CfIA Annual Report 2015-2016

Center of Excellence

THE UNIVERSITY OF MEMPHIS
Center for Information Assurance

CfIA Director: Dr. Dipankar Dasgupta

Professor, Department of Computer Science

CfIA Co-Director: Dr. Judith C. Simon

Professor, Department of Business Information Technology

http://cfia.memphis.edu

Introduction

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. The Center 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 (NSA) and the Department of Homeland Security (DHS). The University of Memphis is the first and only institution in the state of Tennessee to achieve both designations, which is valid until 2021. The Center for Information Assurance (CfIA) represents a flexible collaboration of multiple academic disciplines and partnership with community colleges focusing on cyber security related topics. Because of its multi-faceted activities, the University of Memphis is in the forefront in the research, education, and outreach on Cyber security in the region, and has been able to

[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

acquire funding in all three areas. The Center introduced two graduate certificate programs in Information Assurance through the Department of Computer Science, and in Business Information Assurance offered through the Department of Business Information and Technology (BIT). The two CfIA directors manage these certificate programs as well as programs for undergraduate students who received Department of Defense (DoD) scholarships (led by Dr. Simon).

The center strategies are to expand activities in the following directions:

- 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).
- 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 secure health informatics, privacy-preserving mobile health, smart grid security and secure supply chain (formation of FIT-CAST).
- Established research collaboration with Oak Ridge National Laboratory and with MIT Geospatial data center (worked on a collaborative project).

Cyber-Security Research Funding:

The Center is actively involved in IA-related projects and received federal funding to support various projects and initiatives, and is currently working on collaborative external grants of $7.5M as follows:[2]

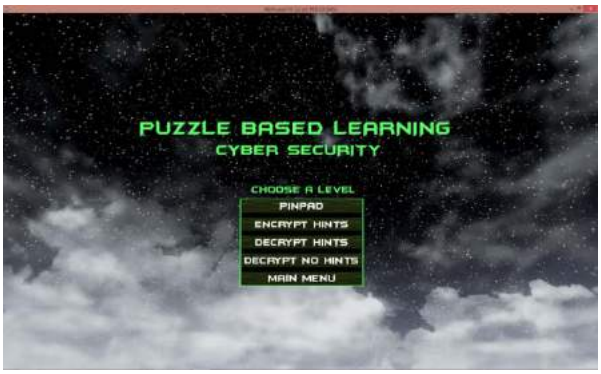
Grant Name	Funding Agency	PI or Co-PI's	Amount	Date Range
ACT Online Courseware Update	FEMA	U of M PI	$207K ((Multi-University grant of $800K)	10/1/13-12/31/16
Collaborative Research: Puzzle Based Cyber Security Learning to Enhance Defensive Skills of Front-Life Technicians	NSF	U of M PI	$364,864 (with Jackson State University) with total funding of $850,000)	06/1/14-05/31/17
Cyber Security Competitive Training Grant	FEMA/DHS	U of M PI	$325K (Multi-University grant of $2.3M)	10/1/14-9/31/17

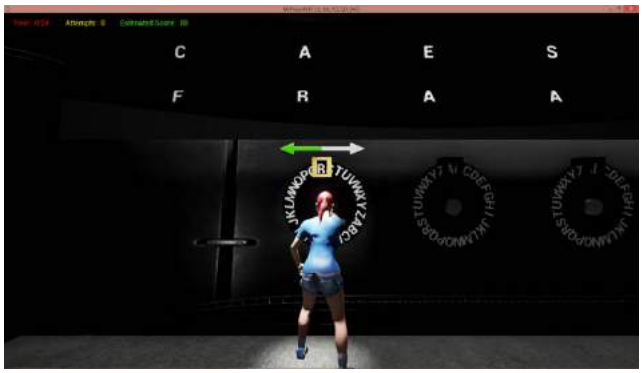
[2] In addition, four other proposals are currently under submission.

