conference on Communications (ICC), pp. 1-6, 2018
5.) M. Won, S. Sahu, K. Park, “DeepWiTraffic: Low Cost WiFi-Based Traffic Monitoring System Using Deep Learning” arXiv preprint arXiv: 1812.08208, 2018

3.5 Cybersecurity Research Collaborations

a) National Cyber Security Preparedness Consortium (NCPC)

As a founding member of a National Cybersecurity Preparedness Consortium (NCPC)[2] 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 (CCSMM), 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.
The following projects have been completed as a member of the NCPC:

2018 Activities

CfIA Staff members engaged in NCPC meetings in 2018.

Carolyn Treadwell-Butler

- Participated in the monthly operational meetings on the first Wednesday of every month
- Participated in the NCPC Partner Web-Based Course Development Training/Process Development Session from Nov. 14-15, 8:30 AM – 4:30 PM at a TEEX Facility (Emergency Operations Training Center (EOTC)) in College Station, TX.

Terrance Campbell

- Participated in the Principal Investigator (PI) meeting at University of Arkansas, Little Rock on behalf of Dr. Dipankar Dasgupta on December 12, 2018.

[2] More information about the NCPC can be found at: http://nationalcpc.org/

FEMA Funded Courses

Understanding Social Engineering Attacks (USEA)

An 6-7 hour online course covering topics on social engineering attack techniques and tools, while also equipping trainees with a better understanding of how attackers use people as the weakest link in order to compromise targeted organizations. Trainees will learn how to adapt to such phishing attacks, develop security awareness, and take preventative measures.

Mobile Device Security and Privacy (MDS/MDP)

In Mobile Device Security (MDS), trainees will learn about mobile network attacks and mobile data leakage issues. Trainees will develop security awareness and learn prevention strategies from both personal and business perspectives. In Mobile Device Privacy (MDP), trainees will learn about mobile malware and mobile privacy issues, which include unauthorized app access to personal information and preventative measures.

NSF Puzzle Based Learning (PBL) Project

Cyber security has increasingly become important due to the sophistication and frequency of online attacks, and these attacks' consequences on organizations' network infrastructures. Different forms of puzzles are in existence for people to think, expand knowledge and stimulate their cognitive ability. One expectation of this project is that the scenario-based cyber security puzzles will be significantly enhanced through the implementation of interactive intelligent tutoring software. Throughout the course of this project, there were many comments that stated that the type of puzzles developed by this project could easily be incorporated into existing courses as supplementary activities to enhance the student's learning. The successful implementation of this project will improve defensive skills of students who pursue a career in the Network and Computer Systems and Computer Network Support Specialists occupations (which includes those who will be enrolled in cyber security courses and programs that will support the front line technician) and allow students to expand into disciplines beyond information technology.

b) Collaborations with FIT-CAST

Following the President M. David Rudd's new vision for the FedEx Institute emphasizing a stronger technology focus (on March 2015), 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 active expand collaborative effort of experts and CfIA has strong research collaborations with FIT-CAST and in the following research projects:

1) PKChain: Decentralized Public-Key Management System based on Blockchain Technology (*Kan Yang, Lan Wang)*

2) Exploring Cyber Security Issue and Solution for Energy Storage at Smart Microgrid System *(Mohd Hasan Ali, Dipankar Dasgupta)*

3) Exploration of the Impact of Malware Warning Messages *(Nirmalee Raddatz)*

4) Machine Learning Approaches to Secure Virtual Machine Migration in the Cloud *(Sajjan Shiva, Deepak Venugopal, Naveen Kumar)*

5) Machine Learning Approaches to Secure Virtual Machine Migration in the Cloud *(Sajjan Shiva, Deepak Venugopal, Naveen Kumar)*

6) Design of Secure Random Number Generators for Cyber Security Applications *(Lih-Yuan Deng, Dale Bowman)*

7) Moral Intuition and Consumer Response to Privacy Norm Violations: An N400 ERP Study *(George D. Deitz)*
8) Exploring Cyber Security Issues and Solutions for Photovoltaic (PV) System Connected to DC Microgrid *(Mohd Hasan Ali, Dipankar Dasgupta)*
9) Case Studies on Health Information Security and Privacy Breach in the United States *(Soumitra Bhuyan)*
10) Content-based detection of Fake Reviews using Deep Learning *(Deepak Venugopal, Naveen Kumar)*

c) 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.

