Women in CYBER SECURITY

Conference 2016

MARCH 31 - APRIL 2
DALLAS, TEXAS

Funded by a National Science Foundation Grant
Award #1303441

Welcome Note

“It only makes sense….”

Half of the US workforce is women and yet only 8-11% is in cybersecurity. So, to address the undeniable critical shortage of cybersecurity professionals in this country, it only makes sense to recruit from the other half …. to create opportunities and pathways such that more women can consider cybersecurity as a viable career option! Not to mention the power of diversity in solving complex challenges unique to this field.

The WiCyS conference was created out of this common sense (with support from National Science Foundation, Award# 1303441) in 2014. Since then WiCyS has become a community of opportunity/advice/answer seekers and providers, mentors and mentees, speakers and listeners, and most importantly, a community of peers.

I am thankful for the support of the WiCyS Steering Committee, advisory board and the 2016 planning team. I want to express my most sincere gratitude to Drs. Janell Straach and Bhavani Thuraisingham, Co-chairs from The University of Texas at Dallas and their team for being a wonderful local host in Dallas. I am blessed to have my Tennessee Tech team who has worked very hard to ensure you have a great circle of peers around you and your precious time is well spent at WiCyS 2016.

This conference has only been possible because of the generous support we have received from our community, industrial and academic sponsoring partners and the federal government. This is a great example of a successful partnership between academia, government and industry, where we have joined hands with a mission to increase participation of women in the cybersecurity workforce.

We are honored to have YOU with us this year. Please take full advantage of the program from the beginning to the end. Attend as many sessions as possible, get to know as many others as possible, learn about trends and techniques, find out about resources and opportunities. Ask names, ask questions, share stories, make friends, find mentors…. sleep and work can wait…. it is not every day you get to meet so many others like you!!

I hope you will leave informed and inspired……

Dr. Ambareen Siraj
Director, Cybersecurity Education Research and Outreach Center
Associate Professor, Computer Science Department, Tennessee Tech
WiCyS Founder and Chair

2016 WiCyS Members

WICYS ORGANIZERS

Dr. Ambareen Siraj (Founder and General Chair)
Director, Cybersecurity Education Research and Outreach Center
Associate Professor, Computer Science Department, Tennessee Tech

Dr. Bhavani Thuraisingham (2016 Co-chair)
Executive Director, Cyber Security Research and Education Institute
Professor, Computer Science, The University of Texas at Dallas

Dr. Janell Straach (2016 Co-chair)
Senior Lecturer, Computer Science, The University of Texas at Dallas

WICYS STEERING COMMITTEE

Dr. Melissa Dark
Associate Dean, Purdue University

Dr. Deborah Frincke
NSA/CSS Director of Research at National Security Agency

Alison Massagli
Senior Cybersecurity Strategist, Trustworthy Computing Division, Microsoft

Dr. Cynthia Irvine
Director of the Center for Information Systems Security Studies and Research at Naval Post Graduate School

Jennifer Henley
Director of Security, Facebook

Sherri Ramsay
Senior Advisor, CyberPoint International

Marisa S. Viveros
Vice President, Strategy and Business Development at IBM Global Telecom Industry

WICYS 2016 ADVISORY BOARD

Dr. Terry V. Benzel
Deputy Director, Computer Networks Division, Information Sciences Institute (ISI), University of Southern California (USC)

Dr. David Dampier
Professor, Computer Science & Engineering, Director, Center for Computer Security Research & National Forensics Training Center, Mississippi State University

Dr. Dawn Beyer
Fellow at Lockheed Martin

Dr. Elizabeth K. Hawthorne
Senior Professor of Computer Science, Union County College

Jim Michaud
President, Human Resources Strategies

Dr. L. Jean Camp
Professor, School of Informatics, Indiana University, Bloomington

Dr. Susanne Wetzel
Associate Professor, Stevens Institute of Technology

Betsy Bevilacqua
Information Security Risk Manager at Facebook

Mona Sana
Technical Staff, ViaSat Inc.

Ruthe Farmer
Director of Strategic Initiatives, National Center for Women & IT (NCWIT)

WiCyS 2016 CONFERENCE COMMITTEE

PROGRAM COMMITTEE

Chris Carlson
Secure Engineering Lead Developer, IBM

Claire Vishik
Trust & Security Technology and Policy Director, Intel Corporation

Litany Lineberry
Instructor of Computer Science, Voorhees College

Malek Ben Salem
Research Manager, Accenture

Morgan Zantua
CREATES Architect, MCL Recruiter

Sofia Bekrar
Senior Security Researcher, VUPEN

Dr. Sumita Mishra
Associate Professor, Rochester Institute of Technology

Dr. Yan Bai
Associate Professor, Institute of Technology, University of Washington Tacoma

SCHOLARSHIP COMMITTEE

Kelley Goldblatt
Cyber Intel Analyst, Michigan State Police

Nicole Janecka
Enterprise Group Legal, Hewlett Packard Enterprise

Tolu Onireti
Ernst & Young

Kimberly Simon
Security Analyst, State Farm

Dr. Suzanne Mello-Stark
Associate Teaching Professor, SFS Program Manager,
Worcester Polytechnic Institute

Jill Blanchar
Information Security Executive, Bank of America

Don Vogel
Senior Lecturer, Computer Science, The University of Texas at Dallas

POSTER SESSION COMMITTEE

Dr. Chutima Boonthum-Denecke
Associate Professor of Computer Science, Hampton University

Emily Brown
Cyber Systems Engineer, Johns Hopkins Applied Physics Laboratory

Dr. Ni An
Research and Teaching Assistant, Drexel University

Dr. Julia Bell
Associate Professor of Computer Science, Walters State Community College

Dr. Khadija Stewart
Associate Professor of Computer Science, DePauw University

WORKSHOP COMMITTEE

Dr. Brandeis Marshall
Associate Professor, Spelman College

Julia Knecht
Engineering Security, Adobe

SPONSORSHIP COMMITTEE

Jennifer Eiben
Community Outreach Manager, CyberPoint International

WiCyS 2016 CONFERENCE COMMITTEE

SPEED MENTORING SESSION COMMITTEE

Anna Ruecker
Privacy Program Manager, Facebook, Inc.

Debbie Taylor Moore
CEO, Cyber Zephyr

Colleen Riccinto
Founder & CEO, Cyber Talent Search

OUTREACH COMMITTEE

Kathleen Smith
Chief Marketing Officer, ClearedJobs.Net

Katie Kennedy
Research Analyst, Cognitio Corporation

CAREER FAIR COMMITTEE

Hosi Karzai
Project Manager, Tennessee Tech University

Linda Avers
Talent Acquisition, Associate Manager, Lockheed Martin Corporation

LOGISTICS COMMITTEE

Rhonda Walls
The University of Texas at Dallas

Suzanne Henry
Tennessee Tech University

CAE LIAISON

Denisha Jackson
CAE Program Manager, NSA

SFS LIAISON

Kathy Roberson
SFS Program Manager, OPM

PROFESSIONAL ORGANIZATION LIAISON

Victoria Thornton
Technical Recruiter, Ionic Security Inc.