Collaborative: An Adaptive Continuous Multi-Factor Authentication Framework	NSA	PI	$240,907	08/15/2015 – 11/17/2016
Cyber Security Competitive Training Grant	FEMA	U of M PI	$473,218 (Multi-University grant of $3.0M)	1/15/2016 – 12/31/2018
GenCyber Summer Boot Camp for High and Middle School Students	NSA	PI	$74,359	3/01/2016-2/28/2017
CAST – FedEx Institute of Technology	UM Foundation	PI	$40,000	11/01/2015-4/30/2017

NSA Research Grant: Developing an Adaptive Multi-Factor Authentication (A-MFA) Methodology (A patent application is submitted on this research and also licensing agreement is underway with a company). The goal of this project is to develop a multi-factor authentication system with adaptive selection of authentication modalities (with their features) in different operating environments making the selection strategy unpredictable to compromise. The objectives of this project are to implement: (i) a trust-based adaptive, robust and scalable software/hardware framework for the selection of authentication factors for continuous and triggered user authentication, (ii) design optimal algorithms to determine the security-aware authentication factors in time-varying environments.

NSF Project on Puzzle-Based Learning (PBL): This research project funded by National Science Foundation (NSF) is to develop innovative "puzzles," using specialized software to help community college students learn the concepts of and approaches to cybersecurity.





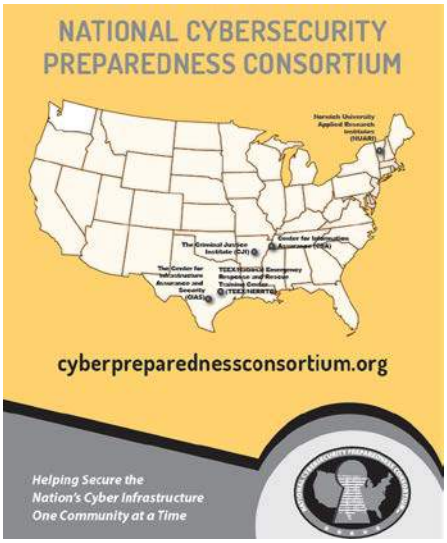
The PBL project introduces computer users to abstract security concepts, enabling critical thinking through solving complex puzzles. A PBL game is developed using Unreal Engine, a platform for creating next generation games. The outcome of the research is producing intelligent learning tools/techniques for cyber security education which is gradually being used by many colleges nation-wide. During 2016, we demonstrated and distributed the PBL software at three national conferences and received excellent feedback on our cybersecurity education focused research. Further details of this project is available at http://www.memphis.edu/cfia/pbl-sec/index.php .

DHS/FEMA Funded Cyber Security Training Program:

During 2006-2010, through a DHS/FEMA competitive grant of $4.2M, the center developed research-based extensive online cyber security training and certification program in three levels—beginner, intermediate, and advanced—in multiple tracks, called Adaptive Cyber-Security Training (ACT Online). These courses, currently hosted at the FEMA website, are being offered nation-wide at the local, state and federal levels and more than 20,000 people completed these courses since 2009. Through the continuous FEMA CTG grants, we are updating these courses on a regular basis and developing new courses. The following is a snapshot of completions (5,578) of our web-based ACT-Online cyber-security courses during the period Oct. 1, 2015 - May 31, 2016. The table shows the list of courses with the annual goal of training per course, goal to date in the performance period, and the last column shows actual completions during the period by course.

ter Management for Critical Infrastructure Protection and Incident ention		5,309	3,528	0	5,578
AWR-138-W	Network Assurance, Web-based	531	352		654
AWR-139-W	Digital Forensics Basics, Web-based	557	368		545
AWR-168-W	Cyber Law and White Collar Crime, Web-based	504	336		710
AWR-169-W	Cyber Incident Analysis and Response, Web-based	279	184		274
AWR-173-W	Information Security Basics, Web-based	846	560		566
AWR-174-W	Cyber Ethics, Web-based	489	328		775
AWR-175-W	Information Security for Everyone, Web-based	1,244	832		1,168
AWR-176-W	Disaster Recovery for Information Systems, Web-based	257	168		359
AWR-177-W	Information Risk Management, Web-based	252	168		175
AWR-178-W	Secure Software, Web-based	350	232		352

National Cyber Security Preparedness Consortium (NCPC)



We are a core founding member of a National Cybersecurity Preparedness Consortium (NCPC)[3] with partner universities University of Texas at San Antonio, Texas A&M University, Norwich University (Vermont), and the University of Arkansas, working together to update and extend the distribution (through FEMA) of our pioneering ACT On-line cybersecurity training and awareness curriculum to first responders and security personnel across the nation. This group of universities that have been cooperating under the Community Cyber Security Maturity Model, have already conducted training and exercises in numerous communities and states around the country or are involved in cybersecurity research. The consortium: (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 defend from and respond to cyber-attacks; (5) serves as a single focal point for states and communities seeking advice and assistance on cybersecurity issues; (6) works with federal agencies to tie state and

[3] *NCPC 2015 annual report is available at the center website (http://www.memphis.edu/cfia/pdfs/ncpc_annual_report.pdf)*

community efforts into existing national programs and initiatives; and (7) conducts research to enhance the ability of states and communities to prevent, detect, respond to, and recover from cyber events.