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

3.6 Cybersecurity Professional Activities

a) Dr. Dipankar Dasgupta

- Dr. Dipankar Dasgupta received the US Patent approved for Adaptive Multi-Factor Authentication System (No. 9,912,657) on March 6, 2018
- Dr. Dipankar Dasgupta took part as a Program Committee Member at the 12th Annual Cyber & Information Security Research (CISR) Conference at Oak Ridge, TN on April 04-06, 2018.
- Dr. Dipankar Dasgupta served as a panelists at the 2018 SEC Academic Conference at Auburn University in Auburn, Alabama from April 8-10, 2018.
- Dr. Dipankar Dasgupta was a guest speaker at the Massachusetts Institute of Technology's 2018 Professional Development Summer Workshop on Applied Cybersecurity, where he highlighted his work on the Adaptive Multi-Factor Authentication system.
- Dr. Dipankar Dasgupta delivered a keynote speech on July 15 at the ACM Workshop on Genetic and Evolutionary Computation in Defense, Security, and Risk Management (SecDef @ GECCO 2018) and presented his A-MFA research at iChain, a company in Tokyo that is currently applying blockchain technology for insurance portfolio management.
- Dr. Dipankar Dasgupta was featured on News Channel 3 in Memphis, TN for "TNReady testing troubles over, for now".
- Dr. Dipankar Dasgupta was interviewd by WMC Action News 5 regarding Cyber Ambassadors Tech Camp.
- Dr. Dipankar Dasgupta organized Symposium on Computational Intelligence in Cyber Security (CICS) at IEEE Symposium Series on Computational Intelligence (SSCI) in Bengaluru, India from November 18-21, 2018.

b) Dr. Judith Simon

- Dr. Judith Simon gave a presentation entitled "Around the world of cyber laws and cultures in 80 days" at the Management Information Systems (MIS) Colloquium on February 16, 2018

- Dr. Judith Simon gave a presentation entitled "A global view of cyber laws and country cultures" at the Management Information Systems (MIS) Colloquium on September 21, 2018

c) Dr. Kan Yang

- Dr. Kan Yang was invited to serve as TPC in the 2018 IEEE Globecom'18 (Communication and Information Systems Security Symposium) in February 2018.
- Dr. Kan Yang was invited to serve as a TPC in the 15th IEEE International Conference on Mobile Ad hoc and Sensor Systems (IEEE MASS'18: Security and Privacy Track) in April 2018.
- Dr. Kan Yang was invited to serve as a TPC in the 10th International Conference on Wireless Communications and Signal Processing (WCSP'18) in May 2018.
- Dr. Kan Yang received a FedEx Institute of Technology Development Grant – Cluster to Advance cyber-Security and Testing (CAST) "PKChain: Decentralized Public-Key Management System based on Blockchain Technology" PI, July 1, 2018 – December 31, 2019 in June 2018.
- Dr. Kan Yang was invited to serve as a TPC in the 1st International Workshop on Distributed Ledger of Things (DLoT'18, CALL FOR PAPER, deadline: September 3, 2018) in August 2018.
- Dr. Kan Yang gave a talk on "Blockchain-based Decentralized Public Key Management for Named Data Networking" at Named Data Networking Community Meeting at NIST in September 2018
- Dr. Kan Yang was invited to serve as a TPC in the 2019 IEEE International Conference on Blockchain (Blockchain 2019) in September 2018.
- Dr. Kan Yang organized the 11th Annual Mid-South Cybersecurity Summit at the FedEx Institute of Technology.

d.) Dr. Xing Gao

- Dr. Xing Gao was invited to serve as a TPC in the 1st International Workshop on Mobile Energy Sharing Networks

e.) Dr. Myounggyu Won

- Dr. Myounggyu Won was invited to serve as a TPC in the 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2018)
- Dr. Myounggyu Won was invited to serve as a TPC in the 15th IEEE Conference on Mobile Ad hoc and Sensor Systems (IEEE MASS'18)

3.7 Cybersecurity Outreach

Apart from working on world-class research, the CfIA provides training and career development services for students and professionals through online and hands-on training and community events, special purpose conferences, and vendor specific training programs.

3.7.1 Annual Cybersecurity Summit

The Center for Information Assurance (CfIA) successfully hosted the 11th Annual Mid-South Cybersecurity Summit on October 5, 2018 at the FedEx Institute of Technology on the University of Memphis campus. Dr. Kan Yang, Associate Director of the CfIA, hosted this year's summit and welcomed students and professionals from multiple areas in the Cybersecurity industry.