CISSE LIAISON

Tamara Shoemaker
Operations Manager, CISSE

INDUSTRY LIAISON

Jessica Gulick
President of KATZCY

GOVERNMENT AGENCY LIAISON

Bill Newhouse
Cybersecurity Convener, NIST, NICE

COMMUNITY COLLEGE LIAISON

Dr. Patty Anderson
Dean, Business & Technology Division, Volunteer State Community College

SOCIAL MEDIA COORDINATOR

Stephanie Silva
AmeriCorps Technology VISTA,
Barbara Bush Houston Literacy Foundation

Jeremy Ey
Systems Administrator, Information Technology Services,
Tennessee Tech University

Thursday, March 31, 2016

Time/ Location	Topic	Presenter(s)
12:00 - 7:30 pm Reg. Desk	**Registration Pick-Up**	
2:00 - 4:00 pm	**Workshop Series 1***	
INNOV-AB	**Workshop 1.1: To Catch a Thief: Think Like One** It's easy to get drawn into thinking that we can address security with tools or policies, but the unfortunate truth is that the only way to be truly effective long-term addressing security issues is by learning to think like the enemy. In this workshop, we will talk about hackers, their motivations, tools and techniques, the Pyramid of Pain, dumb security ideas, and more. We will execute some sample hacks and will move beyond "stamp collection security" to understanding the secure computing principles illustrated.	**Christina Carlson** (Target Inc.)
Maverick	**Workshop 1.2: GenCyber Summer Camps for Students and Teachers** GenCyber provides free summer camps for K-12 students and teachers to raise awareness, interest, and adoption of cyber security principles and trends. This session will provide an overview and history of the program and details on the application process, funding model, curricular successes, and future direction. With 100 camps scheduled for 2016 and additional future growth anticipated, all conference participants are encouraged to attend and learn how to get involved in GenCyber.	**Steven LaFountain** (NSA), **Tony Coulson** (California State University, San Bernardino), and **Ashley Podhradsky** (North Dakota State University)
INNOV-CD	**Workshop 1.3: Exploitation Development 101** This workshop will introduce the participants to the basics of stack-based x86 exploitation development. Students will learn what remote code execution is, why it's bad, and how to prevent it. During the course, students will also learn basic methods for developing a working exploit for a known vulnerability. The end goal will be for students to gain remote code execution on a virtual machine, by exploiting a known vulnerability, using an exploit they craft. Prereqs: Basic Python, Laptop w/VMware or VirtualBox installed. Provided: Attacker/Target virtual machines (.ova format).	**Lilith Wyatt** (Cisco)
4:30 - 6:30 pm	**Workshop Series 2***	
INNOV-AB	**Workshop 2.1: CyberSecurity Club: 101 from Inception to Installment and Beyond** It is difficult to spark interest in cybersecurity among students with only classroom instructions, which are more on rules than tools. Also, many schools do not offer dedicated security classes. One of the solutions to address this issue is to establish a university cybersecurity club to increase students' interest, involvement and knowledge in cybersecurity. This workshop will share strategies and resources for creating and sustaining a cybersecurity club. It will address how to create and manage a club from scratch, motivate and engage students into participating in different club activities, and find sponsorships and mentorships through networking.	**Dustin Gardner** and **Vitaly Ford** (Tennessee Tech), **Lindsay Hefton** and **Kelly Luk** (Texas A & M University)

*Registration required for each specific workshop. If space is available, walk-in registrations will be taken on a first come first serve basis for workshops.

Time/ Location	Topic	Presenter(s)
Maverick	**Workshop 2.2: Tools and Strategies for Cybersecurity Education** Cybersecurity education still struggles with a lack of tools and support to help educators successfully teach security concepts. Challenges include a large amount of course material that must be taught within tight timeframes, a shortage of real-world case studies and teaching materials, and a scarcity of affordable hands-on cybersecurity lab environments. This workshop will address these questions: Where is cybersecurity education today? How can educators be supported to increase the level of cybersecurity course content adoption? The goal of the workshop is to support faculty that may have interest incorporating cybersecurity curriculum content into their course syllabuses and provide awareness of the Cyber Education Project for the 'Cyber-Sciences' degree program.	**Scott Buck** (Intel)
INNOV-CD	**Workshop 2.3: Hiring for Diversity in CyberSecurity** This workshop will provide some practical strategies to find, recruit, and hire more women in cybersecurity. It will also delve into how to retain women already working in the field. This workshop is designed for people who have a role in recruiting, HR, or just those that want to take helpful notes back to HR departments about things they could be doing better. Expect to learn the following: how to write better job descriptions to be more inclusive, tips on better resume review, ideas about better sourcing of candidates, conducting thoughtful and equitable interviews, and using metrics to find out where you are losing women in the chain of hiring.	**Brooke Hunter** (New America/Open Technology Institute), **Sandra Mcleod** (Cisco Systems), and **Jaqueline Koehler** (Cisco Systems)
5:00 - 6:30 pm Harvesters	**Pitch Your Idea (For Educators)** Looking for external support to take your idea on cybersecurity education/research/outreach one step further? Want to seek guidance? You can sign up for a 7-minute feedback opportunity.	**NSF, DHS,** and **NSA**
7:30 pm Various Rooms	**Networking Socials**	

Friday, April 1, 2016

Time/ Location	Topic
8:00 am - 1:00 pm Reg. Desk	**Registration Pick-Up**
8:30 - 10:00 am	**Breakfast**
ENTRPS 1-6	***Welcome*** ***Opening Remarks:*** **Victor Piotrowski** (National Science Foundation) ***Keynote:*** **Jillian Munro** (SVP, Fidelity Investments, Enterprise Cybersecurity) **The Business of Cybersecurity** Cybersecurity is no longer just a technology problem, it has become a business differentiator. As the topic is discussed around the table of company boards and government task forces, the face of Cybersecurity professionals is changing as well. The speaker will share her experiences and observations she's made throughout her career of the different facets of that new face, highlighting how non-traditional skills now apply in the area of Cybersecurity.

Time/ Location	Topic	Presenter(s)
10:00 - 10:45 am	**Session: 5 Minute Lightning Talks**	
ENTRPS 1-6	**Online Cybersecurity Resources for Skill Development and Outreach** Self-study has great value, and directly addresses challenges such as funding, traveling, training and constricted programs. This talk is centered around finding awesome online security resources on a variety of subjects for the purpose of building individual and group skills/awareness.	**Michelle Hardesty** (University of Cincinnati)
	CyberCorps®: Keeping Peace in Cyberspace This session will provide information on the CyberCorps®: Scholarship for Service (SFS) program: What it is, who can apply, which universities have the SFS Scholarship, and how to find out more.	**Kathy Roberson** (Office of Personnel Management)
	Nobody Expects the Spanish Inquisition! This talk will present surprising ways a security internship 3000 miles away has had a long-lasting impact on an aspiring professional's career goals.	**Andrea Frost** (Western Washington University)
	The Secret Life of a Code: How Reverse Engineering Exposes its Hidden Agenda Although Reverse Engineering has a theoretical foundation, because of the complexity of programs it can only be implemented with tools for automatic code analysis. This talk will provide pointers about how to use these tools, and how to interpret the pseudocode.	**Aranya Ajith and Rebecca Powell** (Florida State University)
	What It Takes to Start Up a Start-up First you had the Wild West, then the Wolf of Wall Street… welcome to the era of the Hacker. Cybersecurity is one of the fastest growing tech careers and the number of companies and VC dollars backing it prove it's a great space to be in. In a mere 5 minutes, learn what it takes to start up a start-up, plus the special nuances that are must-haves for a newly burgeoning cybersecurity software company.	**Rani Khan** (PRAESIDIO)
	Establishing a Curriculum to Help Women with a Non-Computer Science Background to Succeed in Cybersecurity It is a big challenge to develop a comprehensive curriculum to train women who do not have computer science backgrounds to become cybersecurity professionals. This talk will present the curriculum initiatives at Columbus State University in this regard.	**Yien Wang** (Columbus State University)
	The Criminal Behind the Screen: The Role of Criminology in Cybersecurity Cyber criminology seeks to unmask the criminals who maliciously use technology for deviant purposes. This is of tremendous value to law enforcement for strengthening proactive and reactive online investigations.	**Jordana Navarro** (Tennessee Tech)
10:45 - 11:00 pm	**Coffee Break**	
11:00 am - 12:30 pm Foyer	**Student Poster Session**	
11:00 - 12:30 pm Maverick	**Resumé Clinic**	
12:30 - 2:00 pm	**Lunch**	
ENTRPS 1-6	***Keynote:*** **Heather Adkins** (Google) **From the Incident Response Mines** Incident Response: a field of mystery and intrigue, where the front-lines are fraught with peril and the rewards are high. Heather Adkins will share experiences on entering the mines, how to navigate them, and what treasure looks like on the other end.	

Time/ Location	Topic	Presenter(s)
2:00 - 2:45 pm	**Distinguished Speakers Session**	
ENTRPS 7	**Cybersecurity Research: Now and Tomorrow** Researchers from various organizations will share their perspective of research trends and needs in this field and their journey along the path.	**Douglas Maughan** and **Ann Cox** (Department of Homeland Security), **Laura Tinnel** (SRI International), and **Elena S. Peterson** (Pacific Northwest National Laboratory)
ENTRPS 8	**Cybersecurity - Where Are the Girls?** Dr. Taylor will talk about how her career in cybersecurity evolved, from writing software for the racetracks to teaching secure coding to college students. She will talk about the importance of bringing more women to the field and also give tips on surviving and thriving in a male dominated industry.	**Blair Taylor** (Towson University)
INNOV BR	**So You Want to Work in Privacy?** A privacy compliance director and an engineer discuss what it means to work in the rapidly-growing field of privacy and user data protection: the day-to-day work, the challenges, and the victories that keep us going and ensure our customers' privacy is protected.	**Malita Barkataki** (Yahoo), and **Alisha Kloc** (Google)
2:45 - 3:30 pm	**Session: Technical Presentations**	
ENTRPS 7	**A Novel Remote Access Testbed for Cyber-Physical Systems (CPS)** Several authoritative government reports and technical literature have documented increasing concerns for highly sophisticated, advanced persistent cyber threats on critical infrastructures like the power grid. Cyber-Physical System (CPS) Security test-beds are essential elements in the R&D ecosystem to develop and validate novel CPS security tools and algorithms for securing the grid and making it attack-resilient. This presentation will briefly describe existing CPS security test-bed efforts, their suitability with respect to providing user access for remote experimentation and a novel remote access CPS security test-bed that enables CPS security experimentation for the power grid.	**Sujatha Krishnaswamy** (Iowa State University)
ENTRPS 8	**The Cybersecurity Profession in Higher Education** Using data from the EDUCAUSE Center for Analysis and Research and related lessons learned from the EDUCAUSE Cybersecurity Initiative, this session will explore information security professional roles at higher education institutions, discuss higher education CISO leadership pathways, and introduce participants to the resources of the EDUCAUSE Cybersecurity Initiative and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC).	**Joanna Grama** (EDUCAUSE) and **Kim Milford** (REN-ISAC)
INNOV BR	**Non-traditional Career Paths for Women in Cybersecurity** This presentation will share various career paths and experiences as federal government attorneys with key responsibilities in developing national cyber security policy for the telecommunications industry and public safety sector at the Federal Communications Commission. It will discuss different perspectives on the important role federal agencies outside of the U.S. national security community play in keeping our nation safe, the cyber-related role and challenges faced by telecommunications service providers and public safety organizations and the interdisciplinary skills needed for success.	**Erika Olsen** and **Dana Zelman** (Federal Communications Commission)
3:30 - 5:30 pm Aviators	**Career & Graduate School Fair with Refreshment Break**	

Time/ Location	Topic	Presenter(s)
3:30 - 5:30 pm	**Workshop Series 3***	
ENTRPS 7	**Workshop 3.1: Big Data Analytics and Cloud for Cyber Security Applications** The workshop will provide an overview of big data analytics and cloud data management techniques to solve cyber security problems such as malware detection. We will also describe the various techniques and introduce students to data sets that they can use to carry out experimentation.	**Dr. Murat Kantarcioglu** and **Dr. Bhavani Thuraisingham** (The University of Texas at Dallas)
ENTRPS 8	**Workshop 3.2: No Skating on Thin Ice** Cybersecurity is a field that is strewn with challenges for those seeking a successful career. Those challenges often mean a perilous journey for women who are laboring to succeed in this male-dominated field. Among the topics discussed in this presentation will be how to overcome the challenges of breaking the glass ceiling in cyber organizations, how to hang on to the glass cliff after success is achieved and how to move beyond the self-doubt of impersonating greatness when approaching the pinnacle of success. This presentation will include a checklist of takeaways to promote future reflection.	**Jane Leclair** and **Denise Pheils** (National Cybersecurity Institute at Excelsior College)
5:30 - 6:15 pm	**Session: Panels**	
ENTRPS 7	**K-12 Outreach in Cybersecurity Education: Successes and Challenges** With extreme shortages in the cybersecurity pipeline, it is crucial to recruit new students into the fields of computing and cybersecurity through K-12 outreach initiatives. This panel highlights K-12 Cyber Outreach Programs in Alabama (University of South Alabama: USA), Hawaii (The University of Hawaii Maui College), Texas (Houston Independent School District: HISD) and California (CalPoly CyberPatriot program) and shares strategies that have been successful and challenges that need to be addressed. In Alabama, USA is taking an active approach in recruiting new students into the fields of computing and cybersecurity through their K-12 STEM Partner School Program, which is expected to be modified and expanded into the public school system. In Texas, students gain self-confidence and awareness of cybersecurity careers while building cybersecurity skills via CyberPatriots, direct mentorship from HISD security staff and by engaging with the wider cybersecurity community partners such as Mozilla.	**Debra Chapman** (University of South Alabama), **Dan Manson** (Cal Poly Pomona), **Diana Bidulescu** (Houston Independent School District), **Debra Nakama** (University of Hawaii Maui College)
ENTRPS 8	**The C5 Project: Potential to Improve our Nation's Cybersecurity Education** Catalyzing Computing and Cybersecurity in Community Colleges, C5, a project supported by the National Science Education, NSF, and led by Whatcom Community College in WA aims to improve undergraduate cybersecurity education at community colleges across the nation and, in turn, strengthen this country's cybersecurity workforce. How is this to be accomplished? C5 has two goals, one of significantly increasing the number of Centers of Academic Excellence - 2 Year, CAE2Y institutions, and two of creating an introductory course that augments cybersecurity with computer science topics and vice versa. This panel will discuss the importance and meaning of the CAE2Y institutions and about the new security infused programming course.	**Elizabeth Hawthorne** (Union County College), **Deanne Wesley** (Forsyth Technical College), **Blair Taylor** (Towson University), and **Melissa Dark** (Purdue University)
INNOV BR	**Data Science of Mentoring to Drive Growth in a Cybersecurity Career** This panel will focus on how to develop a productive mentoring relationship that leads to growth in a cybersecurity career. Constant career growth to remain relevant both in the vertical and horizontal career path is crucial in the ever evolving cybersecurity field. Have you ever wondered why you need a mentor to grow or how can you be an effective mentor? How does a mentor impact your career progression?	**Tolu Onireti** (Ernst & Young), **Deirde Warner** (Cisco), and **Anna Ruecker** (WISP)
6:15 - 7:45 pm	**Dinner**	
ENTRPS 1-6	***Keynote:*** **Yael Kalai** (Microsoft) **Delegating Computation** Cloud computing, computations and data are increasingly being delegated to powerful remote servers. This brings new computational challenges: How do we ensure privacy? How do we guarantee that computations are performed correctly? This talk mainly focuses on the latter question.	

*Registration required for each specific workshop. If space is available, walk-in registrations will be taken on a first come first serve basis for workshops.

7:45 - 8:30 pm ENTRPS 1-6	**Speed Mentoring Session**	
8:30 - 9:30 pm ENTRPS 7 & 8	**Social Activity**	

Saturday, April 2, 2016

Time/ Location	Topic	Presenter(s)
8:30 - 9:45 am	**Breakfast**	
ENTRPS 1-6	***Opening Remarks:*** **Regina Wallace-Jones** (Facebook) ***Keynote:*** **Shelley Westman** (IBM Security) **From Law to Cybersecurity: What I learned on my journey.** Unique career path from Law into the field of Cybersecurity as well as the lessons she learned along the way.	
9:45 - 10:15 am	**Session: 5 Minute Lightning Talks**	
ENTRPS 1-6	**5 Ways Serving in Nonprofit Can Help Your Cybersecurity Career** There is enormous opportunity for nonprofit service in security, and this talk will increase awareness of these to both give back and also build strong skillsets.	**Margaret Morton** (AFCEA Founders Chapter)
	Building a Security-sustaining Security Community The objective of building a community of Security Advocates is to embed security knowledge and practices into each individual in order to scale anywhere. Find out how we can collaborate and leverage with each other to build such a community of like-minded people.	**Alka Gupta** (Cisco)
	Detecting The Mismatch between Privacy Policy and Android Application Code With the increase in market share for the Android operating system, comes an increase to end user privacy risk as mobile applications (apps) built for the Android have access to sensitive personal information about users' locations, contacts, and unique device information. This talk will present contributions in protecting privacy for Android users.	**Jianwei Niu** (University of Texas San Antonio)
	Cyber Intelligence: An Emerging Specialty Focusing on Analysis of Cyber Threats and Actors With the explosive proliferation and increased sophistication of data breaches, imagine yourself as a cyber intelligence specialist or cyber analyst who is an essential member of a cyber security team. This talk will provide an overview of cyber intelligence and methodologies for profiling cyber threat actors.	**Edna Reid** (James Madison University Intelligence Analysis Program)
10:15 - 10:45 am	**Group Picture Session (Location to be announced)**	

Time/ Location	Topic	Presenter(s)
10:45 - 11:30 am	**Distinguished Speakers Session**	
ENTRPS 7	**What's Next: Navigating the Dynamic Cyber Landscape with Impact** Industry leaders from Booz Allen Hamilton and Intel discuss the power of collaboration in addressing cyber threats and vulnerabilities. They share their personal journeys to cyber leadership and the exciting work Booz Allen Hailton and Intel are pursuing through their partnership.	**Patricia Goforth** (Booz Allen Hamilton) and **Allison Cerra** (Intel)
ENTRPS 8	**Strategies for Preparing a Future Cybersecurity Workforce** Cybersecurity workforce development is a prominent national security issue, and the lack of cybersecurity talent is a problem that permeates both the public and private sector. DHS and NSA will discuss comprehensive cybersecurity strategies being spearheaded by their respective departments to attract and retain the cybersecurity workforce.	**Renee Forney** (Department of Homeland Security) and **Lynne Clark** (National Security Agency)
INNOV BR	**What Really Matters** Two cybersecurity leaders will share their best practices and lessons learned for succeeding in this industry. Resources for entering and progressing in the cybersecurity field will also be provided.	**Michele Myauo** (Microsoft) and **Christina Carlson** (Target)
11:30 - 11:45 am	**Refreshment Break**	
11:45 - 12:30 pm	**Session: Technical Presentations**	
ENTRPS 7	**Security Study and Comparative Analysis of Mobile Programming Languages and Their Security Mechanisms** This presentation discusses a comparative analysis of a subset of OWASP top ten mobile vulnerabilities and seeing how Swift, Objective-C and Android programming languages safeguard against these risks and how the built-in platform security mechanisms for Android and Apple for the chosen subset of OWASP vulnerabilities compare when placed side-by-side.	**Vanessa Santana** (Iona College)
ENTRPS 8	**Malware Analysis - An Undergraduate Course** Malware analysis is the process of examining malicious software to understand the nature of their threat. This process requires a multifaceted set of skills and knowledge including: operating systems concepts, programming (high level and low level), networking concepts, solving puzzles and connecting the dots. Security companies are continuously looking to hire skilled malware analysts in order to develop ways of blocking malware. Few undergraduate programs in the US include malware analysis in their curriculum.	**Areej Albataineh** (Our Lady of the Lake University)
INNOV BR	**Save Your Keys in Hardware: Hardware Security Module** Irrespective of all the encryption, storing your secrets in software is no longer perfectly secure. This talk will provide an Introduction on Hardware Security Module (HSM), a secure alternative (hardware) to store information. It will present various reasons HSM is considered to be safe, how it is currently being used by many industries, different factors to consider while choosing an HSM and how HSMs soon will be available as a service by cloud providers. The case study of SafeNet Luna HSM will be discussed with a high level demonstration.	**Neetu Jain** (SoftLayer - IBM)
12:30 - 1:00 pm	**Birds-of-a-Feather Sessions**	

Time/ Location	Topic	Presenter(s)
ENTRPS 7	**The Widening Cybersecurity Gap Between DC and Silicon Valley: The Causes, Implications, and Solutions** This Birds-of-a-Feather Session will provide participants the opportunity to discuss the root causes of the DC/Silicon Valley divide, why it matters for cybersecurity, and brainstorm some concrete ideas for ways each of us can work toward ameliorating the gap.	**Andrea Little Limbago** (Endgame)
ENTRPS 8	**Strategies to Motivate More Female Students in Cybersecurity** This session will brainstorm and address questions such as how we can increase the number of female students pursuing a degree in cybersecurity, what has worked and what has proven to be difficult.	**Susanne Wetzel** (Stevens Institute of Technology)
INNOV BR	**Finding Career Paths in Cybersecurity** Getting into information security happens differently. Professionals from varying backgrounds who have done so will share tips and discuss resources for getting into the security field.	**Michelle Hardesty** (University of Cincinnati) and **Manasa Punugu** (The Ohio State University)
1:00 - 2:30 pm	**Lunch and WiCyS Poster Awards**	
ENTRPS 1-6	***Keynote:*** **Margaret N. White** (Bank of America) **The Long Way Around - From Software Engineering to Cyber Security** Wondering how on earth to narrow your information technology or computer science field of study? How choosing "wrong" turned out to be right.	
2:30 - 4:30 pm	**Workshop Series 4***	
Maverick	**Workshop 4.1: CTF 101** Join members of the Facebook Security Team for an introduction to Capture the Flag (CTF) competitions! CTFs are security games that encourage players to solve security puzzles in a safe and controlled environment. CTFs typically consist of challenge "levels" that represent real security issues found in networks and systems. In these competitions, players will compete with each other, often in teams, to see who can solve these levels first and thereby win valuable points to progress up a leader-board. This workshop will provide a basic introduction to how these competitions work, and progress on to hands-on game play in teams! The goal is to expose players to the most common methods hackers use to break into systems, which better prepares them to defend those systems and networks in the future.	**Jackie Bow and Michael McGrew** (Facebook)
Made In Texas 8	**Workshop 4.2: Mock Forensics Crime Scene Investigation Utilizing the Chain of Custody** This workshop will explore a mock crime scene investigation where participants will gather evidence, process, and report the evidence as they are led to the truth of a crime. Participants will learn how to acquire evidence from a SATA drive and USB drive using a Write-Blocker. Participants will also learn about following the chain of custody and how it is utilized in a forensics investigation.	**Deanne Cranford-Wesley** (Forsyth Technical Community College) and **Francisco Salinas** (South Texas College)
Made in Texas 10/11	**Workshop 4.3: Breaking the Bank to Save Web Apps** This workshop will explore common web application vulnerabilities like Cross-Site Scripting (XSS), Cross-Site Request Forgery (XSRF), application logic flaws, and more. After some demonstrations, students will be turned loose on MehBank, an intentionally vulnerable online banking application. Takeaways: Learning to defend by learning to break and basic understanding of OWASP top 10. Prerequisites: HTML, Basic JS, Laptop, Firefox with Firebug or Chrome, Burp Suite	**David Tomaschick and Niranjanaa Ragupathy** (Google)
Thank you for joining us at the 2016 Women in Cybersecurity Conference! See you next year!		

*Registration required for each specific workshop. If space is available, walk-in registrations will be taken on a first come first serve basis for workshops.

Student Poster Session Abstracts

Poster ID: 2
Jade Seymore, David Garcia and Luis Mojica
Bethune Cookman University, Southwestern College and University of California Berkeley
(Group) Undergraduate

Web Privacy Census: Cookies and HTML5 Double as Flash Fades: The Web Privacy Census aimed to increase public policymakers awareness of web tracking with data to support the idea of increasing measures to give more consumers privacy online. As policymakers consider different approaches for addressing Internet privacy, it is critical to understand how interventions such as negative press attention, self-regulation, Federal Trade Commission enforcement, and direct regulation affect tracking. We seek to explore: How many entities are tracking users online? What website categories have the most cookies placed on a single visit? Continuing on from previous studies, here we report on the state of Internet tracking on the most popular websites. We compare data with the 2012 Web Privacy Census and discuss the patterns and trends we see surrounding the current state of web privacy. We predict that we will see more adoption of fingerprinting methods. In the future we hope to collect and show what websites track users using the fingerprint tracking method.

Poster ID: 3
Lola Obamehinti
University of North Texas
(Group) Graduate

Effects of Users' Privacy and Security Concerns on Adoption of Mobile Apps: Does privacy and security concerns significantly affect whether a user decides to keep mobile application on their phone? This paper investigates the extent to which privacy concerns and risks might result in users ultimately rejecting mobile applications. Previous literature relating to mobile applications, users' privacy concerns and their motivations for adopting or rejecting a mobile application will examined. Additionally, the author discusses the technology acceptance model and privacy calculus theory to present a new model addressing mobile application adoption based on those previous theories.

Poster ID: 4
Kebra Thompson, Sarah Lytle and Kyle Sessions
University of Washington Tacoma
(Group) Undergraduate

Secure Election Protocol Implemented on Microcontrollers Communicating Wirelessly: This project involved the implementation of a secure election protocol in both hardware and software. The implemented protocol was introduced in A Secure and Optimally Efficient Multi-Authority Election Scheme (CraGenSch97). The overall system consists of two stations that handle different portions of the protocol and communicate with each other through the use of Wixel programmable USB wireless modules. A voter enters his or her identification at the voting station and makes a selection. The encrypted vote is then sent to the second station where it is used to calculate the result at the end of the election. This second station is the bulletin board and displays all of the pertinent values after the election has concluded. The time taken to carry out these processes is slower on the small device than on a larger computer but was reasonable.

Poster ID: 17
Aranya Ajith and Rebecca Powell
Florida State University
(Group) Undergraduate

Software Protection Against Reverse Engineering Threats: When adversaries use reverse engineering tools to unravel legitimate and/or about-to-be copyrighted software for various malicious reasons, it is necessary to have an anti-reverse engineering tool that can obfuscate code where reverse engineering tools would be rendered useless. The Hardened Anti-Reverse Engineering Systems HARES has been one of the more interesting anti-reverse engineering tools proposed by Jacob I. Torrey. There are several other anti-reverse engineering tools, such as the upcoming Intel SGX. The common feature of these tools is that they use mechanisms derived from the Trusted Computing Module that invoke trusted program executions. Our work focuses on a broader HARES approach that exploits the protection offered by a separate trusted decryption platform on which encrypted instructions get decrypted and then executed in the normal way. The trusted decryption platform cannot be modified, corrupted or physically removed, without destroying it and making the obfuscated programs unreadable.

Poster ID: 59
Preeti Ravindra and Sumana Suresh
Carnegie Mellon University
(Group) Graduate

Digital Forensics For Cloud Data: Nowadays, a vast amount of data is stored on the cloud. Enterprises and individuals alike are looking to migrate data to cloud completely. Data storage in the cloud poses an entirely different set of problems when it comes to digital forensics. This has opened up an entirely different research area in the form of digital forensics in the cloud. Many classic traditional tools have failed to extract forensic data from the cloud. Our research approach is to see whether mobile phones can provide a different view of data on the cloud, with respect to the transient nature of the cloud. The focus of our research problem is to analyze forensic data collected from mobile devices with and without cloud storage and observe the differences in data from a forensics perspective. We hope that determining the difference(s) if any, in the data collected from a device that has cloud storage and a device that doesn't, will add value to the already existing research in the field of cloud forensics.

Poster ID: 61
Anahita Davoudi
University of Central Florida
(Group) Graduate

Behavior-based Attack Detection in Social Recommender Systems: Fake and spam profiles have affected the rapidly growing social recommendations platforms and online shopping websites. In this paper, different attacks on user's relationships and items being rated are analyzed to capture the user behavior resulting in fake ratings and fake relationships. A framework has been proposed to identify malicious users in recommender systems. A directed social graph is used to model social relationships between users in the network. Based on social relationships of users and rating assigned by users to items, multiple criteria are introduced to distinguish the normal behavior from suspicious one. Then modified trust based matrix factorization method is applied to the opinion dataset to check the difference in the rating prediction and clustering the user profiles based on the values for the proposed criteria. Error evaluation metrics are used to compare the performance in the proposed model.

Poster ID: 65
Erin Devivies
United States Naval Academy
(Group) Undergraduate

99 Problems and Cybersecurity is Definitely One: A Characterization, Analysis, and Proposal of Solutions to the Problems Incited by Human Vulnerability within the Cyber Realm: Cyber Security in the USA has been treated as a problem with a "one-size-fits-all" solution that does not address the individualized vulnerabilities that exist relative to the stark contrasts in technological literacy and dependency that vary across different generations. The author proposes that there exists a three-way generational divide in terms of technological literacy and dependency to which the human vulnerability in the cyber realm can be attributed. The author defines and characterizes the three generations and their respective levels of technological literacy and dependency, examines the degree of anomaly present as a result of such, and finally proposes possible solutions for the most vulnerable practices within each age group. This paper offers a meta-analysis of the existing research surrounding generational groups and their behavior in regards to technology. Moreover, it contains a proposal for a feasible and efficient plan for cyber policy and education reform in the United States in an effort to perpetuate a more secure America in cyberspace.

Poster ID: 68
Vishakha Jain
Carnegie Mellon University
(Group) Graduate

Finer Control over Application Permissions in Android M: Previous versions of Android employed the 'all-or-nothing' model wherein a user will have to accept and give all the permissions requested by the application before installing else he should not install the application altogether. With the release of Android M, runtime app permissions model has been introduced. A user can now select which permissions to allow or disallow at run-time. During execution, user can also select if the permission should be allowed/disallowed access for the application's lifetime or for that one-time use only. With the proposed solution that lies mid-way, the aim is to provide users with fine grain controls over application permissions. For this, I build a permissions model which is baked into Android OS that would provide the ability to control individual permissions for every application based on certain intuitive factors like time of day, frequency of probe requests, location and battery status. This could help alleviate some of the security/privacy concerns of smartphones.

Poster ID: 69
Candice Whitaker, Britny Rominger and Deanne Cranford-Wesley
Forsyth Technical Community College
(Group) Community College

RFID Vulnerabilities and the Future of Payment Card Industry (PCI): As financial institutions begin to distribute microchips to consumer; we will explore the technology: myths: truths and future impact to the consumer market and personal identifiable information (PII) on security.
The use of RFID technology in credit cards, has been around since 1969: giving criminals plenty of time to find the exploits. Recently many financial institutions have moved customers over to a newer credit card that features an EMV chip in place of the antiquated RFID technology of previous years. However does this make our financial information and transactions any safer? These are the issues we will attempt to address in this paper. We will be demonstrate how criminals gain access to sensitive credit card information as well as how the new EMV chip technology used in credit cards and discuss the research that supports our theory.

Poster ID: 87
Yu Pu and Jens Grossklags
Penn State University
(Group) Graduate

Investigating Interdependent Privacy in Social App Adoption Scenarios: Theoretical Results and Behavioral Evidence: The popularity of third-party apps on social network sites and mobile networks increasingly highlights the problem of the interdependency of privacy. It is caused by users installing apps that often collect and potentially misuse the personal information of users' friends who are typically not involved in the decision-making process. We conduct three studies in the area of interdependent privacy to address the existing literature gap within this problem area and to work towards practical solution approaches. Motivated by the economic theory of other-regarding preferences, our research studies to which degree users take their friends' privacy into consideration when they make app adoption decisions. We present results from two simulations utilizing an underlying scale-free network topology to investigate users' app adoption behaviors in both an early adoption phase and later adoption periods. As a result, it may be necessary to limit the data sharing of friends' information, or to increase the involvement of users in the decision-making process over information sharing initiated by others.

Poster ID: 93
Dijana Vukovic
Norwegian University of Science and Technology, Trondheim
(Group) Graduate

Privacy Issues on Android Mobile Devices: People use smart phone applications in different areas of their lives: taking photos and publishing them online, sending e-mail, scanning QR codes, instant messaging, etc. These are just a small subset of possibilities for these kinds of applications available nowadays. Installing an application usually means granting privileges to the application, such as: Internet access, camera access, etc. Granting the privileges can lead to privacy issues that will affect the end user. In this paper security of the Android operating system has been discussed and one example of exploitation of its weaknesses – camera-based attack - to violate the end user's privacy is given. Potential solution for the privacy issues is discussed and an overview of improvements related to privacy on new Android OS – Marshmallow is given.

Poster ID: 100
Rima Asmar
Tennessee Tech
(Group) Graduate

Automated Extractor Generation for Packed Malware: In order to bypass the AV scanners, and hinder the process of analysis and reverse engineering, malware writers had come up with several techniques to obfuscate the malware and automatically generate variants of the original malware instance. Among the used techniques is "Malware packing". Packing malware refers to the process of reorganizing the structure of the executable via compressing, encryption, bundling and insertion of junk or anti-analysis code. With the increased number of packed malware (around 80% in 2013), and the increased cost of generating extractors for existing packers (over 470 in 2013), most AV scanners detect any packed executable as malicious. Consequently, the approach used by AV vendors increases the rate of false positives. To deal with the threat, it is necessary to develop an automated framework for generating resilient purpose built extractors to mitigate the manual cost drawback and the dynamic approach's limitation. Our project proposes to implement a system that automatically generates extractor in a timeframe of 1 – 10 minutes, which provides significant speed up over the 6 hours to 6 months it takes currently to manually write an extractor.

Poster ID: 102
Cariana Cornel, Caralea Cornel, Dale Rowe, Samuel Moses and Sarah Cunha
Brigham Young University
(Group) Undergraduate

Girls Cybersecurity Camp: The information technology industry demand for cybersecurity analysts and awareness is increasing. The "employment of information security analysts is projected to grow 37 percent from 2012 to 2022, much faster than the average for all occupations". Today, "Women represent just 10 percent of the cybersecurity workforce". Thus, to increase the percentage of people going into cybersecurity, primarily women, we must start at the base: schools. Through schools the introduction of information security can be made with emphasis on the need to be cyber savvy and also address the importance of balanced teams, which would be comprised of both men and women. However, schools are unable to keep up with this need due to lack of resources or availability. Therefore, a camp has been formed to provide an opportunity to give an introduction to cybersecurity and to address the gender biased challenge by reaching out to girls at local schools. The first successful Girls Cybersecurity Camp (GCC) at Brigham Young University (BYU), was held during the summer of 2015 with an attendance of more than 35 students. BYU/CSRL will thus continue to provide hosted camps in the future.

Poster ID: 103
Laura Martin
NIATEC
(Group) Graduate

Quantifying Value in the Design Stage: How can we increase the security of our information systems? Future systems can be made more secure by building security in at the earliest stages of design. This research examines the problems inherent in the status quo. The benefits of built in security will be enumerated. Finally, an attempt will be made to quantify quality and value in design as it relates to security.

Poster ID: 105
Bianca Colón-Rosado and Humberto Ortiz-Zuazaga
University of Puerto Rico, Río Piedras Campus
(Group) Undergraduate

Techniques for Anomaly Detection in Network Flows: Benford's Law: A general method for detecting anomalies in network traffic is an important unresolved problem. Using Network Flows it should be possible to observe most anomaly types by inspecting traffic flow. However, to date, there has been little progress on extracting the range of information present in the complete set of traffic flows in a network. We start using the subspace method to detect anomalies in the following different types of traffic flows: bytes, packets and IP-flow counts. Using PySILK we implemented the Benford's law to detect any type of anomalies affecting Transmission Control Protocol (TCP) flows, including intentional intrusions or unintended faults and network failures in general, those anomalies will be detected by investigating the first-digit distributions of the inter-arrival times of TCP SYN packets. The Benford's Law was effective and an important advantage of this method is that malware cannot easily adapt their communication pattern to conform to the logarithmic distribution of first digits. We need to validate the method with labeled or simulated data and build an alerting system to notify of anomalies as soon as they are detected.

Poster ID: 108
Shilpa Kumari and Xiaohong Yuan
North Carolina Agricultural and Technical State University
(Group) Graduate

Demystifying Ad Fraud: With the advent of Internet the landscape of advertising has significantly changed. The wide spread use of Internet allows advertisers to reach significantly more consumers through online advertisement compared to traditional advertising media. Furthermore, cost efficiency, convenience in targeting relevant market segment, and ability to quickly disseminate content changes, make online advertisement more attractive to advertisers. However, currently online advertisement is facing challenges associated to advertisement frauds (Ad Fraud) such as ad replacement, ad stacking, click fraud, and click hijacking. It is of paramount importance to develop technologies for counteracting advertisement frauds for a fair and transparent online advertisement ecosystem. In this work, a course module was developed to teach students about online ad servicing architecture, associated security vulnerabilities and how they can be exploited. A lab is setup for students to simulate different steps of ad replacement fraud using three ubuntu virtual machines from SEED Project. This poster will present aforementioned components of course module and will discuss our teaching plan.

Poster ID: 109
Krystal Le
Lewis University
(Group) Undergraduate

Securing DNS Server Against Denial-of-Service Attacks: Domain Name System (DNS) is the Internet's phone book. One of its functions is to resolve domain and host names into Internet Protocol (IP) addresses that computers need in order to communicate with each other. Over the years, the DNS-based Denial of Service Attacks has become one of the most common destructive attacks on the Internet. In order to find a way to secure DNS against DOS attack, I set up a virtual machine that runs a DNS server, launch a denial-of-service attack against it, then install/configure, protections and show that they help mitigate the attacks.

Poster ID: 112
Brenda Villarreal
Laredo Community College
(Group) Community College

Client Side Exploit: In today's technological world, we are faced with many dangers when we connect to networks such as the Internet. The overall protection of valuable data is not always guaranteed and there should be more awareness of what dangers we are faced with in order to protect valuable data and ourselves. In this project we learn about two main types of threats that we must be aware of: social engineering and key logging software along with a few other threats by using two virtual machines, Kali Linux and an unpatched version of Windows XP. Once the victim opens the e-mail that seems legit, the attacker can now execute malicious key logging software into the remote system in order to grab user names, passwords, and other valuable data that can be used for malicious agendas. Everyone who is connected to the Internet and who uses e-mail services should be aware of the dangers that come with its use. Not only that, but users must be vigilant as to what pages they visit and what files they open on e-mails because we are all victims of these types of attacks.

Poster ID: 114
Grace Rodriguez and Humberto Ortiz Zuazaga
University of Puerto Rico
(Group) Undergraduate

Using Visualization to Improve Analysis of Anomaly Detection in IPv6 Flows: In order to ensure long-term growth, network operators and companies have been starting to implement IPv6 in their network. However, new individual products that use IPv6 are very exposed to malicious attacks because their bugs and security vulnerabilities haven't been discovered and fixed yet. That's why we have decided to test IPv6 flow data to find new ways to improve security. In this research, we are classifying a flow anomaly for those packets with an inexplicable amount of data (bytes). Even though the implementation of IPv6 is relatively new, there can be a lot of flows in just one day. Analyzing all of these flows individually is almost impossible and very time consuming. Therefore, we have decided to create and use visualization tools that will allow us to picture our data better and analyze them more efficiently. One approach we have taken is to use the fields in IPv6 flows data of source Address, destination Address and Destination Port, convert them into decimals of a range from 0 to 1 and use them as coordinates to display a 3D cube.

Poster ID: 125
Jasmine Carson, Oliver Nichols, Chris Bonham, Paul Bond, Wayne Simpson and Michael Crow
North Carolina AT State University, The University of Tennessee at Chattanooga
(Group) Graduate

Exploring the Vulnerabilities and Prevention of Raspberry Pi System: With the growing popularity of the lightweight yet efficient Raspberry Pi, users may lack the knowledge to properly secure a Raspberry Pi, leaving it and potentially the network it is attached to vulnerable to attacks. The purpose of this project is to explore system vulnerabilities as related to the Raspberry Pi, and implementations that are designed to withstand such vulnerabilities and/or decrease the potential for an exploit to result from such vulnerability. The following vulnerabilities and prevention methods in relation to Raspberry Pi will be explored: (1) Password cracking; (2) Man in the Middle Attack; and (3) Cross Site Scripting (XSS) Attack on openzwaveme.

Poster ID: 130
Parisa Kianmajd
University of California at Davis
(Group) Graduate

A Privacy-Preserving Coordination Mechanism for Smart Communities: Smart communities of the future have features that make them susceptible to novel forms of cyber-attack and a potential loss of privacy for the citizens they serve. These distributed systems need to be responsive to the individual needs of citizen owners yet still maintain the ability to coordinate actions across a neighborhood or larger metropolitan area. The question we wish to address is, as frameworks emerge to handle these unique challenges, how can we provide security and privacy for such open and decentralized environments? We propose the use of bitcoin block chain together with some cryptographic primitives to guarantee that in the absence of a trusted third party, users can reach an optimal resource allocation plan while remaining anonymous. We choose a virtual smart electric micro-grid as our use-case. Block chain can provide the means to build and maintain a distributed storage of privacy sensitive energy usage information and coordinate the distribution of energy without a single owner. Moreover, block chain provides us with append-only immutable records, which is essential for our system and ensures the users cannot insert fake points to their energy usage points history.

Poster ID: 144
Katherine Seale and Dr. Todd Jeffrey McDonald
University of South Alabama
(Group) Graduate

Integrating Relational Data Frameworks into Risk Assessment of Networked Medical Devices: Threats in networked medical devices could be avoided with prevention and countermeasures by incorporating modern threat modeling tools and frameworks that utilize risk analysis. This study investigates the viability of risk assessment models as an indicator to cyber security vulnerabilities in medical environments. Our research refines a database-driven model that manages vulnerabilities and risk in networked medical devices and validates the model using real-world data. We perform a case study analysis based on data from medical devices used in the College of Nursing's simulation unit at the University of South Alabama. We examine this real-world data from the perspective of different threat models and risk assessment frameworks, such as the STRIDE model. Based on the acquired data in the case study, we research vulnerabilities and mitigation strategies for specific medical devices. We expand existing database models to support query capabilities and risk assessment techniques that ultimately improve security in healthcare-based IT organizations that use medical devices.

Poster ID: 146
Jarilyn Hernandez Jimenez, Jeffrey Nichols, Katerina Goseva-Popstojanova and Stacy Prowell
West Virginia University, Oak Ridge National Laboratory
(Group) Graduate

A Malware Detection Framework Based on Power Consumption Monitoring: Malicious code or malware is one of the most serious security threats on the Internet today. The main problem with malware is that typically they avoid detection by rewriting portions of itself so that it is syntactically very different, but semantically identical; replacing byte sequences in an executable with completely different byte sequences that have the same net effect on the system. To address these limitations, we propose an approach that uses an unavoidable consequence of intrusion – consuming electrical power – to detect the presence of rootkits, and uses an inherent property of malware – it must modify the operating system to avoid detection – to detect intrusions. The main objective of this research is to determine if malware generates a signal in the power consumption of a general-based computer once the machine is being infected. Future works includes the detection of rootkits by also monitoring the kernel events of the machine. In addition, we would like to test if the proposed approach can detect rootkits from external power observations for limited function machines, such as SCADA devices.

Poster ID: 147
Sujatha Krishnaswamy
Iowa State University
(Group) Graduate

Cyber Security Testbed for Accelerating Smart Grid Innovations and Deployments: Several authoritative government reports and technical literature have documented increasing concerns for highly sophisticated, advanced persistent cyber threats on critical infrastructures like the power grid. Cyber-Physical System (CPS) Security test-beds are essential elements in the R&D ecosystem to develop and validate novel CPS security tools and algorithms for securing the grid and making it attack-resilient. The engineering of CPS security test-beds requires significant investments in money, time and modeling efforts to provide a scalable, high-fidelity, real-time attack/defense platform. Therefore, there is a strong need in the research community to build CPS security test-beds. Power Infrastructure Cyber Security test-bed is one such effort in enabling access to a broader user community. The poster will give an overview of capabilities of Power Infrastructure Cyber Security Laboratory at Iowa State University and successfully executed implementation efforts by the "Power Cyber" team namely (1) Remote Access Framework; (2) CPS Security Testbed federation; (3) Training and Outreach.

Poster ID: 149
Lindsay Von Tish
Lewis and Clark College
(Group) Undergraduate

Malware Analysis For Beginners: Every day there is new malicious code being sent out to unsuspecting victims. Because most malware is packaged or obfuscated it can be hard to tell what it does. Luckily, there are many malware analysis tools that make it much easier to understand malware. Strings searches a piece of malware for sequences of printable characters. While this tool only works on unpacked pieces of malware, it is very useful in determining what a piece of code does. IDA is a disassembler for binary programs. It creates maps of the program's execution without the original source code. It shows what the program does in both assembly language and in a readable format that is similar to the program's original code. Wireshark is a network monitoring tool. It "understands" the encapsulation of networking protocols which means it displays the fields along with the meanings of the different network protocols. It can read traffic from a file or capture traffic using pcap. Using wireshark, an analyst can recognize malicious communication attempts, such as downloads, DNS resolution requests, or bot traffic.

Poster ID: 154
Miranda Jahn, Dr. William Glisson and Dr. Mike Jacobs
University of South Alabama
(Group) Graduate

Investigating a Medical Mannequin: The use of simulation related medical devices such as medical mannequins has increasingly been incorporated into the training of medical professionals. As more technology is incorporated into healthcare environments, researchers are investigating vulnerabilities that may affect various medical devices. While no cases have been reported on compromised medical devices harming a human, research has shown that several medical devices have the capability to eventually do so. Compromising individual medical devices impacts a relatively small number of individuals. Previous research has demonstrated the act of successfully breaching a production-deployed medical training mannequin, an iStan, in a live-environment. This research performs a forensic analysis on an iStan after it has succumbed to attacks from an Android application. This study investigates the residual data recovered from a compromised medical training mannequin and supporting equipment as well as an Android device in order to identify information for a forensic investigation.

Poster ID: 165
Ni An and Steven Weber
Drexel University
(Group) Graduate

On the Performance Overhead Tradeoff of Distributed Principal Component Analysis via Data Partitioning: This poster presents our work on evaluating two distributed principal component analysis (PCA) algorithms on a real domain name system (DNS) query dataset. PCA is not only a fundamental dimension reduction method, but is also a widely used network anomaly detection technique. Traditionally, PCA is performed in a centralized manner, which has poor scalability for large distributed systems, on account of the large network bandwidth cost required to gather the distributed state at a fusion center. Consequently, several recent works have proposed various distributed PCA algorithms aiming to reduce the communication overhead incurred by PCA without losing its inferential power. Our work evaluates the tradeoff between communication cost and solution quality of two distributed PCA algorithms on a DNS query dataset from a large network. We also apply the distributed PCA algorithm in the area of network anomaly detection and demonstrate that the detection accuracy of both distributed PCA-based methods has little degradation in quality, yet both achieve significant savings in communication bandwidth.

Poster ID: 167
Kathryn Burks, Shaun Westlund and Philip Westrich
Tennessee Technological
(Group) Undergraduate

Cyber Security Awareness through Immersive Visualization: As the internet has become more readily available, it has become all the more essential to educate today's young adults about the many security risks of using the internet and the threats that lurk in cyberspace, as well as on the basic concepts essential to an understanding cyber security. By young adult we mean someone between the ages of twelve and eighteen (middle to high school). The field of Cyber Security has only recently gained a lot of attention over the last decade, and, consequently, there are not many resources that exist today for young adults to gain the necessary awareness and knowledge to surf the web safely. Video games have been used as an effective education tool for youth since they naturally are more engaging and attractive to this age group. Keeping this in mind, we have been developing an immersive 3D video game, using the Unity3D game engine as well as Occulus Rift, to teach young adults about cyber security concepts in an engaging and memorable way.

Poster ID: 168
Rakesh Verma and Avisha Das
University of Houston
(Group) Graduate

Security Analysis of Phishing URLs: Our research is mainly aimed at analysis and detection of Phishing URLs. We use the online learning classifiers on a set of rich features, Character N-grams extracted from phishing URLs and then we perform a security analysis of our approach. Building a classifier which gives high accuracy does not always suffice, we also have to keep in mind that the classifier is accurate as well as robust at the same time. We in our work probe deep into these datasets and analyze the nature of the URLs in the datasets used as well as in misclassified URLs based on different aspects like the presence of common country codes and how the frequency varies across the datasets, presence of server side language extension markers, presence of special characters, to mention a few. We found that more than 25% of the phishing URLs from all the datasets contain country codes and more than 45% of these URLs contain special strings, e.g. server side language extensions. More than 70% of the phishing URLs contain special characters.

Poster ID: 170
Parisa Kaghazgaran
University of North Texas
(Group) Graduate

Privacy Preserving EEG-based Authentication System: Recent advances in Brain-Computer Interfaces (BCIs) and devices capable of recording electrical activity of the brain has opened the door for their application in nonmedical domains such as information security. Electroencephalograms (EEG) is an electrophysiological monitoring method to record electrical activity of the brain and research has shown it can be used for authentication either as an alternative to passwords or in combination with other mechanisms in multi-factor authentication. However, EEG signals carry a wealth of information and can reveal private information about the user. This brings significant privacy challenges to EEG-based authentication mechanisms and other applications of EEG. I aim to present the first privacy-preserving authentication system based on EEG signals using a combination of Arithmetic sharing, Homomorphic encryption, and oblivious transfer to address privacy issues of EEG signals and protect privacy of their owners.

Fannie Mae serves a critical role in the nation's housing finance system. In the secondary mortgage market, we provide reliable, large-scale access to affordable mortgage credit across the country at all times so people can buy, refinance, or rent homes. Fannie Mae is there when people need us most.

Our vision is to be America's most valued housing partner.

Our workforce is a diverse and talented group of people who welcome the opportunity to be on the front line of change.

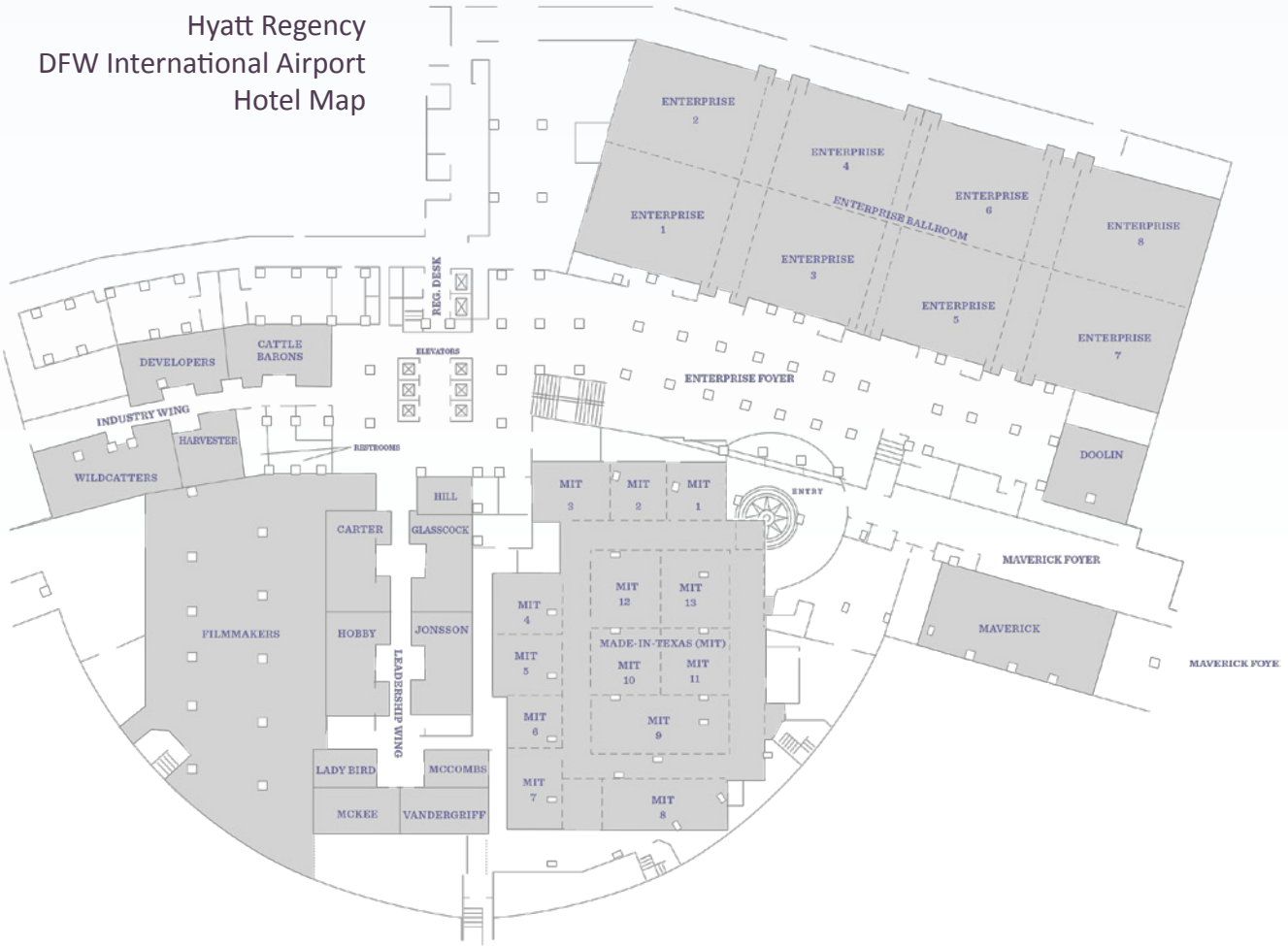
Our workplace is one of the most inclusive places to work in the financial services sector.

Join our team!
Put your unique talents to good use as we work to improve our nation's housing finance system.

Go to the Fannie Mae Careers website, **www.fanniemae.com/careers**, and click "Job Openings" to view current opportunities, full job descriptions, and to apply online.

FannieMae®

Hyatt Regency
DFW International Airport
Hotel Map



NOTES

THANK YOU TO OUR SPONSORING PARTNERS

Cybersecurity Education, Research & Outreach Center
TENNESSEE TECH

Diamond Sponsoring Partners

Platinum Sponsoring Partners

Gold Sponsoring Partners

Silver Sponsoring Partners

Bronze Sponsoring Partners

Media Sponsoring Partners