To date, in addition to developing and delivering Online Cyber Security Training to more than 20 thousand citizens, members of the consortium have conducted 63 cybersecurity exercises with over 3850 participants and delivered cybersecurity training to 53 communities in 22 states and reached over 3300 students. Members of the consortium have also begun the implementation of the Community Cyber Security Maturity Model (CCSM) in 6 states. The CCSMM provides a foundation from which states and communities can develop viable and sustainable cyber security programs. 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.

Hosted Annual Cyber Security Summit on October 16th:

Center for Information Assurance (CfIA) hosted the eighth annual Mid-South Cyber Security Summit Friday, October 16, 2015 at the FedEx Institute of Technology. Distinguished speakers discussed topics such as health information security, cloud security and cybercrime. Information assurance and cyber security experts were onsite for presentations and networking to address current issues of cyber security. There were several pre-summit events on Oct. 15, including a Community College Workshop and FEMA training hosted by TEEX (Texas A&M Engineering Extension Service). This event was a huge success; more than 150 people participated from the community and local industry. The picture shows Dr. Judy Simon (CfIA Co-Director) is moderating a panel at the summit. To learn more about the annual Mid-South Cyber Security Summit, visit cybersummit.memphis.edu.

Center Researchers and Staff:

- Dr. Alexander Semenov (Post-Doctoral Research Scholar from Finland visited for one month).
- Dr. Arunava Roy (Post-Doctoral Research Scholar worked from August 2014 - Jan 2016), and then joined the National University of Singapore.
- Dr.Ameya Sanzgiri (Research Assistant Professor March 2015 - December 2015) and currently at Google, Inc.
- Dr. Bo Chen joined as Research Assistant Professor in June 2016.
- Dr. Debasis Ghosh (from FedEx participate in our weekly research meeting) and involve in research publications.
- Dr. Mike Nolen (our alumni comes from Jackson TN to participate in our weekly research meeting) and involve in Big Data research.
- Abhijit Kumar Nag (current Ph.D student)- working on Adaptive Multi-Factor Authentication
- Kul Prasad Subedi (current Ph.D student) – working on system security and pen testing
- Mustafa Hajeer (current Ph.D student) – working on Bigdata and cyber security
- Sujit Shrestha (current Ph.D student) – working on mobile device security and privacy issues
- Daya Ram Budhathoki (current Ph.D student) – working on security issues in Software Defined Networks.

- John Shrein (current MS student)
- Vamsi krishna Polam (current MS student)
- Adithya K Murthy (current MS student)
- Sharifa Begum (current MS student)
- Mona Mishra (volunteered in summer, join MS in Fall 2016)
- Rhythm Syed (UG summer intern from Purdue University)
- Lorrayne A Mallott (Staff)
- Erica Boyce (Staff)
- A list of advisory board members is available at http://www.memphis.edu/cfia/people/index.php.

Ph.D. student Mustafa Hajeer interned at Intel Corp. over Summer 2015 and is continuing to work there over the fall and spring, and will go back as an Intel employee after his Ph.D defense. As part of a team of systems engineers, he is developing end-to-end platform solutions for Intel's Data Center, Mustafa is also working on various areas, including developing methodology and flow for cutting edge storage and networking solutions around the following areas of Cyber security/information security and Bigdata.

Abhijit Kumar Nag won 1st Place for his research poster on An Adaptive Approach towards the Selection of Multi-factor Authentication at the 11th and 12th Annual Computer Science Research Day. He also received award at the University Research Forum (pictures below show receiving awards).

Undergraduate Student Success in Cyber Security Research

The Center for Information Assurance (CfIA) has established a successful student-centered research environment involving both undergraduate and graduate students. Most remarkably, this initiative has allowed for the interaction and collaboration of students across different disciplines, engaging not only undergraduate students within the computer science department, but those from Engineering, Communications, Business, and History departments working side-by-side with Ph.D. students and faculty. These students are involved in a number of diverse projects such as cutting-edge research in authentication to game-based puzzle exercises for education to research-driven training material for cybersecurity outreach activities.