Speakers

This year's Summit welcomed professionals from across the nation to give presentations on cybersecurity as it relates to both their organizations and average users. Speakers included Michael

Rodriquez (City of Memphis), Dr. Xinhua Ling (XLNTEC Inc), Steve Crocker (Methodist Le Bonheur Healthcare), David Brink (Boeing Global Services), and Bryan Mitchell (FedEx Global).

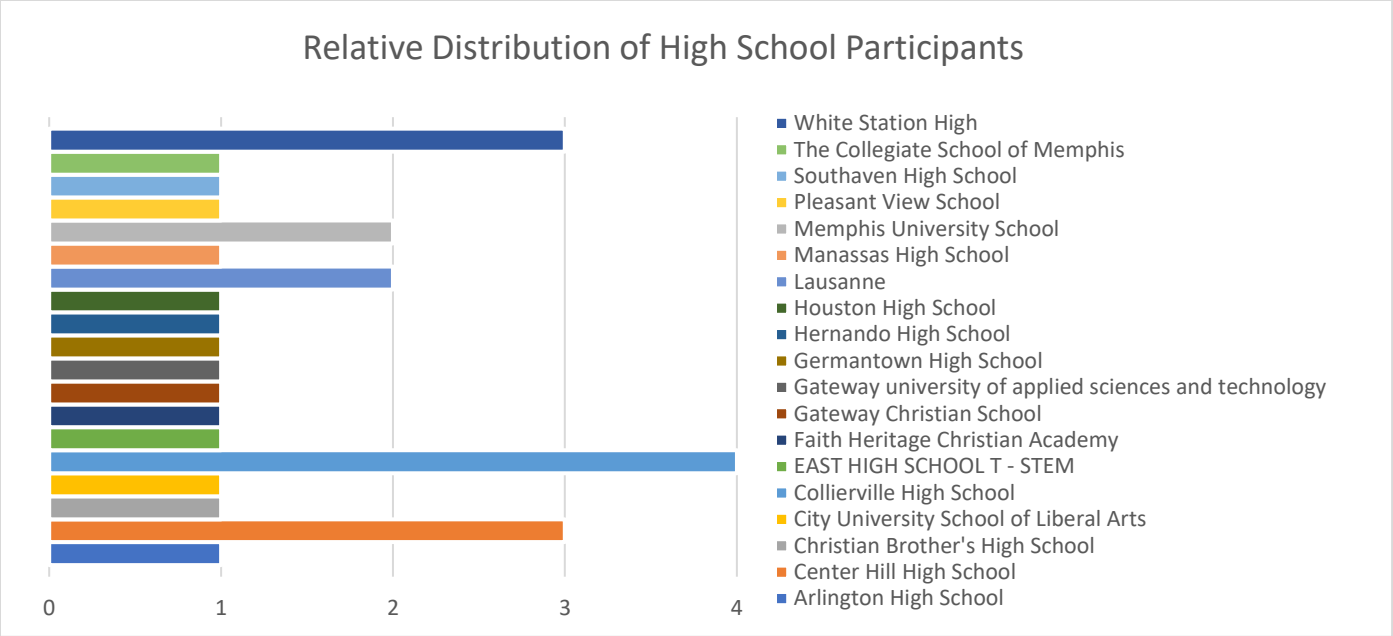
Presentations

Presentation topics included data security, blockchain, healthcare security, system security and IoT security. Interactions among the presenters and attendees made it a highly engaging event. The highlight of the Summit was the afternoon panel discussion on challenges and opportunities in cybersecurity. Dr. Xinhua Ling moderated the panel focusing on the latest cybersecurity challenges in corporate, data breaches, and expectations from industry & universities. The panelists, with a wide range of expertise in IT security, IoT and risk assessment, participated in the discussion. The panelists were: David Brink (Boeing Global Services), Bryan Mitchell (FedEx Global), and Dr. Kan Yang (University of Memphis).

For detailed information about the Center, visit https://www.memphis.edu/cfia/. The full report for the 2018 Cyber security summit is available at https://www.memphis.edu/cfia/cybersummit/index.php

3.7.2 2018 Cyber Ambassador Tech Camp

Over 25 high school students, from different places, came to the University of Memphis to learn more about the concepts of cybersecurity, ethical hacking, coding, computer science and technology. The chart below displays that campers came from 19 different schools across the mid-south region. The highest number of applicants came from Collierville High School.



