L E A R N W O R K L E A D

women in CYBERSECURITY

WiCyS

PITTSBURGH 2019

MARCH 28-30, 2019

WICYS 2019 VIP SPONSORS

facebook

CISCO

Fidelity INVESTMENTS

LOCAL UNIVERSITY HOST

Carnegie Mellon University

TABLE OF CONTENTS

HOURS OF REGISTRATION

THURSDAY	12:00 pm - 8:00 pm
FRIDAY	7:00 am - 7:00 pm
SATURDAY	7:00 am - 12:00 pm

PICK UP AND PURCHASE WICYS BRANDED GEAR

Kings Plaza Room, 2nd Floor

THURSDAY	4:00 pm - 7:00 pm
FRIDAY	7:00 am - 8:15 am &
	10:45 am - 12:00 pm
	3:00 pm - 4:00 pm
SATURDAY	7:00 am - 8:15 am

Limited quantities/sizes of WiCyS-branded socks, pashmina scarves, beanies, cardigans, T-shirts and fleece jackets are available.

USE THE APP

Courtesy of PayPal

BOOST YOUR EXPERIENCE

Haven't had a chance to explore yet? After downloading the Whova app to your mobile device, use your email address to sign in. You can browse the agenda, view speakers and sponsors, and connect with other attendees of the conference.

CODE: wicyj

TAG US #WICYS2019

WIN LODGING & REGISTRATION TO WICYS 2020!

Enter the social media contest on Facebook, Twitter or Instagram! Use #WiCyS2019 on a public page or on the WiCyS Facebook event wall to share pictures and stories of your time at the conference.

Winners will be announced after the conference.

SNAPCHAT @ WICYS

Thanks to @FidelityJobs for the Custom Snapchat WiCyS conference filter!

- Make sure your location services are on in your mobile device.
- Open Snapchat and take a picture
- Swipe left or right to see the custom WiCyS conference filter.
- Send to your friends or make it your story.
- Send snaps to @FidelityJobs on Snapchat!

WELCOME TO THE 6TH ANNUAL WiCyS CONFERENCE!

FROM WICYS

Today is a special day for all of us. We started our journey in 2014 as an annual conference and today we meet as an independent organization. Over the years, we became more than an annual gathering. We started a movement together. You spoke. We heard. Now WiCyS is your voice.

The WiCyS 2019 program offers many choices—to LEARN new solutions, challenges, trends, best practices, career development tips, and resources; to WORK your skill and talent in presenting, asking the right questions, finding mentors, being a mentor, trying out for opportunities; and to LEAD initiatives for empowerment. We are grateful to our local host CMU and the WiCyS conference planning committee who worked so hard to place these choices in front of you.

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

Dr. Janell Straach
Chairman of the Board

This conference and organization exist to highlight your accomplishments, connect you with a network of peers, and bring opportunities and resources to the community. Whether you are an individual or an organization, we are here to support your goals that align with our diversity mission. Now, let us work together for success in increasing representation of women in cybersecurity workforce, a challenge that will need our collective action well beyond this conference and into a year-long effort.

Together, let's build more bridges in this "City of Bridges"!

FROM CMU

It's a beautiful day in the neighborhood as we welcome WiCyS 2019 to Pittsburgh! Carnegie Mellon University (CMU) has sparked innovation since its founding in 1900 and we're proud to be the birthplace of cybersecurity.

In 1989, CMU's Software Engineering Institute founded the world's first computer security incident response team, the CERT Coordination Center. In 2003, we created CyLab Security and Privacy Institute and launched one of the nation's first security degrees at the Information Networking Institute.

Today, women head all three of these major CMU centers focused on security and privacy. Reflecting our dedication to diversity, CMU's proportion of undergraduate women in computer science and engineering soars above national averages. Our founder Andrew Carnegie famously said, "My heart is in the work."

We hope to inspire you to put your whole heart into this incredible WiCyS experience. We believe you are the future of cybersecurity and are proud to host the next-generation of security researchers, hackers and leaders in Pittsburgh!

Dr. Dena Haritos Tsamitis
Barbara Lazarus Professor in Information Networking
Director, Information Networking Institute (INI)
Founding Director, Education, Training and Outreach, CyLab
College of Engineering, Carnegie Mellon University

Bobbie Stempfley
Director, CERT Division
Software Engineering Institute (SEI), Carnegie Mellon University

WICYS BOARD OF GOVERNORS

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

Dr. Janell Straach
Chairman of the Board
Director
University of Texas Dallas

Dr. Costis Toregas
WiCyS Board Treasurer
Director
George Washington University

Dr. Dawn M. Beyer
Senior Fellow
Lockheed Martin Space

Dr. Cynthia Irvine
Director
Naval PostGraduate School

Prajakta Jagdale
Red Team Program Manager
Palo Alto Networks

Jay Koehler
Diversity, Inclusion & Engagement Manager, Security & Trust Organization, Cisco

Margaret Morton
VP, IT Compliance, Risk & Cybersecurity,
Société Générale Americas

Dr. Greg Shannon
Chief Scientist
Carnegie Mellon University

Stephanie Siteman
Info Security & Operations Manager
Facebook

2019 WICYS CONFERENCE

KEYNOTE SPEAKERS

ON FACEBOOK LIVE

TELL YOUR FRIENDS

WiCyS will be streaming the keynotes live! Text, Tweet and Snapchat!
Check the App for keynote bios.

Michele Schochet, Facebook

Courage, Passion and Data: Boldly Challenge the Status-Quo in a Perpetually Evolving Security Threat Landscape

Facebook Security strives to create and maintain an environment which makes it possible for more than 2 billion people around the world to connect and share with each other safely. Traditional security models have focused on the mitigation of threats posed by outsiders; however, relevant cybersecurity methodologies evolve and are holistic in approach. At Facebook, my team builds solutions that proactively inhibit an attacker's ability to compromise our data or systems. Every day I ask myself "What if the threat originated internally and was unintentional?" The honest answer requires more than courage, it requires a commitment to challenge the status-quo using data and an open mind. All of us own Security, instilling a sense of passion, ownership and accountability is key to survival in a perpetually evolving security threat landscape.

Wendy Nather, Cisco

Solving For the Security Poverty Line

For organizations that don't have full IT capabilities, the cascading effects include security. It's not just a matter of providing cheap or free security software, or scanning and scolding until regulators step in. The dynamics in cybersecurity are much more complex, and will need serious efforts from the whole community to address them. In this talk, we'll lay out the problems and the challenges facing our society.

Dr. Lorrie Cranor, Carnegie Mellon University

Tales of an Accidental Computer Science Professor

How can we put privacy policies on every smart light bulb and thermostat, and who would want to read them all anyway? How can we help people create stronger passwords without increasing the chance that they will forget them? I'll share highlights of my journey from student journalist to "accidental" computer science professor, with stints in technical standards, entrepreneurship, fiber arts, fashion design, and government service. I'll talk about how I became interested in making privacy and security usable, and some of the research problems I've investigated at the intersection of security, privacy, usability, and human behavior. I'll discuss ways to attack security user study participants without actually putting them at risk; how we determined that many people will pay extra for better privacy when shopping online; and how the Today Show camera crew ended up in my kitchen.

Patricia Denno, Fidelity Investments

Securing Yourself in a Social Media-, App-, and IOT-crazy world

90% of all cyberattacks start with a seemingly innocuous email. The presentation will introduce in general terms the concept of threat actors (cybercriminals, nation states, hacktivists, and insiders), introduce how those threat actors are attempting to steal/collect information about you and what they can do with it. The presentation will introduce the concepts of phishing, spear phishing, business email compromise, extortion, and malicious software, and conclude with relatively simple steps to avoid being a victim to these attempts.

Dr. Dawn Beyer, Lockheed Martin

The Art of Cutting Glass!

Dr. Dawn Beyer is a Senior Fellow. Senior Fellows are recognized as the most experienced, most successful, most technical elite group in a corporation. This is the highest level of excellence in the individual contributor technical career path. There are usually very few senior fellowships awarded each year and the competition for them is intense. Let's just say, the chances of becoming a Vice President of a large corporation are a lot higher than becoming a Senior Fellow. Dr. Beyer will share her unconventional path to Senior Fellow. This talk will surprise, enlighten, inspire, and challenge you!

THANK YOU TO OUR
CONFERENCE SPONSORS

VIP SPONSORS

DIAMOND SPONSORS

PLATINUM SPONSORS

GOLD SPONSORS

SILVER SPONSORS

BRONZE SPONSORS

PROGRAM PARTICIPATION

TRACKS AND SESSIONS

Today's Technology and Challenges Track
Current issues and challenges, advances in research and development (R&D), experimental findings

Looking Ahead Track
Important technology/ R&D trends, challenges on the horizon, upcoming solutions, tomorrow's vision

Best Practices Track
Institutional/ operational/ academic best practices, tools, techniques, approaches

Career Development Track
Leadership, advancement, transition

PRESENTATIONS

Presentations highlight innovations, research & development projects, internships/ co-ops experiences, service learning and outreach projects, or other experience related to cybersecurity. Presentations are 45 minutes long, including time for Q&A.

WORKSHOPS

Workshops are free hands-on sessions (technical / professional development) on any topic related to cybersecurity. Hands-on workshops in any cybersecurity area are welcome. Workshops are 2 hours long.

BIRDS OF A FEATHER (BoaF)

Birds of a Feather are informal discussion sessions on just about any topic related to cybersecurity, that elicit participant discussions. These sessions can be a great way to share ideas and be introduced to current issues or trends. BoaF sessions are 45 minutes long.

LIGHTNING TALKS

Lightning talks highlight fresh ideas, unique perspectives, valuable experiences, and emerging trends in cybersecurity. Lightning Talks are 5-minute presentations that aim to jump-start discussions and collaborations while soliciting feedback from the community.

PANELS

Panels provide opportunities to discuss a current relevant topic in cybersecurity. Panel organizers are responsible for selecting appropriate panelists to participate. In addition to the moderator, there can be up to 4 panelists, and each panel is 45 minutes long.

POSTERS

Student posters will be judged in two categories: Undergraduate and Graduate. Winners in each category will be awarded a student travel grant for a future security conference and Runners Up will be awarded a tech prize.

THANK YOU TO OUR
WiCyS COMMITTEES

DR. AMBAREEN SIRAJ
Conference Chair

LOCAL HOST COMMITTEE

DR. DENA HARITOS TSAMITIS
Program Co-Lead
Barbara Lazarus Professor in Information Networking; Director Information Networking Institute (INI); Founding Director, Education, Training and Outreach, CyLab, College of Engineering
Carnegie Mellon University

BOBBIE STEMPFLEY
Program Co-Lead
Director CERT Division, Software Engineering Institute
Carnegie Mellon University

MICHELE TOMASIC
Operations & Logistical Lead
Divisions Operations Manager, Carnegie Mellon University

PROGRAM COMMITTEE (PC)

LISA LAFLEUR
PC Co-Chair
Business Chief Information Security Officer, Raytheon

CELESTE MATARAZZO
PC Co-Chair
Data Science Expert, Lawrence Livermore National Laboratory

DR. ASHLEY PODHRADSKY
PC Co-Chair
Beacom College of Computer and Cyber Sciences at Dakota State University

COLLEEN RICCINTO
PC Co-Chair
Founder and CEO, Cyber Talent Search

ALEX FOLEY
Cyber Security Analyst, Bell

BICH T VU
Associate Staff, MIT Lincoln Laboratory

DR. JUNIA VALENTE
Postdoctoral Research Associate, The University of Texas at Dallas

DR. MEG LAYTON
Director of Engineering, Cyber Security Services, Symantec

SONYA HSIU-YUEH HSU
Professor/Program Coordinator, University of Louisiana

DR. WEI LI
Professor, Nova Southeastern University

DR. CHEN ZHONG
Assistant Professor, Indiana University Kokomo

KAREN LEUSCHNER
National Security Agency

KRISTEN BENEDUCE
Senior Cybersecurity Researcher, Sandia National Laboratories

LAURA PAYNE
BMO Financial Group

KUHELI SAI
Ph.D. Student at the University of Pittsburgh

DR. BYRON J. WILLIAMS
Assistant Professor, CISE - University of Florida

VIVIANA WESLEY
Principal Consultant, Halock Security Labs

SONYA HSIU-YUEH HSU
Associate Professor/Program Coordinator for B.S. Informatics, University of Louisiana at Lafayette

SCHOLARSHIP COMMITTEE

DR. JANELL STRAACH
WiCyS Chairman of the Board

AMELA GJISHTI
Cyber Security Analyst, Bank of America

DR. BARBARA HEWITT
Assistant Professor, Health Information Management, Texas State University

DIANE M. JANOSEK
Defense Intelligence Senior Executive Service, National Security Agency

MARI GALLOWAY
COO, Founding Board Member/Sr. Security Architect, Women's Society of Cyberjutsu/Las Vegas Sands Corp

DR. PUSHPA KUMAR
Teaching Faculty, The University of Texas at Dallas

DR. AMELIA ESTWICK
Program Director, National Cybersecurity Institute

DR. MARTINA BARNAS
Sr. Assistant Dean for Research, SICE, Indiana University Bloomington

DR. NATHAN FISK
Assistant Professor, University of South Florida

SANDRA MCLEOD
Senior Manager, Security & Trust Organization, Cisco Systems

SARAH MORALES
Outreach Program Manager, Security Engineering, Google

DURBA KABIR
Software Engineer, Project Lead, Verizon Communications Inc.

THANK YOU TO OUR
WiCyS COMMITTEES

POSTER SESSION COMMITTEE

DR. CHUTIMA BOONTHUM-DENECKE
Professor, Hampton University

INDRAKSHI RAY
Professor, Computer Science Department, Colorado State University

DR. SMRITI BHATT
Assistant Professor, Texas A&M University-San Antonio

CAREER VILLAGE, RESUME CLINIC & MENTORING COMMITTEE

ANDREA FROST
Senior Software Security Engineer, Dell EMC

ANASTACIA WEBSTER
California State University San Bernardino

KELLEY GOLDBLATT

MARCELLE LEE
CEO and Founding Partner, Fractal Security Group, LLC

ROSALIND MCCULLOUGH
Doctoral Student, University of Alabama in Huntsville

OPERATIONS AND LOGISTICS COMMITTEE

TALY WALSH
Lead - Operations
Executive Director, WiCyS

LANA RICHARDSON
Sponsor Support
Community Care Manager, WiCyS

CHRISTA C. JONES
Director of Marketing and Communications, Carnegie Mellon University

KAITLYN CARROLL
Mobile App
Tennessee Tech University

ANDREW HENLEY
Website & Community Forum
Tennessee Tech University

COLLEEN HUBER
CRM
Nelly Group

VOLUNTEER COORDINATION COMMITTEE

ANGIE JARKA
Illinois Institute of Technology

SUZANNE HENRY
Tennessee Tech University

WORKSHOP COMMITTEE

ESSIA HAMOUDA
California State University San Bernardino

SUSAN MCGEEVER
IBM

CAREER FAIR COMMITTEE

MARY JANE PARTAIN
Career Fair Concierge
Director, University of Texas-Dallas

KARL SHARMAN
Vice President, BeecherMadden

RAYMOND A. HANSE
Wentworth Institute of Technology

CINDY HECKMAN
Software Engineering Manager, Raytheon

SOCIAL MEDIA AND PR COMMITTEE

JENNIE KAM
Security Researcher, Cisco

ADITI CHAUDHRY
Cybersecurity Engineer, Capital One

MANSI THAKAR
Information Security Analyst, Playstation

LYNN DOHM
Media Relations
President, The Nelly Group

SCHEDULE
AT A GLANCE

LEARN

THURSDAY • MARCH 28

8:30 am - 4:00 pm	NSA-NSF GenCyber Day at WiCyS	STERLING
2:00 pm - 4:00 pm	Workshops (4 concurrent)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2
3:00 pm - 6:00 pm	Career Village (Resume Review & Mock Interviews)	BRIDGES
4:30 pm - 6:30 pm	Workshops (4 concurrent)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2
7:00 pm - 8:00 pm	Scholarship for Service (SFS) Meet & Greet	KINGS TERRACE
7:00 pm - 9:00 pm	Mentoring Socials	VARIOUS, SEE BOX P. 9
8:00 pm - 9:00 pm	1:1 Meet-Up Session: Educators w/ Funding Agencies	KINGS TERRACE

WORK

FRIDAY • MARCH 29

8:15 am - 10:45 am	Keynote & Lightning Talks **(Breakfast 8:15-8:45 am only)**	BALLROOM 1 & 2
10:45 am - 12:00 pm	Student Poster Session	BALLROOM FOYER
10:45 am - 12:00 pm	Career Fair	KINGS GARDEN
10:45 am - 12:45 pm	Career Village (Resume Review, Mock Interviews, Office Hours with Cyber Professionals)	STERLING
12:00 pm - 12:45 pm	Presentation Sessions (4 concurrent)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2
12:45 pm - 2:15 pm	Lunch, Keynote, Lightning Talks **(Lunch avail. until 1:00 pm)**	BALLROOM 1 & 2
2:15 pm - 3:00 pm	Presentation Sessions (4 concurrent)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2
2:15 pm - 6:30 pm	Career Fair	KINGS GARDEN
2:15 pm - 6:30 pm	Career Village	STERLING
3:30 pm - 5:30 pm	Workshops (3 concurrent) and Panels (2 consecutive)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2
5:45 pm - 6:30 pm	Birds of a Feather (4 concurrent)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2
6:45 pm - 8:30 pm	Dinner & Keynotes **(Dinner 6:45-7:15 pm only)**	BALLROOM 1 & 2
8:30 pm - 9:00 pm	Special Event	BALLROOM 1 & 2

LEAD

SATURDAY • MARCH 30

8:15 am - 10:15 am	Keynote & Lightning Talks **(Breakfast 8:15-8:45 am only)**	BALLROOM 1 & 2
10:15 am - 10:45 am	Group Picture	KINGS GARDEN
10:45 am - 11:30 am	Presentation Sessions (3 concurrent)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2
10:45 am - 11:30 am	Meet-Up Session for WiCyS Student Chapters	COMMONWEALTH 1
11:30 am - 12:15 pm	Presentation Sessions (3 concurrent)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2
11:30 am - 12:15 pm	Meet-Up Session for WiCyS Affiliates	COMMONWEALTH 1
12:15 pm - 1:00 pm	Panels (4 concurrent)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2
1:00 pm - 2:30 pm	Lunch, Closing Remarks, Awards **(Lunch avail. until 1:15 pm)**	BALLROOM 1 & 2
2:30 pm - 4:30 pm	Workshops (4 concurrent)	BALLROOM 3 & 4, COMMONWEALTH 1 & 2

facebook

University Students

University Grads

Start your career by doing something meaningful. You'll hit the ground running, learn from the best in the industry and build products for billions of people around the world. There's no limit to the impact you can make at Facebook.

Facebook Interns

World-class mentors, our open culture and opportunities to make a real impact are just a few reasons why our intern program was ranked #1 by Glassdoor two years in a row. Discover for yourself what makes interning at Facebook the ultimate learning experience.