(In order from left to right: Mathew Jackowski from Rhodes college, Berkeley Willis, Aaron Marshall, Dr. Dagupta, McKintrick Swindle, Robert Ebstrom, Rachel Brandon)

Student Team won Second place at CANSec Cyber Defense Competition

Cyber Security student team won second place in the prestigious **CANsec Cyber Defense Competition**, held in Little Rock Arkansas, on October 24, 2015. The participants as Blue Team have to manage services, report intrusions, and complete the challenges. The other teams (mostly organizers) act as White Team that enforce rules, setup infrastructures and as Red Team enumerate and exploit vulnerabilities in Blue Team services. The competition is held annually as a part of the CANsec workshop. The CANSec (formerly, KanSec) workshop has brought together researchers and practitioners in networking and security related fields in the central area of the US since spring of 2012, and has attracted attendees from all across the U.S.

The students competed against Cyber Security teams from several other Universities and Colleges across the U.S. before winning second place in the day-long competition. The goal of the competition was to provide students with a platform to apply theoretical knowledge into practice, and to obtain hands-on cyber security experiences. During the competition, the teams were asked to oversee a small corporate network, to manage all critical services, and to defend against external attacks. The University of Memphis winning team included two graduate students (Kul Subedi, Sujit Shrestha) and two undergraduates (Robert Edstrom, Nick Gordon) who are involved with the Center for Information Assurance (CfIA). “It was a valuable experience, and one I’m very glad to have been a part of” said Robert Edstrom, and another student on the team said “I think we all learned a great deal from working as a team”.

Students Participation National-level Competition:

The U of M team participated in Cybersecurity, Education & Diversity Challenge Week at the University of Connecticut on October 29, 2015. The following universities and organizations participated after preliminary selection.

Though our team could not reach to the top three positions, they performed exceptionally well in this **CyberSEED** national cyber security competition.

In addition, two undergraduate students received awards in poster presentations at 12th Annual Computer Science Research Day, 2016. They are **Robert Edstrom** got 1st Place for his research entitled Puzzle Based Learning in Cyber Security Education; and **Berkeley Willis** (with Graduate Partner: **Sujit Shrestha**), got 3rd position for his research on Web Application Security Exercise and Testing Platform.

CfIA Director and Co-Director's specific activities/achievements:

- During the academic year 2015-16, Prof. Dasgupta published 13 research papers (and 3 under submission) of which there are 4 journal articles, 1 book chapter, and 5 papers in international conference proceedings as well as 3 Technical Reports.

- Prof. Dasgupta is working with his research scholars (Arunava Roy and Abhijit Nag) in a Book Project titled A*dvances in User Authentication Systems*, publisher: Springer-Verlag (in preparation).
- Prof. Dasgupta also involved in 5 Ph.D Committees (three in Computer Science and two in Electrical Engineering and they are Abdullah Eid Abu Hussein, Daqi Dong, Md. Mahbubur Rahman, Mohammad A Sadi, Md Kamal Hossain and a number of Masters' committees. He mentored several graduate students in IA graduate certificate program.
- Prof. Dasgupta gave a presentation on Adaptive Multi-Factor Authentication (MFA) on 1st Annual Research Workshop on Advances & Innovations in Cyber Security, in University of Memphis, Memphis, TN on June 10, 2016.
- Prof. Dasgupta's Ph.D. student Abhijit Nag received 1st place in U of M's Student Research Forum held on April 1, 2016.
- Prof. Dasgupta's undergraduate student Robert Edstrom won 1st place in U of M's Student Research Forum held on April 1, 2016.
- Prof. Dasgupta gave an invited talk at the Computer Science Department, University of Tennessee, Knoxville, TN, and April 7, 2016 (Host: Dr. Qing Charles Cao).
- Prof. Dasgupta presented a research paper at 11th Annual Cyber and Information Security Research (CISR) Conference held at Oak Ridge National Laboratory, Oak Ridge, TN, and April 4 - 6, 2016.
- Prof. Dasgupta gave an invited talk in the Dept. of Computer Engineering & Computer Science at the University of Louisville, KY on March 25th (Host: Prof. Olfa Nasraoui).
- Prof. Dasgupta gave an invited talk at the special session on Partnering with Industry and Academia at T&E Workshop on March 17th, Arlington Virginia.
- Prof. Dasgupta gave an invited talk at Regional Symposium "Graduate Education and Research in Information Security",'GERIS'16, on March 8, 2016, at SUNY Binghamton University, Binghamton, New York.
- Prof. Dasgupta attended the National Cybersecurity Preparedness Consortium (NCPC) Principal's meeting at Washington DC on March 15, 2016.
- Prof. Dasgupta was interviewed by a local TV Channel (FOX 13) and telecast on Feb. 19, 2016.
- Prof. Dasgupta gave an invited talk on 5th International Conference on Fuzzy and Neural Computing, FANCCO-2015, India, December 16-19, 2015.
- Prof. Dasgupta gave an invited talk on Adaptive Multi-Factor Authentication (MFA) at the Department of Electrical Engineering and Computer Science and CASE Center, Syracuse University, Syracuse, NY 13224-5040 November 18, 2015.
- Prof. Dasgupta organized a Symposium on Computational Intelligence in Cyber Security (CICS) at IEEE Symposium Series on Computational Intelligence (SSCI) at Cape Town, South Africa, December 7-10, 2015.
- Prof. Dasgupta gave keynote speech at St. Louis at Cyber Security workshop (STL-CyberCon), University of Missouri-St. Louis, November 20, 2015.
- Prof. Dasgupta attended the NIST-NICE conference at San Diego from November 1-4, 2015
- Prof. Dasgupta gave an invited talk at 9th International Research Workshop on Advances and Innovations in Systems Testing at FedEx Institute of Technology, the University of Memphis, and October 20, 2015.