The full report can be viewed here: https://www.memphis.edu/cfia/pdfs/cybercamps/cyber-ambassador-2018-summary-report.pdf

3.7.3 Online Cybersecurity Courses

Online courses we developed focused on various aspects of Cybersecurity. These FEMA funded courses are free for all users. Our most recent course is entitled *Cyber Identity and Authentication*.

3.7.4 2018 Cybersecurity Radio Program

Initiated monthly broadcast on Cyber Safety and best Practices from the University's radio channel. Here are the links for two radio broadcasts:

- **Cybersecurity Radio Show 1**
- **Cybersecurity Radio Show 2**

3.7.5 Professional Development Workshops

Hosted two Cybersecurity Professional workshops on August 3rd and another on October 12, 2018

3.7.6 St. Michael's Catholic School (8th Grade Students)

In collaboration with the Boy Scouts of America Chickasaw Council, we have been conducting a series of 50-minute Cybersecurity Awareness and Career Exploration sessions using puzzle-based learning principles since November 2018 and will conclude February 2019.

3.7.7 University of Memphis TigerLIFE Program

Conducted two 90-minute Cybersecurity Awareness and Career Exploration workshops for a University of Memphis TigerLIFE Community Engagement class consisting of 12 students November 2018. One of the workshop was conducted during National Cybersecurity Career Awareness Week. We are making plans to pilot a Cybersecurity internship for select University of Memphis TigerLIFE during the 2019 Spring semester.

3.7.8 Manassas High School Cybersecurity Emersion Program (Special Needs Students)

In collaboration with the University of Memphis TigerLIFE Program, we conducted a 50-minute Cybersecurity Awareness and Career Exploration workshop for Manassas High School Special Needs Students (Freshman, Sophomore, Juniors, and Seniors) during National Cybersecurity Career Awareness Week. One student voiced an interest in wanting to participate in TigerLIFE upon graduating in 2019.

3.7.9 Greater-Memphis Special Needs Population Cybersecurity Awareness Project

Convened several meetings with providers of training services for the Special Needs Population in Memphis to identify that types of Cyber Safety and Security service could we provide this population in collaboration with University of Memphis TigerLIFE Program.

3.7.10 Boys Scouts of America Chickasaw Council (Cybersecurity Merit Badge Project)

Developing of a Cybersecurity Merit Badge Series for the Boys Scouts of America Chickasaw Council, which serves over 7,000 adolescents across Shelby County, TN; Crittenden County, AR; and 14 counties in Northern, MS. We are finalizing the series and are working with the Chickasaw Council to identify a research project for which to submit an IRB application.

3.7.11 Boys Scouts of America Chickasaw Council (Training Chair)

Serving as the 2019 Training Chair (Terrance R. Campbell) for Boys Scouts of America Chickasaw Council, which serves over 7,000 adolescents across Shelby County, TN; Crittenden County, AR; and 14 counties in Northern, MS.

3.7.12 Rebrand Cities Memphis

On November 5, 2018, Rebrand Cities in collaboration ATT Foundation, WordPress, Epicenter Memphis and the Center for Information Assurance, launched its Memphis Programming aimed at assisting entrepreneurs design and deploy a website as part of its effort to bring 10,000 entrepreneurs nation-wide online. AT&T Foundation and WordPress.com. We are planning to pilot a model for training Hamilton Cybersecurity Program students to assist in the process in a manner that assist them prepare for the CompTIA IT Fundamentals certification exam starting in February 2019.

For detailed information about the Center for Information Assurance, please visit http://www.memphis.edu/cfia or contact: cfia@memphis.edu

3.8 Student Activities

3.8.1 CfIA Students continue RSO activities

A group of students from the Center for Information Assurance formed a Registered Student Organization that was open to all University of Memphis students in 2017 and continued activities into 2018. This RSO, called Nu11t3s3r, has since competed in Cyber Defense competitions.

3.8.2 DOE Cyber Defense Competition

A team of undergraduate students at the Center for Information Assurance (CfIA), who formed a registered student organization (RSO) open to all U of M students last year, won 1st place (Regionally)/5th Place (Nationally) in the Department of Energy Cyber Defense Competition on April 7, 2018 at the Oak Ridge National Laboratory in Oak Ridge, Tennessee. The team was comprised of five Computer Science majors (Craig Miller, McKittrick Swindle, Jon Walter Cobb, Johnathon Hardin, and Coby Glass). For a few of these students, this was their second time competing (and winning) as a member of their RSO.