Facebook University

Experience what it's like working inside the bold, fast-paced culture at Facebook. Facebook University offers experience in engineering and business roles to rising college sophomores from underrepresented communities.

facebook.com/careers

2019 WICYS CONFERENCE

THURSDAY AGENDA

TIME	DESCRIPTION	LOCATION
8:30 am - 4:00 pm	***GenCyber Day at WiCyS***	STERLING
12:00 pm - 8:00 pm	***Registration Open***	REGISTRATION, 2ND FLOOR
2:00 pm - 4:00 pm	***Workshop Series 1***	
	Cyber Fire: Puzzle-Based Training Neale Pickett and Grace Herrera, *Los Alamos National Laboratory*	COMMONWEALTH 1
	ATT&CK and Threat Actors Kat Seymour, Heather Linn, Ken Smith and James Thomas, *Bank of America*	BALLROOM 3
	Red Team Your Resume: Insiders Share Secrets Kaitlin O'Neil, Kelly Albrink and Kate Broussard, *Bishop Fox,* Troy Steece, *McAfee,* and Linda Martinez, *Protiviti*	BALLROOM 4
	Blue Team Capture the Flag (CTF) Elizabeth Schweinsberg and Bridget Pelletier-Ross, *Facebook*	COMMONWEALTH 2
3:00 pm - 6:00 pm	***Career Village (Resume Reviews and Headshots)***	BRIDGES
4:30 pm - 6:30 pm	***Workshop Series 2***	
	Distributed Forensics Across Time and Space Elena Kovakina and Jesus Aguilar, *Google*	BALLROOM 4
	Gaining Initial Access in a Penetration Test Krysta Coble, Kelly Thiele, Laura Puterbaugh and Petya Lopez, *Dept. of Homeland Security*	BALLROOM 3
	WiCyS Social CTF Village and Competition Dr. Dan Manson, *Cal Poly Pomona,* Kaitlyn Bestenheider, *Tevora,* Franz Payer, *Cyber Skyline,* and Jeana Cosenza and Vicente Gomez, *Pace University*	COMMONWEALTH 2
	Advanced APT Hunting with Splunk Lily Lee and John Stoner, *Splunk Inc.*	COMMONWEALTH 1
7:00 pm - 8:00 pm	***Scholarship for Service (SFS) Meet & Greet (see box, p. 19)*** Stephanie Travis and Sandra Cyphers, *OPM*	KINGS TERRACE
7:00 pm - 9:00 pm	***Mentoring Socials***	VARIOUS (SEE BOX BELOW)
8:00 pm - 9:00 pm	***1:1 Meet-up Session for Educators w/ Funding Agencies (see box, p. 19)*** Dr. Victor Piotrowski, *National Science Foundation* and Maureen Turney, *National Security Agency*	KINGS TERRACE

VISIT THE SOCIALS

Socials are held Thursday, March 28 from 7:00 pm - 9:00 pm

- **Facebook**/BALLROOM 1
- **Walmart**/STERLING 1
- **Raytheon**/STERLING 3
- **CMU**/BENEDUM
- **Google**/BRIGADE
- **Cisco**/BALLROOM 2
- **Symantec**/STERLING 2
- **Bank of America**/DUQUESNE
- **McAfee**/RIVERS

2019 WICYS CONFERENCE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00 am - 7:00 pm	***Registration Open***	REGISTRATION, 2ND FLOOR
8:15 am - 10:45 am	***Breakfast, Conference Opening, Keynote and Lightning Talks***	BALLROOM 1 & 2
	Keynote Introduction: President Farnam Jahanian, *Carnegie Mellon University*	
	***Keynote:* Courage, Passion and Data: Boldly Challenge the Status Quo in a Perpetually Evolving Security Threat Landscape** Michele Schochet, Director, Security, *Facebook*	
	Lightning Talks	BALLROOM 1 & 2
	Sizzle vs.Steak: Why Leveraging Soft Skills is Key to Succeeding in Tech Megan Kaczanowski, *S&P Global*	
	Prob-C: Security Offloading to Edge Wenhui Zhang, *Pennsylvania State University*	
	Practical, Hands-on Cybersecurity Education with CHEESE Christine Kirkpatrick, *San Diego Supercomputer Center* and Dr. Baijian Yang, *Purdue University*	
	Reframing Usable Privacy and Security to Design for "Cyber Health" Cori Faklaris, *Carnegie Mellon University*	
	Be Bold. Ask Questions. Gabby Raymond, *The MITRE Corporation*	
	Training a Backdoor into Deep Reinforcement Learning Agents Marina Moore, *New York University*	
	Hacking Hired: Work the Vectors, Get the Offer Rachel Harpley, *Recruit Bit Security*	
	Everything We Need to Know About Secure Design Can Be Explained by Star Wars Dr. Ann-Marie Horcher, *Central Michigan University*	
10:45 am - 12:00 pm	***Student Poster Session***	BALLROOM FOYER
10:45 am - 12:45 pm	***Career Fair***	KINGS GARDEN
10:45 pm - 12:45 pm	***Career Village (Resume Reviews, Mock Interviews, Office Hours)***	STERLING
12:00 pm - 12:45 pm	***Presentation Sessions 1***	
	Double Your Might: A Data Science Primer for Security Analysts Joanna Hu, *Exabeam*	BALLROOM 3
	Security and Privacy Challenges for Connected and Autonomous Vehicles Lily Yang, *Intel*	BALLROOM 4
	We Can Do It! Becoming a 21st Century Rosie the Riveter Michelle Duquette, *Battelle* and Kelley Goldblatt, *Capitol Technology University*	COMMONWEALTH 1
	All the Colors of INFOSEC Cynthia Cox, Mary Sawyer, Muoi Landivar and Shawn Richardson, *Palo Alto Networks*	COMMONWEALTH 2

2019 WICYS CONFERENCE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
12:45 pm - 2:15 pm	***Lunch, Keynote and Lightning Talks***	BALLROOM 1 & 2
	Keynote Introduction: Don Erickson, CEO, *Security Industry Association (SIA)*	
	***Keynote*: Solving For the Security Poverty Line**	
	Wendy Nather, Head, Advisory CISOs, Duo Security, *Cisco*	
	Lightning Talks	BALLROOM 1 & 2
	Hostage Negotiation for InfoSec Sarah Kennedy, *HCA*	
	You Can Do It! The Power of Cybersecurity Sisterhood! Diane M. Janosek, *National Cryptologic School, National Security Agency*, Shade Adeleke, *Prince George's Community College,* Dr. Vitaly Ford, *Arcadia University* and Dr. Pauline Mosley, *Pace University*	
	Domain Misconfiguration in the Wild Mia Gil Epner and Luna Frank-Fischer, *Expanse, Inc.*	
	Managing the Guest List—Third Party Vendors Stacey Romanello, *RBC*	
	"What Do You Mean It's Not a Security Issue?" Natalie Attaya, *IBM*	
	Recalculating Women in Cyber Georgia Reid, *Cybercrime Magazine*	
2:15 pm - 3:00 pm	***Presentation Sessions 2***	
	The Art and Science of Shrinking the Cybersecurity Gender Gap Laura Bate, *New America* and Dr. Davina Pruitt-Mentle, *National Institute of Standards and Technology (NIST)*	BALLROOM 3
	Hacking Your Day-To-Day Travel Addy Moran, *Raytheon*	COMMONWEALTH 2
	Footprinting Bigfoot—An External View of an Organization's Internet Presence Dori Clark, *Walmart*	BALLROOM 4
	Discovering and Inspiring Young Women Who Will Excel in Cybersecurity Michele D. Guel, *Cisco* and Alan Paller, *SANS Institute*	COMMONWEALTH 1
2:15 pm - 6:30 pm	***Career Fair***	KINGS GARDEN
2:15 pm - 6:30 pm	***Career Village***	STERLING
3:30 pm - 5:30 pm	***Workshop Series 3***	
	National Cybersecurity Curriculum Program: Labs and Resources for Your Classroom or Student Club Dr. Blair Taylor, *National Security Agency Contractor* and Maureen Turney, *National Security Agency*	BALLROOM 3
	Apprenticeships Powered by Industry—Build Your Talent Pipeline Wendy Brors, *Maher & Maher,* Carolyn Renick, *U.S. Department of Labor & Employment - Office of Apprenticeship*, Marian Merritt, *NIST NICE,* Tony Marshall, *ISG* and Trey Clark, *IBM*	BALLROOM 4
	Acquiring and Retaining Cybersecurity Talent: A Proven Model Deidre Diamond, *CyberSN* and *Brainbabe*	COMMONWEALTH 1

2019 WICYS CONFERENCE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
3:30 pm - 5:30 pm	***Panel Series 1***	COMMONWEALTH 2
	#METOO Cybersecurity: Managing Monsters without Losing Your Mind Diana Kelley and Lisa Lee, *Microsoft*, Edna Conway, *Cisco* and Kelley Misata, *Sightline Security*	
	Securing Critical Infrastructure Ashley Billman, Kristine Arthur-Durett, and Theora Rice, *Pacific Northwest National Laboratory* and Kristen Quade, *E-ISAC*	
5:45 pm - 6:30 pm	***Birds of a Feather (BoaF)***	
	Avoid Reinventing the "Wi" in WiCyS: How Common are Gender and Recruitment Challenges? Aryn Pyke and Erica Mitchell, *Army Cyber Institute, Westpoint*	COMMONWEALTH 1
	Surviving and Thriving as a Woman in Cybersecurity Emily Heath and Jen Burns, *The MITRE Corporation*	BALLROOM 3
	Internet Trolls and Cybersecurity Natasha Ferguson, *Highline College*	BALLROOM 4
	Cybersecurity Education: What Have We Still Not Figured Out for Greater Impact? Dr. Garima Bajwa and Dr. Mary-Margaret Chantre, *Capitol Technology University*	COMMONWEALTH 2
6:45 pm - 8:30 pm	***Dinner and Keynote***	BALLROOM 1 & 2
	Keynote Introduction: Dhivya Chandramonleeswaran, Lead Security Researcher, *Adobe* ***Keynote:* Tales of an Accidental Computer Science Professor** Lorrie Cranor, Director, *CyLab, Carnegie Mellon University*	
8:30 pm - 9:00 pm	***Special Event: CMU Bhangra!***	BALLROOM 1 & 2

Founded in 2006, CMU Bhangra endeavours to entertain its audiences by striking the balance between high levels of dancing, entertainment, and passion on stage. With our dancing we entertain, with our expressions we charm, and with our hearts we inspire. We believe that if we can make the audience feel something, that's it. We hope you enjoy catching a glimpse of the CMU Bhangra dance team!

2019 WICYS CONFERENCE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00 am - 12:00 pm	***Registration Open***	REGISTRATION, 2ND FLOOR
8:15 am - 3:00 pm	***Luggage Storage***	KINGS GARDEN A
8:15 am - 10:15 am	***Breakfast, Keynote, & Lightning talks***	BALLROOM 1 & 2
	Keynote Introduction: Diane Downey, Senior Software Architect, *Synopsys*	
	Keynote: Securing Yourself in a Social Media-, App-, and IoT-Crazy World	
	Patricia Denno, VP Global Intelligence Operations, *Fidelity Investments*	
	Lightning Talks	
	Don't Ask What You Want to Be When You Grow Up, But Ask... Nancy Lim, *Department of Homeland Security*	
	Making Sense of Netflow Network Traffic Pamela Toman and Haley Sayres, *Expanse Inc.*	
	Spotting Security Flaws in Code Before It's Written Yasmine Kandissounon, *Rackspace*	
	Hacking Humans: Addressing Vulnerabilities in the Advancing Medical Device Landscape Gabrielle Hempel, *Accenture*	
	A War Of Minds: The Role of Cognitive Science and the Arts in Thwarting Cyber Crime Dr. Monica Lopez, *La Petite Noiseuse Productions*	
	People (Users) are a Data Source—Are You Leveraging Them in Your Detection Strategy? Tonia Dudley, *Cofense*	
	Digital Forensics for SCADA Systems Rima Asmar Awad, *Oak Ridge National Laboratory*	
	Cybersecurity Strategies to Combat Human Trafficking Danielle Borrelli, *Cal Poly San Luis Obispo*	
10:15 am - 10:45 am	***Group Picture & Bag Check***	KINGS GARDEN B
10:45 am - 11:30 am	***Presentation Sessions 3***	
	To the Left, To the Left—How Beyoncé Can Help Us Develop and Deploy Secure Code Aditi Chaudhry, *Capital One*	COMMONWEALTH 2
	The Role of Deception in Attack Decisions Using Cybersecurity Scenarios Dr. Palvi Aggarwal and Dr. Cleotilde Gonzalez, *Carnegie Mellon University*	BALLROOM 3
	Working Together: How the Postal Service Builds an Inclusive and Exceptional Cybersecurity Workforce Lisa Holman, *United States Postal Service*	BALLROOM 4
10:45 am - 11:30 am	***Meet-Up Session for WiCyS Student Chapters (see box, p. 21)*** Moderated by Susan Jeziorowski and Julianne Cox, *Tennessee Tech University*	COMMONWEALTH 1
11:30 am - 12:15 pm	***Meet-Up Session for WiCyS Affiliates (see box, p. 20)*** Moderated by Marcelle Lee, *Fractal Security Group,* Amelia Estwick, *Excelsior College,* Racquel James, *Department of Defense,* and Nikkia Henderson, *General Services Administration*	COMMONWEALTH 1

2019 WICYS CONFERENCE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
11:30 am - 12:15 pm	***Presentation Sessions 4***	
	Cybersecurity: Hollywood vs. Reality Rinki Sethi, *IBM* and Prajakta Jagdale, Vidya Gopalakrishnan and Archana Muralidharan, *Palo Alto Networks*	COMMONWEALTH 2
	A Social Engineering Experiential Learning Project for Undergraduate Students Dr. Aunshul Rege, *Temple University, Department of Criminal Justice*	BALLROOM 3
	Cybersecurity Trends: Today Leading into Tomorrow Rachel Giacobozzi, Alpana Tyagi and Holly Parrish, *Ernst & Young*	BALLROOM 4
12::15 pm - 1:00 pm	***Panel Series 2***	
	Developing Security Products with a Little Help from Your Friends: Best Practices for Effective Cross-Functional Engagement Robyn Frye, Archana Ramamoorthy, Meera Nathan, Jason Lucibello and Sheetal Kanade, *Workday*	COMMONWEALTH 2
	Paying It Forward: How Women in Tech Groups Can Spark a Culture Shift, and How You Can Help! Dr. Dena Haritos Tsamitis and Era Vuksani, *Information Networking Institute, Carnegie Mellon University,* Saralee Kunlong, *YP*[SM] and Divya Ashok, *Salesforce*	BALLROOM 3
	Millennials in Cyber Dina Haines, *Utica College,* Nikkia Henderson, *University of Maryland University College*, Nishae Brooks, *Our Lady of the Lake University*, Bich Vu, *MIT Lincoln Lab* and Cara Zissman, *Ford Motor Company*	BALLROOM 4
	We Got Skills! Women Veterans Transitioning into the Cybersecurity Workforce Dr. Amelia Estwick, *National Cybersecurity Institute at Excelsior College,* Racquel James, *Department of Defense,* Molly Handy, *Symantec* and Joyous Huggins, *Defender Academy*	COMMONWEALTH 1
1:00 pm - 2:30 pm	***Lunch, Closing Remarks, Awards***	BALLROOM 1 & 2
	Keynote: the Art of Cutting Glass! Dr. Dawn Beyer, Senior Fellow, *Lockheed Martin*	
2:30 pm - 4:30 pm	***Workshop Series 4***	
	Listening to Internet Background Radiation Luna Frank-Fischer and Pamela Toman, *Expanse, Inc.*	BALLROOM 4
	Blockchain Technology and the Future Dr. Cynthia Irvine and Dr. Britta Hale, *Naval Postgraduate School*	COMMONWEALTH 1
	Pittsburgh CTF: Steal the Steel Dr. Vitaly Ford, *Arcadia University*, Amela Gjishti, *Bank of America* and Daniel Tyler, *Optum*	BALLROOM 3
	CTF4 Noobz: Tools and Tips for Cybersecurity Competitions Marcelle Lee, *WiCyS Mid-Atlantic Affiliate*, Lisa Jiggetts and Mari Galloway, *Women's Society of Cyberjutsu*	COMMONWEALTH 2

2019 WICYS CONFERENCE
WORKSHOPS

WORKSHOP SERIES 1
Thursday • 2:00 pm - 4:00 pm

Cyber Fire: Puzzle-Based Training
Neale Pickett and Grace Herrera,
Los Alamos National Laboratory

Cyber Fire is a computer security incident investigation training program within the U.S. Department of Energy. In this puzzles-only sampler of the event, you will use your laptop or mobile device to step through puzzles that teach investigation techniques. Cyber Fire establishes a hands-on environment where participants are encouraged to take risks and make mistakes with access to veteran responders to help explain approaches to puzzles and how they relate to real investigations. This hands-on event is heavy in practical application of cybersecurity skills such as mathematics, manual/automated packet inspection, static/dynamic analysis and disk/memory image inspection.

ATT&CK and Threat Actors
Kat Seymour, Heather Linn, Ken Smith and James Thomas,
Bank of America

This workshop introduces you to some basic techniques used to replicate threat actor behavior. You will work hands-on in putting a threat model to the test and trying various techniques like command injection and using the penetration testing framework Metasploit to accomplish an objective from the perspective of a threat actor. You should come away from the workshop with an increased understanding of how threat actors follow a chain of events to accomplish an objective, as well as a better understanding of how to protect yourself personally and professionally from a variety of threat actor techniques. You will be provided some pre-reading/pre-work to help make the most of this hands-on workshop.

Red Team Your Resume: Insiders Share Secrets
Kaitlin O'Neil, Kate Broussard, Kelly Albrink, *Bishop Fox,*
Troy Steece, *McAfee* and Linda Martinez, *Protiviti*

Are you applying for jobs in cybersecurity, and do you want recruiters to actually look at your resume? If you answered 'yes,' then maybe it's time to consider having your resume "red teamed." Each panelist will share their personal stories surrounding their starts in the industry. The path to success is rarely linear, and a well-rounded security resume should reflect that reality. Insights will include: certifications you'll want to earn, career highlights you may be ignoring and traditional versus non-traditional security backgrounds. The InfoSec job of your dreams is within your reach; it may require tearing apart your resume to land it. This panel will provide you with enough perspectives to feel like you have the knowledge to position yourself as a competitive candidate.

Join us for a Blue Team CTF — Solve security puzzles using network and host-based forensics in a Jeopardy-style CTF. Get a taste for what working on the Blue Team is like with real-world data and examples pulled from our actual jobs. No experience necessary! Bring a laptop with wifi and software to run a VM (e.g. VMware or VirtualBox); we'll provide you with the other tools needed to solve the puzzles. Puzzles will range in difficulty and subject, so everyone will find something they can work on, and forming teams will be encouraged. We'll play with PCAPs to dissect network traffic, emails to diagnose phishing, and Windows Event Logs to track down the malware.

Blue Team Capture the Flag (CTF)
Elizabeth Schwinsberg and Bridget Pelletier-Ross,
Facebook

Join us for a Blue Team CTF — Solve security puzzles using network and host-based forensics in a Jeopardy-style CTF. Get a taste for what working on the Blue Team is like with real-world data and examples pulled from our actual jobs. No experience necessary! Bring a laptop with wifi and software to run a VM (e.g. VMware or VirtualBox); we'll provide you with the other tools needed to solve the puzzles. Puzzles will range in difficulty and subject, so everyone will find something they can work on, and forming teams will be encouraged. We'll play with PCAPs to dissect network traffic, emails to diagnose phishing, and Windows Event Logs to track down the malware.

SFS MEETUP

SCHOLARSHIP FOR SERVICE

Thursday, 7:00-8:00 pm - Kings Terrace

Come and meet SFS (CyberCorps) students, faculty and agencies participating in the program. Learn how to get into the program. Network with fellow students currently in the program.

1:1 FUNDING MEETUP

EDUCATORS & FUNDING AGENCIES

Thursday, 8:00-9:00 pm - Kings Terrace

For Educators, this sessions provides one-to-one conversations with program directors/managers at various funding agencies such as NSF and NSA.

2019 WICYS CONFERENCE
WORKSHOPS

WORKSHOP SERIES 2

Thursday • 4:30 pm - 6:30 pm

Distributed Forensics Across Time and Space

Elena Kovakina and Jesus Aguilar, *Google*

Welcome to Cyber Forensic Affordances (CFA). For the length of this workshop, you are a part of the CFA investigative team trying to solve the mysterious Greendale case. This interactive workshop will introduce timeline building and analysis with open source digital forensics tools. We will use the processing depth of Plaso and the analytic and collaborative capabilities of Timesketch to achieve our goals and solve the case. You will learn how to build timelines, analyze logs data from multiple machines and tell exciting stories with your insights.

Gaining Initial Access in a Penetration Test

Krysta Coble, Kelly Thiele, Laura Puterbaugh and Petya Lopez, *Department of Homeland Security*

Have you ever wondered what it would be like to hack into a government agency? We can tell you all about that—legally, of course! At the Department of Homeland Security (DHS), the National Cybersecurity Assessments and Technical Services (NCATS) team works to help federal and state governments enhance their cybersecurity posture through a variety of free services. As phishing campaigns are the most successful attack vector from real-world threats, our workshop will cover how we use phishing as a method to gain initial access into our customer networks.

This workshop provides a high-level explanation of the hacker methodology with hands-on experience in the Exploitation/Initial Access phase. We are operating under the assumption that all legal agreements and scoping has already been conducted to start the assessment and considered completion of the Reconnaissance phase. To start, we'll discuss infrastructure setup and assessment prerequisites. Next, we'll craft phishing emails and attach "malicious" payloads that report back to our attack platform when clicked. Finally, we'll achieve situational awareness of our current access and strategize our next steps in the assessment.

WiCyS Social CTF Village and Competition

Dr. Dan Manson, *Cal Poly Pomona*, Kaitlyn Bestenheider, *Tevora,* Franz Payer, *Cyber Skyline,* Jeana Cosenza and Vicente Gomez, *Pace University*

The National Cyber League (NCL) offers engaging, entertaining, measurable and scalable methods of learning to enlist a new generation of cybersecurity professionals. Following up on our highly successful NCL workshop at WiCyS 2018, we will host an immersive social NCL Capture the Flag (CTF) to take place during the entire WiCyS 2019 conference.

Activities will occur in an NCL village. This will be a multi-station space with something for everyone. There will be dedicated spots for fellow NCL student champions, who will help run challenge category-specific work groups training students and coaches alike in categories such as Cryptography, Log Analysis, Network Traffic Analysis, Web Access Exploitation, Password Cracking and more.

Students can talk with NCL Chief Player ambassador Kaitlyn "CryptoKait" Bestenheider to learn how NCL jump-started her education and career. Educators and coaches can learn about incorporating NCL into their classroom curriculum from Chief Coach ambassador Steven Miller. Recruiters and talent scouts can meet with NCL commissioner Dr. Dan Manson to learn how they can use NCL's Scouting Report to find top talent in their area! Challenges for this entire conference-long CTF will be tailored for the WiCyS community in an effort to drive students to learn more about WiCyS as part of their research to solve challenges. Competition winners will receive prizes and a free game code for the next NCL season, and all students will receive NCL swag.

Advanced APT Hunting with Splunk

Lily Lee and John Stoner, *Splunk Inc.*

You wanna learn how to hunt the APTs? This is the workshop for you. Using a real-world type dataset, this workshop will teach you how to hunt the fictional APT group Taedonggang. We will discuss the Diamond model, hypothesis building, LM Kill Chain and MITRE ATT&CK framework and how these concepts can frame your hunting. Then we will look deep in the data using Splunk and OSINT to find the APT activity riddling a small startup's network. We will walk you through detecting lateral movement, the P of APT and even PowerShell Empire. At the end, we will give you a similar dataset and tools to take home to try newly learned techniques yourself.

AFFILIATES MEETUP

STAY TOGETHER WITH WICYS

Saturday, 11:30 am-12:15 pm - Commonwealth 1

Join the five established regional affiliates as they share lessons learned in starting a new WiCyS affiliate. You don't need to reinvent the wheel! Learn from the WiCyS Mid-Atlantic Affiliate as members of the first WiCyS Affiliate share guidelines on structure, maintaining a nexus to WiCyS national, officer elections, sponsorship, logistics, communications, membership recruitment and social media.

2019 WICYS CONFERENCE
WORKSHOPS

WORKSHOP SERIES 3

Friday • 3:30 pm - 5:30 pm

National Cybersecurity Curriculum Program: Labs and Resources for Your Classroom or Student Club

Dr. Blair Taylor, *National Security Agency Contractor* and Maureen Turney, *National Security Agency*

Faculty, are you looking for cybersecurity curriculum and resources? Cybersecurity clubs, are you looking for enrichment activities and exercises that help students enhance their cybersecurity knowledge and skills?

In this workshop, you will access, use and download cybersecurity curricula, labs and resources freely available through the National Security Agency's National Cybersecurity Curriculum Program (NCCP). Over 50 schools and universities have developed effective and engaging cyber curriculum modules in needed topic areas including networking, risk management, cybersecurity laws and policies, cybersecurity principles, secure coding, ethics and cyber threats and vulnerabilities. This workshop will provide an overview of NCCP and allow faculty and students time to access and download curriculum from www.clark.center. By the end of this workshop, you will leave with your own library of curriculum resources for your classroom or clubs.

Apprenticeships Powered by Industry - Build Your Talent Pipeline

Wendy Brors, *Maher & Maher*, Carolyn Renick, *U.S. Department of Labor & Employment - Office of Apprenticeship*, Marian Merritt, *NIST NICE,* Tony Marshall, *ISG* and Trey Clark, *IBM*

Think apprenticeships can't work in cybersecurity? Think again. Across the world, companies are struggling to find skilled talent. We must rethink the way we approach education, especially in innovative industries where technology rapidly outpaces traditional education and training. It is time to innovate talent development, and no one is better situated to do that than the industry innovators themselves.

This workshop will dig deep into two successful cybersecurity apprenticeship programs that are building their cybersecurity talent pipeline. Integrated Systems Group (ISG), a small technology company, and IBM are two very different companies addressing the challenge of finding, training and retaining talent through apprenticeships. Maher & Maher and the U.S. Department of Labor and Employment are partnering with companies like ISG, IBM and national trade associations to create and deliver tools and support to help companies of all sizes as well as explore and implement apprenticeships as a modern talent development solution.

This workshop will provide access to those tools and resources to help you customize a program that will work for you and the women you seek to fill the talent pipeline. You will learn the key elements of high-quality programs and how to partner with educators and other public and industry partners to access existing tools while building a program that will work for you.

Acquiring & Retaining Cybersecurity Talent: A Proven Model

Deidre Diamond, *CyberSN* and *Brainbabe*

Workforce development is reliant on the combination of a subject-matter common language framework of projects and tasks. Job descriptions are then derived from this same framework definition. A career development plan based on standardized projects and tasks, along with a culture that allows for psychological safety, will allow you to acquire and retain talent. When we combine daily processes of business operations derived from a subject-matter common language, in which all teammates know their role and the roles of others on the team (along with a culture that allows humans to think, feel and perceive without negative consequences), we can truly experience workforce development in any subject-matter profession. Come hear how to achieve this success in cybersecurity. Between our technology and our theories, we are showing that organizations can obtain cybersecurity talent in less than 60 days and retain them.

STUDENT CHAPTER MEETUP

GROW WITH WICYS

Saturday, 10:45 am-11:30 am - Commonwealth 1

Interested in joining or starting a WiCyS Student Chapter at your institution? Come to the Student Chapter Meetup! 49 WiCyS Student Chapters have launched over the last 6 months. You will hear about successes as well as challenges from Chapter leaders, learn how to overcome those challenges, share your story, and find peer support. You will also learn how Student Chapters can secure funding for their activities, as well as use the WiCyS Online Community Forum and Social Media outlets.

Join us and get inspired to bring cybersecurity awareness and cyber-engagement activities to your campus.

2019 WICYS CONFERENCE
WORKSHOPS

WORKSHOP SERIES 4

Saturday • 2:30 pm – 4:30 pm

Listening to Internet Background Radiation

Luna Frank-Fischer and Pamela Toman, *Expanse, Inc.*

Beneath the surface of the internet, there is a huge amount of "noisy" packets that are illegitimate attempts to connect to services. This noise is persistent, consistent and loud. The majority comes from bots and worms like Mirai and WannaCry, which blindly attempt to infect their internet neighbors and spread their reach. The existence of background radiation is an emergent property of the networked internet, and trends in background radiation give defenders insight into the relative attention of attackers.

Blockchain Technology and the Future

Dr. Cynthia Irvine and Dr. Britta Hale, *Naval Postgraduate School*

Blockchain technology (BT) supports distributed ledgers and has been identified as a mechanism that can support applications ranging from crypto currencies and event logs to supply chain security and as a cause of and mitigation for climate change. This two-hour, interactive workshop will introduce you to the basic concepts associated with BT and prepare you to ask critical questions regarding blockchain proposals, applicability and implementations. You will learn how to set up a simple blockchain lab and be guided through a simple exercise.

In this workshop, we'll support you in standing up software to observe internet background radiation, and we'll enable you to perform basic analyses on what you see and report on those findings. You will establish AWS machines in varied locations, log the connections received and work together to identify the ports that garner substantial interest. You will walk away with an understanding of how internet scanning fits into the landscape of cybersecurity as both an omnipresent source of attacks and a powerful defensive tool. You will be empowered to independently build on what you learn during this workshop and engage in larger conversations about internet security with new context and skills.

Pittsburgh CTF: Steal the Steel

Dr. Vitaly Ford, *Arcadia University,* Amela Gjishti, *Bank of America* and Daniel Tyler, *Optum*

Capture the Flag competitions (CTFs) have become a defacto standard for cybersecurity training. As a result, CTFs are a great way to showcase your cybersecurity skills and build your resume. There are many CTFs available (like https://ctftime.org/) that cover such topics as cryptography, steganography, forensics, exploitation and web attacks. However, very few are focused on the secure coding aspects of software engineering. In this workshop, we plan to teach secure coding through a team-based, Pittsburgh-themed "Steal the Steel" CTF (steel will represent the flag points for each challenge as Pittsburgh is known for steel production and having the most bridges than any other city in the world).

CTF4 Noobz: Tools and Tips for Cybersecurity Competitions

Marcelle Lee, *WiCyS Mid-Atlantic Affiliate,* Lisa Jiggetts and Mari Galloway, *Women's Society of Cyberjutsu*

Interested in cybersecurity competitions but don't know where to start? Or have you tried one or two or 10 and want more practice? In this hands-on keys workshop, we will explore different types of competitions from Capture the Flag to offense/defense and everything in between. In addition, we will review various tools of the cyber trade. These will become part of your toolkit to solve cybersecurity competition challenges! You will be provided with a virtualized environment that will be used to explore techniques associated with reconnaissance, scanning and enumeration, and exploitation. Also featured will be forensic challenges, hash-cracking, binary analysis, crypto decoding, etc. The challenges are related to topics covered in the EC Council Certified Ethical Hacker (C|EH) certification.

PRESENTATION SESSIONS

PRESENTATION SESSIONS 1

Friday • 12:00 pm - 12:45 pm

Double Your Might: A Data Science Primer for Security Analysts

Joanna Hu, *Exabeam*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Artificial intelligence (AI) and machine learning are in the air. It's hard to research a new security technology without running across these terms. With the development of new applications and hacker skills, traditional security technology increasingly suffers from two drawbacks: large false alarms and unknown threats. Advances in data science can help security systems identify hidden patterns and weak traits of attacks with no predefined rules but with much higher accuracy. For example, machine learning can identify which new activities are really suspicious while dismissing false alarms through profiling user and system behaviors.

Machine learning can also provide more context information to help an investigation classify if a user is an executive; link all accounts belonging to one single user together; identify the personal emails of an employee and use deep learning to detect anomalous SQL query commands. The machine learning models can evolve automatically by incorporating new input data and analysts' feedback.

Attendees will learn: The key disciplines of data science, machine learning, artificial intelligence, deep learning, etc.; a few use cases on how security analysts can partner with data scientists to improve security (detecting if a user changes his normal behavior, identifying employees' personal emails based on email logs, using deep learning to identify anomalous asset names); tough questions to ask vendors about how they apply machine learning and artificial intelligence; what's over the horizon as machine learning and AI progress.

Security and Privacy Challenges for Connected and Autonomous Vehicles

Lily Yang, *Intel*

TRACK: LOOKING AHEAD

The automobile industry is undergoing major disruptions due to technological advances in artificial intelligence (AI) and connectivity that promise to significantly improve both safety and transportation efficiency on the road. The development of Connected and Autonomous Vehicles (CAV) has attracted a lot of investment and public attention. CAVs also have become a shining target for attacks and hence an interesting platform to study its security, privacy risks, implications and challenges. In addition to advanced onboard sensors such as cameras, LIDAR and radars, cars also have become increasingly connected not only to the network but also to each other (vehicle-to-vehicle or V2V), to pedestrians or to roadside infrastructures such as smart traffic lights. Such V2X capability further improves the safety on the road as wireless radio does not have the line of sight limitation of most onboard sensors and can provide longer range, therefore receiving information from cars that may be obstructed.

This presents a fundamental security challenge as cars now not only have to rely on the onboard sensors but also have to trust information received from other cars that are random strangers. One of the fundamental technologies which CAVs are being developed for is machine learning methods such as DNN for perceptions as cameras are being deployed as the eyes of CAVs. This presentation will examine the newly emerged security threats and privacy concerns in the exciting domain of CAV and provide a brief overview of the industry and research community on these topics.

We Can Do It! Becoming a 21st Century Rosie the Riveter

Michelle Duquette, *Battelle* and Kelley Goldblatt, *Capitol Technology University*

TRACK: CAREER DEVELOPMENT

You hear it in the news: Government lacks "cyber warriors," networks are susceptible to hackers and data is being stolen. But what does it really take to work for the government, and what is it like to help solve these problems? Thousands of cybersecurity jobs are unfilled within the government and technology companies that support federal contracts. How do you become a 21st Century Rosie the Riveter?

All the Colors of INFOSEC

Cynthia Cox, Mary Sawyer, Muoi Landivar and Shawn Richardson, *Palo Alto Networks*

TRACK: BEST PRACTICES

Students are aware that cybersecurity is a growing field with many job opportunities. However, many students appear to only be aware of the Red/Blue/Purple function because these are mentioned during security breaches. There are many other functions and skill sets found in an information security department, and we need even more diverse skills and mindsets to solve tomorrow's challenges.

CAREER VILLAGE

FREE CAREER ADVICE

Thursday, 3:00 pm-6:00 pm - Bridges;
Friday, 10:45 am-12:00 pm and
2:15 pm-6:30 pm - Sterling

Need your resume critiqued? Come to the Career Village on Thursday!

Need a professional headshot? Free headshots are being taken Thursday 12:00 pm - 6:00 pm in the Foyer.

On Friday, stop in for mock interviews, resume reviews, and one-on-one advice from cybersecurity professionals.

PRESENTATION SESSIONS

PRESENTATION SESSIONS 2

Friday • 2:15 pm - 3:00 pm

Hacking Your Day-To-Day Travel

Addy Moran, *Raytheon*

TRACK: LOOKING AHEAD

Cars, public ground transportation, boats and aircrafts are all prominent modes of transportation for 7.5 billion people across the world. All of these rely on message-based protocols to operate, which are used across military, government and civilian applications. Among the most common protocols are MIL-STD-1553B (aka 1553), Modbus and CAN bus. These are unencrypted and contain documentation with "gray" areas that allow different implementations and little to no input validation. Due to these insecurities, many forms of attack can and do compromise these systems such as signal and address spoofing, fuzzing attacks and message injection. These attacks are getting more and more common due to the simplicity of the protocols and relatively inexpensive tools necessary to complete an attack.

Across the world, there is offensive and defensive research being conducted to protect against known vulnerabilities. There are two MIL-STD-1553B products Raytheon is developing that would help prevent message injection, spoofing and fuzzing attacks. One is similar to "NMAP for 1553," which is an on-tarmac network parser to help identify components that shouldn't be there. The other product acts as a device that finds malicious messages being sent across the bus during flight. There also is research being done on encrypting these protocols.

Footprinting Bigfoot—An External View of an Organization's Internet Presence

Dori Clark, *Walmart*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

What's the easiest way for a novice malicious actor with limited skills to exploit your organization? Through the often exposed, unknown and unsupported internet facing assets—an organization's external digital footprint. The best bug bounty stories often start with, "I found this site that X company didn't realize was still out there." What could you see if you approached your organization like a bug bounty hunter or malicious attacker trying to find old, forgotten, unprotected doors to the castle?

This talk covers strategies, open-source tools, data sources, mapping and automation techniques I use to map and understand the giant footprint of our Walmart organization and practical ways to apply them to any size firm. I will discuss strategies for applying data from both technical and business sources to improve the accuracy of the footprint in a rapidly evolving organization. I also will demonstrate practical application of this data to identify vulnerable targets that need evaluation to keep an organization secure.

The Art and Science of Shrinking the Cybersecurity Gender Gap

Laura Bate, *New America* and Dr. Davina Pruitt-Mentle, *National Institute of Standards and Technology (NIST)*

TRACK: BEST PRACTICES

The cybersecurity field is unique in many ways, but its struggles with diversity, equity and inclusion is not one of them. There is, for example, a lot we can learn from how other disciplines have addressed tricky problems around the recruitment, retention and advancement of women. In November 2018, New America hosted a workshop with support from the National Initiative on Cybersecurity Education (NICE) on women in cybersecurity. At this WiCyS session, we hope to share our findings and present clear, actionable recommendations to shrink cybersecurity's gender gap.

The November workshop drew on the experience of longtime advocates of gender diversity within the cybersecurity community and additionally on new perspectives from experts in behavioral science, organizational change, business strategy, innovation and other disciplines. We will present what we learned from these experts, focusing on specific actions that different demographics (students, business leaders, educators, male allies) can take to engage and advance women in cybersecurity. We also will present, and seek input on, a resource we developed for this project: a community scan of the organizations working on women in cybersecurity and the resources that are available to students, educators and others in the community.

Discovering and Inspiring Young Women Who Will Excel in Cybersecurity

Michele D. Guel, *Cisco* and Alan Paller, *SANS Institute*

TRACK: CAREER DEVELOPMENT

The combination of an extreme shortage of technically advanced cybersecurity professionals and the low profile (12%) that women have in the field, make pursuing a cyber career a great option young people today, especially girls. Three questions have stumped policy makers and educators trying to make that promise into reality:

1) How to entice and delight young women and double or triple the number of young women who enter this field, at a national scale;

2) How to determine, in advance, which young women are most likely to excel in advanced cybersecurity roles;

3) How to accelerate young women's (and men's) mastery of deep technical skills, in rural, inner city and other schools that may not have teachers who have that deep technical mastery.

In this session, you'll learn about surprisingly promising answers to all three questions—from pilot programs in the United Kingdom and in 16 U.S. states involving 35,000 high school and college students. You'll also hear about a national test, in 26 U.S. states with 2,000 high schools and colleges beginning during WiCyS.

PRESENTATION SESSIONS

PRESENTATION SESSIONS 3

Saturday • 10:45 am - 11:30 am

To the Left, To the Left—How Beyoncé Can Help Us Develop and Deploy Secure Code

Aditi Chaudhry, *Capital One*

TRACK: LOOKING AHEAD

The goal of DevSecOps is to build on the mindset that "everyone is responsible for security." It is about pushing security left and automating core security tasks. In the song 'Irreplaceable', Beyoncé had the right idea when she sang "to the left, to the left." We want to push security to the left of the SDLC to ensure that application security starts as one codes.DevSecOps allows developers to focus on writing high quality and secure code, enabling teams to release titanium applications. This presentation will cover how DevSecOps can be used by an enterprise to develop and deploy secure code. We will discuss the origins of DevSecOps and how it differs from DevOps, the importance and benefits of DevSecOps, how to implement DevSecOps in a production environment and challenges faced during implementation.

The Role of Deception in Attack Decisions Using Cybersecurity Scenarios

Dr. Palvi Aggarwal and Dr. Cleotilde Gonzalez, *Carnegie Mellon University*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Deception, the art of making someone believe in something that is not true, may provide a promising real-time solution against cyber attacks. Honeypots are one of the effective deception tools in the network defense to lure hackers. They are servers that mimic a real server with high value, but they are actually fake.

This research aims to understand the motives and processes involved in making attack and defend decisions in cybersecurity scenarios involving deception. We use laboratory experiments and build computational cognitive models that represent the process by which attack and defend decisions are made in simplified, simulated scenarios. We will report on the results of a laboratory experiment using a game designed to investigate the role of deception (i.e., amount and timing) on a hacker's decisions. Results revealed the average proportion of attacks was lower and non-attacks were higher when deception occurred late in the game and when the amount of deception was higher. This result found in an abstract simplified scenario was replicated in a real-world simulation tool called the HackIT. HackIT is a cybersecurity tool that allows us to create various cyber situations and map to real-world cyber attack scenarios by involving two phases: probe and attack.

The probe phase involves scanning webservers in the network for vulnerabilities while the attack phase involves gaining access to different computers and stealing information or compromising computer systems. By using the HackIT tool, one can create networks of different sizes, use deception and configure different webservers as honeypots, and create any number of fictitious ports, services, fake operating systems and fake files on honeypots. The HackIT tool can run various network commands that include nmap, use_exploit, ls and scp. Learning about the decisions of hackers and analysts in the HackIT tool can help cybersecurity teams train analysts against hackers and their different attack strategies in simulated real-world settings. The development of the HackIT game was a step toward analyzing human decisions in cybersecurity environments.

Working Together: How the Postal Service Builds an Inclusive and Exceptional Cybersecurity Workforce

Lisa Holman, *United States Postal Service*

TRACK: BEST PRACTICES

The Postal Service Corporate Information Security Office (CISO) safeguards the information technology infrastructure at the center of a $1.4 trillion mailing industry. In doing so, our organization supports the cybersecurity needs of the USPS corporate network and mail processing environment, protecting more than 310,000 handheld scanners, 168,000 computers and 8,500 pieces of automated mail-handling equipment. To sustain and grow Postal Service operations, CISO relies on a state-of-the-art cybersecurity workforce capable of defending the organization against an evolvs, serves as the foundation for our industry-leading approach to cybersecurity leadership development. This session will provide an inside look into the programs CISO leverages to develop the next generation of skilled, diverse and high-potential cybersecurity leaders. These include both internal CISO offerings—like the innovative CISO Academy, a 17-week training program covering over 30 cybersecurity focus areas—and enterprise-wide leadership initiatives that help CISO grow and maintain a world-class talent pipeline. You will learn strategies for developing a collaborative and effective workforce in the midst of a crippling cybersecurity talent shortage. You'll also learn how CISO builds a diverse and inclusive workforce that provides development opportunities for employees across all walks of life.

Don't leave before picking up your free button and sticker at the WiCyS Booth!

PRESENTATION SESSIONS

PRESENTATION SESSIONS 4

Saturday • 11:30 am - 12:15 pm

Cybersecurity: Hollywood vs. Reality

Presenters: Rinki Sethi, *IBM,* Prajakta Jagdale, Vidya Gopalakrishnan and Archana Muralidharan, *Palo Alto Networks*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Cybersecurity is now a frequent spotlight in Hollywood films and television programs. But have you ever wondered how realistic the portrayal is of this field and the professionals who work in cybersecurity? We have designed a panel to share with you what Hollywood has gotten right and where they miss the reality of being a cybersecurity professional. The panel includes amazing speakers whose experience in the field ranges between two and over 15 years and encompasses fields like incident response, product security, red team and risk management, among others. Through this conversation, you will discover what the day-to-day life of a cybersecurity professional entails and hear the tales of Hollywood-esque excitement these professionals have faced in their careers. You also will learn about the variety of characters that make up real-world cybersecurity teams and how they match up to what the entertainment industry would have us believe. We are hopeful the panel will enlighten you on the expectations and challenges this profession presents.

A Social Engineering Experiential Learning Project for Undergraduate Students

Dr. Aunshul Rege, *Temple University, Department of Criminal Justice*

TRACK: BEST PRACTICES

The human element is often regarded as the weakest link in cybersecurity. However, education efforts focus primarily on the technical aspects of cybersecurity and downplay the relevance of the human factor. One way to exploit this human vulnerability is through social engineering, where cybercriminals use persuasion and manipulation to get targets to reveal private information.

This talk shares efforts to engage undergraduate social science and computer science students in a hands-on social engineering project across the fall 2017 and spring 2018 semesters. It uses the experiential learning framework that promotes "learning by doing." Specifically, this talk focuses on a "shoulder surfing" project, where students were divided into teams of three to four members. Each team had to take a picture of any of the opposing team member's screen while they were surfing or viewing their Facebook, Twitter, LinkedIn or other social media accounts. The teams had to include a clear screenshot of the rival team member's activity and a partial shot of their face to successfully identify that person.

The talk offers a comparative analysis of these projects over the two semesters, sharing the experiences and challenges faced by both the students and myself. It also details the issues of designing projects that follow university ethics standards, training students in human subjects research ethics, generating relevant instructions and rubrics, and evaluating student engagement and learning. To conclude, I will initiate dialog in the area of hands-on learning for students across multiple disciplines.

Cybersecurity Trends: Today Leading into Tomorrow

Rachel Giacobozzi, Alpana Tyagi and Holly Parrish, *Ernst & Young*

TRACK: LOOKING AHEAD

At a strategic level, this presentation will explore the top 10 cyber threats, and how these trends have impacted 2018 and their probability of impacting 2019. As we walk through the threat landscape, we will provide some examples of how these prolific threats manifest themselves in every day incidents across all industries. Then we will dive deep into how companies can better track and manage two of the biggest security threats: vulnerabilities and phishing. This presentation will provide guidance on how to track and analyze internal network indicators to tackle phishing threats. We will then explore how to best track the latest vulnerabilities and assess the impact to your company to help drive updates in a timely manner.

BIRDS OF A FEATHER

BIRDS OF A FEATHER

Friday • 5:45 pm - 6:30 pm

Surviving and Thriving as a Woman in Cybersecurity

Emily Heath and Jen Burns, *The MITRE Corporation*

TRACK: BEST PRACTICES

This session will discuss common problems and issues faced, tips for developing effective coping strategies and methods of constructing support networks. The discussion will focus on challenging or uncomfortable situations where a colleague or coworker expresses a sexist attitude or sexist views, intentional or not. The purpose is to allow attendees to take a step back and give themselves time to think through an appropriate response. Strategies like leaning into a conversation to avoid being interrupted, owning your statements to sound authoritative and effectively taking the credit for your work will be explored. Potential scenarios for discussion range in severity, and the interests of attendees will guide the conversation. Possible additional topics for discussion include avoiding and handling common female stereotypes, recruiting allies and engaging in outreach efforts.

Internet Trolls and Cybersecurity

Natasha Ferguson, *Highline College*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Anyone who spends time on the internet will come across what is known colloquially as a troll. Trolling activity can range from a relatively harmless comment on a news site, doxing a person with different political views or even serious criminal behavior against a person, group of people, government or business. How do we defend against trolling behaviors to protect the masses from bullying or companies from attacks? What motivates trolls? How do we determine who is a troll and what is trolling behavior? Is trolling a form of free speech? This talk will get different perspectives about trolling and how to combat it.

Avoid Reinventing the "Wi" in WiCyS: How Common are Gender Disparities and Recruitment Challenges?

Aryn Pyke and Erica Mitchell, *Army Cyber Institute, West Point*

TRACK: CAREER DEVELOPMENT

Those attending WiCyS already have, at the very least, an ear to the rail or a foot in the door of the cybersecurity domain. Many other women, who have ample drive, creativity and intellect, have opted out of cybersecurity pursuits, however.

In this session, we will discuss factors that influence women to self-select out of this domain. Given the diversity of WiCyS attendees, we hope to explore the extent to which gender disparities and recruitment challenges are common across different cybersecurity roles and sectors such as cybersecurity educators, researchers, industry professionals and civilian and military public sector professionals. Since some issues are shared across sectors, we will avoid re-inventing the wheel through developing and disseminating common solutions. Instead, we will identify and learn about roles and/or sectors that have made the most progress in resolving gender disparity.

For less progressive sectors where this disparity remains particularly pronounced and challenges may be somewhat distinct—e.g., the military cyber workforce—this discussion can serve as a catalyst to generate potential solutions informed by the collective insights of cybersecurity sisters in other sectors.

Cybersecurity Education: What Have We Still Not Figured out for Greater Impact?

Dr. Garima Bajwa and Dr. Mary-Margaret Chantre, *Capitol Technology University*

TRACK: LOOKING AHEAD

The field of cybersecurity has exploded in the last decade and its landscape is rapidly evolving with emerging technologies such as Blockchain, Internet of Things, Deep Learning, and Quantum Computing. The goal of the Birds-of-a-Feather session is to talk about the experiences of both educators and students in navigating through the cyberspace. The discussions will highlight the lessons learnt and bring insights into what our community has yet to figure out to have greater impact in moving ahead. Specifically, we will discuss the following;

- Fundamental barriers to large scale cybersecurity education
- Metrics to assess the quality of cybersecurity education
- Data sharing of real-world cybersecurity case studies
- Diversity in pipeline

2019 WICYS CONFERENCE
PANELS

PANEL SERIES 1

Friday • 3:30 pm - 5:30 pm

#METOO Cybersecurity: Managing Monsters without Losing Your Mind

Diana Kelley and Lisa Lee, *Microsoft,* Edna Conway, *Cisco* and Kelley Misata, *Sightline Security*

TRACK: CAREER DEVELOPMENT

Harvey Weinstein gets the headlines, but harassment happens in all professions. In the cyber world, with only 11 percent of workers being women, it can be hard to speak out about unwanted overtures and delayed career advancement. But it doesn't have to be that way. We are a group of four women leaders in cybersecurity who have dealt with harassment, bullying and bias in our careers.

The panel will start with each woman sharing her #METOO story. We will then address specific approaches on how to manage harassment and bias including: how to report to higher ups, how to help educate team members on being inclusive and respectful, where to find help and support, and clear examples of what we did in our careers to overcome the bias or harassment and succeed. We'll then open up the discussion as a safe space for others to heal through sharing their own stories and supporting one another with advice on how to continue to grow and succeed. The panel is led by moderator Diana Kelley.

Securing Critical Infrastructure

Ashley Billman, Kristine Arthur-Durett, and Theora Rice, *Pacific Northwest National Laboratory* and Kristen Quade, *E-ISAC*

TRACK: LOOKING AHEAD

Critical infrastructure is the backbone of the world's economy, security and safety. It represents the confluence of physical systems, cyber systems, government and private industry. Securing this infrastructure is an exciting and diverse field that requires many perspectives and areas of expertise. This panel will focus on different disciplines within securing critical infrastructure and how collaboration is the key to success including Industrial Control Systems (ICS), Data Science, Cybersecurity Analytics and Government and Private Industry Bring it All Together. The overarching theme of this panel is that complex problems require a multidisciplinary approach, and a diversity of teams is critical to achieve this. The panel will have participants from different fields of study and practice within the domain to provide input and examples of how collaboration is key to address the challenges presented by securing critical infrastructure.

PANEL SERIES 2

Saturday • 12:15 pm - 1:00 pm

Developing Security Products with a Little Help from Your Friends: Cross-Functional Engagement

Robyn Frye, Archana Ramamoorthy, Meera Nathan, Jason Lucibello and Sheetal Kanade, *Workday*

TRACK: BEST PRACTICES

We operate in a world where the pace of change within innovation causes many positive disruptions to our everyday lives. Ridesharing and other industry-disrupting companies have altered how products are perceived and have brought a revolutionary shift in the way they bring products to market. In this era of constant evolution, it is critical to keep customer security, privacy and compliance in mind while delivering products that scale for the growing user base. Brand value is dictated by how much a company invests in both meeting customer requirements as well as on keeping their data safe, secure and private.

In a day and age when product expiry dates are dictated by the fluid market condition, how do you build products that not only satisfy the customer requirements but adhere to proper security protocols and standards to keep data safe? How do you comply with privacy guidelines set forth by standards and regulatory boards to help businesses meet best practices? How do you build products that are resilient and modular in nature that are both scalable and maintainable in case we detect industry vulnerabilities?

Join these subject matter experts and exceptional leaders from Workday's privacy, security, compliance and technology operations teams to engage in a lively discussion on the product development road to production and the critical teams you must engage in order to avoid last minute roadblocks, timeline delays or your project being killed. We'll discuss the pitfalls to avoid and best practices to consider as you lead your product from concept to delivery. Our goal is to leave you with tangible tips and tricks you can employ to build privacy and trust into the very fabric of your product offering. After all, these are key areas that should be considered from day one, not as an afterthought.

Paying It Forward: How Women in Tech Groups Can Spark a Culture Shift, and How You Can Help!

Dr. Dena Haritos Tsamitis and Era Vuksani, *Information Networking Institute, Carnegie Mellon University,* Saralee Kunlong, *YP℠* and Divya Ashok, *Salesforce*

TRACK: BEST PRACTICES

What's the secret to attracting and retaining more women in cybersecurity and technology in general? I'll sit down with three dynamic women leaders in the tech industry to discuss women's groups, how to change the culture in cybersecurity, the role of gender allies and the movement behind equal respect.

2019 WICYS CONFERENCE
PANELS

Research shows that culture matters when it comes to increasing the number of women in tech. A welcoming and supportive environment is a necessity, and women's groups play a vital role, especially in a field like cybersecurity, where women make up only 24 percent of the workforce. In 2005, the graduate student organization Women@INI (WINI) at Carnegie Mellon University (CMU) was founded to address the unique challenges faced by women in the male-dominated field of engineering. WINI fosters a respectful, inclusive environment that allows women to openly discuss common struggles they face in the field, demonstrate their qualifications with confidence and serve as role models for the next generation of women in STEM. In 2002, there were only two women in an incoming class of 34 students—just under six percent. In fall 2018, the INI welcomed an incoming class made up of 42 percent of women.

This significant increase is not coincidental, it was the result of intentional efforts to create an environment that would attract, empower and support women. WINI has created a culture of paying it forward. In this panel, two alumnae will share how WINI inspired them to get involved in women's organizations at their workplaces. Saralee Kunlong started YP Women at YP, and Divya Ashok is president of Salesforce Women's Network, known informally as "Femmeforce." My WINI co-founder Chenxi is a founder of the Equal Respect movement and crusader for the booth babe ban at the RSA Conference. Together, we will discuss how to create an equal playing field with equal respect for all and spark a culture shift in organizations while also inspiring participants to start women's groups and other employee resource teams in support of diversity at their schools and workplaces.

Millennials in Cyber

Dina Haines, *Utica College*, Nikkia Henderson, *University of Maryland University College*, Nishae Brooks, *Our Lady of the Lake University*, Bich Vu, *MIT Lincoln Lab* and Cara Zissman, *Ford Motor Company*

TRACK: CAREER DEVELOPMENT

Millennials, defined as those born between the early 1980s and the 2000s, are expected to be the largest workforce in U.S. history. This panel is filled with open and candid dialogue amongst millennial women employed in cybersecurity. Discussions will focus on career hurdles and challenges; lessons learned and successes; measures to address stereotypes and harassment in this career field; and the value millennials bring to business.

We Got Skills! Women Veterans Transitioning into the Cybersecurity Workforce

Dr. Amelia Estwick, *National Cybersecurity Institute at Excelsior College,* Racquel James, *Department of Defense,* Molly Handy, *Symantec* and Joyous Huggins, *Defender Academy*

TRACK: CAREER DEVELOPMENT

Tired of hearing about the cybersecurity workforce shortage? Look no further than our women veterans who have served in the United States Armed Forces (Army, Navy, Air Force, Marine Corp and Coast Guard) to fill those cybersecurity jobs! According to the U.S. Department of Veterans Affairs, there are over 20 million veterans in the U.S., and women account for nine percent of the veteran population (Pew Research). That's almost two million women veterans who have received highly specialized training working in demanding careers such as cyber operations, information security and IT. Unfortunately for women veterans who have specialized in these demanding careers, many may not realize they have the transferable skills to transition into the cybersecurity civilian workforce. This panel is comprised of women veterans who have successfully transitioned into civilian cybersecurity jobs in spite of the many barriers some of them have experienced and continue to face. They will share their narratives and level of resiliency in obtaining gainful employment within the cybersecurity workforce.

2019 WICYS CONFERENCE
LIGHTNING TALKS

LIGHTNING TALKS 1

Friday • 9:35 am – 10:45 am

Sizzle vs.Steak: Why Leveraging Soft Skills is Key to Succeeding in Tech

Megan Kaczanowski, *S&P Global*

TRACK: CAREER DEVELOPMENT

Selling others (the sizzle) on your ideas (the steak) is often seen as a superfluous skill by highly skilled, highly technical people. However, successfully convincing others to implement your ideas is a key element of success. Having great ideas or technical skills is only half the battle. If you aren't able to successfully communicate to someone (like upper management) what your idea is and why it matters, it's as though it was never proposed. Understanding how to communicate to a variety of audiences and taking ownership over your proposals is crucial to career advancement. This talk will discuss how to take complete ownership of your proposals and offer practical tips on how to improve your proposals in order to get your ideas implemented.

Prob-C: Security Offloading to Edge

Wenhui Zhang, *Pennsylvania State University*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Emerging technologies (Internet of Things systems, augmented reality and virtual reality systems, autonomous cars) bring extra network-facing attacking interfaces to legacy microcontrollers. Malicious payloads embedded in network packets could exploit and subvert machine-code execution. This may introduce tremendous damage if not detected and handled efficiently. Combating these threats via embedding security functionality on real-time operating systems interrupts their normal operations. Offloading security functionality to the cloud brings latency and privacy issues making it unsuitable to combat these threats.

Edge clouds are uniquely positioned to provide these security functions within required latency margins without taxing battery and compute resources in the edge devices. In this paper, we build and evaluate intrusion detection methods suitable to run in an edge cloud as a security monitor to check malicious network flows and protect our systems. We investigate two methods to improve throughput of our system and conclude flow splitting is the more recommended technique. Since network is the expected bottleneck, we conduct stress tests for our system with kernel TCP stack bypassing techniques and give out some guidance numbers to configure it to support 5G wireless throughout, which is at least 20 gigabits per second. Code is open sourced and can be found at https://www.akraino.org.

Practical, Hands-on Cybersecurity Education with CHEESE

Christine Kirkpatrick, *San Diego Supercomputer Center* and Dr. Baijian Yang, *Purdue University*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Develop your cybersecurity skills without compromising your own computer or spending hours setting up a complicated virtual machine (VM) and sandbox environment. Instead, through your web browser, launch cloud-based environments that will lead you through detecting and untangling exploits that are key to understanding today and tomorrow's cybersecurity threats.

The Cyber-Human Ecosystem of Engaged Security Education (CHEESE) project supplements and enhances traditional cybersecurity education with hands-on, practical experience in common cybersecurity flaws and solutions. CHEESE uses cloud-computing, containerization and the NDS Labs Workbench framework to develop a scalable web platform for hosting community-contributed demonstrations of cybersecurity concepts. We will talk about ARP poisoning, SQL Injection and the HeartBleed bug hosted on CHEESE.

Reframing Usable Privacy and Security to Design for "Cyber Health"

Cori Faklaris, *Carnegie Mellon University*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

The continued susceptibility of end users to cybersecurity attacks suggests an incomplete understanding of why some people ignore security advice and neglect using best practices or tools to prevent threats. A more detailed and nuanced approach can more accurately help target security interventions for end users according to their stage of intentional security behavior change. In this talk, you will learn about the Transtheoretical Model (TTM) of Behavior Change for use in a cybersecurity design context as part of a larger reframing of information privacy and security as a crisis of public health. You will view a visual diagram of six TTM Stages of Change and associated intervention strategies, as adapted from medical and wellness literature for use in encouraging exercise, sobriety and smoking cessation. These strategies will be related to examples of security interventions currently in use, such as password strength indicators and Facebook trusted contacts.

Be Bold. Ask Questions.

Gabby Raymond, *The MITRE Corporation*

TRACK: CAREER DEVELOPMENT

The ability to ask questions has many benefits, especially during technical presentations. This workshop will present the Technical Question Toolbox, a set of question formulas, to give you the devices you need to quickly formalize invigorating questions regardless of whether the topic is familiar or foreign. You will practice asking questions based on a set of prepared excerpts. This talk is intended for people at all phases in their careers who have trouble speaking up.

2019 WICYS CONFERENCE
LIGHTNING TALKS

Training a Backdoor into Deep Reinforcement Learning Agents

Marina Moore, *New York University*

TRACK: LOOKING AHEAD

Deep reinforcement learning is a method of training neural networks as they gain experience. The neural network learns from successes and failures throughout its lifetime, allowing it to gain human-like experiences. This allows the agent to learn from what it encounters and constantly improve. Deep reinforcement learning models can be costly to train, which may be outsourced. Outsourced training provides opportunities for an attacker and can be influenced by a malicious user.

We explore the effectiveness of adding backdoors to deep reinforcement algorithms during both the initial training and as the agent explores the world. Initially, we test agents using Deepmind's AI Safety Gridworlds, a set of small environments with various goals and rewards for agents. Using this environment, we develop agents that score well unless there is a certain trigger, which is a single pixel of the gridworld. We show the agent can be trained to recognize this trigger during the initial training. If the training is outsourced, an attacker could alter the training data to create a backdoor. Later, we see if this can be replicated by adding the backdoor without access to the code. This experiment in the AI Safety Gridworlds can be extended to a variety of real world applications. We investigate the threat of training time attacks on deep reinforcement learning agents and give practical attacks against an AI Safety Gridworld agent.

Hacking Hired: Work the Vectors, Get the Offer

Rachel Harpley, *Recruit Bit Security*

TRACK: CAREER DEVELOPMENT

There are no traditional career paths in cybersecurity, but the recruiting process often lacks transparency. Come learn from an insider to build your own career. This talk, "Hacking Hired," identifies the four primary vectors of your job search and shares insights on how to work these vectors to your advantage to create the career you want. From a high-level, these vectors are the tools, technology, organizations and people. This is open to professionals at every stage in their career.

Everything We Need to Know About Secure Design Can Be Explained by Star Wars

Dr. Ann-Marie Horcher, *Central Michigan University*

TRACK: BEST PRACTICES

Every new wave of technology goes through the same growing pains, focusing on "making it work" instead of having secure design. Principles for secure design were described by Jerome Saltzer and Michael Schroeder in 1975. To apply these principles, software designers must understand and remember them. This presentation uses situations and plot points from "Star Wars" to explain the principles of secure design.

LIGHTNING TALKS 2

Friday • 1:50 pm – 2:15 pm

Hostage Negotiation for InfoSec

Sarah Kennedy, *HCA*

TRACK: BEST PRACTICES

On a weekly basis, I have a responsibility to explain how someone is doing their job incorrectly. I'm a security vulnerability engineer, and the purpose in my current career is to find vulnerabilities in all types of systems for one of the largest healthcare companies in the U.S. I have learned many unique skills for how to handle these type of situations.

One of the tactics my team has used is hostage negotiation. There is no middle ground in information security; there is fix the problem or mitigate it until it's fixed. A technical situation is not nearly as critical as a hostage situation, but it's possible that a vulnerability we find will at some point impact a patient's care and safety. During these conversations, people get defensive over their systems. They treat me like I have just called their baby ugly, and they come out swinging. I've been challenged in these conversations for being a woman, for not being the most senior person on my team and for my perceived lack of intelligence. People have gone to my higher ups to bypass my team because they don't like our processes and procedures, but ultimately we have very strong upper management support for what we do and they end up working with my team anyway.

During this talk, we will discuss what my day-to-day looks like and how I use various styles of communication to get the best possible outcome of getting an issue corrected with as little disagreement as possible. I also will discuss how I got into this position and the steps I'm taking to further advance my career in InfoSec.

You Can Do It! The Power of Cybersecurity Sisterhood!

Diane M. Janosek, *National Cryptologic School,* Shade Adeleke, *Prince George's Community College,* Dr. Vitaly Ford, *Arcadia University* and Pauline Mosley, *Pace University*

TRACK: BEST PRACTICES

From one to many: with 50 WiCyS student chapters and 4 WiCyS affiliates in a few months duration, we have just begun! You can join us too. Our work is both rewarding and satisfying as we see the fruits of our labors in bringing women together with a common goal of empowerment, diversity and inclusion, and professional growth. Cybersecurity sisterhood is unstoppable!

2019 WICYS CONFERENCE
LIGHTNING TALKS

Domain Misconfiguration in the Wild

Mia Gil Epner and Luna Frank-Fischer, *Expanse, Inc.*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Domain names make up a core piece of the modern internet. Our websites depend on the security and reliability of the Domain Name System (DNS) to translate human-readable domain names to IP addresses. This lightning talk will cover the prevalence and severity of common DNS and domain misconfigurations. Using passive DNS, Expanse has a global view of what questions DNS servers are answering and what the answers are. From this data, we have observed numerous violations of best practices. By focusing on three common misconfigurations, we will demonstrate the frequency and severity of problematic DNS records.

The first misconfiguration is long CNAME chains and CNAME loops. These chains exhaust DNS resources, increase complexity for an organization and in the worst case can leave servers unable to answer the client's query. The second misconfiguration is DNS results that resolve to internal IP addresses. At times, these records are inserted intentionally by network operators but run the risk of exposing the internal network structure of an organization, leaving that organization more vulnerable to attack. The final misconfiguration category is problematic PTR records. This talk will provide guidelines for organizations as well as facilitate a discussion about why these problems are prevalent.

Managing the Guest List—Third Party Vendors

Stacey Romanello, *RBC*

TRACK: BEST PRACTICES

Organizations spend hours creating security frameworks and policies to defend themselves. Yet, are you prepared for cybersecurity attacks through vectors like third party vendors? Organizations are dependent on third party vendors for necessary services, which may require access to sensitive data. Lax security through these vendors have cost companies the trust of their customers and millions of dollars.

The Target data breach in late 2013 shows that large companies are no more protected from attacks if their third party vendor security is lacking–it only takes one point of entry to compromise the entire system. Target's vendor's security breach allowed attackers to steal over 70 million names, email addresses and debit and credit card details from their customers, leading to a huge loss of trust from the public, which translated into a loss of revenue as this attack happened during the busiest retail season of the year. Even "air gapped" systems not directly connected to the outside world can be infiltrated by malicious actors finding their way in through third parties.

It's clear that vendor security directly affects your own security. The question becomes, how do you assess vendor security, and what is an acceptable level of risk? Different third parties require varying levels of access and security, and it's important to determine how to limit their access but ensure they can still effectively perform their jobs. To defend against cybersecurity threats, security should be a strategic partnership.

"What Do You Mean It's Not a Security Issue?"

Natalie Attaya, *IBM*

TRACK: BEST PRACTICES

In a world where cybersecurity breaches are increasing in number, organizations are quick to assume security is to blame when something goes awry. However, when investigations turn up evidence proving otherwise, we are all reminded of the importance of thoroughly vetting, testing and QAing technology before putting it into production, especially when the stakes are high. During this lightning talk, Natalie Attaya will discuss results of her work with a government agency investigating an election event that led to a disruption in the voting process. This engaging discussion will explore what happens when cybersecurity incident investigations find no evidence of a security incident. It also will highlight the fact that technology problems are not always cybersecurity issues and the value of remaining diligent in testing and QA when implementing new technology.

Recalculating Women in Cyber

Georgia Reid, *Cybercrime Magazine*

TRACK: CAREER DEVELOPMENT

In a world where cybersecurity breaches are increasing in number, organizations are quick to assume security is to blame when something goes awry. However, when investigations turn up evidence proving otherwise, we are all reminded of the importance of thoroughly vetting, testing and QAing technology before putting it into production, especially when the stakes are high. During this lightning talk, Natalie Attaya will discuss results of her work with a government agency investigating an election event that led to a disruption in the voting process. This engaging discussion will explore what happens when cybersecurity incident investigations find no evidence of a security incident. It also will highlight the fact that technology problems are not always cybersecurity issues and the value of remaining diligent in testing and QA when implementing new technology.

SWAG EXCHANGE

DON'T LOVE IT? EXCHANGE IT!

Stop by the Swag Exchange table in the Ballroom Foyer.

LIGHTNING TALKS

LIGHTNING TALKS 3

Saturday • 9:35 am - 10:15 am

Don't Ask What You Want to Be When You Grow Up, But Ask...

Nancy Lim, *Department of Homeland Security*

TRACK: CAREER DEVELOPMENT

In my generation as a young child, one was often asked by adults, "What do you want to be when you grow up?" Having limited access to career options, they were narrowed to being a doctor, engineer or lawyer. I also was taught that you have to tell the truth and be true to your word. Therefore, providing an answer to the aforementioned question further narrowed my options. Our world today is full of options and opportunities with information and resources readily accessible largely due to innovation, technology and interconnectedness. Therefore, instead of asking what do you want to do when you grow up, ask what kind of problem you'd like to solve today. Over the course of our professional career and life, the kinds of problems we like to solve will change and evolve.

Making Sense of Netflow Network Traffic

Pamela Toman and Haley Sayres, *Expanse Inc.*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Even well-monitored organizations are usually unaware of the traffic going into and out of their network edges. It is rarely technically or financially feasible to instrument every ingress/egress point, and tracking interactions is only increasingly challenging as infrastructure moves into the cloud and as mergers and acquisitions bring highly disparate networks into contact with each other.

Without instrumentation and actionable analysis, IT and security organizations set policies but are unable to identify whether and where those policies might be broken. The gaps add unnecessary security risks to organizations. Logging "netflow" on routers makes it possible to detect and measure potential data breaches and asset misconfigurations. Routing devices write sample traffic to disk, documenting the sources and destinations of a subset of the traffic they transmit. Once an organization's complete network edge has been mapped, analysts can attribute interactions to specific organizational endpoints—even endpoints that are not on local premises and are falsely believed to be highly instrumented. With longitudinal netflow monitoring through standards like NetFlow, IPFIX and sFlow, it is possible to more fully characterize and secure a network edge. Anyone who attends this lightning talk will learn about the netflow standards for documenting network traffic, the limitations of the standards and a vision for the future in which data collected according to the netflow standards will assist with the monitoring challenges posed by the modern IT security environment.

At the conclusion of the short presentation, you will understand how network communications work and the ways and places by which interactions are logged. Following the talk, you will be prepared to delve into deep discussions around additional risks that might be visible within netflow data and the privacy/security trade-off inherent in tracking netflow data.

Spotting Security Flaws in Code Before It's Written

Yasmine Kandissounon, *Rackspace*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Tremendous advancements in technology in recent years have fueled a rise of complex applications with equally complex attack surfaces. This heightens the need to unveil and address security issues as early as possible in the software development life cycle to avoid costly consequences. Formal methods and model checkers have been leveraged to uncover runtime issues as early as the design phase. For instance, developers on cutting-edge projects such as AWS and Azure have used model checking tools to help design systems and have found serious, highly subtle bugs in products such as S3, EC2 and Azure's CosmosDB. In this presentation we will discuss model checking in designing secure systems and explain how the model checking tool Alloy helped unearth a tricky security flaw in our authentication and authorization system at Rackspace.

Hacking Humans: Addressing Vulnerabilities in the Advancing Medical Device Landscape

Gabrielle Hempel, *Accenture*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

As technology advances, the health care critical infrastructure sector comprises much of the potential attack surface of the national security landscape. Medical devices are being fitted with "smart" technology in order to better serve patients and stay at the forefront of health technology. However, devices that enable connectivity, like all other computer systems, incorporate software that is vulnerable to threats. Medical device recalls increased 126 percent in the first quarter of 2018 mostly due to software issues and vulnerabilities. Abbott and Bayer, among other medical device companies, had recalls on devices based on weaknesses discovered by both government security entities and academic institutions. These devices, which included pacemakers, infusion pumps, and MRI machines, were found to have vulnerabilities ranging from buffer overflow bugs to the presence of hard-coded credentials that easily lent to unauthorized access of proprietary information. A breach of any one of these devices could compromise data confidentiality, integrity and availability, as well as patient safety.

In order to mitigate these types of vulnerabilities, the FDA issued a guidance, as well as a vulnerability scoring system, in order to assess impact. This system assesses the attack vector, the complexity, risk and severity of both patient harm and information compromise, and the remediation level. By utilizing a more rigid system along these guidelines, there is hope that the threat of a medical device attack will be diminished.

2019 WICYS CONFERENCE
LIGHTNING TALKS

A War Of Minds: The Role of Cognitive Science and the Arts in Thwarting Cyber Crime

Dr. Monica Lopez, *La Petite Noiseuse Productions*

TRACK: LOOKING AHEAD

Despite millions being invested in sophisticated software and infrastructure, cyber criminals continue to attack users, systems and networks in ever more simple and creative ways. The continued use of phishing and malware-related spam emails along with the emergence of new file types in spam attachments, for example, continue to trick users and evade security researchers alike. Cybersecurity is not keeping up with hackers at a fast enough pace. Why? Because a traditional computational-technology perspective is insufficient. Human-centered factors like cognition and behavior must also be considered if hackers' malicious ways are to be thwarted.

Combining insights into how we humans perceive, interpret, react and interact with each other in a constantly changing environment within cyber tools and interfaces is key to not only predicting, identifying and problem-solving cybersecurity vulnerabilities before they arise, but also in how we educate the user to be their own best line of defense. This implies a new way of thinking for the cyber industry regarding security, data governance and tactic whereby cognitive strategies regarding creative thinking and doing take center stage. Making a theoretical and cognitive analogy between real-time improvisation and adaptive creativity within the arts to the inventive threats perpetrated by hackers, I argue for the multidisciplinary integration of the cognitive psychology of creativity with cybersecurity R&D.

People (Users) are a Data Source—Are You Leveraging Them in Your Detection Strategy?

Tonia Dudley, *Cofense*

TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

After years of training users to report phishing emails, they are now providing great intel that you didn't even have to pay for. Are you using it to search for maliciousness in your environment (sending it to your SEIM) or to your data lake? Are you sharing those free IOCs with your threat intel teams that are trying to protect your brand? Or pushing the IOCs to your endpoints to protect your assets when they're off your network? The objective of this talk is to demonstrate the value of indicators of compromise that can be gained from user-reported phishing messages and discussing how these can help mitigate the risk to the organization if a user does click on a link or open the malicious attachment. This session also will cover the latest in phishing threat intelligence trends.

Digital Forensics for SCADA Systems

Rima Asmar Awad, *Oak Ridge National Laboratory*

TRACK: LOOKING AHEAD

Security aspects of SCADA environments and the systems within them are increasingly a center of interest to researchers and security professionals. As the rise of sophisticated and nation-state malware flourishes, traditional digital forensics tools struggle to transfer the same capabilities to systems lacking typical volatile memory primitives, monitoring software and the compatible operating-system primitives necessary for conducting forensic investigations. Even worse, SCADA systems are typically not designed or implemented with security in mind nor were they built to monitor and record system data at the granularity associated with traditional IT systems. SCADA systems were not designed with the primary goal of interacting with the digital world. Consequently, forensics investigators well-versed in the world of digital forensics and incident response face an array of challenges that prevent them from conducting effective forensic investigation in environments with vast amounts of critical infrastructure.

In order to bring SCADA systems within the reach of the armies of digital forensics professionals and available tooling, both researchers and practitioners need a guide to the current state-of-the-art techniques, a road-map to the challenges lying on the path forward and insight into the future directions R&D must move. We present a survey into the literature on digital forensics applied to SCADA systems and cover the challenges to applying digital forensics to SCADA. Toward the end, we will present recommendations for future SCADA forensics works.

Cybersecurity Strategies to Combat Human Trafficking

Danielle Borrelli, *Cal Poly San Luis Obispo*

TRACK: BEST PRACTICES

Human sex-trafficking is a prevalent phenomenon impacting most nations in the world. Victims endure separation from family members and loved ones and face isolation as well as physical, emotional and sexual abuse. Individuals often have symptoms of post-traumatic stress disorder on par with war veterans and torture survivors. This issue is exacerbated by the use and development of technology as traffickers use common social media platforms, websites and gaming applications to recruit, sell and exploit individuals. Anonymity offered by such encrypted technology enables criminals to avoid capture and subsequent prosecution while further exploiting victims as photographs and videos are continuously distributed without any guarantee of complete content removal. To effectively fight this growing humanitarian crisis, innovative cybersecurity training as well as growth in the cyber professional workforce must occur.

STUDENT POSTERS

STUDENT POSTERS

Friday • 10:45 am – 12:00 pm

1. Using Deep Learning to Generate Relational Honey Data

Nazmiye Ceren Abay, Cuneyt Gurcan Akcora, Yan Zhou, Murat Kantarcioglu and Bhavani Thuraisingham, *University of Texas at Dallas*

Although there has been a plethora of work in generating deceptive applications, generating deceptive data that can easily fool attackers received very little attention. In this paper, we discuss our secure deceptive data generation framework that makes it hard for an attacker to distinguish between real versus false data. We also discuss how to generate such deceptive data using deep learning and differential privacy techniques. In addition, we discuss our formal evaluation framework.

2. Statistical Learning of APT TTP Chains from MITRE ATT&CK

Rawan Al-Shaer, Mohiuddin Ahmed and Ehab Al-Shaer, *University of North Carolina Charlotte*

MITRE ATT&CK provides rich and actionable information about APT tactics, techniques and procedures (TTP). However, this information will be highly useful for attack diagnosis and mitigation if we can reliably construct TTP chains and predict future attack steps. In this poster, we present our preliminary statistical analysis to characterize the correlation of the occurrence of these techniques within an APT attack in order to construct potential TTP chains and predict, based on observed malicious activities, attack techniques that adversaries might perform to pursue their goals.

3. Slow Drip DDoS Attack Foundation Work

Sonia Arora and Anderson Nascimento, *University of Washington*

Various service provider users around the world reported a new type of DNS Distributed Denial of Services (DDoS) attack, which uses DNS as attack vector. It is referred to as SlowDrip attack and plagues customers by exhausting computational resources by overwhelming DNS servers via a huge number of random sub domain queries. These attacks have impacted internet service providers worldwide. In this poster, we propose to look for various classifiers for early detection. To identify key characteristics, we analyze the choices of target and the patterns of actors which generate attacks using exploratory data analysis and feature engineering. It is our hope that the details will aid in a full diagnosis of this malicious activity and ultimately lead to resolution of the threat by the global security community.

4. Classification of Malicious and Benign PDFs Using Static Features and Metadata

Sai Himabindu Boddupalli, *University of Colorado Boulder*

There has been an unprecedented rise in potential threats and attacks on the cyberworld on a daily basis. PDF is a soft target for many malware writers as it is one of the most commonly used file format. Embedding PDFs with malware easily accomplishes the target, most of the time by the victim merely opening the file. In some cases, the PDF even requires the user to enter important credentials. This is mostly an illusion as the user is made to think that he/she is performing some operation. In reality, his/her credentials are either stolen or the action triggers a URL in the background, which downloads malware onto the system. These attacks are well obfuscated to deceive users. The ways to detect such malicious PDFs can be classified as static and dynamic. Static examination involves making use of the structural features of the PDF source code. Dynamic features involve run-time elements of the PDF by executing it in an isolated virtual environment. Some metadata properties play a monumental role in classification of benign and malicious PDFs. In this paper, a novel combination of static features and metadata has been used to develop feature sets that will enable the identification of malicious PDFs with high accuracy. This is highly helpful to the cybersecurity industry, and this project provides new insights into malware classification and guides the developers to come up with a new approach to tackle the problem of malicious PDFs.

5. Exploration of CMS Open Payments Data using Network Modeling and Machine Learning Techniques for Anomaly Detection of Relationships

Udaysree Buchupalli and Ayokomi Lasisi, *University of Louisiana at Lafayette*

This paper is concerned with the problem of financial relationships and transactions in the Center for Medicaid and Medicare Services (CMS) open payments data. We have especially focused on research payments data for our exploration. For this reason, we considered a machine learning model using unsupervised learning techniques to see financial relationships that exist within research payments data such as physicians and teaching hospitals, applicable manufacturers and physicians using Dirichlet process, which is a non-parametric probabilistic programming technique. We analyzed the results obtained through network analysis and probabilistic models. We have done network analysis to find structural inconsistencies and anomalous nodes connected to diverse communities. We could not get a clear picture through this. We detected 134 communities showing the relationship between GPOs and physicians using the community detection fast greedy algorithm. The objective of unsupervised learning involves the construction of Mixture Models and using Markov chain Monte Carlo algorithm to predict the class of the sample. This is used to model and analyze the data with the samples obtained and group them into the same class known as clustering. This also determines how the data is distributed, known as density estimation. The output of the community detection algorithm was fed into Tableau for better visualization. The efficiency and

accuracy of the Tableau analysis made it feasible to be used for the detection of many transactions for only one purchasing organization in such large complex payment data. All such cases will further be investigated by subject matter experts in Medicaid and Medicare Services.

6. TCB Minimizing Model of Computation (TMMC)

Naila Bushra, *Mississippi State University*

The trusted computing base (TCB) of a computing system includes all hardware and software that assume trustworthiness. In the traditional (von Neumann) computational model, memory is considered part of the TCB. However, a large number of security breaches result from illegitimately reading, writing and updating information stored in the memory. Therefore, memory cannot be completely trustworthy in practice. In the proposed TCB minimizing model of computation (TMMC), memory and I/O devices are not considered part of the TCB. The goal of the TMMC model is preserving the integrity of process execution. The proposed model follows a two-party protocol involving a prover and a verifier. The prover is responsible for the actual execution of the system processes and stores memory contents in an Authenticated Data Structure (ADS). Verifier, which has very limited (and trustworthy) memory, is responsible for verifying the correctness of process execution by the untrusted prover. In the TMMC model, a process is constrained as a set of "permitted state transitions," and correctness can be readily verified by resource-limited verifiers. The TMMC model for process execution is thus an alternative to the conventional procedural model for executing processes. The proposed model can be used for "securely" executing a wide variety of real-world processes when converted into permitted state transitions.

7. Cybersecurity Classroom - Hack Me If You Can

Meagan Carmon, Tyler Oakley, Charlotte Lewis, Lexi Winters, Jared Ponton, Devin Beasley, Claire Hacker and Dani Mills, *John A Logan Community College*

Seventy percent of educators use technology daily with their students, but cybersecurity and its sub-components (e.g., cryptography) are not being taught at the same priority level. The internet era has thrust upon educators a need to show children the importance of computer usage or, more specifically, how internet information is created, stored and transferred. Educational games have been used to help aid learning over the years. The goal of this project is to integrate cultural diversity, cybersecurity and creativity into an innovative educational game. The target age group is middle school children, ages 10 to 14. The project is designed as a cybersecurity game to assist and enhance children learning STEM programs. The goal is to show the correlation between video game-based learning and retention of information. The video game was developed using Python (a computer coding language). It also uses multiple cryptography tools to solve puzzles, similar to Where in the World is Carmen Sandiego? A pretest, setting a baseline, will be administered to all class participants to assess their level of understanding in history, cybersecurity and cryptography. After the game has been played, scores are given based on how well the students completed each puzzle, if they used any hints or if they captured the hacker. After the game is completed, students in the STEM program are tested to see what information they retained. As a control, children from STEM are split into two groups. Group A will be taught using the game while Group B will be taught with more traditional classroom techniques such as lecture and PowerPoints. After completion, both groups are scored on tests to compare the difference between the type of implemented learning. The outcome we hope to achieve is that the video game will show a higher level of information retention as well as help stimulate growth within the STEM program as opposed to their traditionally taught peers. The final goal is to spark interest in STEM-related jobs, particularly cybersecurity. The entire project was developed based on requests from local educators looking for better educational tools that show diversity and teach children about worldwide cybersecurity developments.

8. Attribute-Based Access Control Policy Mining Problem: Thinking Differently

Shuvra Chakraborty, Ram Krishnan and Ravi Sandhu, *University of Texas at San Antonio*

Protecting information or other resources from unauthorized access is a major component in security enforcement; that is where access control comes into play. Right now, many access control models are available for limiting resource or object access to legitimate users only, among them are the popular RBAC, DAC and MAC. Attribute-Based Access Control (ABAC) is a comparatively newer member in this area, where any sort of authorization request is verified with respect to corresponding user and object attribute data. Although ABAC has taken a considerable amount of time to become defined, now it is one of the strong competitors to other popular counterparts. ABAC rules can capture different characteristics of users, objects and possibly other entities (e.g., environment, time or location) but for the sake of simplicity, only two entities (user and object) are considered in this study. However, shifting to ABAC from an existing model is an exhaustive task in the absence of any supporting method.

To ease or partially automate this migration process, the solution of ABAC mining finds out accurate policy rules with respect to existing authorizations and accompanying attribute data. Although some solutions are already available, our approach was the first step towards Boolean algebra in the field of ABAC mining problem. This is a fairly straightforward approach for generating consistent ABAC rules with respect to given user and object attribute data and a set of authorizations. Here, the number of rules in the policy is equal to the total number of permissions in the system. The generated policy is further minimized using Espresso heuristic logic minimizer, a popular Boolean logic function minimization technique. Boolean algebra can accurately manage PERMIT, DENY and DON'T CARE aspects of policy rules. Moreover, defining policy rules in the sum of minterm form for each permission is highly favorable for hardware implementation (i.e., PLA, FPGA) as well. Handwritten and randomly generated cases were used for testing purposes. Additionally, an application of our current approach in policy refinements is briefly described here.

STUDENT POSTERS

9. Design-Based Security Solutions for the Additive Manufacturing Cyber-Physical System

Fei Chen and Nikhil Gupta, *New York University*

Additive manufacturing (AM), also widely as known as 3D printing, is one the fastest growing industrial fields in the past decade. The digital AM process chain relies heavily on cloud-based resources and software programs that are connected to the internet starting from the first step of product design to the final step of manufacturing the part using a 3D printer. The AM cyber-physical system is vulnerable to threats, such as sabotage and intellectual property theft by inside and outside attackers.

Traditional cybersecurity tools are implemented as the first line of defense. However, design files such as computer aided design (CAD) are immediately exposed once cybersecurity is breached. The stolen CAD files can be used to reproduce counterfeits in exactly the same quality as the original components using the AM process chain, which causes companies significant monetary losses for extended periods. A novel and innovative approach based on creating design features in the solid models used for AM is developed to provide a second line of defense. These design features are embedded in CAD models as security features against counterfeiting, reverse engineering or other illegal reproduction. They interfere with the integrity of the design, effectively restricting high-quality manufacturing to only a unique set of processing settings and conditions, such as digital file resolution, slicing orientation and temperature. Under all other conditions, the 3D-printed part suffers from poor quality, premature failures and/or malfunctions. This design approach can layer with blockchain technology for IP verification and protection. It also can augment the network security tools deployed by cybersecurity experts to develop a robust strategy for high-value parts.

10. Yubikeys as an Instrument for Security Education: Combating Apathy, and the Lack of Computer Security Curriculums in High Schools

Leslie Choi and Rebecca Sexton-Lee, *Portland State University*

Data breaches aren't unusual occurrences anymore, and 2018 has been an eventful year for a sector that is vastly popular with the younger generation: social media. Facebook suffered an attack that left 50 million users' personal data exposed. Quora also had a breach that exposed user data such as encrypted passwords and links to other social media accounts. Even Google announced a bug in the system exposed users' data on their Google+ network and will be shut down.

Despite all of this, there doesn't seem to be an imminent boycott of social media sites, as it has become so integrated in our daily lives in both personal and business matters. Since social networks are here to stay, the best actionable step to mitigate these security breaches is to educate users. However, many high schools don't have computer security curriculums that would help increase access to computer science as a career or adequately equip high school students with the skills to protect their own personal information online. Poorly designed passwords and two-factor authentication schemes perpetuate this disconnect by making security difficult or costly to use. To address this, we aim to teach high school students how to use Yubikeys - inexpensive physical USB devices - as a way to literally put security back into their hands and potentially bring back personal responsibility in protecting users' accounts.

11. Image Encryption and Decryption using Blowfish Algorithm and Water Embedding Techniques

Nivetha Elangovan, *University of Washington*

The biometric technologies involved are based on ways in which individuals can be uniquely identified through one or more distinguishing biological traits, such as fingerprints, hand geometry, iris patterns, voice waves, DNA, etc. The authentication scheme is an important cryptographic mechanism through which two communication parties could authenticate each other. Biometric technologies are used to secure a wide range of electronic communications, including enterprise security, online commerce and banking, even just logging onto a computer or smartphone. The main aim of this project is to propose an authentication based on steganography objects using biometrics in wireless networks and to perform an authentication mechanism for ration shop application in rural areas by encryption and data hiding.

12. Can Capture the Flag Writeups be Used to Teach Cybersecurity?

Kammi Kai Hefner, *Capitol Technology University*

This poster showcases the results of an online survey conducted in January 2019 to explore the use of Capture the Flag (CTF) writeups to teach cybersecurity. CTF competitions began nearly 20 years ago. The competitions have been described in literature from an observational perspective, providing anecdotal insights such as how they are educational, effective, engaging, enjoyable and entertaining. Yet, there is minimal academic research dedicated to statistically investigating the educational effects (e.g., learning gain, motivation gain) of using CTF exercises and/or CTF writeups as integral parts of a CTF competition to teach cybersecurity. Impromptu conversations with long-time CTF competitors revealed their writeups are often an overlooked resource for cybersecurity learning.

The purpose of this grounded theory research will be 1.) To build demographic profiles (e.g., gender, age, schooling, level of CTF competition knowledge, level of CTF competition success) for those individuals who use or don't use CTF writeups (i.e., competing in a CTF competition; attending a security-related conference hosting a CTF competition; competing in a social gathering or not), 2.) To explore why or why not CTF enthusiasts use writeups, 3.) To identify the salient parts of a CTF writeup (e.g., summary of the challenge, code snippets, traps and pit falls, work flows), 4.) To identify the learning styles of CTF writeup users, 5.) To discover if accessing, executing, reading, reviewing and/or using CTF writeups is a beneficial route for those individuals interested in learning cybersecurity. The presenter will brief the results of the survey and offer recommendations for further studies.

STUDENT POSTERS

13. Securing Connected Vehicles

Christine Hysell, *University of Redlands* and Yomara Donis, *California State University, San Bernardino*

The safety of public roads and highways are at risk with the emergence of connected vehicles. Risk management, along with policy implementation, is crucial to ensuring the operability and safety of connected vehicle networks integrated into automotive and transportation infrastructure. We have taken a multifaceted approach toward understanding the landscape surrounding the policy and regulation of connected vehicles. Connected vehicles are ubiquitous on American roads and highways. As their presence has grown, so has concern that they have become a target for a growing number of cyber attacks facing the nation. The threat landscape for connected vehicles has expanded now that physical access is no longer required for a hack to occur. Researchers have discovered wireless technologies can serve as a vulnerable entry point for cyber threats.

The National Highway Traffic Safety Administration (NHTSA) has not finalized vehicle-to-vehicle and vehicle-to-infrastructure communication using the 802.11p standard. This motivates the need to further understand and explore the strengths and weaknesses of the standard in vehicle communications. However, access to environments that enable researchers to understand and explore 802.11p is limited to a few research laboratories and the NHTSA due to their high cost and complexity. To simulate real world applications and test for vulnerabilities within vehicle-to-vehicle communications using protocol 802.11p, we built a distributable virtual CAN bus vehicle communication environment.

14. Constant Learning Model to Improve Static Malware Analysis

Moumita Kamal, Joe Bivens and Dr. Doug Talbert, *Tennessee Tech University*

Android Permissions Malicious software or malware nowadays pose an increasing threat to sensitive data and network systems. With the advancement of technology and the omnipresence of internet connectivity and online services, this menace is getting even greater every day. Malcode writers are coming with new and well-built malware and on top of that, are using different techniques to obfuscate their malcode. So, it is very important to have malware detectors that are effective and efficient. Two of the most popular techniques in malware analysis are static and dynamic malware analysis. Static analysis, albeit less accurate, is much simpler and fast. This analysis is done only by looking at the binary of a program without executing it. Dynamic analysis, on the other hand, requires real-time analysis of the malicious program in execution. This is a much more complex yet effective technique. In this work, we attempted to create a constant learning model that uses static analysis classifiers to detect malware and tries to improve the classifier using feedback from dynamic malware analysis. We focused our analysis on android mobile malware and determined what features produced the best results on malware detection. We also determined the best set of classifiers that alone or combined, gives the most accurate results.

15. Why Johnny Still Can't Pentest: A Comparative Analysis of Open-Source Black Box Web Application Vulnerability Scanners

Rana Khalil, *University of Ottawa*

Web application vulnerability scanners are automated tools used to crawl a web application to look for vulnerabilities. These tools are often used in one of two ways:

1) Point-and-Shoot (PaS) mode- In this approach, the scanner is only given the root URL of an application and asked to scan the site.

2) Trained mode- The scanner is first configured and trained to maximize the crawling coverage and vulnerability detection accuracy.

Although the performance of leading commercial scanners has been thoroughly studied, very little research has been done to evaluate open-source scanners. With so many open-source web application vulnerability scanners available, how do you choose which one to use? Is it worthwhile to make the investment in configuring and training your scanner, or should you stick with the PaS approach? Are there any critical limitations associated with the open-source scanners?

This research presents the results of a feature and performance comparison of five leading open-source scanners run in both PaS and Trained modes. We analyze the crawling coverage, vulnerability detection accuracy, scanning speed, reporting and usability features of the scanners. In this study, we share:

1) Differences in crawling coverage, vulnerability detection accuracy and speed when scanners are run in PaS and Trained modes.

2) Tasks that were critical in maximizing the crawling coverage and vulnerability detection accuracy.

3) Web technologies that scanners had difficulty crawling.

4) Classes of vulnerabilities that were not detected by the scanners.

We also compare the performance of the tested scanners with the well-known commercial scanner Burp Suite Professional to determine if commercial scanners have a significant added value compared to open-source scanners.

16. Investigating the Dark and Deep Web Crimes: An Examination of Tracing the Identities of Anonymous Suspects

Francisca Afua Opoku-Boateng and Ashley Podhradsky, *Dakota State University*

The advent of computers and technology has made several facets of human life (economic, social, cultural and political dimensions) easy and comfortable. However, there have been accompanying challenges in the form of dark web and deep web crimes, which often warrant forensic investigations by local, state and federal agencies. The dilemma in these investigations has to do with anonymization and obfuscation techniques exhibited by online suspects, hence making it difficult to track their location and activities. In the US, the issue of anonymity became a major subject of discussion and interest after

the Edward Snowden saga. In more recent research, while many people use The Onion Router (TOR) for anonymous web browsing, some use it to access the dark web for nefarious purposes. Furthermore, TOR provides a platform for anonymity for people with malicious intent who could be engaged in illegal activities such as money laundering, child pornography or endangerment, the sale of drugs and weapons, hacking and assassination services, malware purchasing or buying passports.

Despite successful efforts by the FBI to shut down the operations of Ross William Ulbricht, who operated under the name "Dread Pirate Roberts," there exist many unknown online users in the dark and deep web. Developing digital forensic practices for identification, extraction and analysis is imperative. Surface web investigations through common browsers such as IE, Chrome, FireFox, etc, have time-tested processes for digital forensic investigations. Dark web and deep web investigations have had limited research and testing. The deep web is far more innocent than the dark web. For this reason, this research examines the effectiveness of forensic investigations and online policing strategies that trace the identities of anonymous suspects. Additionally, it will look to analyze host-based dark web artifacts to identify what sites were accessed and corresponding metadata.

17. Toward Measuring the Effectiveness of Telephony Blacklists

Sharbani Pandit and Mustaque Ahamad, *Georgia Institute of Technology*

The convergence of telephony with the internet has led to numerous new attacks that make use of phone calls to defraud victims. In response to the increasing number of unwanted or fraudulent phone calls, several call blocking applications have appeared on smartphone app stores, including a recent update to the default Android phone app that alerts users of suspected spam calls. However, little is known about the methods used by these apps to identify malicious numbers and how effective these methods are in practice.

In this paper, we are the first to systematically investigate multiple data sources that may be leveraged to automatically learn phone blacklists, and to explore the potential effectiveness of such blacklists by measuring their ability to block future unwanted phone calls. Specifically, we consider four different data sources: user-reported call complaints submitted to the Federal Trade Commission (FTC), complaints collected via crowd-sourced efforts (e.g., 800notes.com), call detail records (CDR) from a large telephony honeypot and honeypot-based phone call audio recordings.

Overall, our results show that phone blacklists are capable of blocking a significant fraction of future unwanted calls (more than 55 percent). They also have a very low false positive rate of only 0.01 percent for phone numbers of legitimate businesses. We also propose an unsupervised learning method to identify prevalent spam campaigns from different data sources and show how effective blacklists may work against such campaigns.

18. Analysis of AES and PRESENT for Encryption in IoT Devices

Nishi Prasad and Prateek Talukdar, *Rochester Institute of Technology*

In the past, cryptographic algorithms were designed with general computers, PCs and their processing powers in mind. But as time passed, there has been a shift and surge in the need to apply the same to embedded devices. This may not prove efficient as they require significant hardware, memory and processing power. The need arose to look at alternatives, such as lightweight cryptographic algorithms to carry out the same process but tailormade for constrained Internet of Things (and/or embedded) devices. In this project, we aim to carry out an in-depth analysis comparing the performance of the most commonly used cryptographic algorithms today - AES against the standard for ultra-lightweight cryptographic algorithms, PRESENT. Our project uses a common reprogrammable hardware platform, the Zedboard 7000-FPGA to contrast the two encryption algorithms. The analysis includes a per-round analysis performance while scaling the input size and hardware complexity.

19. Hacking Biomedical Devices

Kelly Rose, *Hofstra University*

With recent rapid advances in technology, the world is more connected than ever before. But with this new interconnectedness comes new vulnerabilities for attackers to exploit. There has been new interest in the field of "biohacking," or the hacking of biomedical technology. Two-thirds of the medical device manufacturing community believes an attack on at least one device they built is likely within a year (as of 2017). Yet, only 17 percent have taken steps to prevent attacks from occurring, and only 22 percent have a response plan in place. This research aims to review likely attacks on common biomedical devices and formulate recommendations for improved security.

STUDENT POSTERS

20. InterChain: Design, Architecture and Applications of the Cost-Effective Interoperable Hybrid Blockchain Framework in the Presence of a Rational Observer with the Division of Mining Power

Kuheli Sai, *University of Pittsburgh*

With the inception of Blockchain, the cyber world has seen a widespread change. It is believed that Blockchain will bridge the Trust Gap into the digital world. Blockchain's decentralized, distributed ledger creates a timestamp on the transaction and maintains a consistent state among all its replicated copy by coming to an agreement via Proof-of-Work. However, allocation of more than 50 percent of the computing power to a single or a set of attacking nodes is enough to create an inconsistent state. The presence of a single blockchain network is prone to the centralization of hashing power due to colluding nodes, which might throw out a legitimate transaction and consequently influence the inclusion of a transaction into the ledger maintained by the blockchain network.

I am addressing these issues by designing a global blockchain network in which the computational power of nodes are divided among two networks where different components of a single application will be deployed onto different networks and mines. However, there is no secure interoperable feature among different blockchain networks. This leads to the first major challenge - designing a new protocol for secure interoperability across different blockchain systems.

In order to circumvent the problem of hashing power centralization, my design enforces the following condition- even if colluding nodes of a single blockchain network throws out a legitimate interoperable transaction, the user will always have the transaction's Proof-of-Presence as long as it is present in other networks. I have demonstrated that the designed secure interoperable protocol will obviate the double spending problem across the network as maintaining honesty to the protocol will be more profitable than colluding and spending the same money twice. Leveraging Ethereum's smart-contract feature in the solidity programming language, I have designed interoperable decentralized application in the context of the crypto-banking system to demonstrate the applicability of the interoperable hybrid blockchain. Implementation of a smart contract for the feasibility study has been performed using solidity programming language. I have tested them by creating a private blockchain network using Ethereum platform and validated the cost-effectiveness of the smart contract deployment.

21. An Evaluation of DGA Classifiers

Raaghavi Sivaguru, Chhaya Choudhary, Anderson Nascimento and Martine De Cock, *University of Washington;* Bin Yu, Vadym Tymchenko, *Infoblox*

Domain Generation Algorithms (DGAs) are a popular technique used by contemporary malware for command-and-control (C&C) purposes. Such malware uses DGAs to create a set of domain names that, when resolved, provide information necessary to establish a link to a C&C server. Automated discovery of such domain names in real-time DNS traffic is critical for network security as it helps detect infection and, in some cases, take countermeasures to disrupt the communication and identify infected machines. Detection of the specific DGA malware family provides the administrator valuable information about the kind of infection and necessary next steps.

In this paper, we compare and evaluate machine learning methods that classify domain names as benign or DGA and label the latter according to their malware family. Unlike previous work, we select data for test and training sets according to observation time and known seeds. This allows us to assess the robustness of the trained classifiers for detecting domains generated by the same families at a different time or when seeds change. Our study includes tree ensemble models based on human-engineered features and deep neural networks that learn features automatically from domain names. We find that all state-of-the-art classifiers are significantly better at catching domain names from malware families with a time-dependent seed compared to time-invariant DGAs. In addition, when applying the trained classifiers on a day of real traffic, we find many domain names unjustifiably are flagged as malicious, thereby revealing shortcomings of relying on a standard whitelist for training a production-grade DGA detection system.

22. Thing Adversaries: Studying the Behavior of Attackers with an Internet of Things Honeypot

Chloe Stapleton, Xenia Mountrouidou, *College of Charleston*; Jason Damron, *Sensilla*

Due to rising numbers of Internet of Things (IoT) devices and a growing number of attacks against them [1], research in IoT defense has gained interest. In order to defend, we need to understand the adversary. Thus, the development of IoT honeypots has been recently on the rise [2, 3]. A honeypot is a convincing set of interconnected devices that imitates a scenario of a real network with the sole purpose to lure adversaries and study their behavior.

We propose a realistic IoT honeypot that mimics a specific environment: namely the computer science department at our university. Using 64 IP addresses unprotected from our school's firewall, we gather passive data about the traffic on these IPs. Specifically, we log events using a Palo Alto firewall and save data from Linux processes such as tcpdump, netstat, top and ps running on Raspberry Pi computers. We then emulate our scenario of the department network that includes a campus security system of webcams, multiple printers and routers, and IoT device websites. Using Scapy, a Python library for computer network packet manipulation, we craft packets then manipulate banner responses from the different IoT devices to achieve a believable high-interaction honeypot. We analyze the responses from adversaries, specifically the incoming commands sent by the attackers and how they are responding to our crafted scapy packets. The customized responses keep adversaries "trapped" longer and continue to communicate with the honeypot, providing us with further details about how they are utilizing IoT devices.

STUDENT POSTERS

The contributions of our work are twofold. First, we create a simple yet effective IoT honeypot with "off the shelf" material and scapy-crafted responses. Second, we create websites to lure adversaries and study their behavior. To our knowledge, there have been no IoT website honeypots even though website portals are an important component of IoT devices. Thus, the analysis of the data from our honeypot will lead to the discovery of interesting new behaviors and attacks.

23. Privacy Preserving Yet Verifiable IoT Devices

Nishchala Tangirala, Ankit Jena and Xinchen Wang,
Carnegie Mellon University

The advent of the Internet of Things (IoT) has tilted the technology landscape at an unprecedented rate. As the market for IoT devices grows twofold, home assistants are becoming more and more ubiquitous. While these devices get smarter and enhance user experience with newer versions, privacy concerns continue to expand. Home assistants like Google Home and the Amazon Echo gather massive volumes of potentially sensitive user data. To the average user, who seems really impressed by the convenience such devices have ushered in, it is very easy to overlook the fact that the microphone on your favorite home assistant might be eavesdropping on everything you're saying. What exacerbates the problem is the lack of a legal framework defining the ownership of the data collected by these devices. In this work, we've designed and implemented a voice assistant that localizes processing of the raw user information on the device while allowing the cloud service provider to verify correct hardware execution of its service through a trusted computing environment in Intel SGX.

24. Zero Knowledge Proofs in Hyperledger Indy

Deepika Vasudevan, Brett Hemenway, Erik Marks, Yihan Wang and Saurav Sharma, *University of Pennsylvania*

In order to endow users with granular control over their data and identities, most distributed ledger technology (DLT)-based identity management platforms have integrated support for zero-knowledge proofs (ZKPs). ZKPs allow a user (credential holder) to convince a verifier of their credentials without revealing the credentials themselves. Hyperledger Indy is a DLT identity management platform being incubated by the Hyperledger Foundation. Its credential system relies on the implementation of a novel protocol referred to in their documentation as AnonCred. The AnonCred implementation consists of various cryptographic constructions, including ZKPs, signatures and dynamic accumulators, many of which are poorly documented. Critically, the correctness and therefore security of AnonCred and its implementation appears to be unverified. This project presents the theoretical foundations of AnonCred and analyses of the AnonCred protocol and its implementation in Hyperledger Indy.

25. MMORPG Trading Covert Channel

Laura Weintraub, Charissa Miller and Joshua Geise,
Rochester Institute of Technology

Covert channels are on the rise in order to secretly transfer information for private communication. Video games are particularly of interest for secret communications because of their popularity, large data network and accessibility at all hours of the day. This paper proposes a covert channel via a common game functionality of massively multiplayer online role-playing games (MMORPGs): player-to-player trading. A trade is only between two players, therefore the contents of the trade are private. In-game trading is very common, thus attention is not drawn to suspicious characters. The encoding of a message is performed using tradable items that correspond to various bit values.

This channel is demonstrated in the online game, Old School RuneScape. It achieved a bandwidth high of 1.600 bits/second with an error rate of 0 percent. Improvements can be made to increase bandwidth by assigning items larger bit values. The approach taken for this implementation can easily be extended to other MMORPGs.

26. Prob-Containers: Security Offloading to Edge

Wenhui Zhang, *Pennsylvania State University*

Emerging technologies (Internet of Things systems, augmented reality and virtual reality systems, autonomous cars) bring extra network-facing attack interfaces to legacy microcontrollers. Malicious payloads embedded in network packets could exploit and subvert machine code execution. This may introduce tremendous damage if not detected and handled efficiently.

Combating these threats via embedding security functionality on these real-time operating systems interrupts their normal operations. Furthermore, limited CPU and memory on these circuits is not suitable for security checking and security enforcement. Offloading security functionality to the cloud brings latency and privacy issues, making it unsuitable to combat these threats. Edge clouds are uniquely positioned to provide these security functions within required latency margins and without taxing battery and compute resources in the edge devices.

In this paper, we build and evaluate an intrusion detection method suitable to run in an edge cloud as a security monitor to check malicious network flows and protect our systems. We investigate two methods to improve throughput of our system via flow splitting and rule splitting, and conclude flow splitting is the more recommended technique. Since network is the expected bottleneck, we conduct stress tests for our system with kernel TCP stack bypassing techniques and give out some guidance numbers to configure it to support 5G wireless throughout, which is at least 20 Gbits per second. Code is open-sourced and can be found at: https://www.akraino.org.

A Global Leader in Cybersecurity Education, Policies, and Research.

Competing at DefCon 2018

Carnegie Mellon University has won four "World Series of Hacking" titles at the DefCon security conference — more wins than any other team in the 21-year history of this international competition.

The problem-solving skills required to win these contests mimic defenses needed in government and business today, to anticipate and prevent real-world cyber attacks.

There is no university better positioned to define and positively impact the space where technology and society intersect, than Carnegie Mellon University.

cmu.edu/wicys

Carolina Zarate
Student, Information Networking Institute

Carnegie Mellon University

CERC
Cybersecurity Education, Research and Outreach Center

The Cybersecurity Education, Research and Outreach Center at Tennessee Tech University seeks the enrichment of the cybersecurity community and its members through education program development, effective research into emerging areas of need, and outreach to students of all ages and grade levels encouraging their participation in STEM experiences and the excitement of the cybersecurity field.

Programs Highlights:

- NSA Center of Academic Excellence – CDE
- First CyberCorps NSF SFS program in the State of TN
- Only DoD Cyber Scholarship (CySP) program in TN
- CyberEagles student cybersecurity club
- NSF Women in Cybersecurity – Founding Institution
- NSF-NSA GenCyber Camps Program
- Defense and offense competition teams

CYBER EAGLES
Tennessee Tech University
We soar to defend

CyberCorps®
Defending America's Cyberspace

Come join our team and experience the world of cybersecurity in its complete spectrum and diversity!

- For more information about our center and its mission, go to http://www.tntech.edu/ceroc.
- Students interested in applying for the highly competitive CyberCorps SFS scholarship, go to https://www.tntech.edu/ceroc/education/sfs.
- Information about our degree programs (B.S., M.S., and Ph.D) can be found at https://www.tntech.edu/engineering/departments/csc.

2019 WICYS CONFERENCE

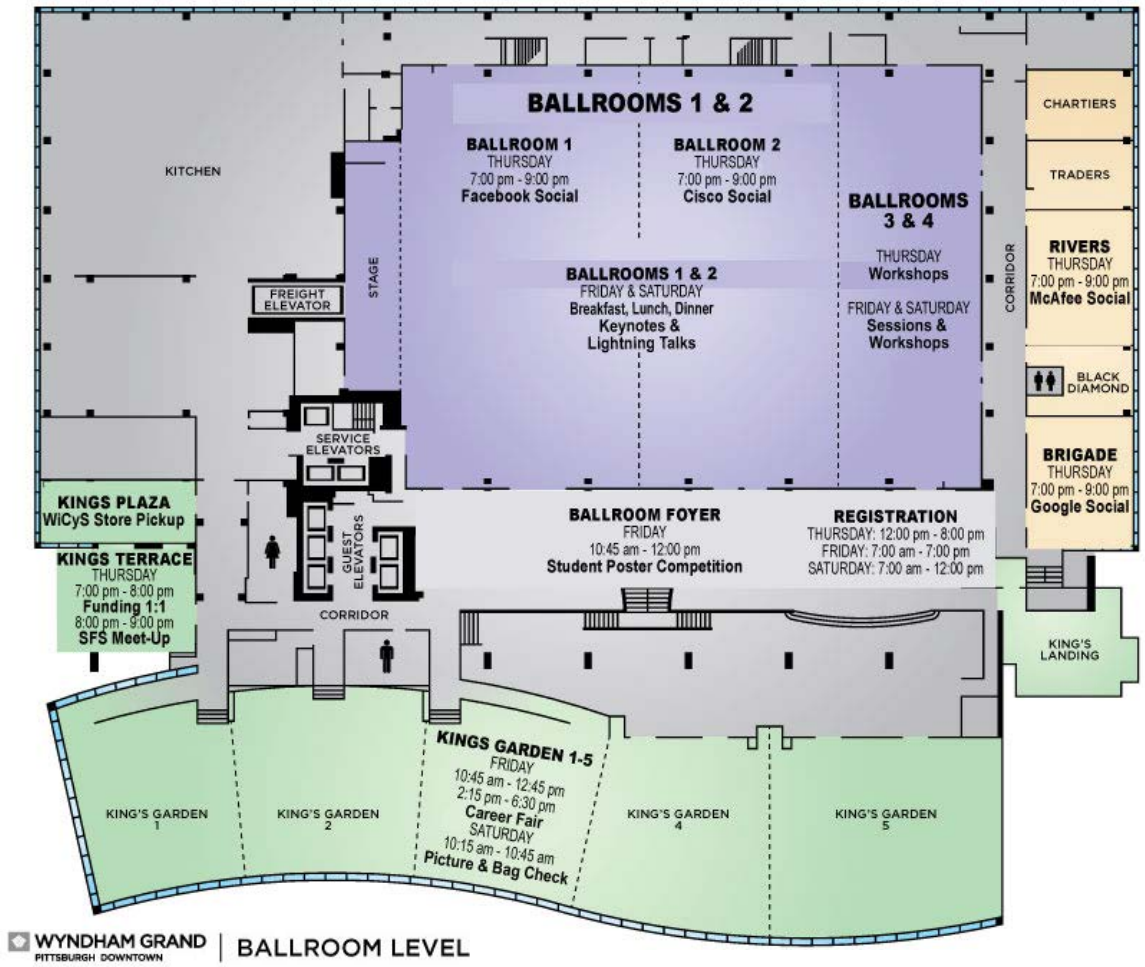
NOTES

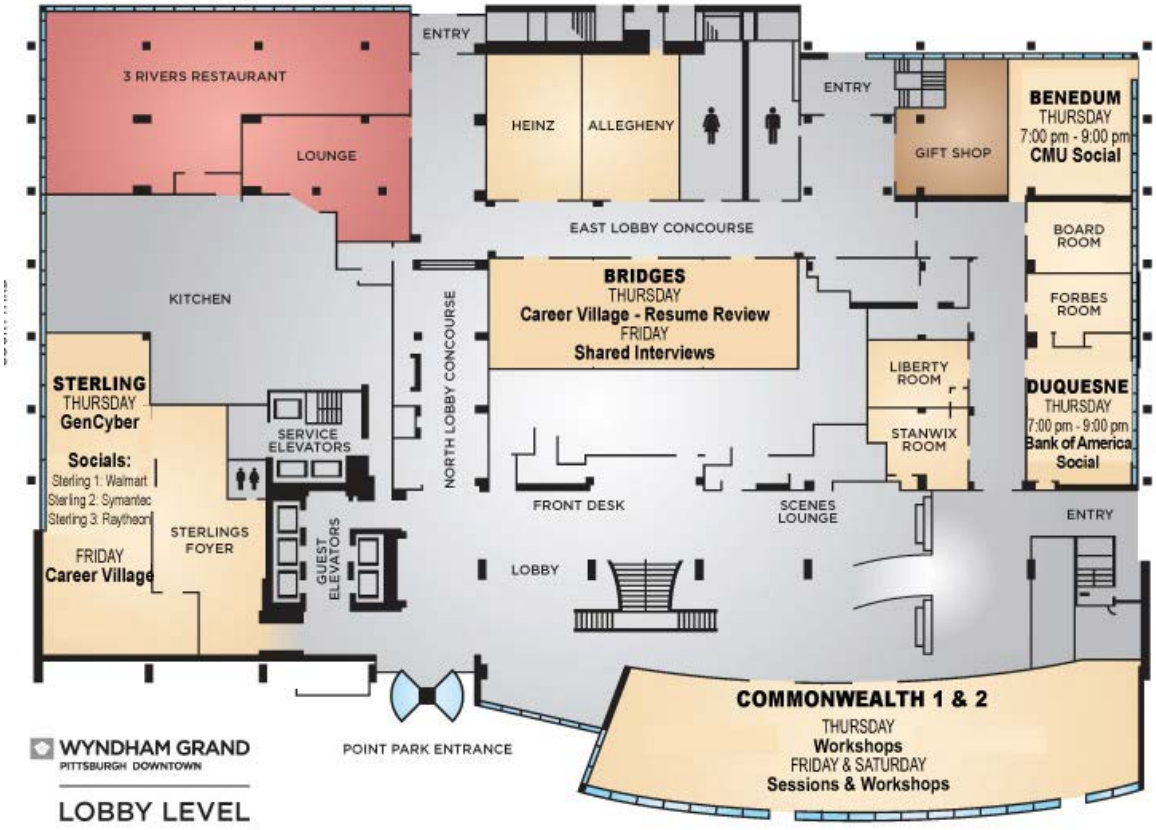
2019 WICYS CONFERENCE

NOTES

2019 WICYS CONFERENCE

NOTES


BALLROOMS 1 & 2
BALLROOM 1
THURSDAY
7:00 pm - 9:00 pm
Facebook Social
BALLROOM 2
THURSDAY
7:00 pm - 9:00 pm
Cisco Social
BALLROOMS 1 & 2
FRIDAY & SATURDAY
Breakfast, Lunch, Dinner
Keynotes &
Lightning Talks
BALLROOMS 3 & 4
THURSDAY
Workshops
FRIDAY & SATURDAY
Sessions &
Workshops
KITCHEN
STAGE
FREIGHT ELEVATOR
SERVICE ELEVATORS
GUEST ELEVATORS
CORRIDOR
CHARTIERS
TRADERS
RIVERS
THURSDAY
7:00 pm - 9:00 pm
McAfee Social
BLACK DIAMOND
BRIGADE
THURSDAY
7:00 pm - 9:00 pm
Google Social
KINGS PLAZA
WiCyS Store Pickup
KINGS TERRACE
THURSDAY
7:00 pm - 8:00 pm
Funding 1:1
8:00 pm - 9:00 pm
SFS Meet-Up
BALLROOM FOYER
FRIDAY
10:45 am - 12:00 pm
Student Poster Competition
REGISTRATION
THURSDAY: 12:00 pm - 8:00 pm
FRIDAY: 7:00 am - 7:00 pm
SATURDAY: 7:00 am - 12:00 pm
KING'S LANDING
KINGS GARDEN 1-5
FRIDAY
10:45 am - 12:45 pm
2:15 pm - 6:30 pm
Career Fair
SATURDAY
10:15 am - 10:45 am
Picture & Bag Check
KING'S GARDEN 1
KING'S GARDEN 2
KING'S GARDEN 4
KING'S GARDEN 5
WYNDHAM GRAND
PITTSBURGH DOWNTOWN
BALLROOM LEVEL


3 RIVERS RESTAURANT
LOUNGE
ENTRY
HEINZ
ALLEGHENY
ENTRY
GIFT SHOP
BENEDUM
THURSDAY
7:00 pm - 9:00 pm
CMU Social
EAST LOBBY CONCOURSE
BOARD ROOM
FORBES ROOM
KITCHEN
NORTH LOBBY CONCOURSE
BRIDGES
THURSDAY
Career Village - Resume Review
FRIDAY
Shared Interviews
LIBERTY ROOM
STANWIX ROOM
DUQUESNE
THURSDAY
7:00 pm - 9:00 pm
Bank of America
Social
STERLING
THURSDAY
GenCyber
Socials:
Sterling 1: Walmart
Sterling 2: Symantec
Sterling 3: Raytheon
FRIDAY
Career Village
SERVICE ELEVATORS
STERLINGS FOYER
GUEST ELEVATORS
FRONT DESK
SCENES LOUNGE
ENTRY
LOBBY
COMMONWEALTH 1 & 2
THURSDAY
Workshops
FRIDAY & SATURDAY
Sessions & Workshops
POINT PARK ENTRANCE
WYNDHAM GRAND
PITTSBURGH DOWNTOWN
LOBBY LEVEL

EVENTS, PRIZES, TRAVEL AWARDS AND SPECIAL ITEMS

SPONSORS - WICYS THANKS YOU!

Adobe . . . . . Friday Dinner
AWS . . . . . Coffee Break
Cisco . . . . . 25 Travel Scholarships
CMU . . . . . Friday Breakfast
CMU . . . . . Conference Bags
CMU . . . . . Conference T-Shirts
CMU . . . . . Charging Stations
CyberWatch West . . 16 Travel Scholarships
Facebook . . . . . 25 Travel Scholarships
Fidelity . . . . . Ten Travel Scholarships
Fireeye . . . . . Two Travel Scholarships
Google . . . . . Scholarships
NYU Tandon . . . . . Coffee Break
PayPal . . . . . Mobile App
SIA . . . . . Friday Lunch
Synopsys . . . . . Saturday Breakfast
Symantec . . . . . Affiliate & Student Chapter Awards
Turner Broadcasting . Coffee Break
Workday . . . . . Lanyards

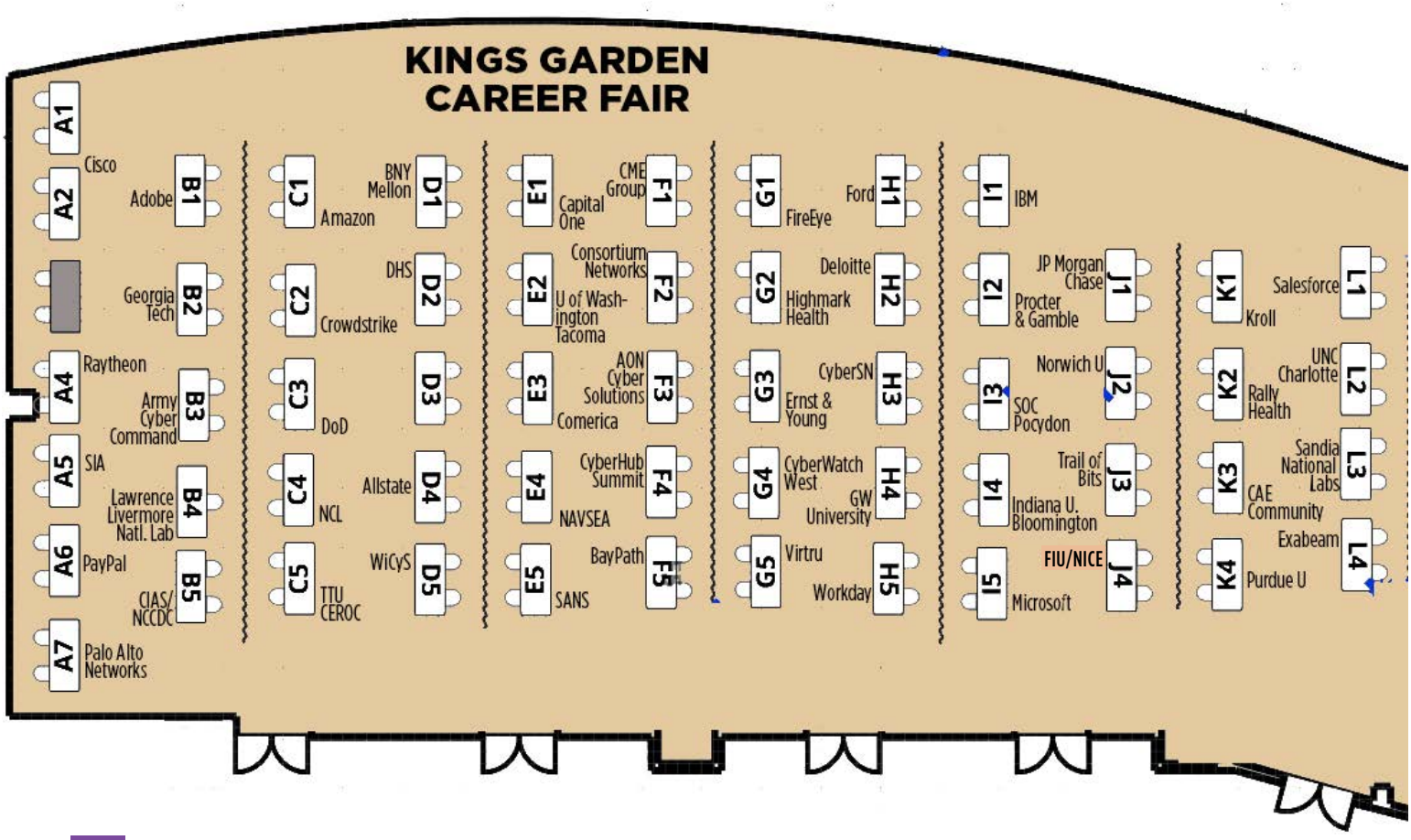
HEY, STUDENTS!

SEE A SPONSOR? SAY THANKS!

Without our sponsors, there would be no WiCyS Conference!

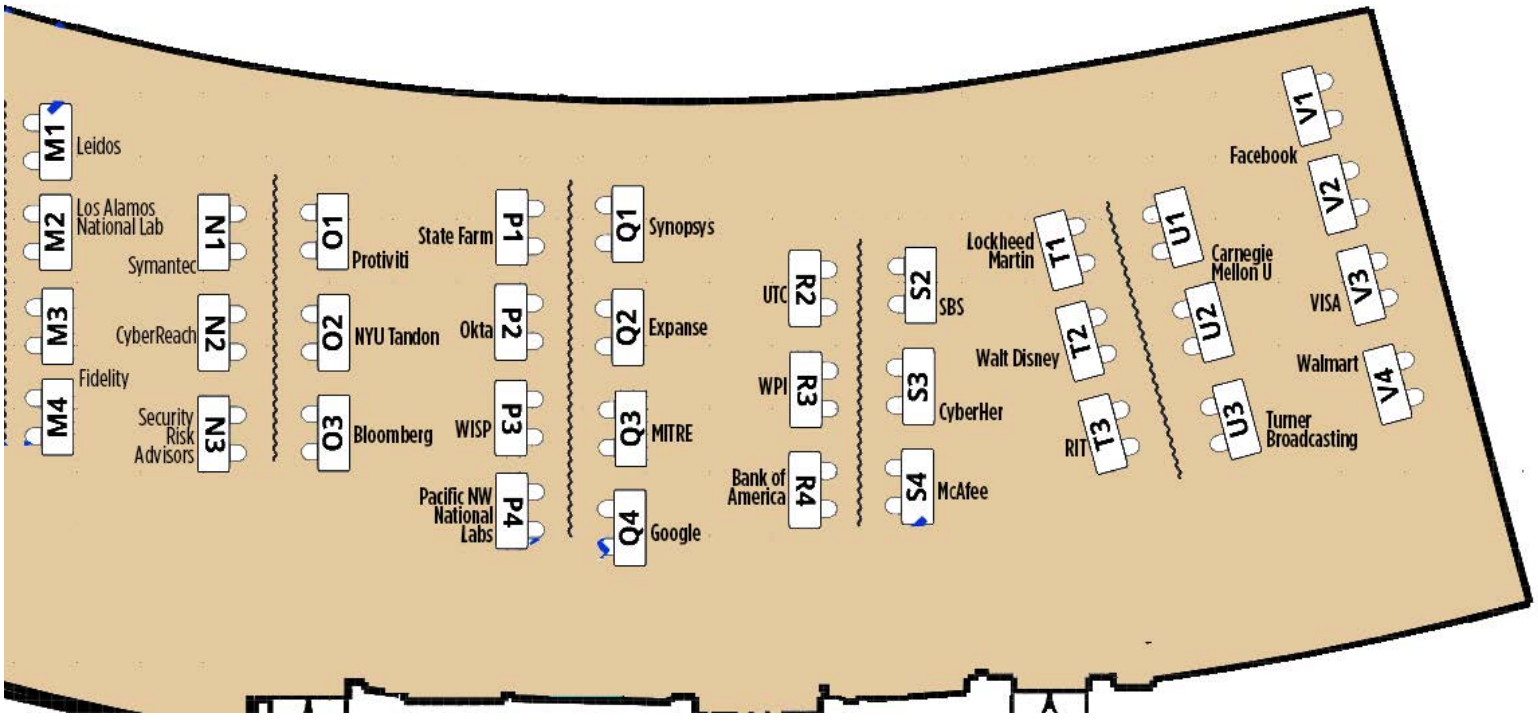
A sincere thanks to the Conference sponsors, whose funding enables 500 students to attend WiCyS on a scholarship.

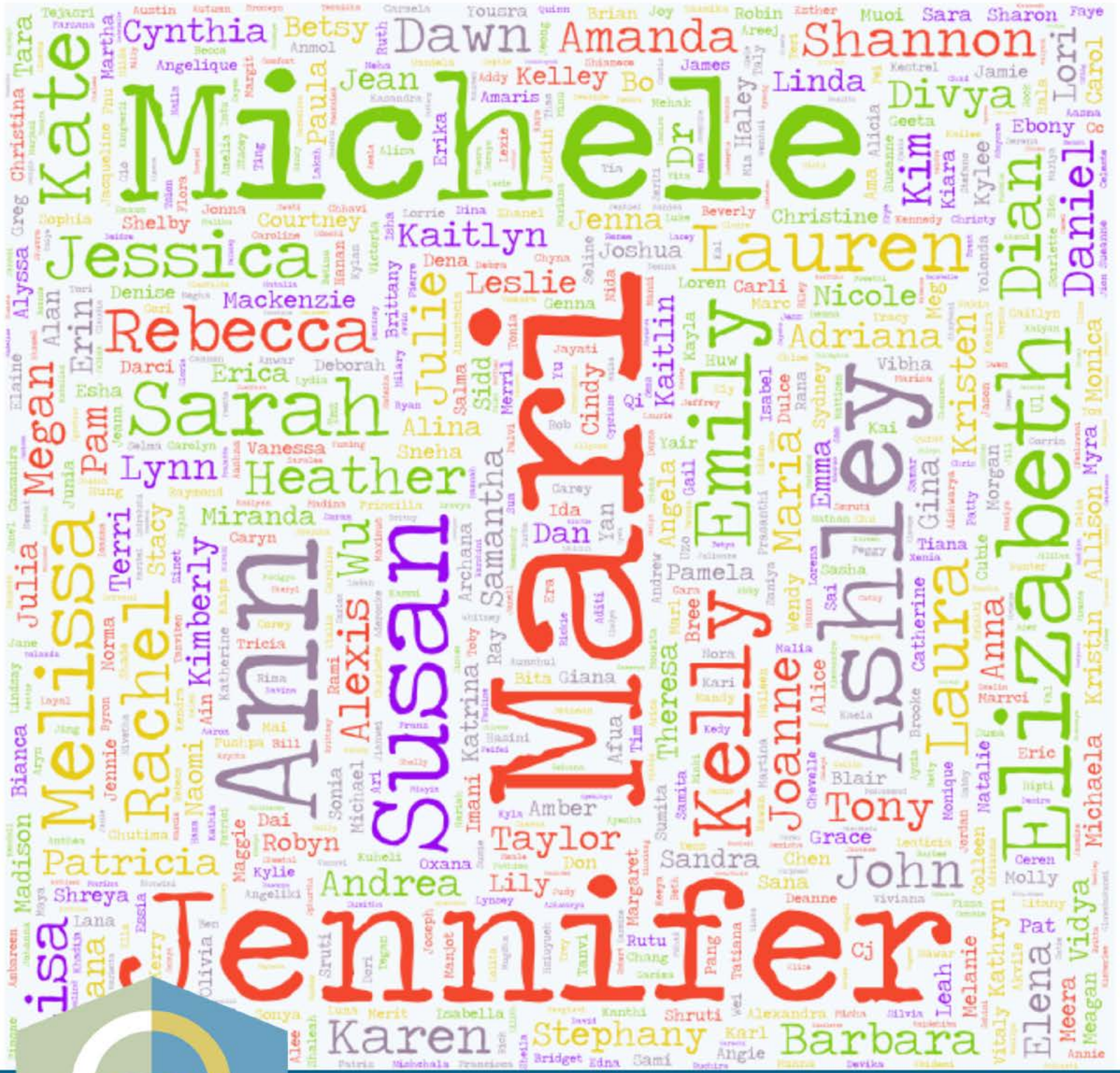
Lodging grants are also provided to faculty.



VIST THE
CAREER FAIR

Adobe B1
Allstate D4
Amazon C1
AON Cyber Solutions F3
Army Cyber Command B3
Bank of America R4
BayPath F5
Bloomberg O3
BNY Mellon D1
CAE Community K3
Capital One E1
Carnegie Mellon . . . . . U1 & 2
CEROC - Tennessee Tech C5
CIAS / NCCDC B5
Cisco . . . . . A1 & 2
CME Group F1
Comerica E3
Community Table . . . . . Z1 & 2
Consortium Networks, LLC F2
Crowdstrike C2
CyberHer S3
CyberHub Summitt F4
CyberReach N2
CyberSN H3
CyberWatch West G4
Deloitte H2
Department of Defense C3
DHS D2
Ernst Young G3
Exabeam L4
Expanse Q2
Facebook . . . . . V1 & 2
Fidelity . . . . . M3 & 4
FireEye G1
FIU / NICE J4
Ford H1
George Washington University H4
Georgia Tech B2
Google Q4
Highmark Health G2
IBM I1
Indiana Univ -Bloomington I4
JP Morgan J1
Kroll K1
Lawerence Livermore National Labs B4
Leidos M1
Lockheed Martin T1
Los Alamos National Lab M2
McAfee S4
Microsoft I5
NAVSEA E4
NCL C4
NYU Tandon School of Engineering O2
Norwich University J2
Okta P2
Pacific Northwest National Labs P4
Palo Alto A7
PayPal A6
Procter & Gamble I2
Protiviti O1
Purdue University K4
Rally Health K2
Raytheon A4
Rochester Institute of Technology T3
Salesforce L1
Sandia National Labs L3
SANS Technology Institute E5
SBS S2
Security Industry Association (SIA) A5
Security Risk Advisors N3
SOC Pocydon I3
State Farm P1
Symantec N1
Synopsys Q1
The Mitre Corporation Q3
The Walt Disney Company T2
Trail of Bits J3
Turner U3
United Technologies - UTC R2
Univ of North Carolina - Charlotte L2
Univ of Washington - Tacoma E2
Virtru Corporation G5
Visa V3
Walmart V4
WiCyS D5
WISP P3
Worchester Polytechnic Institute R3
Workday H5





JOIN WICYS IN SUPPORTING WOMEN IN CYBERSECURITY

Join Women in CyberSecurity (WiCyS) in moving the needle from the 10-20% representation of women in the cybersecurity workforce to a balanced and diverse makeup. Established in 2012 by Dr. Ambareen Siraj of Tennessee Tech University through a National Science Foundation grant, WiCyS is a non-profit organization offering many membership, sponsorship and collaboration benefits.

Learn more about participating, sponsoring and partnering with WiCyS by contacting info@wicys.org.

Visit wicys.org