- Prof. Dasgupta served as a Program Committee (PC) member of International Conference on Green Computing and Internet of Things (ICGCIoT) organized by GCET at Greater Noida, India, in October 8-10, 2015.
- Prof. Dasgupta served as a panelist at the session on Cybersecurity 2015 & Beyond at 29th Annual SIM Memphis Strategy Series, Wednesday September 30, 2015.
- Prof. Dasgupta gave an invited talk at DHG Cyber Security Forum at Memphis (Host: Eric J Spiegel) on August 19, 2015.
- Prof. Dasgupta served as a Program Committee (PC) member of the Second BRICS Congress on Computational Intelligence and the Sixth International Conference on Swarm Intelligence (ICSI 2015) jointly held in Beijing, China, from June 26 to 29, 2015.
- Prof. Dasgupta gave an invited talk Cyber Security Workshop at Arkansas State University, Jonesboro, AR, on August 14, 2015.
- Prof. Dasgupta gave Keynote Speech at International Conferences in Advances in Information Technology, Boroda, India on June 1, 2015.
- Prof. Dasgupta served as a Technical Program Committee (TPC) member for the 2015 IEEE Congress on Evolutionary Computation (IEEE CEC 2015) held in Sendai, Japan, May 25-28, 2015.
- Prof. Dasgupta gave a Keynote speech at Queen's University Graduate Computing Society Conference, Kingston, Canada sponsored by the ACM Distinguished Speaker program, May 7, 2015.
- Prof. Dasgupta offered a Tutorial on "Puzzle-Based Learning in Cyber Security Education" at the 2015 EDUCAUSE Security Professionals Conference at the Hilton Minneapolis, May 4-6, 2015 in Minneapolis, MN.
- Prof. Dasgupta is an Advisory Board of Geospatial Data Center (GDC) at Massachusetts Institute of Technology (MIT) since 2012.

- Prof. Simon gave two cyber ethics presentations during the year.
- Prof. Simon was a presenter on “Cybersecurity Employment Pipelines: Successful Paths to Careers in Cybersecurity” at the 1st Annual Research Workshop on Advances & Innovations in Cyber Security, in University of Memphis, Memphis, TN on June 10, 2016.
- Prof. Simon engaged in recruiting for scholarship grants for students interested in military careers.
- Prof. Simon received the designation as the U of M ISACA academic advocate, which has led to initiating new course content where she teaches COBIT 5 content. She is a member of the Memphis ISACA chapter.
- Prof. Simon become a member of the Greater Memphis IT Council and attends their quarterly meetings, which gives her some contacts with a variety of businesses locally.
- Prof. Simon is an active member of the Memphis Chapter of the Society for Information Management (SIM), which meets monthly and provides an annual “Strategy Series” that is very widely attended.
- Prof. Simon is an author on a research paper being presented at the annual conference of the Association for Information Systems (AIS) in August. It is entitled *Security Risks Related to Employee “Extra-Role” Creation of an “Online-persona***”.** This paper will be submitted later to an MIS journal for possible publication.
- Prof. Simon is involved in another research project which is in progress and is related to hacker motivations and business processes being used to protect against hackers.