3.8.3 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 2018 NSA CodeBreaker Challenge, a team of students (comprised of both Undergraduate and Graduate students) from the CfIA managed to place 33rd nationwide. They competed against more than 200 universities.

3.8.4 Raymond James Visit & Competition

On February 23rd, the Center for Information Assurance partnered with the Department of Corporate Engagement and Career Services to host a meeting for Raymond James executive, Kishen Sridharan. During the student session of the meeting, students presented their cybersecurity-related work and gave a demonstration of the tools that they helped develop. Raymond James visited again in September to meet with students again.

A group of students were also invited to participate in the Raymond James Capture the Flag event. This team placed 5th out of 12 teams. This team was also the only team in the competition to have women competitors.

3.8.5 Television Interview

PhD Student, Jamal Mosakheil, was interviewed by News Channel 3 on how to avoid the growing number of phishing emails.

3.9 Alumni News

Former Cybersecurity student, Charles Lancaster, Jr. received the 2017 Sedgwick Most Valued Performer Award. Charles, who is currently an IT Systems Analyst Technician, joins 52 other Sedgwick colleagues from the U.S., Canada, UK, and Ireland who were recognized for exemplary performance of their duties. Charles also received Sedgwick's prestigious 2017 Diamond Award.

4. Media Exposure

2018 was a productive year for the Center. A list of the Center's media appearances can be seen below:

- *UofM: Launch your career in Computer Science* – The Center for Information Assurance was mentioned in an editorial that was written by Study International on February 22, 2018 for the University's Computer Science department.

- *TNReady Testing troubles over, for now* – Dr. Dipankar Dasgupta was interviewed by WREG News Channel 3 for the attack on the TNReady Testing system.

- *Cyber Ambassadors Tech Camp* – Dr. Dipankar Dasgupta and Erica Boyce were interviewed by WMC Action News 5 for the Cyber Ambassadors Tech Camp that was hosted in June 2018.

- *Cyber Ambassadors Tech Camp Radio* – Dr. Dipankar Dasgupta and Kelly Freeman were interviewed by WUMR 97.1 FM for the Cyber Ambassadors Tech Camp.

- *Local Good News: University of Memphis 2018 Cyber Ambassadors Tech Camp* – Terrance Campbell was interviewed by Local 24 Memphis for the Closing Ceremony of the Cyber Ambassadors Tech Camp.

- Mid-South MSK Group Patients Warned After Major Data Security Breach – Dr. Dipankar Dasgupta was interviewed by Local 24 Memphis for the large data breach at MSK Group.

- *Consumer Alert: How to avoid possible phishing emails* – Jamal Mosakheil was interviewed by WREG News Channel 3 for tips on how to avoid possible phishing emails.

5. Special Achievements

Continued to promote the Cybersecurity Concentration for Undergraduate Program in Department of Computer Science. Dr. Dasgupta and Dr. Yang developed the Curriculum to support the cybersecurity

concentration. Some students have already chosen the cybersecurity concentration program which demonstrates the first success in this cybersecurity concentration. A number of TV interviews, invited talks and trainings were performed during the academic year.

The Center also recorded two Cybersecurity Radio segments on the Campus' own radio station (WUMR U92 FM). These segments can be found here: https://www.memphis.edu/cfia/community_outreach.php.

Dr. Dipankar Dasgupta was also awarded the Hill Professorship award, which was created to recognize outstanding research achievement.

6. Plans for the next coming academic year

Goals: The next year's goals are to

- Continue expand our research capabilities by collaborating with faculty across campus (from different discipline) and other universities and company partnerships.
- Involve students at the graduate and undergraduate levels in research and education. Support Graduate Certificate Program in Information Assurance and undergraduate concentration in Cyber Security to provide students with hands-on experiences on various computer security-related tools.
- Seek both internal and external funding to conduct research in Cloud Security and Mobile Security, Web Security, Authentication and Identity, IoT Security, Healthcare security and privacy, etc.
- Outreach activities to promote cyber safety and privacy issues

Expected outcomes: CfIA activities will produce research publications, increase funding and student enrollment to move to High-Research University. We expect to continue a wide range of activities so to make the center in the forefront of research, education, and outreach on cyber security in the region and receive funding in all three areas.