

#WiCyS2020

2020 WiCyS CONFERENCE

DENVER, CO | MARCH 12-14, 2020

VIP SPONSORS:



FACEBOOK



TABLE OF CONTENTS

- Welcome3
- Board of Directors3
- Keynote Speakers4
- Thanks To Sponsors5
- Thanks to Committee Members . .6-8

- Track and Session Guide9
- Schedule at a Glance. 10
- Thursday Agenda 12
- Friday Agenda 13-15
- Saturday Agenda 17-18

- Pre-Conference Sessions 19
- Workshop Descriptions . . . 20-23
- Presentation Descriptions . . 24-26
- Birds of a Feather Descriptions . . 27
- Panel Session Descriptions . . . 28
- Lightning Talk Descriptions . . 29-32
- Student Poster Descriptions . 33-43

- Sponsor Ads 44-58
- Notes 58-60
- Career Fair Booths. 61
- Venue/Room Maps 62-63

BADGE PICK-UP HOURS

THURSDAY 7:00am - 7:00pm
FRIDAY 7:00am - 6:00pm
SATURDAY 7:00am - 9:00am



USE THE APP

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.

APP CODE: SeeHerAsEqual2020



SOCIAL MEDIA

Win Lodging & Registration to WiCyS 2021!

Enter the social media contest on Facebook, Twitter or Instagram! Use **#WiCyS2020** on a public page or on the WiCyS Facebook event wall to share pictures and stories of your time at the conference.

Winners will receive notification on social media and email after the conference.

SNAPCHAT @ WiCyS

Use Our 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 #WiCyS2020 filter.



W i C y S 2 0 2 0

WELCOME TO THE 7TH ANNUAL WiCyS CONFERENCE

We all have a story to tell. Mine is a journey where my beliefs and passion led me to WiCyS. From being curious about the first conference proposed by Dr. Ambareen Siraj back in 2014 to becoming involved with the operations of the conference since 2015, my love for WiCyS has grown and continues to be unstoppable. So it's only natural that my heart is full now to be here, as executive director, welcoming you to the seventh annual WiCyS conference!

Out of 1,600+ in attendance, there is only one YOU! This conference is for your unique self to embrace the excitement, take advantage of the networking and learning opportunities at each session, engage at the WiCyS community tables, attend a Meetup, challenge yourself in the NCL competition, find mentoring in the career village plus much more! I encourage you to surpass your comfort zone and do something that you've never done before, either for your professional growth or to pay it forward. WiCyS became the nonprofit organization it is because of the community who had a need for it and who relentlessly supports it. This is YOUR community now, so discover your empowerment, and let WiCyS be your story's next chapter!

Lynn Dohm

WiCyS Executive Director



WiCyS BOARD OF GOVERNORS

Dr. Ambareen Siraj

*WiCyS Founder & Board Member
Director, Cybersecurity Education,
Research and Outreach Center
Tennessee Tech University*

Dr. Janell Straach

*Chair of the Board, WiCyS
Faculty,
Rice University*

Dr. Costis Torgas

*WiCyS Board Treasurer
Director,
George Washington University*

Dr. Dawn M. Beyer

*Senior Fellow
Lockheed Martin Space*

Jenn Henley

*Vice President,
Infrastructure at Facebook*

Dr. Cynthia Irvine

*Director,
Naval PostGraduate School*

Prajakta Jagdale

*Senior Manager, Information Security,
Palo Alto Networks*

Jay Koehler

*Diversity, Inclusion & Engagement
Manager, Security & Trust Organization,
Cisco*

Allison Miller

*Vice President of Global Enterprise,
Cyber Security Office,
UnitedHealth Group/OPTUM*

Michele Schochet

*Director, Infrastructure,
Chan Zuckerberg Initiative*

Dr. Greg Shannon

*Chief Scientist,
Carnegie Mellon University*

2020 WiCyS CONFERENCE

KEYNOTE SPEAKERS

Sandra McLeod, Cisco Systems

“We’re all in this together: Transforming Security at Cisco”

Building secure solutions requires a commitment to security at every step in the process. However, creating that culture of security and accountability can be a challenging journey. Hear how we are transforming product security at Cisco from a program of policing to building partnerships and working together with product teams to improve security and reduce risk for our customers.



Sandra McLeod is currently Director of Cisco's product security risk assessment group, protecting Cisco's products and customers through attack-focused security evaluations, red team exercises, and penetration testing. Her passion for helping product teams build secure solutions comes from many years of working on the other side, developing and operating financial and medical software solutions. Since joining Cisco 8 years ago, Sandra has had the opportunity to hold a number of different roles, including leading the development of automated security testing services for Cisco's Cloud offerings. Today her focus is on partnering with Cisco's product teams to identify and mitigate security vulnerabilities, driving down risk and improving the security of our products.

Gretchen Block, Optum

“Power, Influence and the Art of Female Leadership”

Gretchen Block will chronicle her own journey from John Deere HealthCare to becoming a global leader at Optum/UnitedHealth Group driving technology risk management across business towers and geography. This keynote will focus on an uncomfortable topic for female leaders around organizational politics, positional and personal power, the juxtaposition of power and influence, and female leadership potential. Female leaders emerging in the workforce must employ savvy and grit to maximize their leadership potential. Sharing her journey, Gretchen will touch on this often unspoken topic with courage and candor.



Gretchen Block began her career in 1995, with John Deere HealthCare. Her roles included IT Asset Management, Computer Operations, and Security. Gretchen joined Optum in 2006, as part of the acquisition of John Deere HealthCare with UnitedHealth Group. With Optum, she has been a part of the Enterprise Security organization, working specifically with risk governance, compliance management, and threat management in support of the broader cybersecurity program. Currently, Gretchen leads the enterprise policy, risk governance, and security operations teams supporting critical business areas within UnitedHealthCare and Optum.

Sid Sidhu, Facebook

“Scaling for the Future”

It is increasingly evident in the industry that security organizations that have served us well in the past are not quite ready to scale for the future. I am afforded a unique opportunity at Facebook by working at the intersection of Production Engineering and Security. In this talk, I will share lessons I learned from scaling infrastructure teams, and how similar drivers can help us evolve our security teams. What brought us to this point isn't enough to help us reach the next level. It will take a skillset evolution, a mindset shift, and cultural and organizational change to help us scale.



As a leader in Production Engineering at Facebook, Sid's team works on scalability of infrastructure services, with a focus on security. Her role gives her a unique perspective on cultural and organizational drivers in scaling infrastructure that can be leveraged to build security teams of the future. Originally from India, Sid has called Silicon Valley home for the last 15 years, with prior stints at Box, Juniper, and Sun Microsystems.

THANK YOU TO OUR 2020 CONFERENCE SPONSORS

VIP SPONSORS



FACEBOOK



PREMIUM SPONSORS



mastercard.

Raytheon

State Farm™

verizon✓

DIAMOND SPONSORS



Bank of America

Carnegie Mellon University
Software Engineering Institute

CERiC



CSSIA

CyberProof™
AUST Global Company



DENSO
Crafting the Core

IBM

RIT

Kroll

A Division of
DUFF & PHELPS

Microsoft



robinhood

MCS@RICE
Computer Science

salesforce

SYNOPSIS™
Silicon to Software™

VISA

Walmart

PLATINUM SPONSORS



CISRE
Center for Information Security
Research and Education

COALFIRE

COLORADO STATE
UNIVERSITY



CyberGRX

Deloitte

EY
Building a better
working world

FIREEYE™

Georgia Tech
Research Institute



LinkedIn



NCYTE
CENTER

paloalto

protiviti



GOLD SPONSORS



bugcrowd

ini
Carnegie Mellon University
Information Technology Institute



Comerica Bank

CYBRARY

elastic

Georgia Tech
Master of Science
in Cybersecurity



MITRE



NYU
TANDEM
SCHOOL OF
ENGINEERING



proofpoint

pure

RunSafe
SECURITY

SecurityRisk

SYNNEX

Technology, Cybersecurity
and Policy Program
UNIVERSITY OF CALIFORNIA, BERKELEY

The
Walt Disney
Company

CISA

U.S. DEPARTMENT OF STATE
BUREAU OF CYBERSECURITY

THE UNIVERSITY
OF ARIZONA

University
of San Diego

virtu

workday

SILVER SPONSORS

BAY PATH
UNIVERSITY

CAPITOL
Technology University

DARKVOWL

Dominion
Energy

EC-COUNCIL/ACADEMIA

Northeastern University
Khoury College of Computer
and Information Sciences

PRAETORIAN

PURDUE
UNIVERSITY
Polytechnic Institute

SAIC
Building Agency

SOPHOS

Spectrum

TOWSON
UNIVERSITY

UNT
COLLEGE OF
ENGINEERING
Department of
Computer Science
& Engineering

W
UNIVERSITY OF WASHINGTON - BOTHELL
MASTER OF SCIENCE IN CYBER SECURITY ENGINEERING

W
MASTER OF CYBERSECURITY & LEADERSHIP
UNIVERSITY OF WASHINGTON - TACOMA

WPI

BRONZE SPONSORS

ACTIVISION

NETFLIX

TWO SIGMA

COMMUNITY COLLABORATORS

CAE
COMMUNITY COLLABORATION

CIAA
COMMUNITY COLLABORATION



CyberCorps
Following American Operations

CYBERSECURITY
COLLABORATION FORUM

CYBER
SECURITY
SENTRY

CYBERTECH
School Events

DiversityComm
Communicating the Difference

FIU
FLORIDA INTERNATIONAL
UNIVERSITY



National Center for
Women &
Information
Technology



NATIONAL
CYBERSECURITY
CENTER

SECUREWORLD



EXCLUSIVE MEDIA PARTNER

CYBERCRIME
MAGAZINE

THANK YOU TO OUR 2020 WiCyS COMMITTEES

CONFERENCE CHAIR

Dr. Ambareen Siraj

Director, Cybersecurity Education,
Research and Outreach Center;
Professor, Computer Science,
Tennessee Tech

LOGISTICS AND OPERATIONS CO-CHAIRS

Janell Straach

Lead - Operations
Faculty, Rice University

Lynn Dohm

Logistical Support
Executive Director, WiCyS

PROGRAM CO-CHAIRS

Celeste Matarazzo

Co-Chair
Data Science Expert, Lawrence
Livermore National Laboratory

Ashley Podhradsky

Co-Chair
Associate Dean, Beacom College of
Computer and Cyber Sciences,
Dakota State University

PROGRAM

Dalal Alharthi

Faculty and Cloud Security Engineer

Garima Bajwa

Assistant Professor,
Capitol Technology University

Shankar Banik

Professor, The Citadel

Emily Darraj

CEO, President,
AI Cybersecurity Institute

Kalika Dennis Sr.

Information Security Risk Analyst,
Thomson Reuters

Deepti Gupta

PhD student at University of Texas,
San Antonio

Lora Vaughn

CISO, Simmons Bank

Eric Chan-Tin

Assistant Professor,
Department of Computer Science,
Loyola University Chicago

Sandra McLeod

Sr. Manager, Cisco Systems

Kelley Misata

CEO and Founder, Sightline Security

Abhilasha Bhargav-Spantzel

Principal Engineer, Intel Corporation

April L. Tanner

Associate Professor/Graduate Program
Director of Computer Science,
Jackson State University

Denis Ulybyshev

Assistant Professor,
Department of Computer Science,
Tennessee Tech University

Jeong Yang

Texas A&M University-San Antonio

Chuan Yue

Professor, Colorado School of Mines

SCHOLARSHIP

Shade Adeleke

Associate Professor,
Prince George's Community College

Gretchen Bliss

Cybersecurity Director,
Pikes Peak Community College

Nathan Chung

Senior Cybersecurity Consultant, EY

Lydia Edwards

Examiner, Department of Commerce

Russ Fellers

VP for Education Programs,
AFCEA-Rocky Mountain Chapter

Hunter Healy

Cybersecurity Analyst,
Ethical Hacking Team, Visa Inc.

Diane M. Janosek

Commandant, National Cryptologic
School & President of WiCyS
Mid-Atlantic Affiliate, NSA

Pushpa Kumar

Associate Professor of Instruction,
The University of Texas at Dallas

Cheryl Ledbetter

Noureen Njoroge

Cybersecurity Consulting Engineer;
President of North Carolina
WiCyS Affiliate, Cisco

Angela Sims-Ceaj

Sr. Water IT Project Manager, City of Aurora

Shannon Strum

Security Engineer, Facebook

THANK YOU TO OUR 2020 WiCyS COMMITTEES

WiCyS COLORADO CONFERENCE SUPPORT CONSORTIUM (WCCSC)

Gretchen Bliss

Lead
Cybersecurity Director,
Pikes Peak Community College

Kyle Arfsten

Director of Client Relationships,
Kforce, Inc.

Steve Beaty

Professor, MSU Denver

Bob Bowles

Director of the Center for Information
Assurance Studies, Regis University

Nathan Chung

EY, Senior Cybersecurity Consultant

Russ Fellers

VP for Education Programs
AFCEA-Rocky Mountain Chapter

Steve Fulton

Coleman Richardson Chair,
Computer Science, USAFA

Angela Hogaboom

President, Open Sky Networks

Terri Johnson

Department Chair
Computer Networking & Cybersecurity
Pikes Peak Community College

Jeff London

Professor, MSU Denver

Marian Merritt

Lead for Industry
Engagement, NIST/NICE

Dan Manson

Research Professor
Desert Research Institute;
Commissioner, NCL

Joe Murdock

Business School Faculty
Uni. of Colorado Denver

Jennifer Peyrot

Teacher, St Vrain Valley Schools

Indrakshi Ray

Professor, Computer Science
Department, Colorado State University

Lt Col Traci A. Sarmiento

Deputy Head,
Computer & Cyber Sciences, USAFA

Angela Sims-Ceja

Senior Water Information Technology
Project Manager, IT Project Management
Office City of Aurora

Patrice Siravo

Director of Commercial Cybersecurity
System High Corporation

Tobi West

Department Chair CIS/CST/CYBR
Coastline College

Chuan Yue

Associate Professor
Colorado School of Mines

Mariyam Zaheer

Security Risk and Compliance Analyst
Gov. Office of Information Technology

OPERATIONS AND LOGISTICS

Michele Tomasic

Operations & Logistical Support
Divisions Operations Manager,
Carnegie Mellon University

Lana Richardson

Sponsor Support
Community Care Manager,
WiCyS

Colleen Huber

CRM,
The Nelly Group

CAREER FAIR

Mary Jane Partain

Career Fair Concierge
Director, University of Texas-Dallas

Patrice Siravo

Director of Commercial Cybersecurity,
System High Corporation

Kyle Arfsten

Director of Client Relationships,
Kforce, Inc.

SOCIAL MEDIA & PR

Aditi Chaudhry

Cybersecurity Engineer,
Two Sigma

Bonnie Jan

Student,
North Dakota State University

Vanessa Primer

Student,
Highline College

Anna Lainfiesta

Security Compliance Analyst,
Zendesk

VOLUNTEER COORDINATION

Cameron Mitchell

Logistical Support
Carnegie Mellon University

POSTER

Chutima Boonthum-Denecke

Professor, Computer Science,
Hampton University

THANK YOU TO OUR 2020 WiCyS COMMITTEES

CAREER VILLAGE

Andrea Frost

*Career Fair Village Lead
Senior Software Security
Engineer, Dell EMC*

Michelle Lindblom

*Security Awareness Manager,
Salesforce*

Kim Huynh

*Cybersecurity Engineer,
Premera Blue Cros*

Colleen R. Murphy

*C|CISO, CISSP, CCTA, ITILv3,
ISSA Fellow, Past President,
ISSA-Colorado Springs
Chapter of the Year 2005,
2008, 2017*

INDUSTRY LEADERSHIP SUMMIT

Michelle Guel

*Co-Chair
Engineer & IoT Security Strategist,
Cisco*

Prajakta Jagdale

*Co-Chair
Cybersecurity Professional,
Palo Alto Networks*

CHAPTER COMMUNITIES

Vitaly Ford

*WiCyS Student Chapter Coordinator
Assistant Professor at Arcadia University
Computer Science and Math Department*

Pauline Mosley

*WiCyS International Chapter Advisor
Assistant Chair & Full Professor of
Information Technology, Pace University
Pace University Faculty Advisor*

AFFILIATE COMMUNITIES

Malia Mason

*WiCyS Affiliate Development Liaison
CEO / Co-Founder of Integrum
WiCyS SoCal President & Co-Founder
AnitaB.org Technology Chair*

Rae Becerra

*WiCyS Affiliate Operations Liaison
Senior Network Engineer,
Museum of Science in Boston*

VETERAN COMMUNITIES

Amelia Estwick

*Lead
Vice President, WiCyS Mid-Atlantic Affiliate
Director, National Cybersecurity Institute,
Excelsior College
U.S. Army Veteran*

Diane M. Janosek

Department of Defense

Racquel N. James

*USAF, Ret.,
Department of Defense*

Marylyn R. Harris

*Executive Director,
Women Veterans Business Center
U.S. Army*

Carl H. Sharperson, Jr.

*President/CEO,
Sharperson's Executive Leadership
US Marine Corps - Veteran*

Corrinne Sande

*Director/PI, NCyTE Center/CS/CIS
Director CAE National Resource Center,
Whatcom Community College*

PROGRAM PARTICIPATION TRACKS AND SESSIONS

CURRENT TECHNOLOGY AND CHALLENGES TRACK

Current issues and challenges, advances in research and development (R&D), experimental findings.

BEST PRACTICES TRACK

Institutional / operational / academic best practices, tools, techniques, and approaches.

LOOKING AHEAD TRACK

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

CAREER DEVELOPMENT TRACK

Leadership, advancement, and 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.

2020 WiCyS SCHEDULE AT A GLANCE

TIME	DESCRIPTION	LOCATION
THURSDAY		
7:00am - 7:00pm	Badge Pick-Up	See map (p.62)
9:00am - 3:30pm	Leadership Summit	Multiple Rooms
12:30pm - 1:30pm	First Timers Guide to WiCyS Conference	Cottonwood 8-9
12:30pm - 1:30pm	Recruiters Session	Cottonwood 6-7
12:30pm - 9:00pm	NCL Coaching	Spruce Lobby
2:00pm - 4:00pm	Workshop Series	Various Rooms
2:00pm - 6:30pm	Career Village Open	Adams Foyer
4:00pm - 7:00pm	Poster Session Check-In	Adams Prefunc.
4:30pm - 6:30pm	Workshop Series	Various Rooms
7:00pm - 9:00pm	Mentoring Socials	Various Rooms
7:00pm - 8:00pm	Educators Funding 1-on-1	Cottonwood 2
8:00pm - 9:00pm	SFS Meet & Greet	Cottonwood 2

TIME	DESCRIPTION	LOCATION
SATURDAY		
7:00am - 9:00am	Badge Pick-Up	See map (p.62)
7:00am - 2:00pm	Shared Interview Space	Maple 1-2
7:00am - 5:00pm	Luggage Storage available	Aurora D
7:30am - 8:30am	Breakfast for Students	Juniper Prefunc.
8:45am - 9:45am	Keynote - My WiCyS Story	Adams Ballroom
9:45am - 10:15am	Group Picture	Adams Prefunc.
10:15am - 12:00pm	NCL Coaching	Spruce Lobby
10:15am - 11:00am	Presentation Sessions	Various Rooms
10:15am - 11:00am	Affiliate MeetUp	Maple 3-5
11:15am - 12:00pm	Presentation Sessions	Various Rooms
11:15am - 12:00pm	Student Chapter MeetUp	Maple 3-5
12:00pm - 12:45pm	Panel Sessions	Various Rooms
12:45pm - 2:00pm	Lunch, Closing Remarks, and Awards	Adams Ballroom
2:30pm - 4:30pm	Workshop Series	Various Rooms

TIME	DESCRIPTION	LOCATION
FRIDAY		
7:00am - 6:00pm	Badge Pick-Up	See map (p.62)
7:00am - 8:00am	Breakfast for Students	Juniper Prefunc.
7:00am - 8:00am	Veteran Group Breakfast	Cottonwood 6-7
7:00am - 8:30am	Poster Session Check-In	Adams Foyer
7:00am - 10:00pm	Shared Interview Space	Maple 1-2
8:30am - 9:45am	Conference Opening, and Keynote	Adams Ballroom
9:45am - 11:45am	Career Fair / Village Open	Aurora Ballroom/ Adams Foyer
9:45am - 11:45am	NCL Coaching	Spruce Lobby
9:45am - 11:00am	Student Poster Session	Adams Prefunc.
10:00am - 11:00am	Allies and Advocates for Action Comm. Meetup	Cottonwood 6-7
11:00am - 11:45am	Presentation Sessions	Various Rooms
11:00am - 11:45am	Lightning Talks	Juniper A-C
11:45am - 1:45pm	Lunch and Keynote	Adams Ballroom
1:55pm - 2:40pm	Presentation Sessions	Various Rooms
1:55pm - 2:40pm	Lightning Talks	Juniper A-C
1:55pm - 5:30pm	Career Fair / Village Open	Aurora Ballroom/ Adams Foyer
1:55pm - 5:30pm	NCL Coaching	Spruce Lobby
2:40pm - 4:40pm	Workshop Series	Various Rooms
4:45pm - 5:30pm	Birds of a Feather	Various Rooms
6:00pm - 7:45pm	Dinner and Keynote	Adams Ballroom
9:00pm - Midnight	NCL Pajama Party	Spruce Lobby
9:00pm - Midnight	NCL Coaching	Spruce Lobby

PICK UP AND PURCHASE WiCyS GEAR

In Foyer by Adams Pre-Function

THURSDAY 12:00pm - 7:00pm

FRIDAY 7:00am - 6:00pm

SATURDAY 7:00am - 12:00pm

Destination: Possible

From where you are to where you want to be, there's a bridge.



Apply now at
cisco.com/go/SecureTomorrow

Learn more: **trust.cisco.com**

© 2020 Cisco and/or its affiliates. All rights reserved.



2020 WiCyS SCHEDULE

THURSDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 7:00pm	Badge Pick-Up	See map (p.60)
9:00am - 3:30pm	Industry Leadership Summit (Invite Only)	Spruce 1-2-3-4 Cottonwood 6-7
12:30pm - 1:30pm	First Timers Guide to WiCyS Conference Moderator: Sarah Kennedy, <i>HCA Healthcare</i> Panelists: Emily Brown, <i>Johns Hopkins Applied Physics Laboratory</i> , Damira Pon, <i>University at Albany - SUNY</i> and Cara Zissman, <i>Paylocity</i>	Cottonwood 8-9
12:30pm - 1:30pm	Recruiter Session - Talent Exfiltration: An Insider's Guide To The Talent Attack Lifecycle Deidre Diamond, <i>CyberSN</i> , and Brainbabe	Cottonwood 6-7
12:30pm - 9:00pm	NCL Coaching	Spruce Lobby
2:00pm - 6:30pm	Career Village Open	Adams Foyer
2:00pm - 4:00pm	Workshop Series (4 Concurrent)	
	Document Yourself: A Framework for Career Advancement Michelle Brenner, <i>ChowNow</i> and Valerie Sharp, <i>Tech By Choice</i>	Adams B
	Let's Hack-a-Thing Remi Cohen, Sara Boddy, and Malcolm Heath, <i>F5 Labs</i>	Cottonwood 8-9
	The Cyber Shuffle: Educational Card Games and Other Unplugged Activities Tania Williams, <i>University of Alabama in Huntsville</i>	Cottonwood 6-7
	Using the DETER Cybersecurity Testbed for Research and Education Jelena Mirkovic, <i>Information Sciences Institute at University of Southern California</i>	Adams C
4:00pm - 4:30pm	Break	
4:00pm - 7:00pm	Poster Session Check-In	Adams Prefunc.
4:30pm - 6:30pm	Workshop Series (4 Concurrent)	
	AWS Security Jam Lounge Hart Rossman and Ashley Smyk, <i>Amazon Web Services</i>	Adams B
	Let's Hunt! Jessica Obryan and Lauren Medica, <i>Viasat</i>	Cottonwood 8-9
	Hunting Hackers for Beginners Caitlin Hanley and Kirstie Failey, <i>Mandiant</i>	Cottonwood 6-7
	Techniques in File Forensics Maria Vicente Bonto-Kane, <i>University of Texas at San Antonio</i>	Adams C
7:00pm - 8:00pm	Educators Funding 1-on-1	Cottonwood 2
7:00pm - 9:00pm	Mentoring Socials	Juniper A-B-C, Maple 1-2-3-4-5, Spruce 1-2-3-4
8:00pm - 9:00pm	Scholarship For Service (SFS) Meet & Greet	Cottonwood 2

2020 WiCyS SCHEDULE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 6:00pm	Badge Pick-Up	See map (p.60)
7:00am - 8:00am	Breakfast Available with Tables in Foyer for Students	Juniper Prefunc.
7:00am - 8:00am	Veteran Group Breakfast The Veteran Breakfast will honor our military and veteran WiCyS members with special recognition to our inaugural Veteran Assistance Program Fellowship Award recipients. The breakfast is open to all military, veteran and special guests.	Cottonwood 6-7
7:00am - 8:30am	Poster Session Check-In	Adams Foyer
7:00am - 10:00pm	Shared Interview Space	Maple 1-2
8:30am - 9:45am	Conference Opening, and Keynote (doors open at 8:15am) Keynote Introduction: Hart Rossman, AWS Keynote: We're all in this together: Transforming Security at Cisco Sandra McLeod, Cisco Systems	Adams Ballroom
9:45am - 11:00am	Student Poster Session & Networking Break	Adams Prefunc.
9:45am - 11:45am	Career Fair and Career Village Open	Aurora Ballroom/ Adams Foyer
9:45am - 11:45am	NCL Coaching	Spruce Lobby
10:00am - 11:00am	Allies and Advocates for Action Community Meetup	Cottonwood 6-7
11:00am - 11:45am	Presentation Sessions (3 Concurrent)	
	The Often Forgotten Part of Security: Account Security & Fraud Mitigation Landscape Stephanie Olsen, Netflix	Juniper A-B-C
	Security Research at the Speed of News Diana Kelley, Microsoft	Maple 3-5
	Losing our Reality: Combating Deepfake Threats Alyssa Miller, AlyssaSec.com	Cottonwood 6-7
11:00am - 11:45am	Lightning Talks (all talks are in the same room)	Juniper A-C
	My First CTF Changed My Life: How CTFs Can Make You a Better Software Developer Melodie Moorefield-Wilson, Pendo.io	
	What's Hot? Maintaining Technical Currencies Through Podcasts Diane M Janosek, WiCyS MidAtlantic Affiliate and Elizabeth Janos, Department of Defense	
	Dwelling in the Dark Web Susan Jeziorowski, Tennessee Tech University	
	Cyberpassport: Building a Community of Cyber Talents Li-Chiou Chen, Pace University	
	Lab Blogging: Transforming Lab Instructions into Student Portfolios Rita Mitra, University of Texas at San Antonio	
	Enhancing Cybersecurity Workplace Cultures with Cognitive Diversity Tylisia Crews, Virginia Cyber Range / U.S. Cyber Range	
	Making Our Work Matter - Cybersecurity for Nonprofits, Results from the Field Kelley Misata, Sightline Security	
	Army Civilian Career Programs in Cyber Andricka Atkins, US Army, ARCYBER	

2020 WiCyS SCHEDULE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
11:45am - 1:45pm	Lunch, Networking, and Keynote (must be seated by noon to eat) Keynote Introductions: Jennifer Merriss, <i>Google</i> and Erin Kroeger, <i>State Farm</i> Keynote: Power, Influence and the Art of Female Leadership Gretchen Block, <i>Optum</i>	Adams Ballroom
1:55pm - 2:40pm	Presentation Sessions (3 Concurrent)	
	Cybersecurity, HPC and Data Science: A DoD Approach to Addressing Cyber Situational Awareness Leslie Leonard, <i>U.S. Army Engineer Research and Development Center (ERDC)</i>	Maple 3-5
	Enabling Veterans to Find Paths to Cyber Careers Moderator: Dr. Amelia Estwick, <i>National Cybersecurity Institute, Excelsior College</i> Panelists: Alice Smitley, <i>NSA</i> , Diane Delaney, <i>IBM</i> , Cynthia McLain, <i>DoL</i> , and Anna Etherton, <i>CISA, DHS</i>	Cottonwood 6-7
	Modern Security in a Quantum Computing World Jennifer Szkatulski, <i>Self</i>	Cottonwood 8-9
1:55pm - 2:40pm	Lightning Talks (all talks are in the same room)	Juniper A-C
	5G Security and Its Risk/Benefit Implications Yuning Zhang, <i>Carnegie Mellon University</i>	
	An Analysis of Data Collection by K-12 Educational Technology Katie Shuck, <i>Dakota State University</i>	
	Hacking Banks, Elections and Your Future: The National Collegiate Pentesting Competition Tom Kopchak, Heather Ricciuto, and Meredith Kasper, <i>National CPTC / Hurricane Labs & IBM</i>	
	Building the Next Generation of Cyber Leaders Margot Conrad, <i>Partnership for Public Service</i>	
	Just Because We Can Doesn't Mean We Should: Will Saying No to Apps Force Developers to Change? Kathleen Hyde, <i>Champion College Online</i>	
	Scenario-Based Cybersecurity Training Through Role-Play Molly Cooper, <i>Ferris State University</i>	
	K-12 Goes Cyber Ruthe Farmer, <i>CSforALL</i>	
1:55pm - 5:30pm	Career Fair Open	Aurora Ballroom
1:55pm - 5:30pm	Career Village Open	Adams Foyer
1:55pm - 5:30pm	NCL Coaching	Spruce Lobby

2020 WiCyS SCHEDULE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
2:40pm - 4:40pm	Workshop Series (4 Concurrent)	
	Seat at the Table: Security Leadership Through Tabletop Exercises Gina Yacone, <i>Agio</i>	Maple 3-5
	Integrating Cybersecurity Industry Certifications in Higher Education Curriculum, and Strategies for Improving Student Certification Pass Rates Laura Malave and Julia Meyer, <i>St. Petersburg College</i>	Cottonwood 8-9
	A Hacker's Mindset: How to Think and Perform Social Reconnaissance Like an Ethical Hacker/Penetration Tester Laura Puterbaugh, Genevieve Marquardt, Jennifer Rodrick, Hillary Carney, Anna Etherton, <i>Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (DHS, CISA)</i>	Cottonwood 6-7
	Understanding USA Jobs and Navigating the Federal Hiring Process Nikkia Henderson, <i>WiCyS MidAtlantic Affiliate</i>	Juniper A-B-C
4:45pm - 5:30pm	Birds of Feather (4 Concurrent)	
	Rising Leadership: A Group Discussion on How to Make a Difference and Have a Positive Impact from the Start of Your Career Kaitlyn Bestenheider and Jeana Cosenza, <i>Tevora / National Cyber League</i> , John McGill and Sophia Anderson <i>National Cyber League</i>	Juniper A-B-C
	Actually, I Was Still Speaking: Everyday Tips for Thriving in a Male-Dominated Environment Anna Skelton, <i>Bank of America</i>	Maple 3-5
	Diverse Paths for Women to Enter Cybersecurity Careers Carol Woody, <i>Software Engineering Institute</i> , Marian S. Merritt, <i>NIST NICE</i> and Kris Winkler, <i>BCG Platinion North America</i>	Cottonwood 8-9
	Underrepresented Women in Cybersecurity Laura Malave, <i>St. Petersburg College</i>	Cottonwood 6-7
6:00pm - 7:45pm	Dinner, Networking, and Keynote (must be seated by 6:15pm to eat) Keynote Introduction: Jennifer Buckner, <i>MasterCard</i> Keynote: Scaling for the Future Sid Sidhu, <i>Facebook</i>	Adams Ballroom
9:00pm - Midnight	NCL Pajama Party	Spruce Lobby
9:00pm - Midnight	NCL Coaching	Spruce Lobby



CAREER VILLAGE

Thursday, 2:00pm - 6:30pm / Friday, 9:45am - 11:45am & 1:55pm - 5:30pm
Located in Adams Foyer

Need your resume critiqued? Need a professional headshot? How about mock interviews? Come to the Career Village for all that and more including one-on-one advice from cybersecurity professionals.



Take your energy & focus to new levels with one of the world's most ambitious technology teams



You can make a difference with a leading information and technology-enabled health services business by:

- Helping people live healthier lives
- Making the health system work better for everyone
- Defining the health services market
- Serving as a health care prime innovator and enabler

150K

team members
collaborating worldwide

222M

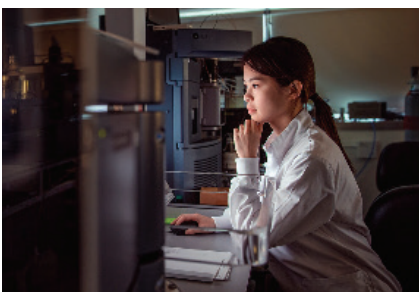
people in our consumer
database

100K+

physicians, practices and
other health care facilities
served

\$3.5B

spent annually on
technology and
innovation



Opportunities in the Technology Development Program (TDP) at Optum

The Optum TDP is a one year program with an opportunity to rotate assignments and participate in development sessions over a one year span. Getting mentorship by our senior leaders and collaborating with the smartest talent in a range of functional domains including Cyber Security, Software Engineering, Data, Architecture, Infrastructure and Operations Engineering and UX/UI

This is your opportunity to do **your life's best work.**

Apply Here: workatoptum.com/

Diversity creates a healthier atmosphere: Optum is an Equal Employment Opportunity employer and all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, age, national origin, protected veteran status, disability status, sexual orientation, gender identity or expression, marital status, genetic information, or any other characteristic protected by law. Optum is a drug-free workplace.

© 2020 Optum Health & Technology. All rights reserved

2020 WiCyS SCHEDULE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 9:00am	Badge Pick-Up	See map (p.60)
7:00am - 2:00pm	Shared Interview Space	Maple 1-2
7:00am - 5:00pm	Luggage Storage available	Aurora D
7:30am - 8:30am	Breakfast Available with Tables in Foyer for Students	Juniper Prefunc.
8:45am - 9:45am	Keynote: My WiCyS Story (doors open at 8:30am) Keynote Introduction: Barbara Mueller, Raytheon What will be your WiCyS story after attending WiCyS 2020? Come hear stories from WiCyS members just like you about how WiCyS has been a part of their career journey.	Adams Ballroom
9:45am - 10:15am	Group Picture / Break with Refreshments	Adams Prefunc.
10:15am - 12:00pm	NCL Coaching	Spruce Lobby
10:15am - 11:00am	Presentation Sessions (3 Concurrent)	
	DIY: Cybersecurity Competitions Susie Heilman and Shannon McHale, <i>The MITRE Corporation</i>	Juniper A-B-C
	A CISO's Guide to Cybersecurity Careers Lora Vaughn, <i>Simmons Bank</i>	Maple 3-5
	Catching the CAN Bus: Car Hacking on a Budget Rachel Velasco	Cottonwood 8-9
10:15am - 11:00am	Affiliate MeetUp	Cottonwood 6-7
11:15am - 12:00pm	Presentation Sessions (3 Concurrent)	
	Exploiting Your Digital Footprint Addy Moran and Vidya Murthy, <i>Raytheon</i>	Juniper A-B-C
	Securing Machine Learning Systems Charlotte Fraser, <i>Microsoft</i>	Maple 3-5
	Gotta Catch 'Em All - Bug Bounty! Chloe Messdaghi, <i>Point3 Security, WoSEC, WomenHackerz</i>	Cottonwood 8-9
11:15am - 12:00pm	Student Chapter MeetUp	Cottonwood 6-7
12:00pm - 12:45pm	Panel Sessions (4 Concurrent)	
	Women Securing the Future with TIPPSS for IoT – Trust, Identity, Privacy, Protection, Safety and Security for the Internet of Things Florence Hudson, <i>FDHint, LLC and NSF CAE at Indiana University</i> , Edna Conway, <i>Cisco</i> , and Cynthia Mares, <i>Disctrict Court Judge, Aurora, Colorado</i>	Juniper A-B-C
	Let's Navigate Together in the Maze of Cybersecurity Certifications Noureen Njoroge, <i>Cisco</i> , Malia Mason, <i>Integrum</i> , and Dr. Mona Lisa Pinkney, <i>Nike</i>	Maple 3-5
	Making Cybersecurity Operations More Efficient: Human and Machine Working Together Awalin Sopan, <i>Sophos</i> , Rekha Bachwani, <i>Netflix</i> , and Michelle Cantos, <i>FireEye</i>	Cottonwood 8-9
	Best Practices for Companies to Engage with Law Enforcement and Counsel in Response to a Cybersecurity Incident Kristy Greenberg, <i>U.S. Attorney's Office for the Southern District of New York</i> , Erin Joe, <i>The Office of the Director of National Intelligence</i> , Amy Mushahwar and Kimberly Peretti, <i>Alston and Bird LLP</i>	Cottonwood 6-7

2020 WiCyS SCHEDULE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
12:45pm - 2:00pm	Lunch, Networking, Closing Remarks, and Awards Closing Remarks: Chandra McMahon, Senior Vice President/CISO, Verizon	Adams Ballroom
2:30pm - 4:30pm	Workshop Series (4 Concurrent)	
	Social Engineering Workshop Aunshul Rege, <i>Temple University, Department of Criminal Justice</i>	Maple 3-5
	Securing the Kernel Aisha Ali-Gombe and Stacy Nicholson, <i>Towson University</i>	Cottonwood 8-9
	Learn Web Application Hacking from Industry Experts Anna Pobletts and Victoria Rosuello, <i>Praetorian</i>	Cottonwood 6-7
	Reverse Engineering for Capture the Flag Christina Johns and Christine Fossaceca, <i>MITRE</i> , and Sarah Kern, <i>CrowdStrike</i>	Juniper A-B-C



2020 WiCyS CONFERENCE PRE-CONFERENCE SESSIONS

PRE-CONFERENCE SESSIONS

Thursday • 12:30pm - 1:30pm

First Timers Guide to WiCyS Conference

Moderator: Sarah Kennedy, *HCA Healthcare*
Panelists: Emily Brown, *Johns Hopkins Applied Physics Laboratory*, Damira Pon, *University at Albany - SUNY* and Cara Zissman, *Paylocity*

Attending WiCyS conference for the first time can be both exciting and frustrating, if not done right. There is so much to do, but so little time! Join us in this session, which is designed just for you: the 1st timers. At one time, we were you. Now we have come back as professionals to share our experiences of what we found useful, what really matters and most importantly how you can get the most out of this experience as a first time WiCyS attendee.

Talent Exfiltration - An Insider's Guide To The Talent Attack Lifecycle

Deidre Diamond, *CyberSN*, and *Brainbabe*

Your talent is being attacked by cybersecurity recruiters every day. The volume and quality of these encounters will only continue to grow. What are you doing to lower the possibility of the right call at the right time? With the talent pool being short nearly 500,000 people in the United States, recruiters in cybersecurity are growing savvier in their strategy to reach your talented professional. You must assume that your superstar will take a call, or multiple calls, from a skilled cybersecurity recruiter with a great opportunity to share. You can get ahead of these recruiters and defend yourself from potential loss.

Deidre Diamond will share how skilled recruiters decide who they will target, how they perform reconnaissance and when/how exploitation and compromise happens. There is an exact moment when your talent's commitment level is compromised. Leaders who have the knowledge of these tactics can prepare and defend from these attacks on your up-and-comer. Ultimately, understanding your talent threat vector allows for your culture to perform at a high level and be enjoyable while lowering risk. How "secure" is your cybersecurity talent?



1:1 FUNDING MEETUP

EDUCATORS AND FUNDING AGENCIES

Thursday, 7:00pm - 8:00pm, Cottonwood 2

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

SFS MEETUP

SCHOLARSHIP FOR SERVICE

Thursday, 8:00pm - 9:00pm, Cottonwood 2

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.



JOB BOARD++

CYBERSECURITY EXCLUSIVE

All WiCyS members can post their resumes on the WiCyS Job Board!

Recruiters, join WiCyS as a Strategic Partner to gain year-round access to the WiCyS Job Board++.

2020 WiCyS CONFERENCE

WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

Thursday • 2:00 pm - 4:00 pm

Document Yourself: A Framework for Career Advancement

Michelle Brenner, *ChowNow* and **Valerie Sharp**, *Tech By Choice*

TRACK: CAREER DEVELOPMENT

The goal of this workshop is to document yourself the way you would document code. You wouldn't expect someone who wants to use the program you built to read every line of code. Instead, they're relying on the design documents and doc strings to know how it works. The same is true with your career. This workshop is about making it easy for you to provide overwhelming evidence of your value to the company. When you can show your return on investment, it's much easier to secure that promotion, raise or new job you deserve. This workshop consists of three parts: Writing your daily accomplishments in the form of success statements; putting them together into a brag sheet; and using them to create your elevator pitch. Using this framework makes it easy to make a habit of documenting, the same way a style guide helps you document your code. You will walk out of the workshop with confidence and a plan to take your next step.

Let's Hack-a-Thing

Remi Cohen, **Sara Boddy**, and **Malcolm Heath**, *F5 Labs*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

In "Harry Potter and the Chamber of Secrets," Mr. Weasley says, "Never trust anything that can think for itself if you can't see where it keeps its brain." This advice holds true when it comes to Internet of Things (IoT) computers. Building IoT Botnets (Thingbots) is so popular, threat actors everywhere are doing it. We'll start the workshop by talking about the IoT, how it's not just home assistants and smartwatches but also things like vulnerable home routers and IP cameras. We will explain how IoT hacking is different on these lightweight devices, and why IoT botnet building is so powerful. After the discussion, we will hack a thing. We will demonstrate a step-by-step walkthrough on how to compromise an IP camera and see its video feed as well as how to compromise a vulnerable router and gain root privileges.

The Cyber Shuffle: Educational Card Games and Other Unplugged Activities

Tania Williams, *University of Alabama in Huntsville*

TRACK: BEST PRACTICES

Come by and let us deal you in! This session features hands-on, unplugged card games to teach cybersecurity terms and concepts. CyberOne is based on the popular game UNO, where players defend their hands with patches and firewalls (instead of wild and reverse cards) while trying to rid their hands of malware. Want to deepen the player's understanding? Players can take the same deck to use as flashcards or for a game of Go Phish. Participants also can sample a game of Cyber Concentration. This game asks players to match Base 10 numerals to their Base 2 equivalent, teaching players the binary numeral system and sharpening their math skills. This session will showcase cybersecurity related board games, such as Cyber Life, and walk participants through the game creation process. Participants will learn how the games are used in camp and outreach settings and receive a link to PDF game files.

Using the DETER Cybersecurity Testbed for Research and Education

Jelena Mirkovic, *Information Sciences Institute at University of Southern California*

TRACK: BEST PRACTICES

The DETER Cybersecurity Testbed provides an advanced outlet where leading researchers and academics conduct critical cybersecurity experimentation and educational exercises. DeterLab emulates real-world complexity and scale necessary to evolve next generation solutions to help protect against sophisticated cyber attacks and network design vulnerabilities. Created under the DETER project in 2003 with joint National Science Foundation and Department of Homeland Security funding, DETERLab has grown to 700 nodes, located at USC/ISI and UC Berkeley. The testbed runs on the enhanced Emulab technology and provides infrastructure, methodologies and tools for cybersecurity experimentation. The testbed is accessible for free to any researcher or educator around the world. This workshop will introduce the DETER Testbed and provide an overview of the tools, technologies and research supported. We will describe how to get access to the testbed and steps to start using it.

2020 WiCyS CONFERENCE

WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

Thursday • 4:30 pm - 6:30 pm

AWS Security Jam Lounge

Hart Rossman and Ashley Smyk, *Amazon Web Services*

TRACK: CAREER DEVELOPMENT

As more and more organizations are moving to the cloud, they are not always having the hands-on exposure they need around security and incident response. An Amazon Web Services (AWS) Security Jam is a fun and interactive event that allows participants from your conference to learn how to use some different AWS services in real-world scenarios. AWS will provide all of the infrastructure. As WiCyS participants wait between various sessions or during meal breaks, they can work on these challenges similar to a Capture the Flag. This event can either be part of a workshop, or we can even run this event for the length of your conference. There is a leaderboard, so at the end of the Jam, we can provide prizes to the top teams and drive some friendly competition. Out of this event, participants will gain a better understanding of the security tooling available within AWS, be able to use those services per AWS best practices, and meet others who have similar interests since this is a team-based activity.

Let's Hunt!

Jessica Obryan and Lauren Medica, *Viasat*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

When you find something hinky on your network, what do you do? This workshop was developed to help you learn how to apply various methodologies to your investigative process, including digital forensics, detection and response, data science and cyber threat intelligence. We will walk you through the steps from finding what appears to be malicious activity on a network to gaining a deep understanding of what the malicious activity really means.

Hunting Hackers for Beginners

Caitlin Hanley and Kirstie Failey, *Mandiant*

TRACK: BEST PRACTICES

Have you ever started a paper and just stared at the blank screen, not knowing what to do next? Incident response investigators can sometimes feel that way when they start a new case. In this workshop, Mandiant Incident Response (IR) consultants, Kirstie Failey and Caitlin Hanley, will walk through several "based on a true story" case studies to help aspiring incident responders develop an investigative mindset and understand some of the challenges they'll face responding to large-scale, enterprise cybersecurity

breaches. This workshop is aimed at newcomers to the IR space and will provide hands-on investigative labs to help attendees hone their forensic examination skills and prepare for a cybersecurity incident.

Techniques in File Forensics

Maria Vicente Bonto-Kane, *University of Texas at San Antonio*

TRACK: BEST PRACTICES

This workshop will present techniques for doing cyber forensic analyses specifically in the area of "file forensics." Attendees will learn the truth to the adage "...do not carelessly download email attachments..." or "do not carelessly click on suspicious links..." They will be introduced to various open source tools now freely available on the internet for use by both script kiddies and cyber professionals. Attendees will be pointed to websites where they can start downloading tools and given cyber artifacts to work with. They will be shown how easy it is to embed data in files using open source tools and how it may be in the form of suspicious images, text files or even scripts that can be saved and executed at the opportune time. The second will demonstrate techniques to determine the presence of and extract embedded data or suspicious malware using open source tools. Attendees will learn easy skills to embed as well as skills for hunting and extracting suspicious data.



VETERANS BREAKFAST

TOGETHER. WE SERVE.

Friday, 7:00am - 8:00am - Cottonwood 6-7

The Veteran Breakfast will honor our military and veteran WiCyS members with special recognition to our inaugural Veteran Assistance Program Fellowship Award recipients.

The breakfast is open to all military, veteran and special guests.

2020 WiCyS CONFERENCE

WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

Friday • 2:40 pm - 4:40 pm

Seat at the Table: Security Leadership Through Tabletop Exercises

Gina Yacone, *Agio*

TRACK: BEST PRACTICES

Imagine that your organization is infected with ransomware. What do you do? From a critical breach to a minor incident, your organization's success lies in the speed of detection, effectiveness in containment and accuracy of remediation. As an IT and security professional, you are on the front line. How should you prepare?

Tabletop exercises are an effective mechanism to shape, enhance and test the awareness of decision makers while the gamification of the exercise yields a higher level of engagement of participants.

Integrating Cybersecurity Industry Certifications in Higher Education Curriculum, and Strategies for Improving Student Certification Pass Rates

Laura Malave and Julia Meyer, *St. Petersburg College*

TRACK: CAREER DEVELOPMENT

Cybersecurity industry certifications are important for validating technical skills, helping students gain entry-level positions, and helping industry professionals position themselves for the next level. By aligning academic curriculum with industry certifications, educators can demonstrate they are teaching current, relevant cybersecurity technical skills in their coursework, and prepare students for success in the industry. In this workshop, we'll discuss integrating cybersecurity industry certifications in academic courses and strategies for supporting students for test taking as well as techniques for improved pass rates.

We will share the free, open source and publisher curriculum, materials, hands-on labs and platforms available for educators to integrate into their current or new courses to align with cybersecurity industry certifications. We'll provide interactive demonstrations of academic curriculum and other interactive support activities. Workshop participants will learn strategies to increase student success rates in cybersecurity industry certifications. Many of these same strategies are applicable to working professionals seeking self study for industry certifications and career growth.

A Hacker's Mindset: How to Think and Perform Social Reconnaissance Like an Ethical Hacker/Penetration Tester

Laura Puterbaugh, Genevieve Marquardt, Jennifer Rodrick, Hillary Carney, and Anna Etherton, *Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (DHS, CISA)*

TRACK: BEST PRACTICES

Imagine a fast-forwarded movie montage of our protagonist diligently staking out a target and planning a course of action. It's not action-packed, but is the necessary precursor to enable the forthcoming fireworks. The foundation of conducting a successful hack is primarily based on preparation. This preparation phase, in the hacker methodology, is "reconnaissance." This workshop begins with a demonstration on how an ethical white-hat hacker approaches assessing a target, the logic behind his/her thoughts, and best practices behind his/her methods. Participants will take part in a hands-on lesson in which they perform reconnaissance using publicly available resources to find information on a target victim, including tips, tricks and technical commands. This exercise will be followed by a discussion on what a hacker would do with the discovered information and how it would benefit his/her penetration test/assessment. We will discuss ways users can apply the skills learned in this workshop toward following an ethical hacking career path. The workshop ends with a Q&A.

Understanding USA Jobs and Navigating the Federal Hiring Process

Nikkia Henderson, *WiCyS MidAtlantic Affiliate*

TRACK: CAREER DEVELOPMENT

The WiCyS Mid-Atlantic Affiliate will present an in-depth workshop on the federal hiring process. It will begin with an overview of the USA jobs platform followed by a live online demonstration. Participants will learn how to navigate the USA jobs platform and build their federal resume within the USA jobs resume builder. Attendees will gain detailed insights into the federal hiring process, tools to identify federal cybersecurity job opportunities, and knowledge on deciphering federal job vacancies. They also will (via a live demonstration) participate in a step-by-step session to build a federal resume.

2020 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

Saturday • 2:30 pm - 4:30 pm

Social Engineering Workshop

Aunshul Rege, *Temple University, Dept. of Criminal Justice*

TRACK: BEST PRACTICES

Social engineering (SE) is defined as any act that influences a person to take action that may or may not be in his or her best interests and is the method of using human behaviors to engage in cybercrime. SE is a technique used to conduct reconnaissance, often the first stage of a cyberattack. Cybersecurity experts agree the human factor is the weakest link in attacks, making SE a major concern. Despite the relevance of SE in cyberattacks, there is a gap in research and education/awareness, which limits the understanding of how the human factor is exploited in cyberattacks. This workshop will introduce attendees to the SE topic, tactics and persuasion techniques used, SE playbooks, and relevance to cyberattacks and cybersecurity. Attendees will engage in a safe, ethical, and fun hands-on social engineering activity in teams. The workshop will end with an interactive discussion. Participants will leave with hands-on experience in SE, an understanding and appreciation of the relevance of the human factor in cyberattacks, and free resources to use at their respective institutions.

Securing the Kernel

Aisha Ali-Gombe and Stacy Nicholson, *Towson University*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

This workshop introduces participants to security architecture in modern operating systems using Linux as a case study. Participants will learn the fundamentals of access control, which covers security kernel, local and remote authentication, object and memory protection, and security auditing. Simulating real-life scenarios, participants will gain a working knowledge of modern password authentication, password strengthening policies using PAM, establishing secure communication with SSH, and the design and implementation of the Discretionary Access Control model (DAC). The workshop will provide a practical hands-on experience with Linux shell and basic systems' commands needed to create users, passwords, access system resources and modify object permissions. Participants will gain skills in password cracking techniques and leverage some flaws in DAC to demonstrate local and remote system exploitations on Linux systems. Finally, we will look at different hardening techniques that can be utilized to improve operating system security.

Learn Web Application Hacking from Industry Experts

Anna Pobletts and Victoria Rosuello, *Praetorian*

TRACK: BEST PRACTICES

Web applications are an integral part of businesses and customers' lives today. However, many developers treat security as an afterthought. This workshop will serve as an introduction to web application security, including both attack techniques and defense mechanisms. We'll cover the basics of web application vulnerabilities and common tools used to test applications. Participants will be guided through short, fun exercises to learn how to use Burp Suite to exploit common vulnerabilities like SQL injection, command injection and authentication weaknesses. The exercises will be geared toward beginners, but also will provide advanced challenges for more experienced cybersecurity engineers. Participants will leave with an understanding of the OWASP Top 10 vulnerabilities and hands-on experience in exploiting a few of these issues. We will provide resources that attendees can use to continue learning after they leave the conference.

Reverse Engineering for Capture the Flag

Christina Johns and Christine Fossaceca, *MITRE*, and **Sarah Kern**, *CrowdStrike*

TRACK: BEST PRACTICES

Interested in expanding your Capture the Flag skillset? Capture the Flag competitions are a great resource for building skills in cybersecurity. However, reverse engineering challenges can be hard to approach as a beginner. This workshop will bootstrap attendees with the skills, tools and resources needed to get started and to continue improving. We will cover computer systems and assembly language basics needed for RE, as well as common tools used to reverse engineer Linux binaries. Attendees will reinforce the material with hands-on exercises and will be able to test their new knowledge on example challenges. Participants should have familiarity with basic Linux command line and familiarity with at least one programming language. A laptop running Debian-based Linux (e.g. Ubuntu) or a Linux virtual machine with ability to install software is required for the exercises and challenges. We will provide installers for additional tools either on a shared drive or USB.

2020 WiCyS CONFERENCE PRESENTATION SESSIONS

PRESENTATION SESSIONS

Friday • 11:00 am - 11:45 am

The Often Forgotten Part of Security: Account Security and Fraud Mitigation Landscape

Stephanie Olsen, *Netflix*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

The adversarial nature of fraudsters ensures they'll attempt to monetize in any way that provides them with a viable return on investment. This starts with taking advantage of product vulnerabilities and transitions into the capitalization of gaps in prevention and detection capabilities across the customer journey.

Stephanie Olsen will talk through the types of online fraud and abuse that occurs most often in some of the biggest products available today. She also will walk through how she's approached creating a path to a more secure experience by reviewing the three stages of defense: Prevention, Detection and Mitigation. She'll provide keys to measure success as it relates to account security and fraud mitigation.

You'll walk away with a better sense of what a security team focused on fraud and abuse does, what threats are most prevalent, and best practices for thinking through risk assessment in this space.

Security Research at the Speed of News

Diana Kelley, *Microsoft*

TRACK: CAREER DEVELOPMENT

Ever watch a news anchor present the latest vulnerability or fast-moving malware and wonder how that story went from research to headline? The behind-the-scenes reality is probably more complicated than you imagine and includes responsible disclosure activities, legal edits, peer and subject matter expert reviews, and keeping the PR/marketing machines tuned to technical truth. In this talk, we'll go over the various moving parts of the research publication process and cover the framework that we developed with our colleagues to ensure the research word got out as quickly, effectively and responsibly as possible. We will share what worked, what didn't, and deliver practical advice on how to set up the process, deal with fast and slow research cycles, manage researcher expectations, handle issues with plagiarism, work with legal reviewers, and determine the best channels for amplifying the message to keep research publication gears smooth. Learn how to build a security research publication process from those who built and managed a program at one of the largest security companies in the world.

Losing our Reality: Combating Deepfake Threats

Alyssa Miller, *AlyssaSec.com*

TRACK: LOOKING AHEAD

As a result of continuing advancements in AI, deepfake media has become increasingly convincing and easy to produce. Experts have warned of the impact this could have on elections and personal security. However, the threats that deepfakes pose to businesses and global markets are receiving less attention and therefore not as well understood. This session will analyze the deepfake threats to our social, political and business systems. Threat vectors in terms of market manipulation, insider trading, extortion and theft of intellectual property will be presented and analyzed. Psychological research into the effects of disinformation campaigns also will be leveraged to provide further context regarding the full impact of these threats. Various detection techniques will be analyzed to show their promise as well as their limitations. The latest research on possible countermeasures to help prevent deepfake creation also will be presented.

PRESENTATION SESSIONS

Friday • 1:55 pm - 2:40 pm

Cybersecurity, HPC and Data Science: A DoD Approach to Addressing Cyber Situational Awareness

Leslie Leonard, *U.S. Army Engineer Research and Development Center (ERDC)*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

The volume, velocity, variety and veracity of cyber data within the Department of Defense information networks (DODIN), specifically the department's enterprise research, development, test and evaluation (RDT&E) network, and the Defense Research and Engineering Network (DREN) present a unique opportunity to explore an unconventional, forward-focused use of high performance computing (HPC) resources in the cyberspace domain. The HPC Architecture for Cyber Situational Awareness (HACSAW) R&D program focuses on a purpose-built architecture and processing pipeline to rapidly ingest, index, assess and query various cybersecurity data sources in order to reduce barriers to real-world data in developing advanced analytics. During this talk, Dr. Leslie Leonard will share real world examples of DoD's efforts to address cybersecurity analytics utilizing HPC. She will share how the success of HACSAW will potentially transform the manner in which the department develops and rapidly transitions next-generation cybersecurity capabilities to the warfighter.

2020 WiCyS CONFERENCE PRESENTATION SESSIONS

Enabling Veterans to Find Paths to Cyber Careers

Moderator: Dr. Amelia Estwick, *National Cybersecurity Institute, Excelsior College*

Panelists: Alice Smitley, *NSA*, Diane Delaney, *IBM*, Cynthia McLain, *DoL*, and Anna Etherton, *CISA, DHS*

TRACK: CAREER DEVELOPMENT

In this panel, several public and private sector organizations will discuss opportunities and resources for veterans who are seeking career opportunities in cybersecurity.

Modern Security in a Quantum Computing World

Jennifer Szkatulski, *Self*

TRACK: LOOKING AHEAD

Join Jennifer Szkatulski as she takes you on a journey of modern security challenges as they progress through an ever-changing world where quantum computing begins to alter all that we know about computing and security. While threats of RSA security encryption failure loom, there are many opportunities that quantum computing systems provide to secure our modern computing systems that we have not yet encountered. Let's explore some examples where quantum computing will affect our current security systems and controls in both positive and negative ways so we can prepare for our uncertain future. Let's learn how we can embrace new technologies to secure our precious systems and the threats on the horizon so we can best prepare for them and create intelligent and effective responses to better protect ourselves in light of and in embracement of future advancements in technology.

PRESENTATION SESSIONS

Saturday • 10:15 am - 11:00 am

DIY: Cybersecurity Competitions

Susie Heilman and Shannon McHale, *The MITRE Corporation*

TRACK: BEST PRACTICES

Want to put your employees/club members to the test while having fun and building camaraderie? Want to put real-world pressure in a safe-to-fail environment while on two hours of sleep and 10 iced coffees? Well now you can! Susie Heilman and Shannon McHale have extensive experience running various cybersecurity competitions: CTFs, Attack/Defend and Hackerthons (that's right, HACKERthons). This presentation will cover everything needed logistically and technically to host a cybersecurity competition at your corporation or university.

A CISO's Guide to Cybersecurity Careers

Lora Vaughn, *Simmons Bank*

TRACK: CAREER DEVELOPMENT

Transitioning from a cybersecurity student to a cybersecurity professional sounds daunting, but it doesn't have to be. In her current role as Chief Information Security Officer and previous roles in cybersecurity management, Lora Vaughn McIntosh helped several recent graduates and career changers successfully make that transition. Unfortunately, it's not always easy to understand what types of cybersecurity careers exist, let alone how to land one. In this talk, she'll share her career journey, some tips on how to learn more about specific cybersecurity roles, and address common questions about cybersecurity careers in the corporate world, including: How do I get my foot in the door; what are some areas of specialization I can pursue in cybersecurity; what's the difference between a cybersecurity analyst, engineer and architect; what can I do to make myself a marketable cybersecurity professional; and how do I prepare for interviews?

Catching the CAN Bus: Car Hacking on a Budget

Rachel Velasco

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

As cars become smarter, their attack surface grows. What exactly can you (and others) do to your own car? This talk will cover core concepts in car hacking: The CAN bus and its protocols, ECUs, and how to manipulate them. Rachel Velasco also will go into recent breakthroughs in automotive security and how to start building your own research workbench.



MEMBERSHIP BENEFITS

TOGETHER. WE THRIVE.

Enjoy year-round benefits of engagement with a unique and powerful community of peers in academia, research, industry and government, sharing ideas, best practices, experiences and more with thousands of women in cybersecurity.

CONTACT: INFO@WICYS.ORG

2020 WiCyS CONFERENCE PRESENTATION SESSIONS

PRESENTATION SESSIONS

Saturday • 11:15 am - 12:00 pm

Exploiting Your Digital Footprint

Addy Moran and Vidya Murthy, *Raytheon*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

Basic reconnaissance involves tracking someone's internet presence. Everyone on the internet leaves a footprint, whether it's past websites affiliated with you, past schools you attended, social media accounts or even homes you've owned. Businesses and individuals are investing more time, money and resources into cybersecurity. Managing publicly-available information can be difficult. For an organization, it may be common to have employees register domains for different projects or have a business subsidiary and their corresponding domains. However, it also is possible to have employees use work emails for registering personal websites or having false positives such as companies with similar or nested names. Individually, social media helps keep friends and family in the loop, but also is easy for an attacker to maliciously use this information. Automation allows us an easier way to crawl the internet and see where your information lies. In this presentation, we will discuss information publicly available for both businesses and individuals as well as how an attacker could exploit this information.

Securing Machine Learning Systems

Charlotte Fraser, *Microsoft*

TRACK: LOOKING AHEAD

Machine learning and AI technologies are rapidly becoming part of our daily lives with amazing potential to transform how we live and work. They also open up a different world of new types of security and privacy vulnerabilities, exploits and mitigations. In this presentation, we'll explore this new world from the point of view of the Microsoft Security Response Center, the central security operations team at Microsoft. We'll explore some of the major classes of machine learning vulnerabilities, how attackers may seek to exploit them, and how Microsoft works to defend against them to keep our customers safe. We'll also talk about how we work with the security researcher community to help protect the ecosystem. Whether you are doing security research into machine learning, or seeking to secure it, we hope to see you there!

Gotta Catch 'Em All - Bug Bounty!

Chloe Messdaghi, *Point3 Security, WoSEC, WomenHackerz*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

Bug bounty has been a long-time craze and become a necessity to keeping organizations safe by crowdsourcing their security. As the demand increases, the supply needs to increase as well. However, getting into the bug bounty space can be tricky and hard to start. This talk approaches the history of bug bounty, the current legal landscape, and the next steps for bug hunting, including how to get started and which tools to use.



AFFILIATE MEETUP

TOGETHER. WE SOAR.

Saturday, 10:15am - 11:00am - Cottonwood 6-7

Come meet affiliate leaders, exchange ideas, best practices, and learn how you can get involved or start your local WiCyS affiliate!

WiCyS STUDENT CHAPTER MEETUP

TOGETHER. WE ACHIEVE.

Saturday, 11:15am - 12:00pm - Cottonwood 6-7

Join us to learn about starting, running, and maintaining the student chapter on your campus. The current chapter Presidents will share their experiences, talk about challenges, and address many issues that commonly arise when being an officer of a student chapter. It's going to be a freestyle session so bring lots of questions with you and let's help each other to succeed in promoting women in cybersecurity on YOUR campus.

2020 WiCyS CONFERENCE

BIRDS OF A FEATHER (BoaF)

BIRDS OF A FEATHER

Friday • 4:45 pm - 5:30 pm

Rising Leadership: A Group Discussion on How to Make a Difference and Have a Positive Impact from the Start of Your Career

Kaitlyn Bestenheider and Jeana Cosenza, *Tevora / National Cyber League*, John McGill and Sophia Anderson *National Cyber League*

TRACK: CAREER DEVELOPMENT

When you first start out in any new career path, it's hard to imagine having a meaningful impact especially in an industry as vast and ever-changing as information security. At the 2019 WiCyS, Kaitlyn Bestenheider received the Rising Leadership Award. After a year of reflection, Kaitlyn and her team of NCL Player Ambassadors realized it does not take an innate talent or gift to make a difference. There are specific, actionable goals every individual can implement at any point in their career regardless of experience level or power within an organization. This will be an open dialogue led by the NCL Player Ambassadors, who will share insights they have discovered and gather the insight of others with a focus on helping entry-level individuals find their voice and positively impact the industry. Topics include: What makes a good leader; what characteristics make you look up to someone; what are the biggest obstacles you find in having your voice heard; how do you want to have a lasting impact on the industry.

Actually, I Was Still Speaking: Everyday Tips for Thriving in a Male-Dominated Environment

Anna Skelton, *Bank of America*

TRACK: CAREER DEVELOPMENT

Look, we all know being a woman in a male-dominated field is not easy. There can be condescension, sneers, inappropriate comments, gaslighting, and a thousand other experiences that make you wonder if doing what you love is truly worth it. Anna Skelton spent most of her life in highly male-dominated environments. Now, she wants to share what she's learned about how to thrive, including how to stand up for yourself, grow your confidence, and show those around you that you've earned your seat at the table, thank you very much. Beyond that, we'll build an audience-led discussion on strategies to make male-dominated workplaces more comfortable for women and non-binary people with the goal of creating an environment that embodies true inclusiveness.

Diverse Paths for Women to Enter Cybersecurity Careers

Carol Woody, *Software Engineering Institute*, Marian S. Merritt, *NIST NICE* and Kris Winkler, *BCG Platinion North America*

TRACK: CAREER DEVELOPMENT

The goal for cybersecurity is protection against criminals and unauthorized use of electronic data or the measures taken to achieve this. However, this does not describe the many avenues for women within technology where cybersecurity expertise is needed. Technology decisions that directly impact an organization's ability to address cybersecurity are made at many levels. Since technology is integral to all domains, including government, defense and finance, the opportunities for addressing cybersecurity are diverse and interesting. Four women in this panel will share their background, expertise and information that helped them achieve important roles in cybersecurity. They will start with an overview of the various cybersecurity roles open to women established in or just entering the workforce, as well as consider questions related to the importance of women joining the field and the value gained from a cybersecurity career. They also will make suggestions for preparing for these roles. At the end, they will solicit questions from attendees to ensure all areas of interest are addressed.

Underrepresented Women in Cybersecurity

Laura Malave, *St. Petersburg College*

TRACK: BEST PRACTICES

This Birds-of-a-Feather session will discuss the status of underrepresented women in cybersecurity: Those self-identifying as black/African American, Hispanic/Latina, Native American, Native Hawaiian, Pacific Islander and Asian. They face many challenges in the workplace, including lack of representation in management roles, salary gap and conscious and unconscious discrimination. We will brainstorm and discuss how to increase, recruit, promote and nurture the number of underrepresented women pursuing academic degrees and cybersecurity careers. We also will discuss best practices and challenges in retaining underrepresented women in academic degree programs and careers as well as available resources for supporting underrepresented women in cybersecurity.

2020 WiCyS CONFERENCE

PANEL SESSIONS

PANEL SESSIONS

Saturday • 12:00 pm - 12:45 pm

Women Securing the Future with TIPPSS for IoT

Florence Hudson, *FDHint, LLC and NSF CAE at Indiana University*, **Edna Conway**, *Cisco*, and **Cynthia Mares**, *District Court Judge, Aurora, Colorado*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

Our increasingly connected world creates great opportunities for increased collaboration and data sharing, leveraging the Internet of Things (IoT) to enable connected systems to improve the human experience and business outcomes. From supply chain efficiency to connected healthcare and smart connected communities, the opportunities are endless. So are the risks. We all use IoT devices, but are they safe? Engineers and computer scientists are designing, developing and manufacturing IoT systems. How do we enable Trust, Identity, Privacy, Protection, Safety, Security (TIPPSS) for IoT systems? What are the implications of the IoT related to privacy, security and each individual's civil rights? This panel of women engineers, scientists, lawyers and a judge representing industry, government, research and academia will share their perspectives and debate how ready we are to deliver TIPPSS for the IoT, the opportunities and risks, and how we all can be part of the solution. They will share the privacy, policy, technology and standards implications and efforts underway regarding TIPPSS for IoT. The panel participants are coauthors of the book "Women Securing the Future with TIPPSS for IoT."

Let's Navigate Together in the Maze of Cybersecurity Certifications

Noureen Njoroge, *Cisco*, **Malia Mason**, *Integrum*, **Dr. Mona Lisa Pinkney**, *Nike*

TRACK: LOOKING AHEAD

As cybersecurity is ever growing, the need for qualified professionals gets wider. Every role requires a special skillset and approved certifications. As the panelists, we will share our security journey and detail which certifications we found most useful to our careers. Many times, people take many certifications, pay so much money for them and yet are unemployed. We want to put a halt to this result and provide the audience with better guidance. By the end of the panel discussion, we aim to: Enlighten the audience on best certification processes, learn how to find free certification training and save money, understand how to best use certifications, and share top certifications that are heavily sought after by major corporations. We believe in thriving together and

sharing our own personal journey to help us connect with the audience and close the confusion gap of certification achievements.

Making Cybersecurity Operations More Efficient: Human and Machine Working Together

Awalin Sopan, *Sophos*, **Rekha Bachwani**, *Netflix*, and **Michelle Cantos**, *FireEye*

TRACK: BEST PRACTICES

Many organizations run a Security Operations Center (SOC) or subscribe to an external security service to keep their data safe. In addition, security analysts in the SOC assess vast amounts of data from multiple sources using various tools. However, there is too much data and too little time. The panelists will describe how they have used machine-learning techniques to accelerate the process of handling cybersecurity events for faster results.

Best Practices for Companies to Engage with Law Enforcement and Counsel in Response to a Cybersecurity Incident

Kristy Greenberg, *U.S. Attorney's Office for the Southern District of New York*, **Erin Joe**, *The Office of the Director of National Intelligence*, **Amy Mushahwar** and **Kimberly Peretti**, *Alston and Bird LLP*

TRACK: BEST PRACTICES

Information security professionals may be responsible for incident prevention, detection and escalation on a day-to-day basis. But when a significant cybersecurity incident occurs, other stakeholders need to get involved, fast. This panel will explore effective strategies for engaging with federal law enforcement and counsel in responding to a cybersecurity incident. They will explore the changing nature of the cyber national security threat to the private sector as well as how and when to engage with law enforcement and counsel. Panelists will address the common misconceptions that company insiders may have when dealing with law enforcement and prosecutors in cybercrime investigations. They also will review the role of counsel in managing privilege and evidence preservation, as well as the company's communication with law enforcement, regulators, investors and customers. The panelists and moderator are four women who have significant cyber experience and bring different perspectives to working with information security personnel in a cyber-crisis.

2020 WiCyS CONFERENCE

LIGHTNING TALKS

LIGHTNING TALKS

Friday • 11:00 am - 11:45 am

My First CTF Changed My Life - How CTFs Can Make You a Better Software Developer

Melodie Moorefield-Wilson, *Pendo.io*

TRACK: CAREER DEVELOPMENT

As a software developer, Melodie Moorefield-Wilson was familiar with writing good code, or so she thought. She repeatedly heard about security vulnerabilities that occurred because of issues with a developer's code base. But how did security researchers manage to find these vulnerabilities? In her talk, Melodie will discuss how she started to learn about Capture the Flag (CTF) competitions, how reluctant she was to get involved and how she overcame that reluctance. She also will discuss how her first CTF completely changed her perspective on software development, and how anyone can get involved in making software more secure and safe. She will provide step-by-step guidelines for beginners to get started and give resources for individuals who want to get started in these competitions. It can be intimidating at first, but anyone can learn if they have the desire. Let's explore CTFs together!

What's Hot? Maintaining Technical Currencies Through Podcasts

Diane M Janosek, *WiCyS MidAtlantic Affiliate* and **Elizabeth Janos**, *Department of Defense*

TRACK: BEST PRACTICES

Women always need an edge, especially in cybersecurity. To maintain technical credentials and currency as a cybersecurity leader, certain podcasts are a must! This lightning talk will highlight the best technical and industry trends, national policy changes and leadership podcasts. Also included will be newer resources on tying together data science, AI and cyber. This five-minute talk will help put you on the path to fluidity in cyber lingo and show you the go-to places to hear the latest trends and developments! The co-presenters are at different stages in their professional journey and will offer different perspectives. Elizabeth Janos is an upcoming graduate student also working with DoD while striving to grow her technical competencies. Diane Janosek uses these resources to sustain and remain current on emerging trends. The audience can relate to this dynamic duo, who always love to have fun together in the workplace while achieving excellence!

Dwelling in the Dark Web

Susan Jeziorowski, *Tennessee Tech University*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

Anonymity tools have grown increasingly popular among web users in response to regular government surveillance, internet censorship and capitalistic data collection, among other reasons. Such tools promote web user privacy but also provide an avenue for cyber criminals to conduct illegal activities on the dark web without fear of consequences. In this presentation, attendees will discover what the dark web is, how it's accessed, and what it's used for. Attendees will learn about the criminal activity enabled by the dark web and the challenges cyber investigators face when dealing with anonymous networks. The presentation will conclude with a discussion of current dark web research, resources and best practices.

Cyberpassport: Building a Community of Cyber Talents

Li-Chiou Chen, *Pace University*

TRACK: CAREER DEVELOPMENT

Connecting with cybersecurity professionals and learning from them are important steps in building a cyber career. To facilitate this process, we developed a system called Cyberpassport, which integrates students' academic and career goals with cybersecurity co-curricular activities. This system is designed for students to search and register for cybersecurity activities, track their own progress, support advisors in their mentoring efforts, and facilitate activity hosts to connect with interested students. This will allow students to generate a resume using information captured in the systems, including activities labeled with skills defined in the National Initiative for Cybersecurity Education (NICE) cybersecurity workforce framework. Cyberpassport enables students to connect with professional development training or co-curricular activities. The system aims to integrate students' career goals with cybersecurity training sessions and connect via these sessions. Cyberpassport will be scalable and can accommodate a diverse range of cybersecurity activities offered.

2020 WiCyS CONFERENCE

LIGHTNING TALKS

Lab Blogging: Transforming Lab Instructions into Student Portfolios

Rita Mitra, *University of Texas at San Antonio*

TRACK: BEST PRACTICES

In this session, we will discuss how to address two issues in cybersecurity lab-based education: How can instructors maintain up-to-date documentation on tools, commands and event analysis? How can students learn the art of documentation and report writing? The nature of cybersecurity is one of constant updates. The typical approach is to search the internet for a blog or forum where the issue has been raised and try proposed solutions until one works, and then move on. We run into this dilemma in undergraduate education. Instructors want to create current and relevant labs for students to hone their analytical skills but avoid reinventing the wheel by linking to documentation online. Students frequently need to troubleshoot outdated assignment instructions and may not describe the issues in lab reports. We found that when students are asked to follow a set of lab instructions and detail and reflect on their process in an introspective manner, they often report in depth on issues they encountered. We asked students to write up a walk-through of our lab instructions in the style of a well-crafted blog or forum post. "Lab blogging" appears to result in better course quality and improved writing and analytical skills.

Enhancing Cybersecurity Workplace Cultures with Cognitive Diversity

Tylisia Crews, *Virginia Cyber Range / U.S. Cyber Range*

TRACK: BEST PRACTICES

The significance of a diverse work team has remained unchanged. However, the scope of what diversity truly encompasses has shifted. Traditionally, building a team of hard-working employees with differences in gender, culture, race, creed, religion, sexual orientation and political beliefs was a major goal. Recent studies of diversity challenged what was traditionally considered "diverse." These discoveries led to a new term, cognitive diversity, which represents the inclusion of people with different ways of thinking, viewpoints and skillsets in a team. Cognitive diversity cultivates a more inclusive and collaborative open space, where people feel empowered to create and implement ideas. The power of having this in the workplace is the same power that companies seek in future leaders. The findings of cognitive diversity research will provide endless opportunities to form strategic approaches to hiring practices in cybersecurity. Exploring this will show how expanding the traditional perspective of diversity includes variances in

perspectives, knowledge bases and opinions to help solve difficult problems.

Making Our Work Matter - Cybersecurity for Nonprofits, Results from the Field

Kelley Misata, *Sightline Security*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

In 2018, Americans gave \$427.71 billion to nonprofit organizations. You, like many WiCyS attendees, may have given time, energy or money to your favorite nonprofit, never giving a second thought to their security preparedness. Our best intentions of bringing cybersecurity superpowers to nonprofits are often met with open arms. However, the reality is that many nonprofits have no idea what they need, and we, as the experts, jump in with solutions we think they need. Join this talk to hear about Dr. Kelley Misata and her new nonprofit start-up, Sightline Security. Missioned to help nonprofits navigate comprehensive cybersecurity with confidence, Dr. Misata will present results from a recent pilot in which her team worked side-by-side with nonprofit organizations. She will illustrate how bringing a business-centric approach using everyday language to nonprofits drives them to improve cybersecurity through improved awareness AND also gives them a seat at the table to own their own security efforts. Attendees will walk away with an understanding of how to use their security capabilities to provide beneficial and measurable progress to their favorite nonprofits.

Army Civilian Career Programs in Cyber

Andricka Atkins, *US Army, ARCYBER*

TRACK: CAREER DEVELOPMENT

The Army is dedicated to the training, education and professional development of its cyber workforce. Army Career Programs for Information Technology and CP 71 exist to raise awareness, encourage and develop the cyber expertise among the Army cyber civilian workforce. This talk will address such opportunities for civilians.

2020 WiCyS CONFERENCE

LIGHTNING TALKS

LIGHTNING TALKS

Friday • 1:55 pm - 2:40 pm

5G Security and Its Risk/Benefit Implications

Yuning Zhang, *Carnegie Mellon University*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

5G is not just a new cellular network system. It also facilitates peer-to-peer communication among Internet of Things (IoT) devices. But the transition from 4G to 5G will be more complicated than just faster cellphones. Parts of the 5G spectrum are not managed by cellular companies but meant for direct device-to-device ad hoc usage. It's only as secure as the devices themselves. As more organizations look for ways to integrate 5G technologies into their business operations, the need for a risk/benefit assessment against this adoption is necessary. The "Race to 5G" competition between the U.S. and China adds another dimension of information security concerns. This could pose serious concerns to the U.S. government and corporate organizations when they consider adopting Chinese technologies. Yuning Zhang's research aims to research these topics and give organizations a framework for evaluating the adoption of 5G technologies. The analysis framework has no predetermined answers, rather, it aims to list relevant benefits and associated risks using the OCTAVE format for individual organizations.

An Analysis of Data Collection by K-12 Educational Technology

Katie Shuck, *Dakota State University*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

The use of technological devices, software and applications has increased dramatically in recent years, especially in the K-12 classroom. Integrated technology has proven to be an effective and engaging tool for multidisciplinary learning environments. Yet, the data being collected through these technology resources is often excessive, potentially violating current laws and disregarding students' rights to reasonable privacy. Katie Shuck's research project analyzes the Terms of Service and privacy policies of technology resources used in these classrooms in order to quantify and classify data being collected. By understanding the data collected through these resources, we can work to improve privacy best practices and educational technology so it protects student data.

Hacking Banks, Elections and Your Future: The National Collegiate Pentesting Competition

Tom Kopchak, Heather Ricciuto, and Meredith Kasper,
National CPTC / Hurricane Labs & IBM

TRACK: CAREER DEVELOPMENT

Do you think you might want to be a pentester some day? Consider participating in the National Collegiate Penetration Testing Competition (CPTC). The CPTC provides college students (like you!) with realistic challenges to prepare for a career in the security assessment field. The competition is designed to mimic a real-world organization while requiring you to excel in both technical and communication skills. We provide a unique environment to prepare you to navigate the technical and administrative challenges you will likely face in your career. CPTC gives you the opportunity to hone on-demand technical and non-technical skills in a realistic environment before you enter the workforce. This talk will introduce you to the CPTC competition director (Tom Kopchak), a former competitor turned volunteer (Meredith Kasper), and one of our industry supporters (Heather Ricciuto), all of whom work together to make this competition happen.

Building the Next Generation of Cyber Leaders

Margot Conrad, *Partnership for Public Service*

TRACK: CAREER DEVELOPMENT

The nonpartisan, nonprofit Partnership for Public Service has teamed up with Mastercard, Microsoft, Workday and 12 federal agencies to launch the Cybersecurity Talent Initiative, a unique cross-sector opportunity for students in cyber-related fields, including computer science, engineering, information science and mathematics. Students will have a chance to work in the federal government for two years and then be invited to apply for a position with one of the corporate partners. In this session, we hope to inspire more young women to continue pursuing cybersecurity-related fields and educate them about the innovative opportunities in the public and private sectors they would be eligible for through this program. Participants will learn about the innovative work the federal government is doing to protect the systems and citizens of the United States. Our distinguished speakers will provide feedback regarding career paths, ways to success and networking advice.

2020 WiCyS CONFERENCE

LIGHTNING TALKS

Just Because We Can Doesn't Mean We Should: Will Saying No to Apps Force Developers to Change?

Kathleen Hyde, *Champion College Online*

TRACK: BEST PRACTICES

Are you the type of person who reads license agreements before clicking the "Accept" button? Do you regularly check the permissions on the apps that you download, install and use? If more consumers opted not to use popular Android apps where developers request unnecessary access to device features and data, would that change the industry and how it views data as a commodity? Should the distinction be whether an app is free or paid? Let's have a conversation about how consumers can effect change and whether all data should be monetized.

Scenario-Based Cybersecurity Training Through Role-Play

Molly Cooper, *Ferris State University*

TRACK: BEST PRACTICES

Cyber attacks are becoming more prevalent. Data, information and other assets can be lost as a result of a cyber attack. Increased sophistication and complexity can add difficulty in defending, recognizing and responding against such attacks. A critical line of defense is well-trained cybersecurity professionals. Development and validation of cybersecurity skills as well as testing cybersecurity preparedness at all levels of an organization is needed before an actual event occurs. Rehearsing cybersecurity situations before they occur could prove beneficial for the decision-making process. Current and future cybersecurity students and professionals need to be prepared and continuously evaluated toward preparedness for cyber defense and response. This research investigates the effects of improving the cybersecurity preparedness gap by using realistic scenario-based role-playing games and tasks to train cybersecurity students on cyber incidents, readiness and response. Results indicated that by rehearsing realistic cybersecurity attacks and situations, students were more involved with class activities, felt more prepared for these situations and improved cybersecurity exam scores in the classroom.

K-12 Goes Cyber

Ruthe Farmer, *CSforALL*

TRACK: BEST PRACTICES

This talk will provide a snapshot of the current state of cybersecurity education for K-12 youth, with a specific lens on opportunities for girls and young women and highlight high-impact programs and opportunities for students, faculty and professionals to support and engage.



WiCyS COMMUNITIES

Visit the WiCyS Communities and join the growing networks of like-minded individuals within WiCyS. Each table has a unique giveaway that you won't want to miss!

Ally/Advocate for Action Community
Together. We Include.

Affiliate Community
Together. We Soar.

Mentor/Mentee Community
Together. We Expand.

Speakers Community
Together. We are the Voice.

Student Chapter Community
Together. We Achieve.

Veterans Community
Together. We Serve.

2020 WiCyS CONFERENCE

STUDENT POSTERS

STUDENT POSTERS

Friday • 9:45 am - 11:00 am

1. Process Oriented Guided Inquiry Learning for Flooding Attacks to the SDN Data Plane

Hanan Alshafer and Yuan Xiaohong, *North Carolina A&T State University*

Software-Defined Networking (SDN) is a new network platform that has a centralized control architecture, which is a suitable environment for attacks such as Distributed Denial-of-Service (DDoS) (i.e., flooding attack), one of the most common threats on network security. This poster describes the in-progress project developing activities for flooding attack to the SDN Data Plane by using Process Oriented Guided Inquiry Learning (POGIL) methodology. POGIL is a student-centered instructional technique that provides activities in the classroom. They are designed to guide students through questions to formulate patterns and relationships toward concept exploration. In the end, students will learn by their own exploration rather than through the instructor. This technique emphasizes the development of process skills such as critical thinking, information processing, teamwork, assessment and problem solving. By introducing a cybersecurity topic such as flooding attacks to the SDN Data Plane, students will deeply understand how and why it happens, be encouraged to think how to create a defense framework, and develop their problem-solving abilities.

Flooding attack to the SDN Data Plane will be covered by introducing the flooding attack to the SDN data plane, examining how this flooding attack happens, and understanding how to prevent the attack. The learning objectives include describing the packet processing in OpenFlow switch and OpenFlow controller as well as identifying table-miss cases; distinguishing how the controller installs dynamic and static (proactive and reactive) flow rules in the switch flow table; demonstrating how the DOS attack on data-plane works and describing the observed consequence; defining DOS attack and amplified attack, and relating amplified attack and DOS attack; and discussing how to prevent the flooding attack to the SDN data plane. In this poster, we will review relevant background on POGIL and effective learning techniques, describe the structure and content of POGIL activity for flooding attacks to the SDN data plane and how we design it. In order to evaluate the effectiveness of these activities, we will create a pre and post survey to get participants' feedback.

2. The EGRBAC Model for Smart Home IoT Access Control

Safwa Ameer, James Benson and Ravi Sandhu, *The University of Texas at San Antonio*

Recently, the concept of Internet of Things (IoT) has gained tremendous attention in both research and industry. In the near future, IoT will affect all industries and the average consumer's daily life. In particular, it will be part of every home, turning them into smart houses where multiple users have complex social relationships using the same smart devices. This requires usable authentication and sophisticated access control specification mechanisms that are currently lacking. In this poster, we introduce the extended generalized role-based access control (EGRBAC) model for smart home IoT. EGRBAC is a dynamic and fine-grained model suitable for a constrained home environment. We provide a formal definition of the model and illustrate its features through several case scenarios. We also provide an analysis of the beneficial attributes of EGRBAC as well as its limitations. Finally, we demonstrate a proof-of-concept implementation for a consolidated use case in Amazon Web Services (AWS) IoT platform followed by a discussion of future enhancements. We envisage EGRBAC as the first step in developing a family of access control models for smart home IoT ranging from relatively simple and complete to incorporating increasingly sophisticated and comprehensive features.

3. Examining the Security and Privacy Needs of Political Activists

Michelle Aninye, Marshini Chetty and Blase Ur, *University of Chicago*

The government surveillance of political activists, both actual and perceived, has been a concern for many years. However, concern and efforts to resist surveillance have grown significantly following the Snowden leaks in 2013. Most recently, the FBI identified several activist organizations and movements as threats to national security therefore requiring surveillance. These government documents inspired previous research led by the implications of extensive monitoring. Researchers found that extensive surveillance negatively impacts the political engagement of citizens, making it important to understand how political activists use technology to improve their technology-based communication with privacy-preserving measures. In this work, we study digital communication amongst political activists using a security and privacy perspective. Through 20 semi-structured interviews with current and former supporters of Black Lives Matter, we explore the role technology plays in political activist communication as well as related

2020 WiCyS CONFERENCE

STUDENT POSTERS

security and privacy concerns and mitigations. Our results highlight unique challenges that political activists must balance, including sharing sensitive information on a large scale while attempting to establish trust and credibility between potential recipients on an individual level. We conclude this study with concrete recommendations to address the security and privacy needs of political activists with recommendations for improving existing technologies, suggestions for developing new tools, and proposals for applying our findings to other organizations in other situations.

4. Intrusion in Wireless Networks Detection Using Machine Learning

Shilpa Bhandari, *Youngstown State University*

As our lives get more and more digital with increasing reliance on wireless networks, intrusion detection systems need to be more powerful to spot unauthorized access. With the current data sets we have, we can train machine-learning models to detect intrusions in wireless networks. These models are built on a set of training data and can identify any future anomalies in the network. Detecting intrusion using machine learning is a difficult problem to solve because the amount of data on intrusions is much smaller relative to normal network transfers. We test which machine learning model can best detect these intrusions. In this project, XGboost, Catboost, LightGBM and Random Forest machine learning models are trained based on the Aegean Wi-Fi Intrusion Dataset (AWID), publicly available data with records of wireless network features during intrusion and normal processing. By passing test data to these learning models, we test them for accuracy, precision, recall and time of execution. Using SHapley Additive exPlanations, we explore which features of AWID best contribute to detect intrusions in a wireless network.

5. Reverse-Engineering Payment Card Skimmer Firmware

Smitha Bhaskar and Nolen Scaife, *University of Colorado Boulder*

Payment card fraud is a multi-billion dollar problem perpetuated in part by card skimmers. These skimmers are devices that make a copy of the sensitive data present in a card's magnetic strip. While the community has a high-level understanding of the devices, no research to date has been able to make confiscated skimmers work in captivity; this prevents the creation of a testing apparatus for future work on skimmer detection. In order to evaluate why we are unable to activate and use real skimmers, we have been studying the existing firmware. Through a combination of firmware-level attacks and

reverse engineering of real skimmers confiscated by law enforcement, we are developing a better understanding of the skimmers' functionality. Such work will aid future research in detection through overcoming existing roadblocks in developing skimmer-testing hardware.

6. How our Smart-Home Device Attacks Give Away our Secrets?

Sai Himabindu Boddupalli, Shivakant Mishra and Mohammed Al-Mutawa, *University of Colorado Boulder*

We continue to embrace technology by increasingly depending on it for survival by furnishing our homes or workplaces with devices that track every second of our lives. It could be a Fitbit watch that tracks our pulse and heartbeat, or a smart assistant like Amazon Echo that responds to queries and adds items to our Amazon shopping cart. The range of functions performed by these devices could be as trivial as fetching the temperature outside or monitoring the movements of a baby in a cradle. Given the sensitive information that these devices capture, they are very vulnerable to side-channel attacks. This compromises information, which if taken advantage of, could be life threatening. Our research presents a step toward exploring if a correlation exists between what is seen through a security camera and network traffic, a side channel. Assuming the attacker accesses the router's network, (s)he can discover a wealth of information by analyzing the devices connected to it. Since the usage of indoor security cameras is increasing and the data generated by this device is sensitive, we decided to experiment. Using Wireshark and Netgear Arlo Pro security camera, we discovered that an attacker connected to the same network as the security camera can easily figure out the presence of members in a home, thus exposing a major security loophole in a device designed for security. It does not end there! We also duplicated it on a Google Home Mini device and discovered how giving it commands can expose the person using it.

7. A Hardware Evaluation of a NIST Lightweight Cryptography Candidate

Flora Coleman, *Virginia Tech*

As the Internet of Things (IoT) continues to grow and expand, the security challenges associated with supporting it are being increasingly evaluated. Many IoT applications are small, portable devices that do not have extensive resources allocated for security purposes. Even if designers make a concerted effort to implement security protocols, most of the standard cryptographic algorithms in use today, e.g., Advanced Encryption Standard (AES) or Digital Encryption Standard (DES),

2020 WiCyS CONFERENCE

STUDENT POSTERS

require significant resources and overhead. Therefore, it is usually impractical for IoT devices with limited resources to support these algorithms. Even cryptographic implementations that are mathematically sound can still leak sensitive information through side-channel attacks, where an observer is able to monitor power, radiation, or other tell-tale signs of the device during operation.

Lightweight cryptographic protocols could be more easily supported by IoT applications in the future. The National Institute of Standards and Technology (NIST) Lightweight Cryptography Standardization Process, which began in 2018 and is expected to conclude in 2021, aims to identify strong, lightweight cryptographic algorithms and include them in future U.S. federal standards. This work provides an overview of one of the candidates in the NIST competition – Schwaemm and Esch (SPARKLE). SPARKLE's specification and source code has been adapted into a register transfer level (RTL) implementation using very high speed integrated circuit hardware description language and is suitable for Field Programmable Gate Arrays (FPGA). The implementation is compatible with a prototype standard called the Hardware API for Lightweight Cryptography, which ensures realistic input-output utility and fair benchmarking against hardware implementations from other candidates. The RTL adaptation of this candidate's algorithms include an authenticated encryption with associated data scheme as well as a hashing mechanism. This work analyzes the performance achieved (e.g., maximum frequency, throughput and power) versus resources required (e.g., number of FPGA look-up tables or slices, energy) for the SPARKLE candidate, and the additional cost of achieving an implementation of SPARKLE protected against side-channel attacks.

8. Learner's Dilemma: IoT Device Training Strategies in Collaborative Deep Learning

Deepti Gupta and Ali Sanam Tosun, *University of Texas San Antonio*; **Smriti Bhatt**, *Texas A&M University-San Antonio*

In recent years, the Internet of Things (IoT) is growing rapidly and billions more devices are expected to grow. These devices generate a tremendous amount of data from health information to social networking. The IoT Artificial Intelligence (IoTAI) systems use this data to improve the intelligence of many applications. In IoTAI, the deep-learning model is often related to size of training data set. Under a reasonable learning mechanism, if there is more training data, the model will be more effective. According to HIPPA rule, all healthcare technology, especially IoT devices, are not allowed to give their data

for training. In order to solve these problems, the current trend is to apply collaborative approaches to deep learning, which keeps data on the device and shares only parameters.

Collaborative Deep Learning (CDL) allows multiple IoT devices to train their models without showing their personal data. During the training time, local gradients of each device upload to a Parameter Server (PS), which performs secure aggregation and sends updated parameters to each device. Plenty of recent research has been done to address communication challenges and privacy issues of federated deep learning. However, one significant research gap is a lack of understanding strategic behavior of rational IoT devices within CDL in shared local gradient protocols. Such understanding is critical for designing appropriate parameters that will foster cooperation within CDL and prevent attacks.

We address this research gap by analyzing the behavior of IoT devices using a game-theoretic model, where each device aims at training a model at a minimum cost of participating in the protocol. We first analyze the Nash equilibria in an N player static game model. To overcome this problem, we propose a novel cluster-based representation to approximately solve games of sharing mechanism to promote cooperation among IoT devices.

9. Map My Murder! A Digital Forensic Study of Mobile Health and Fitness Applications

Courtney Hassenfeldt, Ibrahim Baggili, and Shabana Baig, *University of New Haven*; **Xiaolu Zhang**, *University of Texas at San Antonio*

The ongoing popularity of health and fitness applications catalyzes the need for exploring forensic artifacts they produce. Sensitive Personal Identifiable Information (PII) is requested by applications during account creation. Augmenting that with ongoing user activities, such as the user's walking paths, could potentially create exculpatory or inculpatory digital evidence. We conducted extensive manual analysis and explored forensic artifacts produced by (n = 13) popular Android mobile health and fitness applications. We also developed and implemented a tool that aided in the timely acquisition and identification of artifacts from said applications. Additionally, our work explored the type of data that may be collected from health and fitness web platforms and web scraping mechanisms for data aggregation. The results clearly show that numerous artifacts may be recoverable and that the tested web platforms pose serious privacy threats.

2020 WiCyS CONFERENCE

STUDENT POSTERS

10. Rogue Device Threats and Response

Katrina Herweg, *California State University, East Bay*

Rogue Device Threats and Response is a poster that describes our work for identifying rogue wireless devices in an enterprise network. We discuss the variety of threats posed and provide guidelines for necessary components for a team to locate and contain rogue devices based on our experiments. We'll show detection strategies through our Wireless Intrusion Detection System, appropriate tools for locating devices and mitigation techniques while still acknowledging the balance between security and usability. With our results, the Security Operation Center is now able to utilize the mapping tools for visual location as well as alerts for physical response. Continuous monitoring efforts allows greater visibility into the wireless network and is seen as a valuable tool to those responding to rogue devices. Automatically generated tickets with rogue device information for quicker response and less labor is our next obstacle since the effort to collect device data is tedious. By implementing these strategies, both technical and policy-based, a wireless team can protect a campus against wireless threats.

11. Lightweight Intrusion Detection for resource constrained IoT devices using Network Traffic and Payload Analysis

Niharika Jain, *University of Washington*

The rapid growth in the popularity of the Internet of Things (IoT) also has exposed the vulnerabilities of these devices leading to significant security concerns. These networks are increasingly prone to attacks such as monitoring and eavesdropping, where network traffic patterns of IoT-based smart-home devices can be used to infer private user information. Because IoT devices are resource constrained and lack computational power, it is difficult to implement any holistic security solution to protect them from adversaries. Network infrastructure plays a critical role in securing any digital product. If implemented correctly, it can secure the device and data while providing valuable information about device misbehaviors. In IoT devices, certain attacks exploit gaps in network protocols or attempt to gain unauthorized access by scanning insecure network traffic.

In this research, we developed an intrusion detection mechanism that persistently analyses the IoT network traffic to detect malicious behavior. Specifically, our solution involves two phases: 1. Low-frequency scan of network bandwidth to detect spikes in network activity, and 2. High-frequency scan of actual packets flowing through the network, and randomly sampling data packets to detect the probability of a breached

IoT device. This solution is designed with resource-constrained devices in mind, and the proposed algorithm is easily reconfigurable for any IoT device.

The adaptive low-frequency scan allowed the network analysis to run transparently as the packet flow through the network is unaltered. We used a sliding window approach to restrict memory. The sliding window and moving average helped smooth out short-term fluctuations while highlighting fluctuations in the bandwidth utilization. In high-frequency mode, random packet analysis selection thresholds could be dynamically throttled to ensure optimal resource utilization. The packet analysis system checked for audio/video stream of data in addition to probing the claimed destination device to verify the legitimacy of the node. The solution had minimal impact on network traffic during either phase. This mechanism made the solution ultra-lightweight and possible to be used with the extreme resource-constrained IoT devices.

12. Did I Agree to This? Silent Tracking Through Beacons

Edden Kashi and Angeliki Zavou, *Hofstra University*

Users' personally identifiable information (PII) collection is a primary revenue model for the app economy and, consequently, user tracking has become increasingly invasive and ubiquitous. Smart devices provide even more access to users' personal information by pinpointing their exact location. Although in most cases users must grant permission before their personal information is tracked or shared with third parties, this is not the case when tracking happens through email or webpage visits. The average user is willing to accept the terms of the often unread "Privacy Policy" to receive the advertised "better user experience," without really being aware of the consequences of this decision. Companies collect user data to feed algorithms that create targeted ads, tailor news recommendations, vary prices of online products, and cater specifically to users' tastes. In the hopes of regaining customers' trust and complying with legal requirements, companies constantly update their privacy policies, which the average user still has little to no understanding of. Web beacons, or tracking pixels, are often embedded into websites, emails and social media to track the activity and data parameters of a user that can be used to profile, target and analyze traffic. Similarly, web bugs can be used with malicious intent while a user is unaware they are being tracked and/or did not agree to their information being logged. Email tracking through web beacons is frequently used in customer relationship management software and accessible browser extensions. This accessibility raises questions if the senders of such emails understand the policies they accept when sending

2020 WiCyS CONFERENCE

STUDENT POSTERS

an email through a third party and if the recipients are informed of the tracking when not explicitly told. We aim to show that the usage of varied beacon tracking methods can create unified profiles against targeted users. We hope that our extensive analysis of beacon tracking will lead to greater awareness of the privacy risks involved with web beacons and motivate the deployment of stricter regulations as well as a more effective notification mechanism when such tracking is in place.

13. Latent Cybersecurity Policy Constructs: Lessons from Congress' Approach to Cybersecurity in the 99th Congress and Beyond

Jennifer Lake, *The University of Texas at Austin*

This work is focused on improving the understanding of the conduct of the U.S. Congress and how it has addressed legislating cybersecurity policy. We ask how can Congress better legislate in the cybersecurity policy space? What policy constructs did Congress take up? Which did they discard? What features of organizations, groups and individuals within Congress are most active in legislating cybersecurity policy? Which organizations, groups and individuals were least successful? Did specific subsets of Congress have an affinity, or aversion, to certain policy constructs? What can all of this tell us about how Congress might legislate cybersecurity in the future?

This poster proposal is a part of a larger research project that will explore how Congress has treated the issue of cybersecurity from the 1970s through 2018 (the 93rd through 116th Congresses). This also will showcase the analysis of its work during the 99th Congress, which passed the Computer Fraud and Abuse Act (CFAA). The work will examine the text of cybersecurity-related bills introduced in Congress and identify not only a dictionary of cybersecurity-related terms but also, more importantly, latent cybersecurity constructs in the bills. These policy constructs will tell us a great deal about how Congress has interacted with cybersecurity as a policy issue, what concepts have been enacted, and what constructs have not been enacted. The illumination of these constructs will provide a comprehensive understanding of the cybersecurity legislative landscape and the policy environment that confronts policymakers today.

The unique contribution of this proposed work is to analyze the full scope of the congressional cybersecurity policy debates. Much has been written concerning existing (enacted) cybersecurity policy, but nothing has yet comprehensively addressed the full scope of the work. So, the first contribution is to compile this complete legislative history. The second significant contribution will

be to develop the latent cybersecurity policy constructs embedded in legislation. The research will use topic modeling techniques paired with selected manual review to conduct the analysis. The third contribution will be to analyze the cybersecurity policy constructs to understand why certain ones were enacted while others were not. This analysis will potentially assist future legislators in establishing cybersecurity policy. The fourth contribution will be an analysis of the current (2020) state of the cybersecurity policy environment and a look ahead at those constructs or issues that still need to be addressed.

14. Intrusion Detection for Wireless Medical Devices Using Generative Adversarial Network

Nhu Ly, *University of Washington*

The rising number of cyber attacks on wireless medical devices have exposed their vulnerabilities and weaknesses and current security controls in place. Because these devices are resource constrained, existing cybersecurity protection solutions are limited in securing healthcare data. Research shows that attackers can bypass traditional security solutions to gain access to the patients' personal data. Therefore, intrusion detection systems that can alert users and healthcare providers to suspicious events are critical to security in healthcare systems. Recently, machine-learning algorithms have been widely applied in intrusion-detection systems to effectively detect attacks. However, these techniques are often subject to adversarial attacks causing the learning models to make false predictions by adding extra noise into the original data. In this research, we aim to address this problem by applying Generative Adversarial Networks (GAN) toward detecting intrusions in wireless medical devices. These networks consist of two neural network models competing against each other in a learning game to raise accuracy. Since the proposed GAN-based intrusion detection system does not require sharing healthcare data to the server for training and testing purposes, it also ensures data privacy.

15. A Computational Framework for Identity using Semantic Web Resources, Dempster Shafer Theory and Argumentation Schemes

Janelle Mason, *North Carolina A&T State University*

This research presents a computational framework for identity that can be used in cyberspace and forensic environments. The current focuses of the framework are on physical crime scenes, where we are determining the potential culprit(s) in a legal case based on the evidence collected on site. We are particularly interested in biometric evidence. The framework shows how various sources of evidence in a crime may conspire

2020 WiCyS CONFERENCE

STUDENT POSTERS

to support various identity judgements. Semantic Web resources, e.g., Resource Description Framework, Resource Description Framework Schema and Web Ontology Language are used in the framework to structure and encode situations. Ontologies are used to depict a network containing situations stitched together by objects, where evidence “flows” (diminishing and combining) along the network. The Analytic Hierarchy Process, a structured systemic process used to determine the level of importance of information in a multi-criteria decision-making problem, is used to determine weight assignments to evidence and incorporated into the Dempster Shafer theory. This theory is used to follow how evidence supports hypotheses on the identity of the culprit in a crime scene. Argumentation schemes are coupled with the theory to derive measures of uncertainty in our identity hypotheses that reflect combining evidence, the reliability of available evidence, and the confidence in identifying potential culprit(s) in our framework.

16. Vulnerabilities of Continuous Glucose Monitoring Systems and mHealth Integration

Aleise McGowan, Michael Black and Scott Sittig,
University of South Alabama

Diabetes mellitus, commonly known as diabetes, is defined as a group of metabolic diseases mainly caused by irregular insulin secretion and/or absorption. Diabetes is a chronic disease increasing its prevalence with 1.5 million Americans diagnosed each year. As physicians’ understanding of diabetes has deepened, there has been a shift in treatment therapies. Straying from previous methods, treatment guidelines highlight the necessity of controlling glycemia. For years, the use of capillary finger sticks was the de facto standard for self-monitoring blood glucose levels. However, the ability to generate a complete narrative of a patient’s glucose would be hampered by the need for frequent measurements, which may be required overnight.

Mobile health technologies that use smartphones are known as mHealth devices. These devices have created options for physicians and patients associated with monitoring and delivering patient treatment, allowing for new opportunities. These areas of opportunity include the collection and monitoring of patient health data, and using that data to help achieve better patient outcomes. Continuous glucose monitoring (CGM) systems allow diabetics to track their glucose levels almost in real time, providing readings every five minutes over a 24-hour period.

However, these opportunities also introduce a unique set of security vulnerabilities due to the implementation

of the mHealth platform. While CGM systems offer tremendous benefits to diabetics, they also have drawbacks. Modern systems utilize wireless technology, such as Bluetooth Low Energy (BLE) communication. This dependency makes CGM systems vulnerable to hacking. By gaining unauthorized access to a system, a nearby hacker could block or modify data sent to the CGM. The security risks introduced through the integration of technologies, such as Bluetooth connections, are seemingly outweighed by the benefits of CGM systems. However, the full extent of patient vulnerability could unfortunately be overlooked. The non-adjunctive use of CGM systems necessitates the accuracy, reliability and safety. In this research, we seek to learn what threats exist or are introduced to patients from CGM systems utilizing BLE transmitting data to mHealth devices.

17. Reading and Replaying CAN Messages

Nishi Prasad and William Van Wart, *Rochester Institute of Technology*

The goal of this work is to understand the basics of how the Controller Area Network (CAN) bus works and interacts with the Electronic Controller Units in a 2011 Honda CR-V with a Linux CAN-to-USB device and Ubuntu VM. The vehicles’ CAN bus was accessed via the sixth pin of its OnBoard Diagnostics port, which is the 500 kbps high-speed CAN bus typically used for transmitting engine critical data. With the use of SocketCAN, a set of open-source CAN drivers and CAN-utils, and a set of command-line utilities, a physical connection was made from the vehicle to the Linux machine, and CAN traffic was recorded, analyzed and replayed. With the vehicle turned on, the cansniffer utility was used to observe traffic on the CAN bus while performing specific stationary functions in the car. After analysis, correlations were made between functionality and specific CAN ID. A CAndump log file was recorded during RPM throttling and replayed using CANPlayer, which further supported the byte analysis.

18. Building a Tabletop Cyber Exercise for Emergency Management

Vanessa Primer, *Highline College*

As part of a Homeland Security Emergency Management Class, we designed and evaluated exercises for emergency management to use as part of the National Preparedness Goal and planning frameworks. This project shows why cyber exercises are necessary today, the mission areas and core capabilities covered, where cybersecurity fits in the National Preparedness Goal, what a tabletop exercise is, and how it can benefit a jurisdiction. This exercise was developed to play out a

2020 WiCyS CONFERENCE

STUDENT POSTERS

ransomware attack organically with a choose-your-own adventure-style tabletop simulation of events. Alternate cyber threats/hazards/risks are available as well that can be built on the base exercise.

19. Security of Perception Module of Autonomous Vehicles

Ayushi Rathore, *Rochester Institute of Technology*

The number of autonomous vehicles on roads is increasing each day. Not only that, but they are becoming more advanced and as a result, attacks on these vehicles are also being elevated. In this poster, we studied attacks on the LiDAR sensor, which is primarily used by the perception module of self-driving cars. We studied how different modules of self-driving cars work, the importance of a perception module, LiDAR spoofing attacks, and its implication and possible defense mechanism for this kind of attack. This study shows the importance of implementing security mechanisms in the mentioned field and how it can affect the industry.

20. Intercomparison of Hardware and Software Intrusion Detection Systems for Controller Area Networks

Katrina Rosemond, *Howard University*

The average modern vehicle can be thought of as a network on wheels executing millions of lines of code. Embedded microcontrollers, also known as Electronic Control Units (ECUs), execute this code in order to control various functionalities within a vehicle, including the safety-critical components and infotainment systems. The most commonly used ECU communication network is the controller area network (CAN). The CAN was originally created to be an internal-only network and designed without security in mind. However, with emerging automotive technologies like autonomy and Internet of Things (IoT) device connectivity, the number of attack surfaces within an automobile continues to increase and expose vulnerabilities within CAN bus. Attackers can use these vulnerabilities to access the network and gain control over ECUs. Therefore, the CAN needs to be hardened to prevent attacks against safety-critical features. While previous work has shown that intrusion detection systems (IDSs) can help harden the CAN bus, these works often can be difficult to reproduce and validate due to various challenges, including limited access to intellectual property and implementation expenses. Thus, the objective of this research is to enable valid and reproducible CAN IDS research by creating hardware and software platforms for experimentation and validation. We will implement both hardware and software CAN controllers and IDS to detect when an attack is

imminent then evaluate each system's performance and implement metrics, including lines of code and cost.

21. Forensic Analysis of Vault Applications

Kayla Rux, Kathryn Seigfried-Spellar and Siddharth Chowdhury, *Purdue University*

Modern digital devices such as laptops, personal computers, mobile phones and tablets have vault apps – applications that hide photos, videos and texts in a secure “vault.” These vault applications allow the user to securely store their personal data, making it difficult for anyone except the device's owner to view files even if they have access to the device. These applications often disguise themselves by pretending to look like others, such as calculators, or only display information when the user enters a valid password. From a law enforcement investigation perspective, offenders may use vault apps to hide illegal images, such as child sexual exploitation or illicit text messages with minors. In these cases, vault applications may serve as a hindrance to law enforcement. While traditional digital forensic tools may be able to recover photos directly stored on the phone, they may not be able to find those secured by photo vaults.

This study aimed to assess what kind of information can still be forensically recovered from such applications, its impact on user privacy, and documentary methods used to extract actionable information from such anti-forensic measures. The five most popular vault applications on the iOS store were analyzed. By analyzing these, a larger audience could be reached from a user and law enforcement perspective. In addition, photos were uploaded to the applications in four different ways: Taking a screenshot, saving from a text message, saving from a browser and using the phone's camera. While studies have been performed on Android operating systems, no testing has been done on the iPhone and iOS ecosystem. Results and findings will be presented, and implications will be discussed.

22. IoT, Cybersecurity and You

Vivian Sargent, *Highline College*

During my internship at Pacific Northwest National Labs (PNNL), I worked on a project called INERTIA that will uncover vulnerabilities and establish global best practices for Internet of Things (IoT) design and usage. IoT is “a system of [unique] interrelated computing devices... objects, animals or people...with the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.” IoT capability takes advantage of the increasingly mobile global lifestyle by providing instant access to remote locations. Conservative estimates find 27 billion devices currently in use with

2020 WiCyS CONFERENCE

STUDENT POSTERS

another 127 devices connected to the internet every second and a projected 76 billion by 2025. This does not include Bluetooth-only devices. As the number of devices increases, so do gaps in security. Recent attacks prove that compromising one of these devices can compromise the entire system. There are three waves of IoT adoption – networked consumer electronics, networked industries and networked everything/networked society. Residential IoT devices like Alexa and mobile phones are commonplace. Commercial IoT devices such as infrared motion sensors and cameras are increasing in popularity. Devices like cars and medical equipment overlap both waves. To obtain vulnerability data, the lab acquired a cross section of these IoT devices for testing. Selection criteria included popularity, unique solution and known vulnerabilities. INERTIA changes the paradigm of IoT by identifying a better definition not as the Internet of Things but the “Interconnectivity” of things. This clarification stipulates that devices do not need a network to communicate. The nascent world of IoT is already one of constant evolution. Oxford defines “inertia” as “a tendency to do nothing or to remain unchanged.” This related acronym denotes the unchanging nature of IoT is change itself.

23. Generative Adversarial Networks (GANs): New Machine-Learning Model to the Cybersecurity Industry

Shekufeh Shafeie, *University of Louisiana*

Generative Adversarial Networks (GANs) spell the end for cybersecurity somehow, and the coin is double sided. They can be used by malware authors to overwhelm anti-malware systems. Authors also can create new forms of malware, which is indistinguishable from real code and thereby undetectable. On the other hand, they also can play a role for good in the cybersecurity industry. At the same time, they can provide us with an opportunity to create our own labelled data with which to better train our own AI systems or detect anomalies. This will enable the identification of new types of attacks more quickly and effectively.

In this poster, I discuss two applications of GANs applied to cybersecurity-related tasks: PassGAN, a deep-learning approach used for password guessing, and Secure Steganography Based on Generative Adversarial Networks (SSGAN). They will no doubt prove extremely effective in helping security analysts compete with ever-evolving threats. In PassGAN, the generator learns the password distribution of the training set. It learns more human patterns and generates passwords similar to human-generated patterns. This means that PassGAN learns things a typical password cracker would never

catch. SSGAN describes researchers' attempts to use GANs to create stenographic schemes. The SSGAN method improved upon earlier work in the field that used another, less performant strategy. It uses one generator and two discriminators. These two projects are only the tip of the iceberg, but perhaps the most famous applications in cybersecurity.

24. Cryptanalysis of WPA3

Neha Sharma and Lakshmanan Murthy, *Rochester Institute of Technology*

In 2016, Key Reinstallation Attack (KRACK) was discovered, making billions of devices vulnerable to data theft and manipulation. It showcased a serious flaw in the way WPA2 was engineered. After the discovery of this attack, Wi-Fi Alliance started the shift toward the successor of WPA2, which would be more secure. WPA3 was launched in 2018 as the next generation of Wi-Fi security. It is built upon WPA2, providing security and countermeasures against attacks that affected WPA2 while also retaining backward compatibility with WPA2. WPA3 introduces three new protocols and suites, namely Opportunistic Wireless Encryption (OWE), Simultaneous Authentication of Equals (SAE) and WPA3-SAE Enterprise that contains new cipher suites and encryption methods to make it difficult for attackers to read a client's data transmission streams. WPA3-SAE, based on dragonfly key exchange, is a Password Authenticated Key Exchange (PAKE), i.e. it turns the password into a high entropy key decreasing the chances of it being discovered. It replaces WPA2-PSK, which was vulnerable to offline dictionary attacks and prevents the KRACK against a four-way handshake. Dragonfly Handshake also provides security when connected with an access point that only supports open Wi-Fi mode. OWE addresses problems in open networks by encrypting all the traffic, hence blocking passive attacks. In transition mode, OWE supports 802.11 “open” authentication. An access point (AP) in OWE transition mode will have two virtual access points: (VAP) one to connect with “open” and the other to connect with OWE. Since SAE uses Dragonfly Handshake, which is a crucial part of WPA3 and affects the Enterprise Security part of WPA3, a lot of research has been done to discover their attackers and their mitigation tactics. Not much attention has been given to OWE suites as its main function is to provide backward compatibility with open mode of Wi-Fi. Our research is divided into two parts. First, we discovered two new attack vectors against WPA3-OWE suite. Because WPA3 is not an authentication protocol and uses Diffie Hellman Key Exchange and since Diffie Hellman Key Exchange is susceptible to Man-in-the-Middle attack, we researched and found that, theoretically, OWE is also susceptible to Man-in-the-Middle attack. For

2020 WiCyS CONFERENCE

STUDENT POSTERS

another attack, we exploited code 77 that an AP sent in one of the management frames if the client requested a cryptographic suite not supported by the AP. Second, we tried to come up with new mitigation schemes for two of the attacks discovered on WPA3-SAE suite, attacked on SAE in downgrade mode and attacked on multiplicative groups that the client and AP agreed on to be used for encryption during the Authentication frame exchange.

25. Extraction of Multimedia Large Objects Using Memory Forensics from the Android Runtime

Sneha Sudhakaran and Golden G. Richard III, *Louisiana State University*; **Aisha Ali-Gombe**, *Towson University*; **Andrew Case**, *Volatility Foundation*

This poster will help attendees gain an understanding of the importance of performing memory forensics on the Android framework and how objects of security and forensic interest might be retrieved. Our focus is currently on the Android runtime (specifically, the memory allocators for ART) and recovering and reconstructing large objects associated with multimedia such as images and video. The memory allocation algorithms, called region-based memory management, are studied to develop a system that recovers vital runtime data structures for Android applications by enumerating and reconstructing allocated objects from a process memory image. We also show the extraction of evidence by decoding multimedia data stored in structures like byte arrays, char arrays and bitmaps in allocated memory regions of the Android runtime. This project explores the advantages of memory analysis in the user land process space. We demonstrate with practical examples the reconstruction of allocated in-memory objects by analyzing the Android runtime. The project illustrates how vital this detection process is in proving attribution on a multi-app platform such as Android. We do a study on multiple libraries used to store such large multimedia objects in Android memory-enhanced awareness of how memory forensics plays a unique role in analysis and recovery of data structures used to store large objects in ART, which in turn helps recover raw multimedia data stored in memory.

26. Analyzing CVE Database Using Unsupervised Topic Modeling

Vanamala Mounika, *North Carolina A&T State University*

To develop secure software, it is important for software engineers to understand different vulnerabilities in software that can be exploited by attackers. A vulnerability database is a platform aimed at collecting, maintaining and disseminating information about discovered computer security vulnerabilities. In this poster, we present a method

for analyzing the vulnerabilities reported in Common Vulnerabilities and Exposures (CVE) database using topic modeling. Topic modeling is statistical in nature to discover the abstract “topics” that occur in a collection of documents. Latent Dirichlet Allocation (LDA) is a technique for content analysis designed to automatically organize large archives of documents based on latent topics measured as patterns of word (co-)occurrence. It has implementations in the Python’s Gensim package. In this research, LDA was implemented to analyze large corpora of vulnerability texts in the CVE and find its prevalent topics. We then mapped the topics generated manually to the Open Web Application Security Project (OWASP) Top-10 vulnerabilities. We analyzed 121,716 unique CVE entries from 2009 until the end of June 2019 using topic modeling and identified emerging trends of OWASP Top 10 vulnerabilities. We performed a series of experiments on topic modeling with LDA algorithm implemented within a scikit-learn package for Python and obtained 10 topics, i.e., non-structured clusters of semantically related words.

The analysis of CVE vulnerability reports includes six phases: 1. Data preprocessing. In this phase, Natural Language Toolkit (NLTK) stop words and spacy model are downloaded. The stop words from NLTK and spacy model are needed for text pre-processing; 2. Text cleaning. Emails, newline characters, special characters and empty spaces are removed and Tokenized; 3. Bigram and Trigram Models are created; 4. Building the Topic Model. The LDA model was built with 10 different topics where each topic is a combination of keywords, and each keyword contributes a certain weightage; 5. Visualize the topics and the associated keywords. The topics produced and the associated keywords are examined using pyLDAvis package; and 6. Mapping topics to OWASP-Top 10. Once the topics are generated, we manually map these topics to OWASP Top 10 risks. We manually assigned a label to each topic using OWASP Top 10 risks. Based on the description provided for these vulnerabilities from the OWASP website and OWASP Application Security Verification Standard, we have prepared a mapping table with a list of keywords that correspond to a vulnerability. We mapped the topics based on the most relevant terms of the particular topic to OWASP Top 10 and then tabulated what percentage of tokens are in each topic every five years from 1999 to 2019 to identify different trends. We were able to find some interesting patterns in the vulnerabilities reported over the years. OWASP vulnerability A2:2017-Broken Authentication, A5:2017-Broken Access Control, A4:2017-XML External Entities (XXE) had a linear increase in the number of vulnerabilities reported and A7:2017-Cross-Site Scripting (XSS) had a linear decrease over the years.

2020 WiCyS CONFERENCE

STUDENT POSTERS

27. An Analysis of the Effects of the Spectre and Meltdown Patches on the Lustre Parallel File System

Amaris Velez-Candelaria, *Polytechnic University of Puerto Rico*; **Adam Good**, *Dakota State University*; **Trevor Bautista**, *Arizona State University*

In a High-Performance Computing (HPC) environment, it is imperative to ensure that systems function securely while maintaining the best performance possible. To meet these performance requirements, it is common to use a parallel file system such as Lustre. However, these requirements also conflict with the Spectre and Meltdown patches notorious for reducing production. This research focuses on evaluating the impact these patches have on the Lustre parallel file system while assuming that the client side is always patched. The Lustre file system was evaluated before and after file system servers were patched for the Spectre and Meltdown vulnerabilities to measure the effect concerning server and client interaction. According to past research, Spectre and Meltdown patches were expected to have a slight effect on the overall Lustre file system and a significant effect on the metadata server (MDS). Our results partially agreed with initial expectations. The overall Lustre file system had a 15% decrease in performance due to the patches, one of the most significant effects observed. Among Lustre servers, the MDS suffered the greatest decrease in performance. Consequently, it has been determined that Spectre and Meltdown patches present an overall significant effect on the Lustre file system. Finally, the effect of the patches on Lustre was more clearly observed as the number of nodes was increased. Due to this observation, future research could focus on executing the same benchmarking processes with a greater number of nodes. Additionally, it may be beneficial to look into the cause of the increase in performance for small-scale patched systems.

28. Cybersecurity Education: A Closer Look under the Theory of Reasoned Actions and Theory of Planned Behavior

Jasmine Washington, **Li-Chiou Chen**, and **Andreea Cotoranu**, *Pace University*

Cybersecurity education plays a key role in preparing students with the skills necessary to defend cyber space. Understanding how students learn about cybersecurity concepts will facilitate the learning process and improve learning outcomes. The goal of this research is to explore if concepts from Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB) can be used to explain student learning in cybersecurity. Empirically, we will use textual data analytics for understanding students' attitudes, knowledge, self-efficacy and intentions toward

learning about cybersecurity through their written reflections. Do students reflect on learning differently when they express different previous attitudes toward learning? By analyzing data collected from students' daily reflections, this research aims at developing a method to understand students' intentions through what they like, what they wish to do, what they have learned as well as their hopes, concerns and expectations.

Pace University hosted GenCyber, a workshop that involved high school teachers learning about cybersecurity concepts to implement at the secondary education level. We collected three years' worth of data from 2017 to 2019. In the workshop, participants were asked to express their attitudes including their hopes, concerns and expectations. During the workshop, participants filled out reflection forms with five questions at the end of each day to verify and reinforce what they learned as well as their intentions toward future learning. For this study, we analyzed the reflections on the following topics: cryptography, web security and a teaching tool used in the workshop called Raspberry Pi.

The reflection questions were grouped by variables based on the concepts from TRA/TPB including attitude, self-efficacy and behavior intention. Attitude refers to the participants' previous beliefs and thoughts toward learning about cybersecurity. Self-efficacy refers to what they thought about their understanding of the lesson and their responses to certain questions. Behavior intention includes what participants perceived as their intended actions. Using textual data analytics, this research analyzed participants' responses using the natural language processing toolkits in Python. Data was anonymized and cleaned by removing participant entries that were incomplete. It was then grouped based on the three TRA/TPB variables stated earlier. We generated a frequency table based on the number of repeated keywords such as cybersecurity or cryptography. Lastly, we correlated the participants' previous attitudes to their behavior intentions.

The expected contribution of this research is to provide insights into cybersecurity education by analyzing empirical data from students in cybersecurity workshops. By using TRA/TPB as a theoretical framework, we were able to extract information from students' written reflections during the learning process and conduct an analysis on the text data using textual data analytics. Although our analysis is preliminary, we expect to learn from these results and improve our data collection instruments and textual analysis techniques.

2020 WiCyS CONFERENCE

STUDENT POSTERS

29. How Does Misconfiguration of Analytic Services Compromise Mobile Privacy?

Xueling Zhang, Xiaoyin Wang, Rocky Slavin, and Jianwei Niu, *University of Texas at San Antonio*; **Travis Breaux**, *Carnegie Mellon University*

Mobile application developers commonly use analytic services to examine their app users' behavior to support debugging, service quality and advertising. Anonymization and aggregation can reduce the sensitivity of behavioral data, and analytic services may encourage the use of these protections. However, developers can misconfigure the analytic services and expose personal information to greater privacy risk. Since people use apps in their daily lives, they may contain a lot of personal information, such as a user's real-time location, health or dating preferences. To study this issue and identify potential privacy risks due to such misconfigurations, we developed a semi-automated approach, Privacy-Aware Analytics Misconfiguration Detector (PAMDroid), which enables the empirical analysis of modern analytic service practices. This poster describes a study of 1,000 top apps using top analytic services with PAMDroid. We found misconfigurations in 120 apps of which 52 also caused a violation of either the analytic service providers' terms of service or the app's own privacy policy.

30. Improving Incident Response and Security through Network Analysis Tools

Daniela Zieba, *University of Illinois at Urbana-Champaign*

This project seeks to develop improved security analysis tools for use within the University of Illinois at Urbana-Champaign's National Center for Supercomputing Applications (NCSA) Incident Response and Security Team. Such tooling will improve NCSA network security across supercomputing clusters hosting valuable scientific data for researchers and private industry partners. Pre-existing passive security monitoring tools developed at NCSA are leveraged to gather data from which we can actively identify potential network vulnerabilities and act accordingly before attackers exploit them. Network data is integrated into customizable reports visualizing anomalies and the network state with the intention of improving the workflow and performance of security analysts on which the overall state of the network is reliant. The project tooling is capable of analyzing new services on the NCSA network and creating reports on a desired basis with custom rules in a specified timeframe. Other rules can be placed on network information such as banner data or port quantities from which services can be identified and hosts can be blacklisted to avoid false, undesired flagging. For example, we don't want to report ports 50,000 to 60,000 as they are used for data

transfer but would always like to flag port 6,443 as it is a likely Kubernetes API. After generating reports for a long enough timeframe, the resulting network data will be used for further analysis of network trends.

While this tooling is initially being developed for internal use at NCSA, it will be open sourced upon completion for possible adoption by similar research institutions rather than adopting expensive and close-source alternatives for network analysis. The purpose is to gather and analyze network data in further detail while improving the workflow of security analysts, which is especially important to consider as continuous security breaches come to light.



ALLIES & ADVOCATES FOR ACTION MEETUP

TOGETHER. WE INCLUDE.

Friday, 10:00am - 11:00am - Cottonwood 6-7

Allies & Advocates are key stakeholders and participants in advancing workplace diversity.

Join the conversation about how to be an effective ally/advocate for action and/or how to effectively work with an ally/advocate.

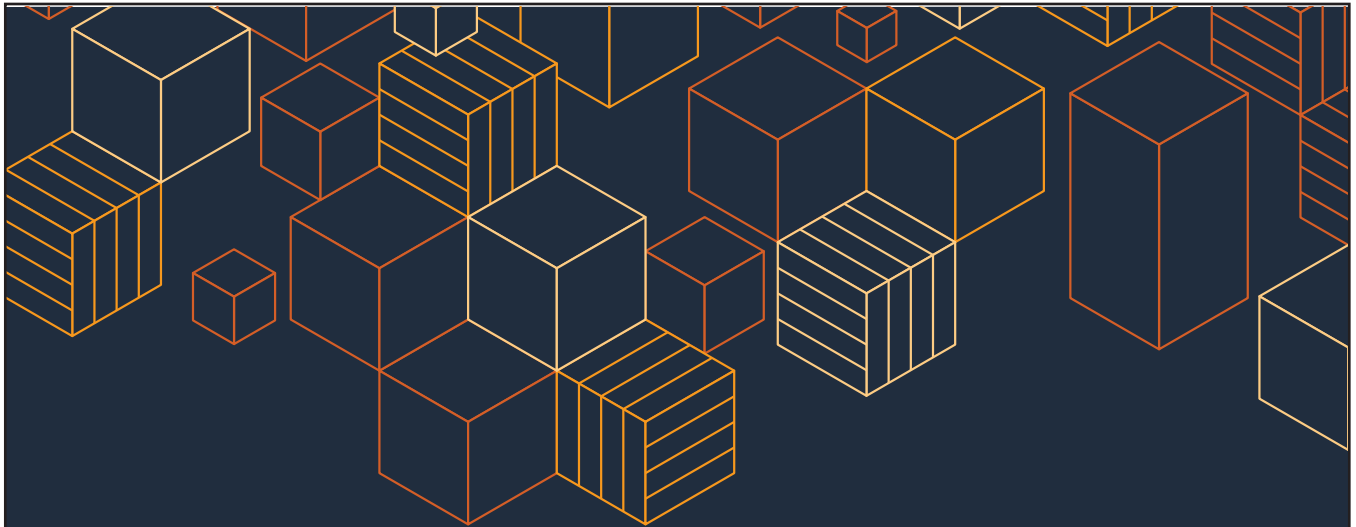


STRATEGIC PARTNERSHIP

ENABLE

The future of women in the cybersecurity workforce lies in our hands. Together with WiCyS and other Strategic Partners, we will make a difference in supporting women in their quest to be hired, retained and advanced in their cybersecurity careers.

CONTACT: INFO@WICYS.ORG



NOT YOUR AVERAGE WORK PLACE.

We're a team of curious leaders pushing each other to be the best for our customers. Come join the AWS Professional Services and AWS Security team where every day is full of meaningful work mixed with a little AWS quirk.

*Stop by the AWS booth to
learn more and enter our
raffle to win a fun prize!*



Create Design Code Build for everyone



Googlers build products that create opportunities for all. Whether it's down the street or across the globe, we want to help people learn, be heard and succeed. Come help us build for everyone.

careers.google.com

We're proud to support Women in Cybersecurity as part of our commitment to fostering diversity and inclusion at Google and beyond.

LEVEL UP

Investigate. Analyze.
Develop. Operate. Protect.

The latest video games are no match
for an exciting career in cybersecurity.

Join a company where anything is possible.
We have the bandwidth. **Do you?**

mastercard.com



Mastercard is a registered trademark, and the circles design is a trademark of Mastercard International Incorporated. ©2019 Mastercard. All rights reserved.

APPLY TODAY TO SECURE TOMORROW




CAREERS AT RAYTHEON

If you're passionate about cyber innovation, we want you as part of our team. Work on critical systems that help secure our nation. Create breakthroughs across multiple products and domains. Enjoy the benefits of working for a global industry leader. Make your talent a key part of our team.


[JOBS.RAYTHEON.COM/CYBER](https://jobs.raytheon.com/cyber)

Raytheon



Thank you for showing us that,
inside all of us, is the ability to
unlock endless possibilities.

State Farm® is proud to
support Women in
CyberSecurity.

 **State Farm®**

State Farm, Bloomington, IL



Verizon Principal,
Network & Information Security

Bring your ability to protect and defend.

Advance your career on our cyber team.

As a cybersecurity expert at Verizon, you'll be helping detect and respond to the ever-evolving threats to our data and technology. As we continue to connect cities, towns and people with the networks of the future, we're looking for the best talent to join our team across a broad range of roles.

**Explore cybersecurity opportunities
now at verizon.com/cybercareers.**

verizon  **cyber
careers**

Verizon is an equal opportunity/disability/vet employer



Automation = Better Outcomes

Adobe is investing in intelligent automation throughout its business. Automation helps better secure our products and services. It also helps provide better data so that issues can be found more quickly, escalation paths are clearer when issues occur, and we can make better informed, quicker decisions.

Learn more these efforts by **visiting the Adobe booth** here at the Women in Cybersecurity (WiCyS) conference or on our blog at:

blogs.adobe.com/security

Interested in joining the Adobe team? We have positions open throughout the company. Learn more about all open positions at:

adobe.com/go/securityjobs



Inspiring the next generation of Cyber Security professionals

Bank of America is proud to support the Women in Cyber Security Conference. Join us at our networking event on March 12th and visit us at the career fair on the 13th to meet our teammates and network with Cyber Security professionals.



Professionals
bankofamerica.com/careers

Students
campus.bankofamerica.com

BANK OF AMERICA

Bank of America is an equal opportunity employer EOE/M/F/Vet/Disability © 2020 Bank of America Corporation. ARTGH839 | GIS-101218

**Carnegie
Mellon
University**
Software
Engineering
Institute



Secure the Future of Cybersecurity

Meet our staff at **Booth 501** and learn more about career opportunities at the CERT Division.

Apply today!

Visit our website for more information.

sei.cmu.edu/careers



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
- WiCyS Student Chapter (CyberEagles-W)
- NSF-NSA GenCyber Camps Program
- CTF, defense and offense competition teams

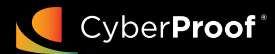


Come join our team and experience the world of cybersecurity in its complete spectrum and diversity!



- 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/programs/csc/index.php>.

A SMARTER SOC



CyberProof Salutes WiCyS

At CyberProof, open and free communication is a guiding principle. We understand that speaking your mind requires responsibility and respect of others so we promote a space where everyone can share ideas, contribute, and collaborate.

We are a start-up, but we think big in everything we do. Our can-do attitude means we are agile and make bold decisions. Learning is a journey and we love exploring new opportunities. We are in the business of cyber security services so if you are interested in working somewhere that embraces change and aspires to improve constantly, please contact us at <https://www.cyberproof.com/career-opportunities>



Discover THE BEACOM COLLEGE of COMPUTER & CYBER SCIENCES



We are proud to present the NSF REU Summer Program, to apply, please visit: cybertraining.pro



Dakota State University is a NSA/DHS CAE in Cyber Defense, Cyber Operations, and IA Research.

FALL 2013-FALL 2019



430% INCREASE
women in computer science
775% INCREASE
women in cyber operations
667% INCREASE
women in network security

As one of the nation's cyber leaders, Dakota State is a proud supporter of women in cyber. We offer elite programs on-campus and online, including undergraduate, graduate programs, research opportunities, and extra curriculars to expand your cyber knowledge.

FOR MORE INFORMATION

DSUCyber.com | CybHER.org

CybHER.org



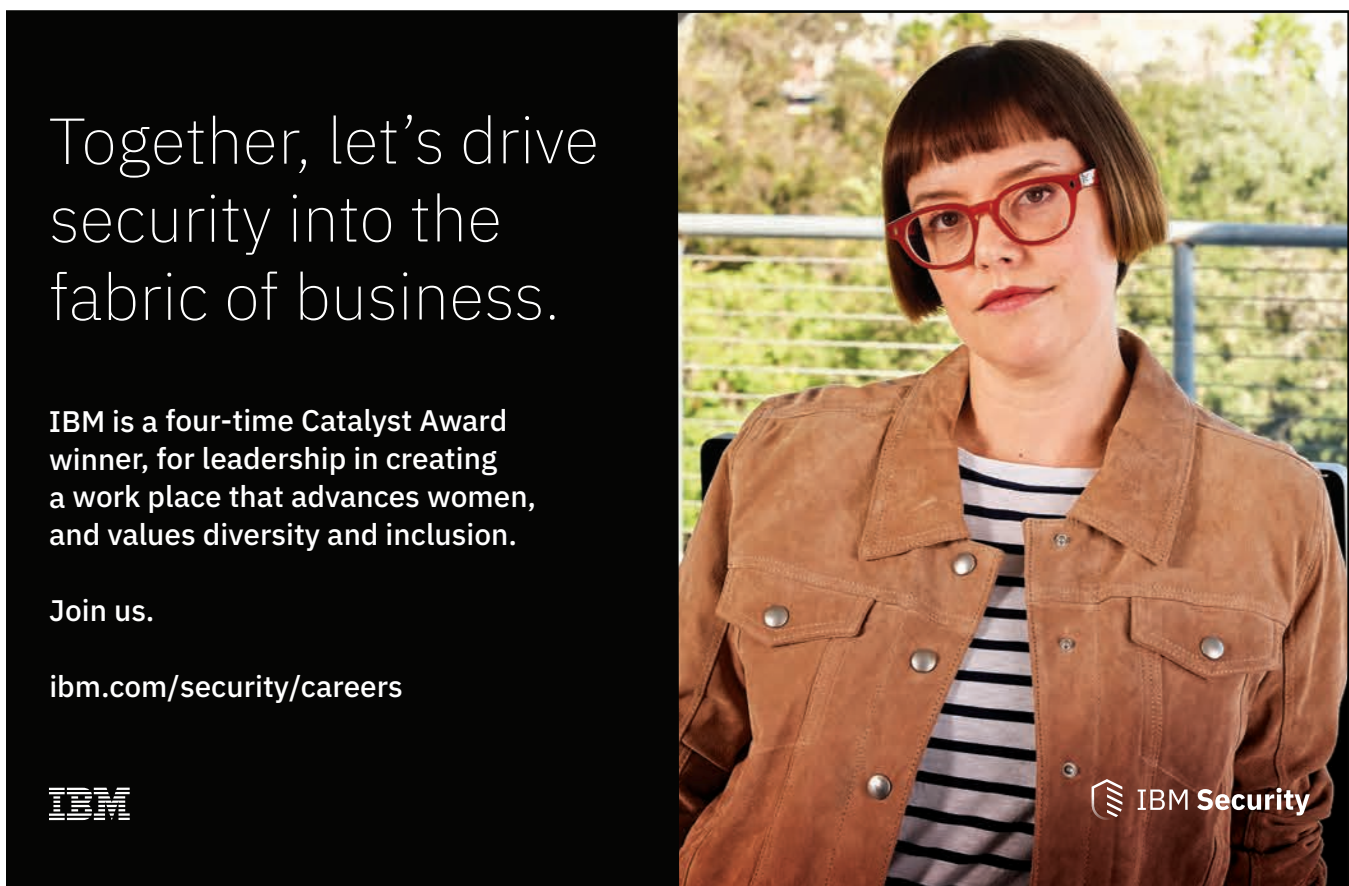
DAKOTA STATE
THE BEACOM COLLEGE of
COMPUTER & CYBER SCIENCES



DENSO
Crafting the Core

It's our diverse culture,
unique strengths, and
strong collaboration that
make DENSO a successful
advanced mobility supplier.

Crafting the Core




Together, let's drive
security into the
fabric of business.

IBM is a four-time Catalyst Award
winner, for leadership in creating
a work place that advances women,
and values diversity and inclusion.

Join us.

ibm.com/security/careers

IBM

 **IBM Security**



Unrivalled Cyber Risk and Breach Response

Experienced security leaders and elite responders to fortify preparedness, detection and response



cyberresponse@kroll.com | kroll.com/cyber

Kroll | A Division of
DUFF & PHELPS

Microsoft at WiCyS

March 12–14, 2020
Denver, Colorado



At Microsoft, we enable organizations to digitally transform with industry-leading protection. By harnessing the power of Microsoft's cloud, we offer customers a security solution that delivers unified coverage, empowers security teams, and delivers great user experiences. Our built-in approach delivers a frictionless experience for end-users, ensuring everyone can get their job done securely regardless of where they work and which tools they use. We also provide your security team with AI and automated capabilities to cut through the noise and eliminate repetitive tasks, so they can focus on what matters with speed and accuracy. Microsoft's comprehensive solution also integrates across the ecosystem by connecting all of your identities, devices, apps, and clouds to help you close gaps in coverage, reduce risk, and simplify your portfolio.

Life as a Microsoft intern

Our interns work on projects that matter—and teams will rely on your skills and insights to help deliver those projects to market. You'll get the opportunity to work on real projects and have fun along the way. Join Microsoft today, and help us shape the business of tomorrow.

<https://careers.microsoft.com/students/us/en>

Stop by the Microsoft booth at the career fair for your chance to win a set of Surface headphones.



RIT | Golisano College of Computing and Information Sciences

Department of Computing Security



The Department of Computing Security (CSEC) advances the state of the art in cybersecurity and provides students with the education they need to launch their careers as world-class cybersecurity professionals. CSEC students get a hands-on education in how to protect computers, networks, and data, and they take that into the world through co-op opportunities with industry leaders and security competitions. Students also work alongside expert faculty to investigate protecting connected cars, defending wireless communications in the Internet of Things, improving online privacy, and many other ways to secure our world.

Established in 2012 as one of the first academic units in the nation, the Computing Security Department at RIT consists of 16 full-time faculty. The department has about 400 students pursuing a Bachelor of Science in Computing Security, 60 students pursuing a Master of Science in Computing Security, and about 10 Ph.D. students with research focused in cybersecurity.

Study BS, MS, and PhD in Computing Security at RIT!
<http://csec.rit.edu>

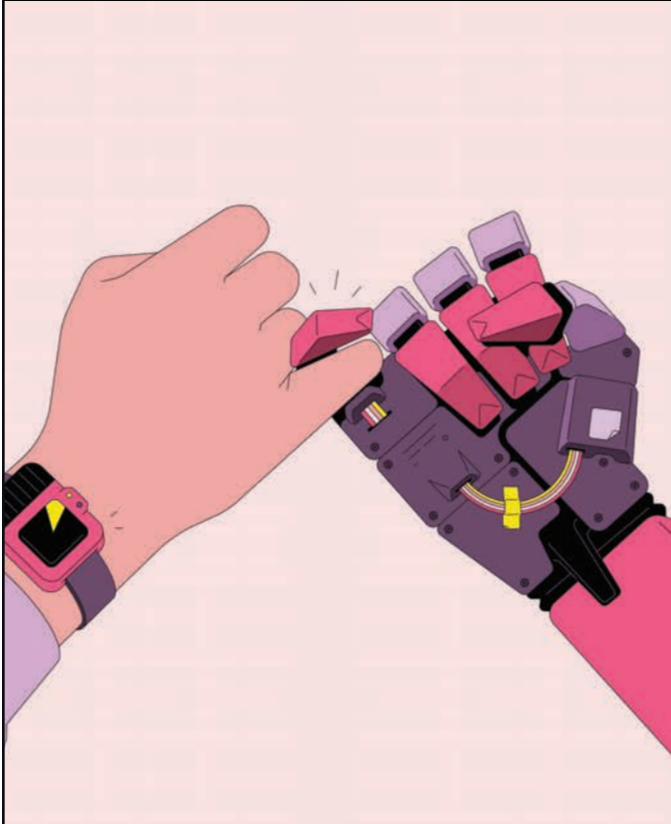
ADVANCE YOUR SKILLS. ADVANCE YOUR CAREER.

Master of Computer Science
Online Program



MCS@RICE
Computer Science

rice.edu/cyber




Robinhood is on a mission to make financial services accessible to everyone, not just the wealthy few.

Building secure products and services is a core component of our mission. We believe a security-minded culture with a strong emphasis on engineering, automation, and diversity of thought is the only way to get there. Come join our Security Engineering team and help us secure the financial services of the future.

<https://careers.robinhood.com>

Robinhood Markets, Inc. 1074091









#1
COMPANIES THAT CARE
3 YEARS IN A ROW!
People, 2019

**ONE OF THE WORLD'S
BEST WORKPLACES
3 YEARS IN A ROW**
Great Place to Work, 2019

#2
ON THE FORTUNE
"100 BEST COMPANIES
TO WORK FOR®"
2019 LIST

Transform *your* everyday.




SYNOPSYS®

Software Integrity Group

**Ignite your passion
for security at Synopsys.**


Visit us at booth #302 to learn more;
we can't wait to meet you!

#lifeatsynopsys


<http://synopsys.com/careers>

At Walmart, we work hard to ensure our team's success through passion and engagement.

We have a feeling you will fit right in.



Join us at careers.walmart.com



Why Walmart Information Security?

TECHNOLOGY
Our mission is to protect critical data by delivering the most advanced innovation and technology to secure our environment.

CAREER GROWTH
We'll help you grow your career by understanding your passions and strengths to enable professional development to achieve your personal career goals.

TRAINING & EDUCATION
We offer training and industry recognized certifications so you can stay knowledgeable and current while preparing for the future.

COMMUNITY
We support community involvement by enabling teams and associates to give back to the community through Walmart funded programs.

Hiring Needs

- Access Control Engineers
- Identity Engineers
- Endpoint Engineers
- Cloud Security Engineers
- Security Testing
- Forensics Engineers
- SIEM Engineers
- Cyber Intelligence Engineers
- Network/Internet Engineers
- Cryptology Engineers
- Risk Analysts
- Project Management
- Security Analytics
- Incident Response
- Compliance (SOX, HIPAA, PCI)

VISA everywhere
you want to be



2020 WiCyS CONFERENCE NOTES

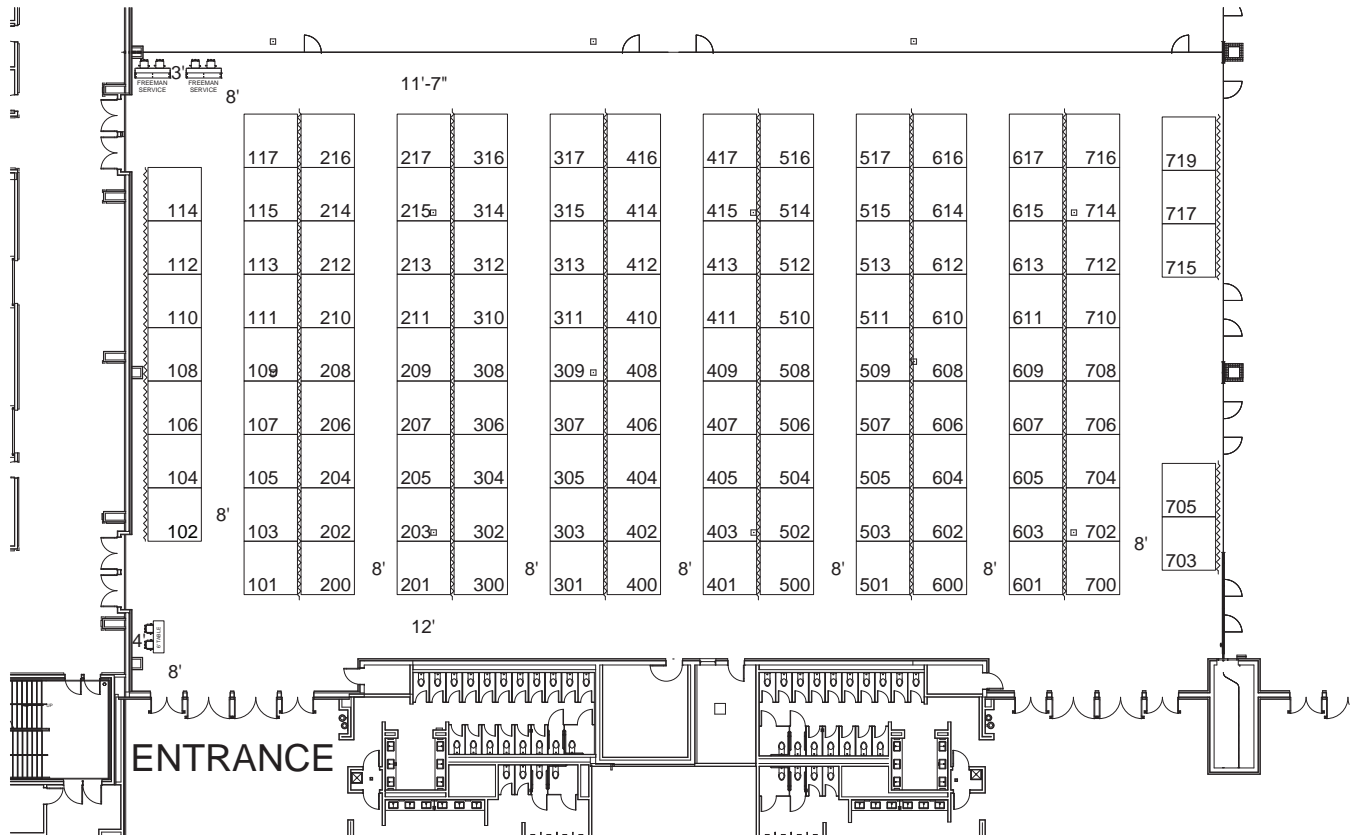
[illegible]

2020 WiCyS CONFERENCE NOTES

This image shows a full page of blank, lined paper. It features approximately 20 evenly spaced horizontal grey lines across its entire width, providing a guide for handwriting or typing. The paper itself is a clean, off-white color.

[illegible]

VISIT THE CAREER FAIR



EVENTS, PRIZES, TRAVEL AWARDS AND SPECIAL ITEMS SPONSORS - WiCyS THANKS YOU!

Amazon	Selfie Station & PJ, Travel Awards
Carnegie Mellon University - SEI	Selfie Station
Cisco	Conference Bags, Travel Awards
Denso	Mobile App
Department of State	Breaks, Charging Station, Travel Award
Facebook	Travel Awards
Google	Travel Awards
Mastercard	Travel Awards
MSU Denver	Headshots
Optum	Conference Shirts, Travel Awards
Palo Alto Networks	Travel Awards
Raytheon	Travel Awards
Salesforce	Career Village Funding
State Farm	Travel Awards
University of Arizona	Travel Awards
Verizon	Travel Awards
Workday	Lanyards

2020 WiCyS CONFERENCE

VENUE MAPS

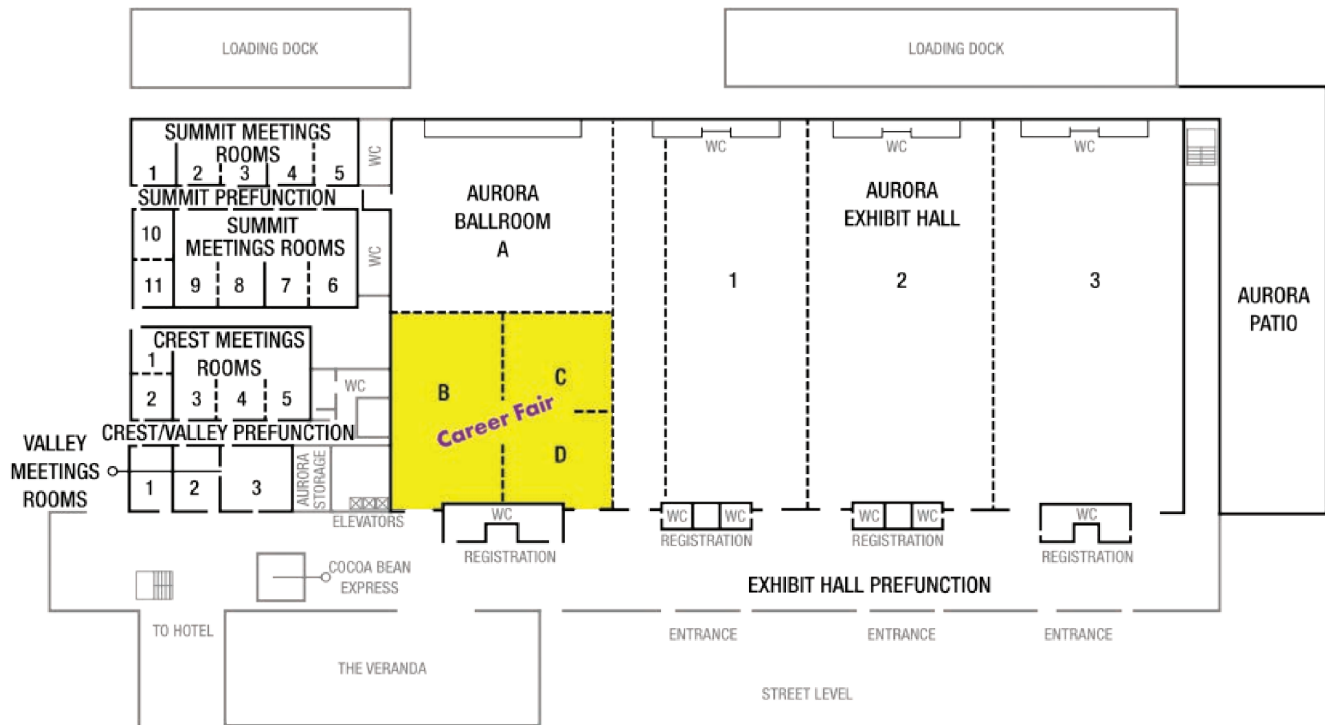
CONVENTION CENTER LEVEL 1



2020 WiCyS CONFERENCE

VENUE MAPS

AURORA BALLROOM / EXHIBIT HALL AND MEETING ROOMS LEVEL 2





WiCyS.ORG

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.