- Prof. Simon has received two teaching awards this past year – one from the Fogelman College and one from the department's Advisory Council.
- Prof. Simon manages the BIT department's very successful graduate certificate program in information assurance management and supervises summer internships for numerous international students who are in this certificate program.

CfIA hosts GenCyber Bootcamp for Middle and High School Students in Summer 2016:

The National Security Agency (NSA) and the National Science Foundation (NSF) funded the University of Memphis through the 2016 GenCyber Bootcamp. There are two 1-week sessions for middle and high school students on cyber safety. The camp covers various aspects of Cyber Hygiene and students learn about privacy, security, and safe browsing while on the internet. They are introduced to cyber ethics and engage in hands-on sessions that allow them to experience real-world data security issues. Students have opportunities to meet cyber experts and industry professionals. The week culminates in a competition where students demonstrate online activities following best practices. This federally funded camp is free for all participants. The high school camp dates are June 20 – June 24 and middle school is July 25 – July 29. This is a unique opportunity for students to learn about Cyber programs at the University of Memphis, a nationally-designated Center for Academic Excellence in Information Assurance. To register visit http://www.memphis.edu/cfia/projects/gencyber.php

Prof. Dipankar Dasgupta was featured on a WMC Action News 5 segment on July 2nd, publicizing the upcoming GenCyber Boot Camp for middle-school students (shown in picture below and two camps

High School Boot Camp June 20-24th

WMC TV Channel Action News 5

Middle School Bootcamp July 25-29th

Our both Bootcamps for high and middle school students were very successfully completed with fun, learning and competitions. Detailed information about the summer camps (Photo Gallery, awards, each day presentations and activity summary,) is available at our Gen Cyber website (http://www.memphis.edu/cfia/projects/gencyber.php).

Formation of CAST: Cluster to Advance cyber Security & Testing

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 will further expand collaborative effort of experts who lead research, education, and technology transfer in cyberspace by pulling together industry partners and research collaborators from a wide range of backgrounds and disciplines (figure

below illustrates the CAST mission). While both centers (CfIA and STEP) will maintain their independent operations in their areas of expertise, CAST will venture new opportunities in the ever changing cyber security and testing challenges that arise within corporations, governments, and other organizations across the Internet-connected world.

- Provide proactive leadership of the region's response to constantly shifting cyber security challenges.
- Inform public policy and find cutting-edge solutions to protect the information of private corporations and Tennessee government agencies.
- Help the Department of Defense and national corporations with software testing education and research.

FedEx Institute of Technology Invests in Cybersecurity Research

As part of the University of Memphis' push to develop strong research competencies in cybersecurity, the FedEx Institute of Technology has made announcement on December 8, 2015 on research awards totaling $190,000 for 12 interdisciplinary projects in the area. They were designated as Cybersecurity Research Fellows of the FedEx Institute of Technology. The 21 recipients involved include researchers from 11 academic departments in seven colleges and schools across the University. They include the Herff College of Engineering, College of Arts & Sciences, Fogelman College of Business & Economics, College of Education, School of Public Health, School of Urban Affairs and Public Policy and University College. Under the FIT-CAST program, research leaders are encouraged to collaborate with junior faculty and graduate students to help make the University the focal point for cybersecurity research excellence in the state of Tennessee. Interdisciplinary perspectives are central to innovation and sense-making when faced with complex challenges like cybersecurity.

Here is the list of research projects and researchers involved:

1. *Investigation and Testing of Cybersecurity - Protective Relay* (Mohd Hasan Ali, Dipankar Dasgupta)
2. *Automated Document Classification - Sensitive Information Disclosure* (Zhuo Lu, Dipankar Dasgupta, Su Chen)
3. *Cloud Computing Security and Privacy Assessment* (Sajjan Shiva)
4. *Security Online - Healthcare Communities* (Naveen Kumar, Deepak Venugopal, Robin Poston, Dipankar Dasgupta)
5. *Cognitive Neuroscience - Security Behaviors in Information Security Contexts* (Thomas Stafford, George Deitz)
6. *Technology Dependency Perspectives on Cybersecurity Failures* (Thomas Stafford, Sanderford Schaeffer)
7. *Exploring a Data-Centric Approach to Securing Smart Homes* (Lan Wang)
8. *Investigating Characteristics of Cyberbullying in Higher Education* (Mitsunori Misawa)
9. *The Effects of Gamification on Security Compliance* (Bill Kettinger, Chen Zhang, Ruby Booth)
10. *Cybersecurity Employment Pipelines: Successful Paths to Careers in Cybersecurity* (Judy Simon, Sandi Richardson, Ruby Booth)
11. *Criminology and Cyber Security Dimensions of Public Health in Urban Environments* (Marian Levy, Andy Kitsinger, Debra Bartelli, KB Turner)
12. *Privacy Data Impact on Retail Consumers and Suppliers* (George Deitz, Mohammed Amini)

FIT-CAST Activities:

- December 3rd, 2015: Cybersecurity Lightning Talks: an evening of cybersecurity research project presentations with special guest speaker: Special Agent Tim Marsh of the Memphis FBI Division.
- February 1-5, 2016: Cybersecurity Certificate Course. This foundational program in cybersecurity is designed to cover the fundamentals of cybersecurity and cybersecurity vulnerabilities (IT background required).
- April 26, 2016: Hosted Cyber Incident Response & Adaptive Defenses by RSA sponsored by InfraGard.
- June 9-10, 2016: 1st Annual Research Workshop on Advances and Innovations in Cyber Security. The workshop was a mixture of presentations and open discussions. Attendees from both academia and industry benefited greatly from the open exchange of ideas and methodologies on cyber security. The Cyber Security Research Workshop featured a half day of tutorials on Thursday, June 9 and a full day of interdisciplinary research paper presentations and industry panels on Friday, June 10, with an evening reception to follow.

Cyber Security Job Market:

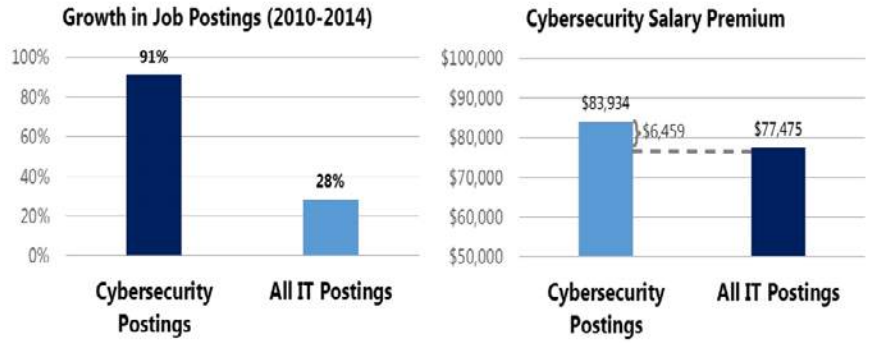
The growing complexities and sophistication of cyber-attacks and threats have prompted government agencies, financial, retail, telecom, and manufacturing sectors to invest in enhancing their cybersecurity efforts in order to protect critical information and assets.

"Cybersecurity Skills Are in High Demand, Yet in Short Supply. More than 50 percent of organizations today seek advice or consulting services to help with their security strategies" – Cisco Report, 2015.

- In 2014, there were 238,158 postings for cybersecurity-related jobs nationally. Cybersecurity jobs account for 11% of all IT jobs.
- Cybersecurity postings have grown 91% from 2010-2014. This growth rate is more than faster than IT jobs generally.
- Cybersecurity posting advertise a 9% salary premium over IT jobs overall.
- Cybersecurity job postings took 8% longer to fill than IT job postings overall.

- For example, in the U.S., employers posted 49,493 jobs requesting a CISSP, recruiting from a pool of only 65,362 CISSP holders nationwide.[4]

The latest research from MarketResearch.com forecasts the global cybersecurity market to jump from $106.32 billion in 2015 to $170.21 billion by 2020. The demand for cybersecurity talent is outstripping supply as evident in charts below[5].



Report Summary:

Directed by Dr. Dipankar Dasgupta, professor of computer science, and Dr. Judith Simon, professor of management information systems (now business and information technology), 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, 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 working at the center were offered high-valued jobs and are in great demand in the job market. From an outside view of this center's successful goal oriented structure, it really reconfirms the University of Memphis's slogan "Driven by doing", and doing in collaboration is something the CfIA does beyond comparison.

[4] According to the International Information System Security Certification Consortium, Inc., (ISC)²® membership counts as of July 14, 2015.
[5] Reference: http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf