

# 2022 WiCyS CONFERENCE

March 17-19  
Cleveland, OH



#WiCyS2022



*VIP Sponsors*



# TABLE OF CONTENTS

- Welcome . . . . .3
- Board of Directors . . . . .3
- Keynote Speakers . . . . .4-5
- Thanks To Sponsors . . . . .6
- Thanks to Committee Members . .8-11
  
- Track and Session Guide . . . . . 12
- Schedule at a Glance. . . . . 13
- Thursday Agenda . . . . . 14-15
- Friday Agenda . . . . . 17-19
- Saturday Agenda . . . . . 21-23
  
- Meet-Ups . . . . . 25
- Workshop Descriptions . . . . .26-31
- Presentation Descriptions . . . 32-36
- Birds of a Feather Descriptions . . 37
- Panel Sessions . . . . . 38-39
- Lightning Talk Descriptions . . 40-42
- Student Poster Descriptions . . 43-52
  
- Sponsor Ads . . . . . 53-63
- Career Fair Booths. . . . . 64
- Venue/Room Maps . . . . . 67-70

## BADGE PICK-UP HOURS

|                 |                        |
|-----------------|------------------------|
| <b>THURSDAY</b> | <b>7:00am - 7:00pm</b> |
| <b>FRIDAY</b>   | <b>7:00am - 6:00pm</b> |
| <b>SATURDAY</b> | <b>7:00am - 9:00am</b> |

### USE THE APP

#### Boost Your Experience

Have you explored the WiCyS Conference App? After downloading the Whova app to your mobile device, use the email address you used to register for the conference to sign in. You can browse the agenda, view speakers and sponsors, connect with other attendees, and ask conference-related questions by sending a message to “Ask Organizers Anything” in the community section.



Scan the code with your mobile device to download the app.

**APP CODE: 2022SeeHerAsEqual**

### SOCIAL MEDIA CONTEST

#### Win WiCyS Prizes!

Be the voice of women in cybersecurity by sharing key takeaways during the conference using the **#WiCyS2022** hashtag.

Showcase the incredible and powerful talent you encounter during the conference on Twitter and Instagram using the **#WiCyS2022** hashtag to get entered to win WiCyS store prizes or a WiCyS 2023 Scholarship.

**Winners will receive a DM on social media or an email after the conference.**



### SNAPCHAT FILTER



#### Use Our Custom Snapchat Filter!

Make sure your location services are on and your Snapchat app is fully updated. Open Snapchat and take a picture, then swipe left or right to add some flare to your conference posts with the custom **#WiCyS2022** filter.



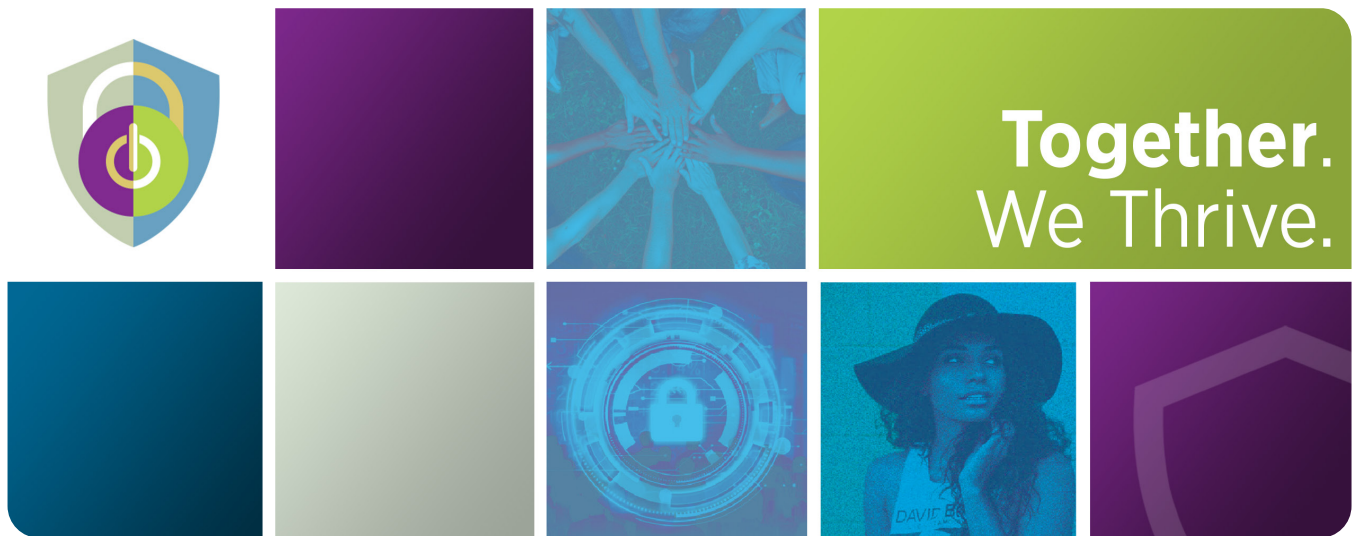
# WELCOME TO THE 9TH ANNUAL WiCyS CONFERENCE

Welcome to WiCyS 2022! How wonderful to once again be able to join as a community to learn and network. Whether this is your first conference or you have attended a previous WiCyS conference, be ready for a packed agenda. Take advantage of all the conference has to offer. Be bold and step out of your comfort zone over the next few days. Introduce yourself to others, try new things, and make a commitment to continue learning and move your career forward. You are part of the community that makes WiCyS strong.

We all welcome you as your authentic selves, here to connect and collaborate while making steady progress on impacting diversity in cybersecurity. A warm and heartfelt thanks to all the hundreds of volunteers that helped make WiCyS 2022 possible and I look forward to meeting many of you over the next few days!

## Janell Straach

*WiCyS Conference Chair and Chair of the Board*



## WiCyS BOARD OF DIRECTORS

### Dr. Ambareen Siraj

*WiCyS Founder & Secretary of the Board, Director/Cybersecurity Education, Research and Outreach Center; Professor/CS, Tennessee Tech*

### Dr. Janell Straach

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

### Dr. Costis Torgas

*Board Treasurer, WiCyS Director, Cyber Security and Privacy Research Institute, George Washington University*

### Dr. Dawn M. Beyer

*Senior Fellow, Lockheed Martin Space*

### Jenn Henley

*Vice President, Infrastructure at Facebook*

### Prajakta Jagdale

*Senior Manager, Information Security, Palo Alto Networks*

### Diana Kelley

*Founder and CTO, Security Curve*

### Jay Koehler

*Software Engineering Manager, AI Services, Red Hat*

### Marian Merritt

*Deputy Director/Lead, Industry Engagement of the National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology (NIST), U.S. Department of Commerce*

### Allison Miller

*CISO and Senior Vice President, UnitedHealth Group/OPTUM*

### Noureen Njorge

*Director, Global Cyber Threat Intelligence, Nike, Inc.*

### Dr. Greg Shannon

*Chief Cybersecurity Scientist, Idaho National Laboratory and Chief Science Officer, Cybersecurity Manufacturing Innovation Institute*

# 2022 WiCyS CONFERENCE

## KEYNOTE SPEAKERS



### Latanya Sweeney

Daniel Paul Professor of the Practice of Government and Technology,  
Harvard University

*“How Technology Will Dictate Our Civic Future”*

Latanya Sweeney pioneered the field known as data privacy, launched the emerging area known as algorithmic fairness, and her work is explicitly cited in government regulations worldwide, including the U.S. federal medical privacy regulation (known as HIPAA). She is a recipient of the prestigious Louis D. Brandeis Privacy Award, the American Psychiatric Association’s Privacy Advocacy Award, and has testified before government bodies worldwide. She earned her PhD in computer science from MIT in 2001; the first Black woman to do so.



### Jen Easterly

Director, Cybersecurity & Infrastructure Security Agency

*“Empowering the Next Generation of Women Cybersecurity and Tech Pioneers”*

\*Joining Virtually

Jen Easterly is the Director of the Cybersecurity and Infrastructure Security Agency (CISA). Ms. Easterly was nominated by President Biden in April 2021 and unanimously confirmed by the Senate on July 12, 2021. As Director, Ms. Easterly leads CISA’s efforts to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every day. Before serving in her current role, Ms. Easterly was the head of Firm Resilience at Morgan Stanley, responsible for ensuring preparedness and response to business-disrupting operational incidents and risks to the Firm.

Ms. Easterly has a long tradition of public service, to include two tours at the White House, most recently as Special Assistant to President Obama and Senior Director for Counterterrorism. She also served as the Deputy for Counterterrorism at the National Security Agency.

A two-time recipient of the Bronze Star, Ms. Easterly retired from the U.S. Army after more than twenty years of service in intelligence and cyber operations, including tours of duty in Haiti, the Balkans, Iraq, and Afghanistan. Responsible for standing up the Army’s first cyber battalion, Ms. Easterly was also instrumental in the design and creation of United States Cyber Command.

A distinguished graduate of the United States Military Academy at West Point, Ms. Easterly holds a master’s degree in Philosophy, Politics, and Economics from the University of Oxford, where she studied as a Rhodes Scholar. She is the recipient of the James W. Foley Legacy Foundation American Hostage Freedom Award and the Bradley W. Snyder Changing the Narrative Award.

A member of the Council on Foreign Relations and a French-American Foundation Young Leader, Ms. Easterly is the past recipient of numerous fellowships, including the Aspen Finance Leaders Fellowship, the National Security Institute Visiting Fellowship, the New America Foundation Senior International Security Fellowship, the Council on Foreign Relations International Affairs Fellowship, and the Director, National Security Agency Fellowship.

# 2022 WiCyS CONFERENCE KEYNOTE SPEAKERS



## Allison Miller

Chief Information Security Officer and Senior Vice President, Optum

*“Walking in Fire”*

Allison Miller serves as the Global Chief Information Security Officer and Senior Vice President for Optum, a division of UnitedHealth Group. In addition to global cybersecurity, Allison has over 20 years of experience in health information systems and crisis management; serving as the Chief Privacy Officer of OptumHealth, Deputy Chief Privacy Officer for UnitedHealthcare and continues as a volunteer EMT serving global communities impacted by disasters.



## Anna Squicciarini

Frymoyer Professor and Cyber Area Chair, Pennsylvania State University

*“Cyber Security Research in Interdisciplinary Units, Challenges and Opportunities”*

Dr. Squicciarini received the Ph.D. degree in computer science from the University of Milan, Milan, Italy, in February 2006. She is currently an Associate Professor in the College of Information Sciences and Technology, Pennsylvania State University, University Park, PA. Since 2019, Squicciarini currently also the Cyber Security Area in the College of IST. During 2006–2007, she was a Postdoctoral Research Associate at Purdue University, West Lafayette, IN.

Dr. Squicciarini is a Fulbright Scholar for US-UK Cybersecurity program. Squicciarini main research interests are in the area of data security and privacy, with emphasis on access control mechanisms. Squicciarini’s work currently focuses on data privacy and on the development of applied machine learning methods for scalable user-centered privacy protection. Further, she applies machine learning models and game theoretic algorithms toward detection and understanding of online deviance. Squicciarini’s work has been funded by industry and various funding agencies, including grants from the National Science Foundation (and a CAREER Award, 2015), Air Force, and Army Research Office.

Squicciarini’s work has also been supported by Google and Hewlett-Packard Research Labs. Squicciarini published more than 80 contributions as papers in international conferences and journals, and she is associate editor for three IEEE and two ACM Transactions. She has supervised several Ph.D. and Master theses since joining Penn State.

## WICYS KEYNOTES



Enjoy the WiCyS 2022 Keynotes? Subscribe to the WiCyS Youtube channel to watch them post-conference. Scan the code with your mobile phone camera to access.



# THANK YOU TO OUR 2022 CONFERENCE SPONSORS

## VIP SPONSORS



## PREMIUM SPONSORS



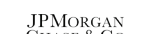
## DIAMOND SPONSORS



## PLATINUM SPONSORS



## GOLD SPONSORS



## SILVER SPONSORS



# Make the difference.

At Bloomberg, we use the power of technology to bring clarity to a complex world. In a career here, you'll help protect products that our global customers rely on to make critical financial decisions. We work on purpose.

Come find yours.  
[bloomberg.com/careers](https://www.bloomberg.com/careers)

**Bloomberg**



| 90  | Go to Restore Original Defaults |                 |                 |               |         |           |         |
|---|---------------------------------|-----------------|-----------------|---------------|---------|-----------|---------|
| Basket  | Major                           | Last Price      | Rate            | BID           |         |           |         |
| Source  | BGN                             | % Change        | Outrights       | Points        |         |           |         |
| 10) Spot  | 3) Forward                      | 12) Bid         | Heat Map        |               |         |           |         |
| USD   | JPY                             | GBP             | CHF             | CAD           | AUD     | NZD       |         |
| 1.0729  | 107.45                          | 0.9760          | 12.804          | 0.8526        | 0.8558  | 0.8538    | 0.8425  |
|   | 1.6724                          | -0.1183         | 1.9927          | 1.3777        | 1.0670  | 1.0682    |         |
|   | 1.5656                          | -0.1107         | 1.8655          | 1.2898        | 0.9884  |           | 0.93615 |
| GBP   | 1.5674                          | -0.1109         |                 | 1.2913        |         |           | 0.93724 |
| CHF   | 1.2139                          | -0.0859         |                 |               | 0.77444 | 0.74      | 0.72582 |
| JPY   | 107.027                         | 0.83926         | 0.9396          | 10137         | 0.8543  | 0.805     | 0.80182 |
| EUR   | 141.40                          |                 | 116.48          | 90.208        | 0.312   | 0.312     | 0.312   |
| USD   |                                 | -0.0707         | 1.1915          | 82379         | 63798   | 0.872     | 0.872   |
|   | 1.6582                          | 0.029           | 1.6494          | 0.852         | 0.852   | 0.852     | 0.852   |
| % Change on Day Range                                     |                                 |                 |                 |               |         |           |         |
| Below -2.5%   | -0.5% to -2.5%                  | -0.05% to -0.5% | -0.05% to 0.05% | 0.05% to 0.5% |         |           |         |
| Rates are from Composite where Bloomberg Bid is available |                                 |                 |                 |               |         |           |         |
| * 9) WB: Regional Market, 10 Year, Ask, 3 Months          |                                 |                 |                 |               |         |           |         |
| Country   | CHI                             | Security        | Price           | Chg           | Yield   | Chg Yield | LC      |
| Americas  |                                 |                 |                 |               |         |           |         |
| United States   |                                 | T 2 % 02/24     | 99.29%          | 0.0%          | 2.5%    | 0.0%      | 2.5     |
| Canada  |                                 | CAN2 % 06/24    | 100.255         | -0.641        | 2.3%    | -0.001    | 2.3     |
| Brazil (USD)  |                                 | BRAZIL4 % 25    | 96.750          | -0.850        | 4.636   | -0.001    | 4.5     |
| Colombia (U...)   |                                 | COLOM 4 % 02/24 | 96.795          | -0.410        | 4.140   | -0.001    | 4.0     |
| Mexico (USD)  |                                 | MEX4 10/02/23   | 101.325         | -0.610        | 3.803   | -0.001    | 3.7     |
| EMEA  |                                 |                 |                 |               |         |           |         |
| United Kingdom  |                                 | UKT2 % 09/23    | 96.3050         | -0.005        | 3.995   | -0.001    | 3.9     |
| France  |                                 | FRF2 % 09/23    | 100.015         | -0.005        | 3.995   | -0.001    | 3.9     |

# THANK YOU TO OUR 2022 WiCyS COMMITTEES

## CONFERENCE PROGRAM CHAIR

### Ambareen Siraj

*WiCyS Founder & Secretary of the Board, Director/Cybersecurity Education, Research and Outreach Center; Professor/CS, Tennessee Tech University*

## CONFERENCE GENERAL CHAIR

### Janell Straach

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

## PROGRAM

### Chutima Boonthum-Denecke

*Co-Lead  
Professor/Director of IAC,  
Hampton University*

### Jennifer Cheung

*Co-Lead  
Cybersecurity Research Scientist,  
NWIC Pacific*

### Meg Layton

*Co-Lead  
Security Architecture and Engineering,  
Children's National Hospital*

### Celeste Matarazzo

*Co-Lead  
Cybersecurity Researcher,  
Lawrence Livermore National  
Laboratory*

### Kelley Misata

*Co-Lead  
Founder and CEO/President,  
Sightline Security/OISF*

### Ridhima Agarwal

*Attack Analyst, JPMorgan Chase & Co.*

### Md. Ahsan Ayub

*Graduate Research Assistant and Ph.D.  
Student, Cybersecurity Education,  
Research & Outreach Center (CEROC)*

### Priyam Biswas

*Offensive Security Researcher, Intel*

### Rachael Crowthers

*Senior Information Security Engineer,  
Optum*

### Melissa Dark

*Founder,  
TeachCyber - DARK Enterprises Inc*

### Esther Goldstein

*Software Engineer, Data Security,  
Salesforce*

### Ashley Greeley

*K12 Project Lead, NSA*

### Courtney Hammond

*Advanced Cyber Security Architect/  
Engineer, Honeywell*

### Judy Hatchett

*VP, CISO, Surescripts, LLC*

### Hanan Hibshi

*Assistant Teaching Professor,  
Carnegie Mellon University, The  
Information Networking Institute*

### Iulia Ion

*Engineering Manager, Google*

### Susan Jeziorowski

*Applied Cybersecurity Engineer, MITRE*

### Paige Kevnick

*Senior Security Analyst,  
Spectrum Health*

### Betsy Lundsten

*Information Security Consultant,  
Securian Financial*

### Evette Maynard-Noel

*Associate Chief, Cybersecurity &  
Infrastructure Security Agency*

### Elena Peterson

*Senior Cyber Security Researcher,  
Pacific Northwest National Laboratory*

### Sarba Roy

*Governance Product Security Engineer,  
Intel Corporation*

### Miranda Skar

*Penetration Tester,  
Aon - Gotham Digital Science*

### Shirley Tian

*Assistant Professor,  
Kennesaw State University*

### Junia Valente

*Red Team Consultant, BlackBerry*

### Shafia Zubair

*Manager, Information Security  
Morningstar*

## SOCIAL MEDIA & PR

### Aditi Chaudhry

*Lead  
Cybersecurity Engineer,  
Two Sigma*

### Maddie Witt

*Lead  
Social Media Specialist, WiCyS*

### Chelsea Conard

*Consultant for Strategy, Risk, and  
Compliance, Kudelski Security*

### Midori Connolly

*Customer Success Manager,  
Yubico*

### Lana Richardson

*Community Care Manager,  
WiCyS*

### Alina Thai

*Threat Intelligence Analyst,  
Allstate*



# THANK YOU TO OUR 2022 WiCyS COMMITTEES

## CLEVELAND CONFERENCE SUPPORT CONSORTIUM (WCCSC)

### Hannah Fritzman Belsito

Chief Experience Officer,  
Destination Cleveland

### Jeffrey Brancato

Executive Director,  
Northeast Ohio CyberConsortium

### Courtney DeOreo

Executive Director, RITE / Sr. Director,  
Tech Talent, Greater Cleveland  
Partnership

### Jay P. Foran

Senior Vice President, Industry &  
Innovation, Team NEO

### Crystal Franklin

Director, K-12 Computer Science  
Education, CSforCLE,  
Cleveland State University

### Shilpa Kedar

Executive Director, CSU T.E.C.H.  
Hub & Co-Executive Director, IoT  
Collaborative, Cleveland State  
University

### Chelsey Kohn

Director, Tech Talent Pipeline,  
Cleveland Metropolitan School District  
& Cleveland State University

### Janine Spears

CSU Faculty Lead for WiCyS CLE,  
Assoc. Professor/CyberSecurity,  
Cleveland State University

## SCHOLARSHIP

### Gretchen Bliss

Director Cybersecurity Programs,  
University of Colorado Colorado  
Springs

### Stacie Bohanan

President, WiCyS Northern AL Affiliate,  
University of Alabama in Huntsville

### Sharon Finden

Senior TPM, Microsoft

### Sharon Hamilton

Associate VP, Strategic Partnerships,  
Norwich University

### Durba Kabir

Technical Manager, NSA

### Sofia Martinez

Pre-College Program Assistant, IT &  
Cybersecurity Student,  
Illinois Institute of Technology

### Danelle Mattison

Cyber System Security Engineer, SR,  
Lockheed Martin

### Sharon Mireku

Executive Paralegal-Independent  
Contractor, Law Firms-Both Private and  
Corporate Environments

### Quintana Patterson

Compliance and Security Analyst,  
University of Colorado Anschutz  
Medical Campus

### Jeff Pelzer

Assistant Professor,  
Hillsborough Community College

### Elizabeth Rasnick

Faculty, Georgia Southern University

### Penelope Rozhkova

Cybersecurity Consultant, Self

### Reshma Shahabuddin

Director of Program Management,  
Sophos

### Julie Agnes Sparks

Security Engineer, Cloudflare

### Mary Wallingsford

Associate Professor,  
Anne Arundel Community College

## OPERATIONS AND LOGISTICS

### Lynn Dohm

Executive Director, WiCyS

### Peter Baldwin

vCFO, WiCyS

### Tia DeBord

Registration Liaison, Globaux Source

### Morgan Garland

Operations Manager, WiCyS

### Colleen Huber

Creative Director, The Nelly Group

### Kimberly Hutcherson

Meeting Space Coordinator,  
Globaux Source

### Pat McCain

Presenter Liaison, Globaux Source

### Lana Richardson

Community Care Manager, WiCyS

### Jessica Robinson

vCISO, WiCyS

### Myriam Saint Jean

Financial Manager, WiCyS

### Michele Tomasic

Director of Operations,  
Software Engineering Institute | CERT,  
Carnegie Mellon University

# THANK YOU TO OUR 2022 WiCyS COMMITTEES

## CAREER VILLAGE

### Andrea Frost

Lead  
Senior Software Security  
Engineer, Dell EMC

### Kim Huynh

Security Program Manager,  
Research and Threat  
Intelligence at Microsoft

### Michelle Linblom

Security Awareness  
Manager, Salesforce

### Elaine G. Suarez

Career Development &  
Exploration,  
Cleveland State University

## CAREER FAIR

### Mary Jane Partain

Career Fair Concierge  
Director, University of  
Texas-Dallas

### Matthew Knickman

Director, Alumni Relations  
& Corporate Engagement,  
Cleveland State University

## POSTER

### Chutima Boonthum-Denecke

Director, Info. Assurance  
and Cyber Security Center,  
Hampton University

### Maanak Gupta

Tennessee Tech University,  
Assistant Professor

### Susan Jeziorowski

Applied Cybersecurity  
Engineer, MITRE

## VOLUNTEER

### Cameron Mitchell

Carnegie Mellon University,  
Software Engineering  
Institute

### Charquetta McCoy-Penn

Executive Assistant, WiCyS

## MENTOR/MENTEE

### Archana Ramamoorthy

Lead  
Director, Cloud Security  
Product Manager, Google

### Deborah Kariuki

Co-Lead  
Faculty, Computer Science  
Ed, UMBC

## CYBERSECURITY STEERING COMMITTEE

### Ambareen Siraj

WiCyS Founder, Director, Cybersecurity  
Education, Research and Outreach  
Center, Tennessee Tech University

### Pj Jagdale

Senior Manager, Information Security,  
Palo Alto Networks

### Diana Kelley

Founder and CEO, SecurityCurve

### Allison Miller

Chief Information Security Officer and  
Senior VP, UnitedHealth Group/Optum

### Meghan Jacquot

Risk Assessment Cybersecurity  
Engineering, Cyber Future Foundation

### Kelley Misata

Founder and CEO, Sightline Security

### Noureen Njoroge

Director of Global Cyber Threat  
Intelligence, Nike, INC.

### Quintana Patterson

Compliance and Security Analyst,  
University of Colorado Anschutz

### Jessica Robinson

vCISO, WiCyS

## RESOURCES

### Lisa Ellrodt

Lead  
Faculty Advisor, Pace University

### Sri Bhamidipati

Technical Staff, Verizon Wireless

### Madeline Estey

Student, Kent Place School

### Maxine Franks

Application Security Agent,  
University Of Nevada Las Vegas

### Meghan Jacquot

Risk Assessment Cybersecurity  
Engineering, Cyber Future Foundation

### Catherine Miri

Student, Savio High School

### Catherine Wairachu

Ait Security And Assurance,  
Towson University

### Anna Yap

Project Manager, Index Analytics LLC

## STUDENT CHAPTER LEADS

### Vitaly Ford

WiCyS Chapter Coordinator  
Assistant Professor,  
Arcadia University

### Pauline Mosley

Assistant Professor,  
Pace University

## PROFESSIONAL AFFILIATE LEADS

### Lynn Dohm

Executive Director,  
WiCyS

### Lana Richardson

Community Care Manager,  
WiCyS

# THANK YOU TO OUR 2022 WiCyS COMMITTEES

## MISSION SUPPORT TEAM

### Felice Ajlouny

VP, Talent Acquisition, Diversity & Inclusion, SentinelOne

### Dawn Beyer

Senior Fellow, Lockheed Martin

### Susan Bullwinkel

Director, Business Delivery Enablement, Enterprise Information Security, Optum

### Valerie Jane Chua

Program Manager, Security Learning & Awareness, Facebook

### Greg Connell

Project Engineer Sr. Stf, Corporate Information Security, Lockheed Martin

### Allie Decrastrro

Program Manager, Global Enablement, AWS

### Josh Dembling

Senior Director, Intel Product Assurance and Security

### Mariana Gardinali

Software Engineer, Cisco

### Meg Gerdes

Senior Tech Project Manager, Business Delivery Enablement, Optum

### Divya Ghatak

Chief People Officer, SentinelOne

### Jenn Henley

Vice President, Infrastructure, Facebook

### Tracey Hilton

Senior Program Manager, Facebook

### Ann Johnson

Corporate Vice President, Microsoft

### Allison Miller

Chief Information Security Officer And Senior VP, Unitedhealth Group/Optum

### Val Miller

Growth Strategies, Security Events, AWS

### Cameron Mitchell

Operations Coordinator, Carnegie Mellon University- SEI

### Sarah Morales

Outreach Program Manager, Security And Privacy, Google

### Melissa Salem

Talent Program Manager, SentinelOne

### Jodi Schaubsluger

Director, Information Security, Optum

### Ashley Smyk

Principal Technical Program Manager, AWS

### Michele Tomasic

Director of Operations, Software Engineering Institute | CERT, Carnegie Mellon University

### Noelle Warburton

Director, Security and Trust Communications, Cisco

### Dasha Zenkovich

Marketing Manager, Microsoft

## RACIAL EQUITY

### Jessica Robinson

Lead vCISO, WiCyS, Founder, Pure Point International

### Sofia Martinez

Steam Facilitator, Illinois Tech Amp/ Co-Terminal Undergrad

### Alyssa Miller

Application Security Advocate, Snyk

### Jennifer Munoz

Student, Indiana University

### Noureen Njoroge

Director Of Global Cyber Threat Intelligence, Nike, Inc.

### Quintana Patterson

Compliance And Security Analyst, University Of Colorado

### Mona-Lisa Pinkney

Senior Director, Governance, Risk, Compliance & Engagement Management, Corporate Information Security, Nike, Inc.

## FINANCE

### Peter Baldwin

vCFO, WiCyS

### Dawn M. Beyer

Senior Fellow, Lockheed Martin Space

### Noureen Njoroge

Director of Global Cyber Threat Intelligence, Nike, INC.

### Miriam Saint Jean

Financial Manager, WiCyS

### Costis Toregas

Director, Cyber Security and Privacy Research Institute, George Washington University



# PROGRAM PARTICIPATION TRACKS AND SESSIONS

## CURRENT TECHNOLOGY AND CHALLENGES TRACK

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

## LOOKING AHEAD TRACK

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

## BEST PRACTICES TRACK

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

## CAREER DEVELOPMENT TRACK

Leadership and advancement.

## CPE TRACK

Sessions that provide CPE Credits.



## TECHNICAL PRESENTATIONS

Technical presentations highlight innovations, research & development projects, internships/co-ops experiences, service-learning and outreach projects, or other interesting experience related to cybersecurity. **Technical 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. The audience is students, educators, professionals and researchers (in any combination or by category). Workshops are 2 hours long. A maximum of four listed presenters. **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 in this area. **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 five-minute presentations** (with or without formal presentations) that seek 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 select appropriate panelists to participate. In addition to the moderator, there can be up to 4 panelists and **each panel is 45 minutes long.**



## STUDENT RESEARCH POSTERS

Student Research Posters provide opportunities for students to present their work for the audience at WiCyS in poster format. Winners in both undergrad and grad category receive travel support for a future security conference of choice. Runners-up also receive prizes. The first listed student will receive an automatic scholarship.

# 2022 WiCyS SCHEDULE AT A GLANCE

| TIME             | DESCRIPTION  | LOCATION                           |
|------------------|--|------------------------------------|
| <b>THURSDAY</b>  |  |                                    |
| 7:00am - 7:00pm  | Badge Pick-Up  | Exhibit Level                      |
| Noon - 9:00pm    | Coat Room  | Room 18                            |
| 12:30pm - 1:30pm | First Timer's Guide to WiCyS   | Room 26 ABC                        |
| 12:30pm - 1:30pm | Recruiters Session   | Room 9                             |
| 12:30pm - 7:00pm | Capture the Flag (CTF) Mentoring   | Rooms 21, 23                       |
| 1:30pm - 4:30pm  | Career Fair Setup  | Exhibit Hall C                     |
| 2:00pm - 4:00pm  | Workshop Series  | Various Rooms                      |
| 2:00pm - 7:00pm  | Career Village Open  | Rooms 20, 22, 24                   |
| 4:00pm - 4:30pm  | Break  |                                    |
| 4:00pm - 7:00pm  | Poster Session Check-In  | Ballroom/Exhibit Level Prefunction |
| 4:30pm - 6:30pm  | Workshop Series  | Various Rooms                      |
| 6:00pm - 7:00pm  | Social Media Ambassador Meeting  | Room 14                            |
| 7:00pm - 9:00pm  | Socials: Cleveland, Deloitte, Google, Palo Alto Networks, Raytheon & Walmart | Rooms 1 - 8                        |
| 7:00pm - 8:00pm  | Educators/Scientists - Meetup With Funding Agencies                          | Room 14                            |
| 8:00pm - 9:00pm  | Federal Scholarship (SFS/CySP) Meetup And Information Session                | Room 14                            |

| TIME              | DESCRIPTION  | LOCATION            |
|-------------------|--|---------------------|
| <b>SATURDAY</b>   |  |                     |
| 7:00am - 9:00am   | Badge Pick-Up  | Exhibit Level       |
| 7:00am - 5:00 pm  | Coat Room  | Room 18             |
| 7:00am - 8:15am   | Military Breakfast   | Room 4              |
| 7:00am - 8:00am   | Breakfast with Tables for Scholarship and Fellowship Recipients              | Ballrm. Level Pref. |
| 8:00am - 5:00pm   | Luggage Storage Available  | Room 7              |
| 8:30am - 9:30am   | Keynote  | Gr. Ballroom ABC    |
| 9:30am - 10:00am  | Picture & Break with Refreshments  | TBD                 |
| 10:00am - 10:45am | Presentation Sessions  | Various Rooms       |
| 10:00am - 10:45am | Lightning Talks  | Room 26 ABC         |
| 11:00am - 11:45am | Presentation Sessions  | Various Rooms       |
| 11:00am - 11:45am | Lightning Talks  | Room 26 ABC         |
| Noon - 12:45pm    | Panels   | Various Rooms       |
| 12:45pm - 2:00pm  | Lunch, Closing Remarks & Keynote<br><i>(must be seated by 1:00pm to eat)</i> | Gr. Ballroom ABC    |
| 2:00pm - 2:30pm   | Travel Stipend Verification  | Ballrm. Level Pref. |
| 2:30pm - 4:30pm   | Workshop Series  | Various Rooms       |
| 2:30pm - 4:30pm   | Workshop Series  | Various Rooms       |

| TIME              | DESCRIPTION  | LOCATION                           |
|-------------------|--|------------------------------------|
| <b>FRIDAY</b>     |  |                                    |
| 7:00am - 6:00pm   | Badge Pick-Up  | Exhibit Level                      |
| 7:00am - 9:00 pm  | Coat Room  | Room 18                            |
| 7:00am - 8:00am   | Breakfast with Tables for Scholarship and Fellowship Recipients          | Ballrm. Level Pref.                |
| 7:00am - 8:30am   | Poster Session Check-In  | Ballroom/Exhibit Level Prefunction |
| 8:00am - 9:00am   | Career Fair Setup  | Exhibit Hall C                     |
| 8:30am - 9:45am   | Conference Opening & Keynote   | Gr. Ballroom ABC                   |
| 9:45am - 11:45am  | Career Fair Open   | Hall C                             |
| 9:45am - 11:45am  | Capture The Flag (CTF) Mentoring   | Rooms 21, 23                       |
| 9:45am - 11:45am  | Career Village Open  | Rooms 20, 22, 24                   |
| 9:45am - 11:00am  | Student Poster Session & Networking Refreshment Break                    | Ballrm. Level Pref.                |
| 11:00am - 11:45am | Presentation Sessions  | Various Rooms                      |
| 11:00am - 11:45am | Student Chapter MeetUp   | Room 26 ABC                        |
| Noon - 1:45pm     | Lunch, Networking & Keynote<br><i>(must be seated by 12:10pm to eat)</i> | Gr. Ballroom ABC                   |
| 1:55pm - 5:30pm   | Career Fair Open   | Hall C                             |
| 1:55pm - 5:30pm   | Capture the Flag (CTF) Mentoring   | Rooms 21, 23                       |
| 1:55pm - 5:30pm   | Career Village Open  | Rooms 20, 22, 24                   |
| 1:55pm - 2:40pm   | Presentation Sessions  | Various Rooms                      |
| 1:55pm - 2:40pm   | Affiliate MeetUp   | Room 26 ABC                        |
| 2:45pm - 3:15pm   | Break with Refreshments in Career Fair                                   | Exhibit Hall C                     |
| 2:40pm - 4:40pm   | Workshop Series  | Various Rooms                      |
| 4:45pm - 5:30pm   | Birds of Feather   | Various Rooms                      |
| 6:00pm - 7:45pm   | Dinner, Networking & Keynote<br><i>(must be seated by 6:10pm to eat)</i> | Gr. Ballroom ABC                   |
| 8:00pm - 9:00pm   | Racial Equity Committee Meet & Greet                                     | Room 7                             |
| 8:30pm - midnight | Capture the Flag (CTF) After Dark Party                                  | Rooms 21, 23                       |

PICK-UP AND PURCHASE  
**WiCyS GEAR**

Visit Room 12 for the WiCyS Store

**THURSDAY 11:00am - 7:00pm**

**FRIDAY 9:45am - 6:00pm**

**SATURDAY 7:00am - Sellout**

# 2022 WiCyS SCHEDULE

## THURSDAY AGENDA

| TIME             | DESCRIPTION   | LOCATION                                  |
|------------------|---|---|
| 7:00am - 7:00pm  | Badge Pick-Up   | Exhibit Level                             |
| 11:00am - 7:00pm | WiCyS Store Open  | Room 12                                   |
| Noon - 9:00pm    | Coat Room   | Room 18                                   |
| 12:30pm - 1:30pm | <b>Your 1st Time at WiCyS? Join Us For Insiders' Tips for Navigating WiCyS!</b><br>Elizabeth K. Hawthorne, <i>Rider University</i> ; Kim Huynh (@alilbyte), <i>Microsoft</i> ;<br>Felicia Jackson, <i>Raytheon</i> ; Marena Soulet, <i>Tennessee Technological University</i> ;<br>Laura Sturgeon, <i>Smoothstack/Bloomberg</i> ; Comfort Uduebholo, <i>Amazon Web Services</i> | Room 26 ABC                               |
| 12:30pm - 1:30pm | <b>Recruiters Session: Developing and Acquiring Security Talent in a Competitive Industry</b><br>Heather Rustin, Gary Simms (@SrSimms), and Anelda Venter, <i>Walmart</i><br><b>(CPE CREDITS: 1)</b>  | Room 9                                    |
| 12:30pm - 7:00pm | Capture the Flag (CTF) Mentoring Available  | Rooms 21,23                               |
| 1:30pm - 4:30pm  | Career Fair Setup   | Exhibit Hall C                            |
| 2:00pm - 4:00pm  | <b>Workshop Series</b> (5 Concurrent)   |   |
|                  | <b>SEED Labs: Hands-on Labs for Cybersecurity Education</b><br>Wenliang (Kevin) Du, <i>Syracuse University</i><br><b>(CPE CREDITS: 2)</b>   | Room 9                                    |
|                  | <b>Get Smarter About the Dumb Protocols on Our Networks!</b><br>Terri Johnson (@tarot03), <i>Pikes Peak Community College</i> ; Keith Nabozny (@keithnab), <i>Macomb Community College</i><br><b>(CPE CREDITS: 2)</b>   | Room 15                                   |
|                  | <b>Enabling Security-by-Design for Cyber Physical Systems Using Threat Modeling</b><br>Deveeshree Nayak, <i>University of Washington Tacoma</i> ; Sarba Roy, <i>Intel Corp.</i><br><b>(CPE CREDITS: 2)</b>  | Room 16                                   |
|                  | <b>"Incident Response Exercises are Fun" and Other White Lies</b><br>Patrice Siravo, <i>Adriano Cyber Consulting</i><br><b>(CPE CREDITS: 2)</b>   | Room 25 ABC                               |
|                  | <b>Breaking into the Field of Ethical Hacking: An Intro to the Field and Core Skills</b><br>Lauren Provost (@ethicalhacks), <i>Norwich University</i><br><b>(CPE CREDITS: 2)</b>  | Room 26 ABC                               |
| 2:00pm - 7:00pm  | Career Village Open   | Rooms 20,22,24                            |
| 4:00pm - 4:30pm  | Break   |   |
| 4:00pm - 7:00pm  | Poster Session Check-In   | Ballroom/<br>Exhibit Level<br>Prefunction |

TO OUR LOCAL HOST,  
**THANK YOU!**

Cleveland Consortium led by Cleveland State University



**CLEVELAND STATE  
UNIVERSITY**



# 2022 WiCyS SCHEDULE

## THURSDAY AGENDA

| TIME            | DESCRIPTION  | LOCATION    |
|-----------------|--|-------------|
| 4:30pm - 6:30pm | <b>Workshop Series</b> (5 Concurrent)  |             |
|                 | <b>Breaking In: Smart Home</b><br>Samantha Chaves and Chesleah Kribs (@hederahacks), Carnegie Mellon University Software Engineering Institute<br>(CPE CREDITS: 2)   | Room 9      |
|                 | <b>The Eight Sins: Mitigation of Security Weaknesses in Automated Configuration Management</b><br>Farhat Lamia Barsha and Akond Rahman (@akondrahman), Tennessee Technological University<br>(CPE CREDITS: 2)                                  | Room 15     |
|                 | <b>How to Draft Strong Cybersecurity Policy</b><br>Jael Lewis and Cara Turbyfill, Walmart<br>(CPE CREDITS: 2)  | Room 16     |
|                 | <b>Into The Breach: Rehearsing and Role-Playing Breach Responses</b><br>Molly Cooper, Ferris State University; Peter Dillman (@DillmansDungeon), Dillman's Dungeon<br>(CPE CREDITS: 2)   | Room 25 ABC |
|                 | <b>Let's Start an R-IoT: A Workshop on the Modern Threat Landscape Facing the Internet of Things</b><br>Sara Friedfertig, Arctic Wolf; Anders Horrocks, Optiv; Alexis Merritt (@ReckedExe), Cisco Talos Intelligence Group<br>(CPE CREDITS: 2) | Room 26 ABC |
| 6:00pm - 7:00pm | Social Media Ambassador Meeting  | Room 14     |
| 7:00pm - 8:00pm | Educators/Scientists - Meetup With Funding Agencies  | Room 14     |
| 7:00pm - 9:00pm | <b>Socials:</b> Cleveland, Deloitte, Google, Palo Alto Networks, Raytheon, Walmart, and Wayfair  | Rooms 1 - 8 |
| 8:00pm - 9:00pm | Federal Scholarship (SFS/CySP) Meetup and Information Session  | Room 14     |

### CAREER VILLAGE

Located in Rooms 20, 22, 24  
 Thursday | 2:00pm - 7:00pm  
 Friday | 9:45am - 11:45am & 1:55pm - 5:30pm

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 purpose  
to new levels.

**200K**

team members  
collaborating  
worldwide

**222M**

people in our  
consumer  
database

**100K+**

physicians &  
health care  
locations served

**\$3.5B**

spent yearly on  
technology &  
innovation

**Starting your career in Cybersecurity?** Consider the Technology Development Program (TDP) at Optum, part of the UnitedHealth Group family of businesses — a one-year, rotational and development program where you'll be mentored by senior leaders and collaborate with talent in Cybersecurity, Software Engineering, Data, Architecture, Infrastructure and Operations, Engineering and UX/UI.

You won't just use technology to help millions receive care, you'll evolve it. From the most advanced development tools and methodologies to the highest levels of cybersecurity, we're creating, sharing and learning new ways to make technology and health care work better every day. Join us and you'll be challenged to do **your life's best work.**<sup>SM</sup>

Apply here: [workatoptum.com](https://workatoptum.com)

UnitedHealth Group (UHG) requires all U.S.-based employees working outside of their homes (i.e., full time, temporary, per diem, and in locum tenens workers; or other worker types who either interact with other co-workers, worksites, clients or customers; or provide care to patients, members or consumers) to be fully vaccinated or receive an accommodation for a medical disability or sincerely held religious belief.

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. © 2022 Optum Health & Technology. All rights reserved.

# 2022 WiCyS SCHEDULE

## FRIDAY AGENDA

| TIME              | DESCRIPTION  | LOCATION                                  |
|-------------------|--|---|
| 7:00am - 6:00pm   | Badge Pick-Up  | Exhibit Level                             |
| 7:00am - 9:00pm   | Coat Room  | Room 18                                   |
| 7:00am - 8:00am   | Breakfast Available with Tables for Scholarship and Fellowship Recipients  | Ballrm. Level Pref.                       |
| 7:00am - 8:30am   | Poster Session Check-In  | Ballroom/<br>Exhibit Level<br>Prefunction |
| 8:00am - 9:00am   | Career Fair Setup  | Exhibit Hall C                            |
| 8:30am - 9:45am   | <b>Conference Opening and Keynote</b> (doors open at 8:15am)<br><i>*Coffee Available Before &amp; During Keynote</i><br><b>Featured Speaker:</b> Jenn deBerge, Mastercard<br><b>Featured Speaker:</b> Robin Shostack, Google<br><b>Keynote:</b> <b>"How Technology Will Dictate Our Civic Future"</b><br>Latanya Sweeney, Harvard University | Gr. Ballroom ABC                          |
| 9:45am - 6:00pm   | WiCyS Store Open   | Room 12                                   |
| 9:45am - 11:00am  | Student Poster Session & Networking Refreshment Break  | Ballrm. Level Pref.                       |
| 9:45am - 11:45am  | Career Fair Open   | Hall C                                    |
| 9:45am - 11:45am  | Capture the Flag (CTF) Mentoring Available   | Rooms 21,23                               |
| 9:45am - 11:45am  | Career Village Open  | Rooms 20,22,24                            |
| 11:00am - 11:45am | <b>Presentation Sessions</b> (4 Concurrent)  |   |
|                   | <b>A Fine Line Between How Much You NEED and WANT to Know With Location Apps</b><br>Christine Horwege, CGI Federal; Cassandra Horwege, University of Pennsylvania<br><b>(CPE CREDITS: 1)</b>   | Room 1                                    |
|                   | <b>Projects, Promotions and Principal Engineers or "How to Pwn Your Lane"</b><br>Heather Lawrence (@infosecanon), University of Colorado, Colorado Springs;<br>Patrice Siravo, Adriano Cyber Consulting<br><b>(CPE CREDITS: 1)</b>   | Room 3                                    |
|                   | <b>CVSS: Changing Vulnerability Scoring Suggested</b><br>Maitreyee Palkar, F5 <b>(CPE CREDITS: 1)</b>  | Room 5                                    |
|                   | <b>Taking One Byte at a Time: Securing 5G</b><br>Natalie Pittore, National Security Agency <b>(CPE CREDITS: 1)</b>   | Room 25 ABC                               |
| 11:00am - 11:45am | <b>Student Chapter MeetUp: This is Your Tribe of Fellow Students, Pull Up a Chair</b><br>Yansi Keim, Purdue University <b>(CPE CREDITS: 1)</b>   | Room 26 ABC                               |

### CPE CREDITS

**CPE Credits** are available for designated sessions. Reference the agenda or session descriptions in the program to identify sessions that qualify. After attending the full session, you will need to submit a form to receive CPE credits. Scan the QR code on the presenter's screen OR locate the volunteers that will be at the back of each session. You will receive your CPE credits via email in the weeks following.

# 2022 WiCyS SCHEDULE

## FRIDAY AGENDA

| TIME            | DESCRIPTION  | LOCATION           |
|-----------------|--|--------------------|
| Noon - 1:45pm   | <b>Lunch, Networking, and Keynote</b><br>(must be seated by 12:10pm to eat, Keynote starts at 12:30pm)<br><b>Featured Speaker:</b> Gili Lev, <i>AWS</i><br><b>Featured Speaker:</b> Felice Ajlouny, <i>SentinelOne</i><br><b>Keynote:</b> “Empowering the Next Generation of Women Cybersecurity and Tech Pioneers” *Joining Virtually*<br>Director Jen Easterly, <i>Cybersecurity and Infrastructure Security Agency (CISA)</i> | Grand Ballroom ABC |
| 1:55pm - 5:30pm | Career Fair Open   | Hall C             |
| 1:55pm - 5:30pm | Capture the Flag (CTF) Mentoring Available   | Rooms 21,23        |
| 1:55pm - 5:30pm | Career Village Open  | Rooms 20,22,24     |
| 1:55pm - 2:40pm | <b>Presentation Sessions</b> (4 Concurrent)  |                    |
|                 | <b>The Rugged DevOps Journey</b><br>Rachael Crowthers and Shua Gamradt, <i>Optum</i><br><b>(CPE CREDITS: 1)</b>  | Room 1             |
|                 | <b>Methodologies and Investigations of Cloud Security Practices in the Healthcare Ind.</b><br>Remi Cohen (@sOmegirlr3m), <i>F5</i> ; Meghan Jacquot (@CarpeDiemT3ch), <i>Recorded Future</i><br><b>(CPE CREDITS: 1)</b>  | Room 3             |
|                 | <b>Mind the Gap: An Insider’s View of Often-Overlooked Key Elements that Can Make or Break Your Next Career Move</b><br>Christine Winchester, <i>DHS Cybersecurity Service</i><br><b>(CPE CREDITS: 1)</b>  | Room 5             |
|                 | <b>Toward Secure Machine Learning with Counterfit</b><br>Amanda Minnich (@NMspinach), <i>Microsoft</i><br><b>(CPE CREDITS: 1)</b>  | Room 25 ABC        |
| 1:55pm - 2:40pm | <b>Affiliate MeetUp: This is Your Tribe of Peers, Pull Up a Chair</b><br>Deborah Kariuki, <i>University of Maryland Baltimore County</i><br><b>(CPE CREDITS: 1)</b>  | Room 26 ABC        |
| 2:45pm - 3:15pm | Career Fair (Break with Refreshments)  | Exhibit Hall C     |
| 2:40pm - 4:40pm | <b>Workshop Series</b> (4 Concurrent)  |                    |
|                 | <b>Create Confidence When it Matters to Take Your Career to the Next Level</b><br>Micha Goebig, <i>Go Big Coaching</i> ; Katrina Zidel, <i>Kreating Boldly, Inc.</i><br><b>(CPE CREDITS: 2)</b>  | Room 1             |
|                 | <b>Your Transformation: Level-Up Your Cyber Career by Translating Transferable Skills</b><br>Christina Stokes (@xTinaStx), <i>Salt Cybersecurity</i><br><b>(CPE CREDITS: 2)</b>  | Room 3             |
|                 | <b>Cybersecurity – An IT Challenge or Business Priority?</b><br>Rob Rashotte, <i>Fortinet</i><br><b>(CPE CREDITS: 2)</b>   | Room 5             |
|                 | <b>Language, Allyship and Self-Accountability: Driving Change in the Cybersecurity Industry</b><br>Racial Equity Committee, <i>WiCyS</i><br><b>(CPE CREDITS: 2)</b>  | Room 25 ABC        |

# 2022 WiCyS SCHEDULE

## FRIDAY AGENDA

| TIME              | DESCRIPTION   | LOCATION           |
|-------------------|---|--------------------|
| 4:45pm - 5:30pm   | <b>Birds of Feather</b> (5 Concurrent)  |                    |
|                   | <b>Cybersecurity Academic Integration Through Outreach</b><br>Joan Labay-Marquez (@JoanMMarquez), <i>University of the Incarnate Word</i>   | Room 1             |
|                   | <b>Why Are There so Many aaS(es) in the Cloud?</b><br>Atia Ibrahim, <i>Optum</i>  | Room 3             |
|                   | <b>I've Got a New Attitude - Staying Motivated, Inspired and Focused</b><br>Jerry Hache and Marti Mondragon (@MartiMominColo), <i>Palo Alto Networks</i>  | Room 5             |
|                   | <b>What Strategies Work To Make You Stay</b><br>Meg Layton (@vamegabyte), <i>Children's National Hospital</i>   | Room 25 ABC        |
|                   | <b>Cultivating Women as Leaders - The Role of Allyship</b><br>Kip Bates, <i>University of California, Santa Barbara</i> ; Reema Moussa, <i>University of Southern California, Gould School of Law</i>   | Room 26 ABC        |
| 6:00pm - 7:45pm   | <b>Dinner, Networking, and Keynote</b><br>(must be seated by 6:10pm to eat, Keynote starts at 6:30pm)<br><b>Featured Speaker:</b> Elvia Novak, <i>Deloitte Risk and Financial Advisory</i><br><b>Featured Speaker:</b> (U//FOUO) Brigadier General Lorna Mahlock, <i>NSA</i><br><b>Keynote: "Walking in Fire"</b><br>Allison Miller, <i>OPTUM</i> | Grand Ballroom ABC |
| 8:00pm - 9:00pm   | Racial Equity Committee (REC) Meet & Greet  | Room 7             |
| 8:30pm - Midnight | Capture the Flag (CTF) After Dark Party   | Rooms 21,23        |

### CAPTURE THE FLAG (CTF) COMPETITION

**Come show your team's cybersecurity skills in a creative and collaborative competition!**

Hosted by:  
**Carnegie Mellon University**  
Software Engineering Institute

The CTF is a team-based event with 2-4 members per team and kicks off **Thursday, March 17 at 12:30pm**. CTF participants will have until **Friday, March 18 at 11:59pm** to solve as many challenges as possible. The CTF will use SEI's web-based competition platform, Gameboard, to provide access to challenges and track each team's score. Challenges from the President's Cup Cybersecurity Competition will test everyone's cybersecurity skills in areas such as forensics analysis, incident response and cyber defense.

#### 1st Place

Pass to WiCyS 2023  
(shared lodging, travel stipend,  
and sponsor donated gifts)

#### 2nd Place

Pass to WiCyS 2023  
(shared lodging and sponsor  
donated gifts)

#### CTF Mentoring

Rooms 21,23  
Thursday | 12:30pm - 7:00pm  
Friday | 9:45am - 11:45am & 1:55pm - 5:30pm

#### CTF After Dark Party

Rooms 21,23  
Friday | 8:30pm - Midnight



Scan the code with your mobile phone camera to find additional details and register for the CTF.



# Apply today to engineer tomorrow

Raytheon Technologies fosters an inclusive culture that harnesses the power of different ideas and experiences to deliver the innovative solutions our customers depend on.



[RTX.com/careers](https://www.rtx.com/careers)

COLLINS AEROSPACE | PRATT & WHITNEY | RAYTHEON INTELLIGENCE & SPACE | RAYTHEON MISSILES & DEFENSE

©2022 Raytheon Technologies Corporation.

# 2022 WiCyS SCHEDULE

## SATURDAY AGENDA

| TIME              | DESCRIPTION   | LOCATION   |
|-------------------|---|--|
| 7:00am - 9:00am   | Badge Pick-Up   | Exhibit Level  |
| 7:00am - 5:00pm   | Coat Room   | Room 18  |
| 7:00am - Sell Out | WiCyS Store Open  | Room 12  |
| 7:00am - 8:00am   | Breakfast Available with Tables for Scholarship and Fellowship Recipients   | Ballrm. Level Pref.  |
| 7:00am - 8:15am   | Military Breakfast  | Room 4   |
| 8:00am - 5:00pm   | Luggage Storage Available   | Room 7   |
| 8:30am - 9:30am   | <p><b>Keynote</b> (doors open at 8:15am)<br/> <i>*Coffee Available Before &amp; During Keynote</i></p> <p><b>Featured Speaker: Alexandra Landegger, Raytheon</b><br/> <b>Featured Speaker: Veena Reddy, GE</b></p> <p><b>Keynote: "Cyber Security Research in Interdisciplinary Units, Challenges and Opportunities"</b><br/> <b>Anna Squicciarini, Pennsylvania State University</b></p>   | Grand Ballroom ABC   |
| 9:30am - 10:00am  | Group Picture / Break with Refreshments   | TBD  |
| 10:00am - 10:45am | <p><b>Presentation Sessions</b> (4 Concurrent)</p> <p><b>Investing in Our Nation's High School and Middle School Cybersecurity Educators</b><br/> <b>Nikki Hendricks, EPIC, TACC, The University of Texas; Joy Schwartz, WeTeach_CS, TACC, The University of Texas</b><br/> <b>(CPE CREDITS: 1)</b></p> <p><b>Building a Scalable Cloud Native Security SIEM</b><br/> <b>Tanvi Kolte (@tanvi_kolte), LinkedIn</b><br/> <b>(CPE CREDITS: 1)</b></p> <p><b>Trapped in the Wolf Den: A Dive into Compromises From Within the Walls of a SOC</b><br/> <b>Lisa Tetrault (@LLTetrault) and Samantha Van Aaken, Arctic Wolf</b><br/> <b>(CPE CREDITS: 1)</b></p> <p><b>Protecting America's Defense Industrial Base with Cybersecurity Services</b><br/> <b>Kristina Walter, National Security Agency</b><br/> <b>(CPE CREDITS: 1)</b></p> | <p>Room 1</p> <p>Room 3</p> <p>Room 5</p> <p>Room 25 ABC</p> |
| 10:00am - 10:45am | <p><b>Lightning Talks</b> (all talks are in the same room) <b>(CPE CREDITS: 1)</b></p> <p><b>Economics and Ethics Behind Successful Free and Open Source Security Projects</b><br/> <b>Olivia Gallucci, Rochester Institute of Technology</b></p> <p><b>Rust - Trust or Bust?</b><br/> <b>Diane Stephens, University of North Georgia, University of Georgia</b></p> <p><b>The Malware Did It!</b><br/> <b>Modhuparna Manna (@modhuparna), Louisiana State University</b></p> <p><b>The Peanut Butter and Jelly Sandwich of Cyber Offense and Defense</b><br/> <b>Breanna H.; Laura L.</b></p> <p><b>Hosting WiCyS Conference: Cleveland Inside Story</b><br/> <b>Shilpa Kedar, Cleveland State University; Gordan Taylor, Destination Cleveland</b></p>  | Room 26 ABC  |

# 2022 WiCyS SCHEDULE

## SATURDAY AGENDA

| TIME              | DESCRIPTION   | LOCATION    |
|-------------------|---|-------------|
| 11:00am - 11:45am | <b>Presentation Sessions</b> (4 Concurrent)   |             |
|                   | <b>Protecting Critical Environments by Leveraging OT Security Controls</b><br>Danielle Gulotta, <i>Security Risk Advisors</i><br>(CPE CREDITS: 1)   | Room 1      |
|                   | <b>Diversity is a Result of Inclusive Cultures</b><br>Deidre Diamond (@deidrediamond), <i>CyberSN and Secure Diversity</i><br>(CPE CREDITS: 1)  | Room 3      |
|                   | <b>Federated Learning for Enabling Secure Smart Communities: Current Technologies, Challenges and Future Directions</b><br>Smriti Bhatt, <i>Purdue University</i> ; Deepti Gupta, <i>University of Texas at San Antonio</i><br>(CPE CREDITS: 1) | Room 5      |
|                   | <b>Let Them In: How Cyber Deception and Adversary Engagement Leads to Better Defense</b><br>Gabby Raymond, <i>The MITRE Corporation</i><br>(CPE CREDITS: 1)   | Room 25 ABC |
| 11:00am - 11:45am | <b>Lightning Talks</b> (all talks are in the same room) (CPE CREDITS: 1)  | Room 26 ABC |
|                   | <b>Ditch the Dichotomy: Embrace the Rainbow</b><br>Kaitlyn Bestenheider (@CryptoKait), <i>RSM US, LLP</i>   |             |
|                   | <b>Importance of Personal Gender Pronouns in and Out of the Workplace</b><br>Ruchira Pokhriyal, <i>Amazon Web Services</i>  |             |
|                   | <b>TrustTalk with TikTok</b><br>Sydney Ng, <i>TikTok</i>  |             |
|                   | <b>The Top Reasons Why Employees Hate Internal Phishing Programs and What You Can Do About It</b><br>Ashley Rose (@AshleyRose_ATX), <i>Living Security</i>  |             |
|                   | <b>Developing a Corporate-Wide and Global Women in Cyber Affinity Group</b><br>MacKenzie Cavanagh, <i>GE Gas Power</i>  |             |
|                   | <b>Leaders – Stop Performance Review Panic!</b><br>Pam Rowland, <i>Grand Canyon University</i>  |             |
|                   | <b>Data Provenance Defense Strategies for GPS Spoofing in Autonomous Vehicles</b><br>Lalitha Donga, <i>Rochester Institute of Technology</i>  |             |

### MILITARY BREAKFAST

**TOGETHER. WE SERVE.**

Saturday | 7:00am - 8:15am  
Located in Room 4

Hosted by:

**Bloomberg**



The Military Breakfast will honor our current military, veterans, and military spouses attending WiCyS 2022. The breakfast is open to all military, veterans, and military spouses. No RSVP is necessary.

# 2022 WiCyS SCHEDULE

## SATURDAY AGENDA

| TIME             | DESCRIPTION   | LOCATION            |
|------------------|---|---------------------|
| Noon - 12:45pm   | <b>Panels</b> (5 Concurrent)  |                     |
|                  | <b>It Takes Many Sailors to Move this Ship: Populating the Cybersecurity Workforce with Talent From Diverse Backgrounds</b><br>Joanna Grama (@runforserenity), <i>Vantage Technology Consulting Group</i> ; Jennifer Pacenza, <i>REN-ISAC</i> ; Amy Starzynski Coddens, <i>Indiana University Bloomington / REN-ISAC</i>  | Room 1              |
|                  | <b>The Power of Six: Creating Cyber Experiences and Building a Talent Workforce Pathway for Women and Underrepresented Students</b><br>Laura Freeman, <i>Virginia Tech National Security Institute</i> ; Sharon Hamilton (@srhamilton13), <i>Norwich University</i> ; Lauren Provost (@ethicalhacks), <i>Norwich University</i> ; Linda Riedel, <i>The Citadel</i>    | Room 3              |
|                  | <b>The Skills Gap Wish List: Students, Industry and Academia</b><br>Dr. Brandy Harris, Pam Rowland, Niya Patterson, and Irene Vallalabos <i>Grand Canyon University</i> ; Tamyria Williams (@iam_tammyw), <i>TWC CORE Consulting, LLC</i>   | Room 5              |
|                  | <b>You've Got This: Stories of Career Pivots and How to Successfully Start a Cyber Career</b><br>Jennifer Bate (@BateJennifer), <i>Deloitte</i> ; Jennifer Cheung (@MsCheungMath), <i>NWIC Pacific</i> ; Meghan Jacquot, <i>Recorded Future</i> ; Ashley Richardson-Sequeira, <i>Palo Alto Networks</i> ; Alma Maria Rinasz (@AlmaRinasz), <i>Bug Bounty Services</i> | Room 25 ABC         |
|                  | <b>The Amazing Race - Coordinating Cyber Vulnerability Disclosure</b><br>Cheri Caddy, <i>U.S. Department of Energy</i> ; Lindsey Cerkovnik, <i>Department of Homeland Security</i> ; Melissa Vice (@vicemel), <i>DOD Cyber Crime Center (DC3)</i>   | Room 26 ABC         |
| 12:45pm - 2:00pm | <b>Lunch, Closing Remarks, and Awards</b> (Must be seated by 1:00pm to eat)   | Grand Ballroom ABC  |
| 2:00pm - 2:30pm  | Travel Stipend Verification   | Ballrm. Level Pref. |
| 2:30pm - 4:30pm  | <b>Workshop Series</b> (4 Concurrent)   |                     |
|                  | <b>Oh Cyber, My Cyber: Rise Up and Hear the Buzzer! Explore the Tools Used to Develop YOU as the Next Generation of Diverse Cybersecurity Professionals!</b><br>Caitlin Boyce, <i>SANS</i> ; Doug Britton, <i>Haystack</i> , Lynn Dohm, <i>Women in CyberSecurity (WiCyS)</i><br><b>(CPE CREDITS: 2)</b>  | Room 1              |
|                  | <b>Putting Privacy in Your Pocket: Controlling Your Privacy in an IoT Connected World</b><br>Lisa McKee, <i>Protiviti/Dakota State University</i> ; Tania Williams, <i>The University of Alabama in Huntsville</i><br><b>(CPE CREDITS: 2)</b>   | Room 3              |
|                  | <b>Purple Team Workshop</b><br>Nathali Cano (@Natha_Sect) and Elaine Harrison-Neukirch (@rubysgeekymom), <i>Scythe</i><br><b>(CPE CREDITS: 2)</b>   | Room 25 ABC         |
|                  | <b>Coding Security Best Practices</b><br>Viraj Gandhi, <i>SailPoint</i><br><b>(CPE CREDITS: 2)</b>  | Room 26 ABC         |

# WiCyS Professional Affiliates

## LEADERSHIP



### WiCyS United States Affiliates

#### Austin

Holly Parrish  
Nikki (Nicola) Hendricks  
Dr. Natasha Thomas (Baker)  
Sara Friedfertig  
Tiffani Nguyen  
Katherine (Kady) Salazar  
Kayla Ventresca

#### Central Alabama

Sherry Barnes  
Angella Carlisle  
Cassandra Brown  
Leigh-Anne Hoffman  
Heather McCalley  
Lora Vaughn  
Kera Dorsey

#### Chicago

Shafia Zubair  
Jan Hertzberg  
Pauline Blatt

#### Colorado

Angela Hogaboom  
Nathan Chung

#### Dallas Fort Worth

Veronica Unnikrishnan

#### Delaware Valey

Nancy Hunter  
Jordan Fischer  
Kathy Padva  
Donna Downes-Matreale

#### Florida

Dr. Eman El-Sheikh  
Marie Perry  
Paulina Mendez  
Ashley Nelson  
Mai Ensmann  
Ami Linish  
Jacqueline Ore

#### Georgia

Sherry Naleszkiewicz  
Brigitte Collier  
Karen Broughton  
Shaleah Grice  
Camille Bolton  
Kruti Vadjikar  
Brandy Griffin  
Michelle Rivers  
Dr. Elizabeth Rasnick

#### Houston

Annie Jamshed  
Abeer Asad  
Anmol Deep Kaur Puri  
Chimeria Gonzales  
Aishwarya Mandikal  
Nader Zaveri  
Fatima Ali

#### Metro NY

Megan Kaczanowski  
Jessica Nelson  
Stacey Romanello  
Viola Sarkantus  
Angeliki Zavou  
Rebecca Gershen  
Ruth Murphy

#### Mid-Atlantic

Meghan Jacquot  
Deborah Kariuki  
Nikkia S. Henderson  
Racquel J. James  
Diane M Janosek  
Amelia Estwick

#### Minnesota

Judy Hatchett  
Tina Meeker  
Kris Boike  
Michael Larson

#### Mississippi

Sarah Lee  
Susan Kelly  
Anna Jackson  
Anna Wan

#### New England

Kelley Misata  
Jennifer McLarnon  
Lisa Kendall

#### NE Ohio

Pam Gerber  
Tiffany McClaskey  
Kathy Peters  
Jenn Zacharias  
Janine Spears  
Krista Burns

#### North Carolina

Noureen Njoroge  
Reena Madan  
Sphurthi Annamraju  
Latisha Scarborough

#### Northern Alabama

Stacie Bohanan  
Rebecca Miller  
Aleise McGowan  
Mayra Paredes

#### Oregon

Mandy Sessions  
LJ Johnson  
Jason Mitsky  
Sandra Morrissey  
Alexis Culp  
Jovita Alphonse  
Sarba Roy  
Whitney Aguilar

#### Phoenix AZ

Dara Gibson  
Pam Rowland  
Zerene Sangma  
Janet Hartkopf

#### San Antonio

Areej Albataineh  
Vanessa Garza Clark  
Smriti Bhatt  
Geeta Goswami

#### San Diego

Jennifer Cheung  
Caitlin Delmore  
Sherawn Jackson  
Michelle Moore  
Megan Deblois  
Viraj Gandhi  
Dru Macasieb  
Amruta Mujumdar  
Jennifer Bate

#### Silicon Valley

Stephanie Olsen  
Kristen Beneduce  
SaiSujitha Venkatesan  
Kylie McRoberts  
Arpita Biswas  
Sofia Bekrar  
Lily Lee  
Suzy Wanja

#### South Dakota

Katie Shuck  
Kanthi Narukonda

#### Tennessee

Barbee Mooneyhan  
Janice Reese  
Raenesia Jones

#### Utah

Kristina Belnap  
Mark Milne  
Sherrie Cowley

#### Western Washington

Zabrina McIntyre  
Andrea Frost  
Masako Long

### WiCyS Global Affiliates

#### ASIA

##### India

Sabna Sainudeen  
Sushmitha Nayak  
Lekshmi Nair  
Preeti Bhisikar

##### Pakistan

Zainab Hameed  
Sehrish Muftaba  
Seema Haseeb  
Farida Damani  
Jannat Ali Kalyar  
Khaula Karim

##### AUSTRALIA

Fiona Byrnes  
Anita Siassios  
Deyan Pejovic  
Amelia Araya  
Jane Chow  
Cassandra Diamond  
Dr. Elena Sitnikova  
Kevin Crowley

#### AFRICA

##### East Africa

Aprielle Oichoe  
Leah Kimata  
Joan Mburu  
Diana Agaba Tukundane

##### Southern Africa

Kerissa Varma  
Michelle Wynne-Griffith  
Leanne Gerbach  
Alizanne Adams  
Loren Hollingsworth

##### Western Africa

Olayinka N.D. Wilson-Kofi  
Audrey Mnisi Mireku  
Abigail Dede, Okley  
Julia Asante-Mensah  
Nina Pearl, Doe

#### CANADA

##### Ontario

Karen Nemani  
Heather Ricciuto  
Pat Antliff  
Helen Krissalis  
Ikjot Saini  
Cathy Ganos

##### Western Canada

Manna Ng  
Sridevi Sadhineni  
Tina Singh  
Juanita DeSouza-Huletey  
Aarti Gadhia

### WiCyS Corporate Affiliates

#### Lockheed Martin

Jaidie Vargas  
Pam Sheary  
Sarah Fries  
Tambre Paster

#### Mitre

Susie Heilman  
Michaela Adams  
Emily Hopkins  
Amy Robertson

### WiCyS Specialty Affiliates

#### Trusted AI

Pamela Gupta

#### Critical Infrastructure

Veronica Kazaitis  
Rosemary Christian  
Courtney Greeley  
Tina Kuhn

#### Military

Kristen Cotten  
Elizabeth Tatulis  
Kelly Jackson  
Martha Laughman

#### Cloud Security

Allie DeCastro  
Anna Cotter  
Val Miller  
Margaret Zimmerman  
Gili Lev



# 2022 WiCyS CONFERENCE MEETUPS

## EDUCATORS/SCIENTISTS MEETUP WITH FUNDING AGENCIES

**Thursday • 7:00pm - 8:00pm**

For Educators and Scientists, this session provides informal conversations with program directors/managers at various funding agencies such as NSF and NSA about potential opportunities related to cybersecurity.

## FEDERAL SCHOLARSHIP (SFS/CYSP) MEETUP AND INFORMATION SESSION

**Thursday • 8:00pm - 9:00pm**

Come and meet students, faculty, and agencies participating in federal scholarship programs and learn how to get into various programs, as well as network with fellow students currently in federal scholarship programs.

## STUDENT CHAPTER MEETUP

**Friday • 11:00am - 11:45am**

**This is Your Tribe of Fellow Students, Pull Up a Chair**

*Yansi Keim, Purdue University*

**CPE CREDITS: 1**

Join this session to learn about starting, running and maintaining the student chapter on campus. Current chapter presidents will share their experiences, talk about challenges, and address many issues that commonly arise as a student chapter officer. This will be a freestyle session, so bring lots of questions and let's help each other succeed in promoting women in cybersecurity on campus. While everyone's cybersecurity journey is different, the presenters' goals are similar: To propel individuals and the surrounding community. Pull up a chair at this Student Chapter Meetup, and let's talk about how to create/engage the community.

## AFFILIATE MEETUP

**Friday • 1:55pm - 2:40pm**

**This is Your Tribe of Peers, Pull Up a Chair**

*Deborah Kariuki, University of Maryland Baltimore County*

**CPE CREDITS: 1**

Come meet leadership from small, medium and large affiliates as they form a freestyle panel to support all efforts in local affiliates. The group will talk about strategies, best practices, social media and more! Bring questions and let's grow stronger! While everyone's cybersecurity journey is different, the presenters' goals are similar: To propel individuals and the surrounding community. Pull up a chair at this Affiliate Meetup, and let's talk about how to create/engage the community.

## MILITARY BREAKFAST

**Saturday • 7:00am - 8:15am**

The Military Breakfast will honor our current military, veterans, and military spouses attending WiCyS 2022. The breakfast is open to all military, veterans, and military spouses. No RSVP is necessary.

### ONLINE WICYS STORE

Visit the online store and purchase WiCyS gear!



### CONNECT WITH THE WICYS COMMUNITY ON SOCIAL MEDIA!

Be a part of the collective strength of the WiCyS community! Follow us on Social Media!



Twitter



LinkedIn



Instagram



Facebook



YouTube

# 2022 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

## PRE-CONFERENCE SESSIONS

**Thursday • 12:30pm - 1:30pm**

**Your 1st Time at WiCyS? Join Us For Insiders' Tips for Navigating WiCyS!**

**TRACK: BEST PRACTICES**

Elizabeth K. Hawthorne, *Rider University*; Kim Huynh, *Microsoft*; Felicia Jackson, *Raytheon*; Marena Soulet, *Tennessee Technological University*; Laura Sturgeon, *Smoothstack/Bloomberg*; Comfort Uduebholo, *Amazon Web Services*

Attending a WiCyS conference for the first time can be both exciting and daunting. There is just so much to navigate through in little time! Join us in this session, if this is your 1st time at the WiCyS conference. As panelists from various backgrounds and interests, we will share our experiences of what we found useful, what matters, and most importantly how you can get the most out of this experience as a first-time WiCyS attendee.

**Recruiters Session: Developing and Acquiring Security Talent in a Competitive Industry**

Heather Rustin, Gary Simms and Anelda Venter, *Walmart*

**TRACK: BEST PRACTICES**

**CPE CREDITS: 1**

Recruiting information security talent is critical to the business operations of all companies and requires commitment and continuous support from leadership. Emerging business imperatives, such as evolving the digital ecosystem, require highly skilled and talented resources to ensure data security and customer trust. It is critically important that organizations take a new and creative approach to finding and retaining resources. In this session, presenters will address the following: Creating intuitive and engaging job descriptions that convey the capabilities needed for roles while creating excitement for the adventure of cybersecurity job opportunities; finding hidden talent by looking beyond the status quo; using non-traditional training, credentialing and certifications to identify critical and in-demand talents; and using culture, diversity, equity and inclusion as a tool for recruiting diverse cybersecurity talent from underrepresented and socioeconomically challenged communities. Join this session to foster a culture of inclusion and creativity by including ALL in the STEM pipeline.

## WORKSHOP SERIES

**Thursday • 2:00 pm - 4:00 pm**

**SEED Labs: Hands-on Labs for Cybersecurity Education**

Wenliang (Kevin) Du, *Syracuse University*

**TRACK: TODAY'S TECHNOLOGY AND CHALLENGES**

**CPE CREDITS: 2**

To improve students' hands-on skills in cybersecurity, over the last 20 years this presenter has developed roughly 40 labs called SEED labs. Today, over 1,000 institutes worldwide are using them in their cybersecurity curricula. Many companies also are using the labs for their internal training and interviews. In this workshop, the presenter will give an overview and demonstrate several labs before guiding participants through some. Participants need to download the provided SEED VM beforehand, as all labs will be conducted inside the VM. Educators, students, professionals and researchers are welcome to attend this workshop.

**Get Smarter About the Dumb Protocols on Our Networks!**

Terri Johnson, *Pikes Peak Community College*; Keith Nabozny, *Macomb Community College*

**TRACK: TODAY'S TECHNOLOGY AND CHALLENGES**

**CPE CREDITS: 2**

Does anyone suffer from FOAQ (fear of asking questions)? How about gaining a better understanding of how network devices communicate with each other? Then this is the workshop to attend! Although IoT devices and computers keep getting smarter, the underlying protocols are not. This workshop will walk through the fundamental protocols used by all devices in communicating with each other and the internet. This will be an interactive workshop where there are no dumb questions! Participants will use Wireshark to visualize how ARP, DNS and other protocols operate. Some key topics covered will be: the parts of ipconfig/ifconfig; how ARP communicates; why subnetting is important; the value of DNS; and how traffic flows from the local network to a server on the internet. Although the workshop has a structure for sharing information on these topics, the presenters will welcome questions from participants to make this an engaging and interactive experience. Participants should have basic knowledge of Network+ or Security+ concepts. Wireshark should be installed before attending the workshop ([www.wireshark.org](http://www.wireshark.org)).

# 2022 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

## Enabling Security-by-Design for Cyber Physical Systems Using Threat Modeling

Deveeshree Nayak, *University of Washington Tacoma*;  
Sarba Roy, *Intel Corporation*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES,  
SMART ABOUT "SMART" THINGS**

**CPE CREDITS: 2**

In a 2021 Cybersecurity Threat Trends report by Cisco, it was revealed that 50% of organizations encountered ransomware-related activity while 48% found information-stealing malware activity. The recent ransomware attack on Colonial Pipeline, the Mirai botnet attack and numerous other IoT security breaches indicate the importance of incorporating security by design in Cyber Physical systems (CPS), which are ubiquitous, from wearable systems to complex critical infrastructure. It is critical to identify threat actors, reduce attack surfaces and take proactive risk mitigation steps during system design and validation phases in CPS as an important process to secure this connected world. In this workshop, attendees will learn fundamentals of CPS, security by design methodologies, best practices and frameworks. They will build a threat model of real world CPS from scratch by incorporating security by design methodologies, brainstorming on identifying misuse patterns involving CPS threats, and discussing the reporting metrics for an effective threat model based on a CPS. This workshop can be attended by anyone who is interested in CPS, threat modeling and security by design.

## "Incident Response Exercises are Fun" and Other White Lies

Patrice Siravo, *Adriano Cyber Consulting*

**TRACK: TODAY'S TECHNOLOGY AND CHALLENGES**

**CPE CREDITS: 2**

Every cybersecurity standard and framework requires incident response (IR) exercises. And yet, it usually feels like pulling teeth to get the right participants to attend (and actively participate in) these exercises. Getting them to review the after-action report is almost impossible! This workshop will help participants resolve the IR exercise reluctance in their organizations. By building efficient and applicable IR exercises and always being prepared before the exercise begins, anyone can make the event more enticing for their organization... maybe even fun. By the end of this workshop, they will have a (nearly) complete IR exercise designed and ready to implement when back in the office. Coupled with the new skills and tools learned during the workshop, attendees will be able to pull off a successful IR exercise that engages stakeholders with realistic events, effectively testing the selected response capability, and providing insight and data that will improve IR procedures across the organization. There may even be enough buzz from the exercise that executives will review the after-action report. The tools and techniques used in this workshop were developed, tested and refined through numerous real-

life exercises. They can be applied to any organization and meet the requirements of the most prominent sources of cybersecurity governance. They are simple enough to be used by the newest cybersecurity professional but include enough detail to support a complex service interruption exercise. Downloadable links will be provided before the workshop for participants who want to build their exercise scenario electronically. Paper copies also will be available for old-school note taking.

## Breaking into the Field of Ethical Hacking: An Introduction to the Field and Core Skills

Lauren Provost, *Norwich University*

**TRACK: TODAY'S TECHNOLOGY AND CHALLENGES**

**CPE CREDITS: 2**

Ethical hackers are in high demand, especially with the increase of vulnerabilities associated with mobile devices, IoTs and cloud computing. In order to be a strong ethical hacker, however, power skills (leadership, persistence and more) as well as technical skills are both major components to success in the field. This workshop includes a discussion of career pathways and certifications to support breaking into the field of ethical hacking as well as hands-on labs where participants will explore crucial power and technical skills for any aspiring ethical hacker. Participants will begin by building core skills -- capture a victim's network traffic with an ARP spoofing attack and then view the results in Wireshark. They will then deploy reverse shells that allow commands to be run on a victim's computer, encrypt files by writing ransomware in Python, and create fake emails using Metasploit, similar to those used in phishing attacks. Case studies in the field will be discussed. At the end of the workshop, participants will be able to describe multiple career pathways to break into the field of ethical hacking; plan a vulnerability assessment and penetration test for a network; execute a penetration test using standard hacking tools in an ethical manner; report on the strengths and vulnerabilities of the tested network; and identify legal and ethical issues related to vulnerability and penetration testing.

# 2022 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

## WORKSHOP SERIES

**Thursday • 4:30 pm - 6:30 pm**

### Breaking In: Smart Home

**Samantha Chaves and Chesleah Kribs**, *Carnegie Mellon University Software Engineering Institute*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, SMART ABOUT "SMART" THINGS**

**CPE CREDITS: 2**

How does a smart home stack up against a hacker? Accompany two penetration testers in a hands-on workshop in exploiting a home network created for breaking in! Using both red and blue team tools and skillsets, participants will help hack into a realistic home network filled with IoT devices and interconnected software and systems. Prior to exploiting and defending the lab environment, attendees receive introductions on the vulnerabilities they may encounter and the defense they should use to circumvent attackers. The presenters will split into an attack and defend scenario with the attendees joining both teams during the course of the workshop. The simulated lab environment is custom-made and will consist of multiple attack surfaces and automated hacking for defenders, allowing attendees to experience both offensive and defensive security in a controlled and safe domain. After completing this workshop, participants will have an increased understanding of the vast types of vulnerabilities that home devices are susceptible to but will be armed with best practices to protect a home and property from malicious hackers. This will be an intermediate-level workshop. A familiarity with a Debian/Kali Linux OS is strongly recommended as well as Linux command line. A certification similar to Network+ or Security+ also is preferred for foundations in security and networking concepts. Bring a laptop with the capability to run a VM and connect to the internet; all other resources will be provided.

### The Eight Sins: Mitigation of Security Weaknesses in Automated Configuration Management

**Farhat Lamia Barsha and Akond Rahman**, *Tennessee Technological University*

**TRACK: TODAY'S TECHNOLOGY AND CHALLENGES**

**CPE CREDITS: 2**

With the proliferation of cloud-based services, such as Amazon EC2 instances, automated configuration management languages are widely used in industry. Examples include Ansible, Chef, Puppet and Terraform. Automated configuration management has helped information technology organizations. With Ansible, NASA increased their software delivery frequency by a factor of 1,200. Despite reported benefits, scripts used for automated configuration management included security weaknesses such as hard-coded passwords. This workshop will focus on security weaknesses that appear in Ansible and Puppet scripts. The workshop also will show how state-of-the-art static analysis tools can be used to find security weaknesses

automatically in configuration management scripts. In the two-hour long workshop, the organizer will first introduce the concept of security weaknesses, how identified security weaknesses are linked with common weakness enumeration entries, and how static analysis tools can help identify security weaknesses in configuration management scripts. In the workshop, participants will use their own laptops, but no additional software and hardware will be required. Presenters will discuss the state of security in automated configuration management in the open-source domain and its benefits. Upon completion of the workshop, participants will provide feedback, which will be integrated into the improvement process of the static analysis tools. Any WiCyS participant with basic computer programming experience can participate in this workshop, including but not limited to undergraduate and graduate students, educators as well as practitioners from government and industry.

### How to Draft Strong Cybersecurity Policy

**Jael Lewis and Cara Turbyfill**, *Walmart*

**TRACK: BEST PRACTICES**

**CPE CREDITS: 2**

Writing the rules down is the easy part. The hard part is deciding what the rules should be. Join two cybersecurity governance experts as they examine what goes into strong policy at three different hypothetical companies. They'll run through identifying the risks and regulations, developing the controls, identifying the audience and drafting the policy.

### Into The Breach: Rehearsing and Role-Playing Breach Responses

**Molly Cooper**, *Ferris State University*; **Peter Dillman**, *Dillman's Dungeon*

**TRACK: BEST PRACTICES**

**CPE CREDITS: 2**

This workshop is an immersive, role-playing, gamified, cybersecurity experience. Participants will be assigned a simulated role (CISO, analyst, communication manager, resource manager, project manager) of a fictitious company experiencing a cybersecurity breach. They will choose what security controls will be used to defend the organization from attack. Participants also will learn cybersecurity planning, CSF strategy, communication, decision making, team building and breach response. This role-playing game helps grow cyber competencies, security control configuration, written and verbal information security communication, and financial forecasting. Each group/table of six will be assigned a company (smart and IoT-based), company roles, tokens and a baseline security strategy of controls. The facilitators and participants will roll dice to determine experience and severity with lots of entertaining yet realistic surprises along the way.

# 2022 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

## Let's Start an R-IoT: A Workshop on the Modern Threat Landscape Facing the Internet of Things

Sara Friedfertig, *Arctic Wolf*; Anders Horrocks, *Optiv*; Alexis Merritt, *Cisco Talos Intelligence Group*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, SMART ABOUT "SMART" THINGS**

**CPE CREDITS: 2**

During this interactive workshop, participants will crawl, walk and run their way through a threat landscape assessment on internet of things (IoT) devices. Don't worry - all those smartwatches will track progress along the way! Participants will crawl over types of IoT devices, common risk types, and frequent adversary techniques associated with the devices. Then, participants will walk through best practices to consider for a threat landscape assessment such as defining the parameters for IoT devices, identifying threats around devices, collecting countermeasures to combat those threats, and evaluating the trade-offs of implementing countermeasures against each threat. By preparing a threat landscape assessment, participants could drive organizational change by determining inefficient budget spending, rebalancing resource allocation and more. Finally, attendees will have an opportunity to run with their knowledge and apply a basic threat landscape analysis to an everyday IoT wearable device. The workshop will conclude with participants sharing and learning from each other's threat landscape assessment on the IoT wearable device.

## WORKSHOP SERIES

**Friday • 2:40 pm - 4:40 pm**

## Create Confidence When it Matters to Take Your Career to the Next Level

Micha Goebig, *Go Big Coaching*; Katrina Zidel, *Kreating Boldly, Inc.*

**TRACK: CAREER DEVELOPMENT**

**CPE CREDITS: 2**

It can be challenging to be seen and heard as a female professional in a male-dominated sphere like cybersecurity and exude an air of confidence when it matters. These days, visibility and confidence seem to be about as vital to taking a career to the next level as expertise and experience. In this workshop, confidence and leadership coach, Micha Goebig, will bust a few misconceptions about confidence and share practices and tools to help attendees step up their authentic visibility and confidence presence. This is for any attendees who are done not feeling seen or heard in the professional environment; who are ready to exchange the sense of not belonging for owning their uniqueness; who want to learn to show up authentically and create safety through self-trust; and need input and strategies to tap into their full potential in their career and life.

## Your Transformation: Level-Up Your Cyber Career by Translating Transferable Skills

Christina Stokes, *Salt Cybersecurity*

**TRACK: CAREER DEVELOPMENT**

**CPE CREDITS: 2**

Whether new to cyber, transitioning careers, or moving ahead as an industry veteran, it's important to take account of skills and make those skills work. This workshop will help attendees define key skill set areas, identify their own transferable skills, and determine how to translate and leverage those skills throughout a career. The cybersecurity industry needs women and allies to dive in with their full potential, not leaving any part behind. Someone's skills, whether they be from other industry roles, schools or volunteering, can assist others in reaching their goals. Transferable skills can be applied to different career paths and roles. Knowing how to identify and translate transferable skills will strengthen employees at every step of their career from entry-level to leadership positions. In this workshop, participants will look not only at hard skills but also soft skills which can transfer across different roles. They will discuss examples of where transferable skills can shine in a career while working to ensure the security goals of an organization and how to leverage them when communicating with other business units for cross-functional collaboration. During this workshop, presenters will walk through methods to prepare for next steps in a career and how to identify important skills for different roles in cybersecurity. It also will cover how to package one's skills and knowledge, align and advocate those skills for success, and effectively highlight skills and knowledge in interviews or on the job. This workshop is for everyone from new grads, career switchers and those seeking more responsibility to current leaders and industry veterans. Together people can strengthen the cyber industry by bringing everyone to the table.

## Cybersecurity – An IT Challenge or Business Priority?

Rob Rashotte, *Fortinet*

**TRACK: BEST PRACTICES**

**CPE CREDITS: 2**

Over the last couple of decades, the cyber threat landscape has evolved from annoying viruses delivered via floppy disks to sophisticated targeted attacks that can cripple a business or inflict physical damage to critical infrastructure. The list of threat actors has evolved to included well-funded organized criminal groups and nation states. In response to this, cybersecurity has evolved from a challenge for our IT departments to a critical priority for Boards and executive teams. While the technical impacts from a sophisticated cyberattack can be very disruptive and costly, the business impacts can often be far greater and can include significant fines, impact to company valuation, disruption to M&A activities, loss of brand loyalty, executive fall out and in some cases jail sentences. This workshop will explore case studies where



# 2022 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

all these impacts were felt by some well-known companies. While some industry sectors are more targeted and prone to cyberattacks than others, all organizations need to develop a good cybersecurity posture and treat cyber threat as part of their overall enterprise risk strategy. This applies equally to for-profit enterprises, government entities, academic institutions, and others. The responsibility for cybersecurity policy and risk mitigation lies squarely with our boards and executive teams. There are many challenges, both technical and business related to achieving a good corporate wide security posture. In this workshop we will explore the business challenges which include potential changes to our Boards and C-suite, selecting a cybersecurity framework, dealing with cybersecurity skills shortages, employee awareness and others. The workshop also will help demystify some of the more common frameworks from organizations such as the National Institute of Standards and Technology (NIST) and the World Economic Forum (WEF). Presenters will discuss the tools available to help organizations develop cybersecurity training and education plans designed to provide not only technical skills to IT and other technical staff, but also cybersecurity awareness training to all employees. They'll discuss the NIST Special Publication 800-50 "Building an Information Security Awareness and Training Program" as well as introduce the National Initiative for Cybersecurity Education. By the end, participants will have access to all of the resources discussed as well as access to a free online Information Security Awareness program for their employees.

## Language, Allyship and Self-Accountability: Driving Change in the Cybersecurity Industry Racial Equity Committee, WiCyS

**TRACK: BEST PRACTICES**

**CPE CREDITS: 2**

WiCyS Racial Equity Committee (REC) will present a workshop on the use of language with individuals and others, and the role everyone plays in creating change in the spaces people occupy. This includes self-accountability, taking responsibility for learning and using one's voice to set the example for others to follow in leading with courage. This workshop will explore the landscape of inclusive language in leadership and how this shift is occurring across industries to allow for more equitable environments where people can thrive. Allyship involves remembering that people don't have to do it alone and the importance of building cross-functional relationships and partnerships. The REC also will share the work they have been doing on behalf of WiCyS to support racial equity within the organization. They look forward to hearing from attendees about what is most important as a member of WiCyS regarding this topic.

## WORKSHOP SERIES

**Saturday • 2:30 pm - 4:30 pm**

### Oh Cyber, My Cyber: Rise Up and Hear the Buzzer! Explore the Tools Used to Develop YOU as the Next Generation of Diverse Cybersecurity Professionals!

**Caitlin Boyce, SANS; Doug Britton, Haystack; Lynn Dohm, Women in CyberSecurity (WiCyS)**

**TRACK: BEST PRACTICES**

**CPE CREDITS: 2**

Identifying and training new cyber talent became an urgent priority in the U.S. about a decade ago and it's only increased since, especially across the globe. Today, there is a transition toward casting a wider net to find those with capability and passion for accelerated training. Fortunately, new types of talent identification tools are being leveraged to identify high potential and skilled candidates far beyond the traditional resume search for certifications or degrees and common screening interview questions. This workshop will explore how successful talent identification and development tools have built growing, scalable programs that are not just bringing more diversity into cybersecurity but also fostering community and encouraging further learning from non-traditional cyber talent. The WiCyS Security Training Scholarship is a multi-stage program that enables every participant to gain new knowledge and skills in cybersecurity, with those progressing to the advanced stages deepening their skills and pursuing jobs immediately upon graduation. The program uses several tools common to other state and national reskilling programs that can save hiring or training managers hours of valuable time and help them make more informed decisions. Participants will work through hands-on exercises and demo different tools in real-world scenarios. They will come away with practical insights and potential solutions for their organization, whether it be a corporate, non-profit or government background. These tools are applicable to both reskilling and upskilling challenges.

### Putting Privacy in Your Pocket: Controlling Your Privacy in an IoT Connected World

**Lisa McKee, Protiviti/Dakota State University; Tania Williams, The University of Alabama in Huntsville**

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, BEST PRACTICES, SMART ABOUT "SMART" THINGS**

**CPE CREDITS: 2**

Data is an organization's most valuable asset. It is collected in everything from purchases and online activities to apps on mobile devices, leaving a digital footprint of information most are not aware is happening. Organizations are finding creative ways to monetize and share data unknowingly to users. Data breaches happen daily, and everyone is a victim of privacy violations. Each person should know how this data trail of information from IoT devices or clicks on a website

# 2022 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

leaves a digital footprint another person may view. This session will address what privacy rights are and how to take steps to manage, track and monitor a user's data, privacy and digital footprint. Join this interactive hands-on workshop, where participants will learn simple steps to be cyber safe in a connected world. The lines between online and offline lives are often inseparable. Participants will explore what privacy laws apply across the U.S. and their privacy rights. Participants will examine how to read privacy notices and know what users are consenting to when approving those website pop-ups. The workshop will cover IoT device security and the best settings to secure data while monitoring devices, and protecting users and their families. Participants also will discuss application security settings to protect their online identity. They will learn the power of OSINT techniques to identify their data online and put users in charge of their digital identity.

## Purple Team Workshop

**Nathali Cano and Elaine Harrison-Neukirch, Scythe**

**TRACK: TODAY'S TECHNOLOGY AND CHALLENGES**

**CPE CREDITS: 2**

Purple teaming is the new kid on the block, sitting between the red and blue teams. In this two hour hands-on workshop, participants will play the role of cyber threat intelligence, the red and blue team. An isolated environment was set up for each attendee to go through a purple team exercise. The workshop will kick off with a short 30-minute presentation of what a purple team is and how it is useful in cybersecurity. Following the presentation, there will be an overview of what to expect in the hands-on lab. Instructors will walk through the lab as attendees follow along in their own VMWare lab environment (provided by Scythe). In the hands-on lab portion, attendees will learn the basics of Command and Control (C2), consume cyber threat intelligence from a known adversary; extract adversary behaviors/TTPs, play the red team by creating adversary emulation plans; emulate the adversary with SCYTHE 3.3 in a small environment consisting of a domain controller, member server and a Linux system; play the blue team and look for indicators of compromise; use Wireshark to identify heartbeat and jitter; and enable Sysmon configurations to detect adversary behavior.

## Coding Security Best Practices

**Viraj Gandhi, SailPoint**

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, BEST PRACTICES**

**CPE CREDITS: 2**

Secure coding is important for every development, engineering team. Roughly 80% of software security problems are caused by insecure coding, which is why secure coding standards are essential. There are several secure coding practices to use. It is important that developers are familiar with known security vulnerabilities to avoid writing code that

is exploitable by already-discovered vulnerabilities. Adopting secure SDLC at every stage of development contributes to early identification of potential vulnerabilities and is more cost effective and less disruptive to release cycle. This workshop will educate attendees on OWASP Top 10 Security principles with examples that need to be considered in secure coding practices. Developers attending this workshop will learn coding mistakes to avoid that introduce vulnerability in the code. Code reviewers will learn how to detect vulnerabilities and help in releasing secure code. Secure coding checklist will be provided as some take home material. The workshop also will cover common pitfalls to avoid that can lead code to an insecure state in common programming languages like JAVA. A hardening guide also will be provided for securing APIs, which is widely used by organizations.

## STRATEGIC PARTNERSHIP

### Your Brand Elevated

The future of women in the cybersecurity workforce lies in our hands. Champion the cause of recruiting, retaining, and advancing women in cybersecurity by becoming a WiCyS Strategic Partner.

Your contributions are key to supporting WiCyS' year-round activities and helping women everywhere achieve their career goals in the cybersecurity field.



**Scan the code with your mobile phone camera to learn more about strategic partnerships!**

# 2022 WiCyS CONFERENCE PRESENTATION SESSIONS

## PRESENTATION SESSIONS

**Friday • 11:00 am - 11:45 am**

### **A Fine Line Between How Much You NEED and WANT to Know With Location Apps**

**Christine Horwege**, *CGI Federal*; **Cassandra Horwege**, *University of Pennsylvania*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, LOOKING AHEAD**

**CPE CREDITS: 1**

Join this session for a real-world discussion with a mother and daughter about roles and responsibilities. How many times has a parent wondered what their child is doing, where they are or who they are with? Parents want to know. The convenience of location apps and social media have made those answers much easier to find than ever before. This convenience has pros and cons related to security, privacy and trust. As users on both sides of the perspective - a parent and child - a mother/daughter team, who also are cyber experts and aspiring cybersecurity undergraduates, will discuss the implications of these location sharing apps, pose questions about the policies surrounding them, and provide insight into creating a safer and more secure interface externally and internally for location applications and services. The mother has over 15 years of experience in IT risk, compliance, cybersecurity and privacy while being a mother of three and Army veteran. The daughter is a University of Pennsylvania computer science major with over six years of coding and app development experience and an aspiring cybersecurity professional as well as a USAF ROTC Cadet.

### **Projects, Promotions and Principal Engineers or "How to Pwn Your Lane"**

**Heather Lawrence**, *University of Colorado, Colorado Springs*; **Patrice Siravo**, *Adriano Cyber Consulting*

**TRACK: CAREER DEVELOPMENT**

**CPE CREDITS: 1**

Once someone lands that first cybersecurity position, the real career journey begins. How does one pwn the workplace in this brave new world? Attendees will walk away with tips on how to find their place in the corporate mission, essential skills for technical project management, how to raise the bar on their technical edge, and how to lead from the front as a subject matter expert. The cybersecurity road may lead to the C-Suite or a technical track to the lab to perform cutting-edge research. Someone might choose to become an engineering wiz or gravitate toward technical project management. Whatever path(s) they take, they'll carry technical and professional skill sets but still need to continue growing and evolving to keep up with the changing cybersecurity environment. But how does someone pick which skills to focus on while traveling through a career? Do they need hands-on practice or will that online

webinar do the trick? Can they stay in the same company or do they need to find somewhere else to grow? Navigation is difficult, and it's different for everyone, but there are some constants that will help anyone make better decisions along the way. This presentation will provide valuable information for professionals in all stages of their careers, from their first cybersecurity position to senior-level manager and seasoned technical expert. If participants have any technical responsibilities or aspirations, presenters will outline core skill sets and growth opportunities to improve technical performance and help navigate a career to land in a role that fits one's skills and interests.

### **CVSS: Changing Vulnerability Scoring Suggested**

**Maitreyee Palkar**, *F5*

**TRACK: TODAY'S TECHNOLOGY AND CHALLENGES**

**CPE CREDITS: 1**

In the Harry Potter books, Mr. Weasley said, "Never trust anything that can think for itself if you can't see where it keeps its brain." With the ubiquity of technology in everyday appliances and critical infrastructure, vulnerability management and patching are more important than ever. Most people are taught that CVSS score is a way to tell how severe a vulnerability is. Vendors are releasing more vulnerabilities than ever for products ranging from smart doorbells to networking gear to cloud connected appliances. The criticality of these convenient devices cannot be understated - they make life easier and, in some cases, act as the backbone of the internet. In this talk, presenters will show statistical research comparing some Internet of Things (IoT) vulnerabilities to critical infrastructure vulnerabilities released between 2019 and 2021. They will answer questions about if CVSS is an outdated methodology. Their research is focused on chance and volume of exploitation from day one to 90 after release. After exploring CVSS score, they will focus on predictive research on if severity is an indicator of likelihood for exploitation. They will give details around the most likely indicators for malicious actor interest. Further, They will give tips and tricks on how to think about patching and remediation in different environments. As individuals become informed cyber citizens in this new world, it is essential for everyone's privacy that vulnerabilities are categorized appropriately. This talk is intended for all audiences where they explain in detail both the methods used and results of their work. No statistics background necessary! Outcomes are focused on impact at a high level. Participants will leave with results of this research, including new ways to think about the severity and the impact of IoT and critical infrastructure vulnerabilities on their worlds.

# 2022 WiCyS CONFERENCE PRESENTATION SESSIONS

## Taking One Byte at a Time: Securing 5G

Natalie Pittore, *National Security Agency*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES,  
LOOKING AHEAD, SMART ABOUT "SMART" THINGS**

**CPE CREDITS: 1**

Taking on a behemoth challenge such as securing 5G is a challenge, and projects like this can often bring about little tangible progress because the problem seems "too big." Through a partnership, the Enduring Security Framework (ESF) maximized its unique position as a cross-sector working group to explore the threats to 5G and subsequently take incremental steps to securing it. ESF released a publicly available 5G threat report on "Potential Risks to 5G Infrastructure" that outlines industry and government generated risks associated with U.S. adoption of 5G infrastructure. The team also followed up with best practices to mitigating threats to 5G's use of cloud infrastructure. This talk will introduce ESF, guide the audience through "Potential Risks to 5G Infrastructure," and provide best practices associated with 5G cloud infrastructure.

## PRESENTATION SESSIONS

**Friday • 1:55 pm - 2:40 pm**

### The Rugged DevOps Journey

Rachael Crowthers and Shua Gamrad, *Optum*

**TRACK: BEST PRACTICES**

**CPE CREDITS: 1**

Most software developers are concerned with writing cool code, not security. Rugged DevOps is an approach to software development engaging developers to create secure code at all stages of the software development lifecycle. This presentation will walk through the journey Optum has taken for a holistic Rugged DevOps approach. In the past few years, society has changed immensely, and the presenters will share their successes and failures in a true DevOps manner. Their approach is divided into three parts: Observability, Engineering, and Knowledge and Learning. They have provided training platforms, security documentation, and clear visibility to top priorities allowing security to be second nature. They've integrated from the beginning to make it clear, security is everyone's responsibility. They will present the topics in a fun, mockumentary-type presentation that makes participants feel engaged but covers challenging culture concepts in an approachable manner.

## Methodologies and Investigations of Cloud Security Practices in the Healthcare Industry

Remi Cohen, *F5*; Meghan Jacquot, *Recorded Future*

**TRACK: BEST PRACTICES**

**CPE CREDITS: 1**

Along with healthcare, 2020-21 highlighted the extreme vulnerability of U.S. operational technology (OT) systems that use the cloud. The COVID-19 pandemic made critical healthcare infrastructure in hospitals prime targets for ransomware and other malicious activity. The move to the cloud for critical systems has not only made life easier for many but has also given attackers a new surface with which to go after targets. In many ways, for many industries without strong traditional security controls, use of the cloud within critical infrastructure has become a trade-off between accessibility and security. This talk will have two parts. The first will focus on research methodology. Before presenting specific analysis, these researchers strive to make this talk accessible by going into depth on how to conduct a study like this by explaining the constraints, limitations and assumptions around their work. The second part will share the initial findings of a case study regarding the current practices of a variety of healthcare centers and their use of the cloud. Healthcare like industrial control systems (ICS) need 100% uptime and must always be online because there can be serious consequences regarding patient care without efficient technology. Participants will walk away from this talk with a better understanding of cloud security practices in real situations and feel armed to better assess and conduct a case study. Attendees should feel empowered to take the next step forward in their research journey and add to the body of cybersecurity knowledge.

## Mind the Gap: An Insider's View of Often-Overlooked Key Elements that Can Make or Break Your Next Career Move

Christine Winchester, *DHS Cybersecurity Service*

**TRACK: CAREER DEVELOPMENT**

**CPE CREDITS: 1**

This is not an average resume review or a one-size-fits-all approach for getting the next job. The presenter will discuss a maturity model for career move preparedness, a formula for the best resumes, simplifying a social profile, interviewing tips, building and implementing a plan for success, how to work with recruiters, and look at the future of cybersecurity through a recruiter's eyes. Participants will learn how to network better, reframe fear in interviews, write better resumes and applications and gain formulas for success. Presenter Christine Winchester works for the Department of Homeland Security, Cybersecurity Service. She is a cybersecurity talent acquisition leader with 20 years of experience in both the private and public sector, including primary experience in the competitive and cleared aerospace, defense and intelligence sector.



# 2022 WiCyS CONFERENCE PRESENTATION SESSIONS

## Toward Secure Machine Learning with Counterfit

Amanda Minnich, *Microsoft*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES,  
LOOKING AHEAD**

**CPE CREDITS: 1**

Machine learning (ML) systems represent a new frontier for cybersecurity. From self-driving cars and fraud detection to face identification and insurability, machine learning models have an immense impact on everyone's lives. Attacks that compromise any of these ML systems could cause huge levels of harm, and as such securing them should be a top priority for any organization with these models. The goal of the presenting team, the Azure Trustworthy Machine Learning Red Team, is to attack large, impactful machine learning models that belong to Microsoft and its customers to evaluate system vulnerabilities and spread awareness. They have found that robust testing of ML models does not occur regularly in most sectors and can be difficult for cybersecurity professionals to know where to start. Based on this need, they created Counterfit, an open-source generic automation framework for attacking machine learning algorithms. Counterfit wraps existing adversarial ML frameworks to bring multiple data types and algorithms into a single tool. In this talk, they will cover what adversarial machine learning is, why everyone needs to secure ML systems, case studies including a real Red Team exercise that they carried out on an internal Microsoft ML system, and a tutorial on using Counterfit to empower attendees to secure ML systems at their organizations. This talk fits nicely with this year's theme, as the security of ML systems represents an underexplored area in the space and is one of the next big frontiers the cybersecurity community needs to proactively address.

## PRESENTATION SESSIONS

**Saturday • 10:00 am - 10:45 am**

## Investing in Our Nation's High School and Middle School Cybersecurity Educators

Nikki Hendricks, *EPIC, TACC, The University of Texas*; Joy Schwartz, *WeTeach\_CS, TACC, The University of Texas*

**TRACK: BEST PRACTICES**

**CPE CREDITS: 1**

With a focus on high school and middle school cybersecurity education, this presentation will showcase a new cybersecurity preparation course for teachers. As more and more high schools are adding cybersecurity courses, there is a high demand for qualified teachers. However, there also is a lack of qualified cybersecurity teachers for this educational level. Educators are feeling uncomfortable and unprepared when asked to teach cybersecurity with little to no experience. Providing teachers with cybersecurity knowledge and education is a priority! Join this presentation as attendees are introduced to the foundational cybersecurity course for teachers developed

by WeTeach\_Cyber, EPIC at the University of Texas at Austin. Designed for teachers new to cybersecurity, this hybrid synchronous/asynchronous course introduces teachers to the fundamentals of both networking and cybersecurity. With more and more emphasis on high school students earning industry certifications and the CompTIA Security+ certification being an entry-level cybersecurity industry certification, they will look at how the course progresses educators from the fundamentals of cybersecurity to the preparation for the CompTIA Security+ certification exam. The presenter and author of the course has traveled this journey to cybersecurity, starting as a middle school librarian, becoming a high school computer science teacher, and then adding cybersecurity education, earning industry certifications and a cybersecurity degree along the way.

## Building a Scalable Cloud Native Security SIEM

Tanvi Kolte, *LinkedIn*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES,  
LOOKING AHEAD**

**CPE CREDITS: 1**

LinkedIn's Incident Response (IR) team is responsible for protecting infrastructure, applications and, most importantly, members. Until about a year ago, the IR team used an in-house system to collect logs, normalize and then build alerts. While the system was working, there were several optimization issues with the pipeline making it a roadblock for applications to ramp to production. It took weeks for an IR engineer to complete log onboarding and build detections for an application/service. The system remained a black box for site reliability engineering teams, making it hard to monitor and respond when things broke. LinkedIn took the learnings from previous processes and aimed to build a next generation logging and detection pipeline that would not just aim to reduce mean time to detection and median time to resolve, but also scale and meet requirements for the rapid development at the company. This talk shares the story of how LinkedIn developed this next generation pipeline and how they have leveraged cloud solutions that helped them automate the onboarding, detection and response processes while managing the code through a continuous integration and continuous delivery flow.



# 2022 WiCyS CONFERENCE PRESENTATION SESSIONS

## Trapped in the Wolf Den: A Dive into Compromises From Within the Walls of a SOC

Lisa Tetrault and Samantha Van Aaken, *Arctic Wolf*

**TRACK: BEST PRACTICES**

**CPE CREDITS: 1**

When it comes to mitigating the impact of any security incident, it's a race against time to ensure the safety of a team's most valuable assets. Organizations rely on email to conduct business, communicate, share information and set daily meetings. Email account compromise is an unsettlingly common method of attack for bad actors and can have a huge impact on business. Business email compromise attacks have already cost U.S. businesses at least \$1.6 billion in losses from 2013 to today. According to the Federal Bureau of Investigation, that number could easily be as high as \$5.3 billion around the world. This presentation will explore real-world examples when there is an attack starting from the detection triage boards. In this interactive session, a team of security operations experts will walk through what detection alerts they see leading up to and during different types of compromises. They will showcase the initial detections, incident response process, remediation steps, and best practices that could have mitigated various forms of common attacks. Participants will get a front-row seat into a thrilling day in the life of an SOC Analyst. Welcome to the den of wolves. They've been waiting for you.

## Protecting America's Defense Industrial Base with Cybersecurity Services

Kristina Walter, *National Security Agency*

**TRACKS: LOOKING AHEAD, BEST PRACTICES**

**CPE CREDITS: 1**

For the better half of a century, the National Security Agency/Central Security Service (NSA/CSS) has led the U.S. government in cryptology and signals intelligence (SIGINT) missions. In partnership with the Department of Defense (DoD) Chief Information Officer (CIO), NSA is actively engaged in lending its technical expertise to identify, mitigate and eradicate threats to the U.S. Defense Industrial Base (DIB). The DIB represents a large and diverse target set for America's key global adversaries who thrive on the theft of intellectual proprietary, defense information and program insights. This presentation will present the compelling story behind NSA's burgeoning DIB cybersecurity mission, one that involves actively collaborating and sharing cyber threat information to disrupt adversaries' attempts to steal critical information and protect industry partners. It also will explain how a new model of provisioning cybersecurity services to DIB companies at scale dramatically expands DoD's security umbrella and the near-term strategy plans for NSA's newest mission focus.

## PRESENTATION SESSIONS

**Saturday • 11:00 am - 11:45 am**

## Protecting Critical Environments by Leveraging OT Security Controls

Danielle Gulotta, *Security Risk Advisors*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, LOOKING AHEAD**

**CPE CREDITS: 1**

By now, the cybersecurity industry is either well aware or catching up to the need to secure OT, but these environments are full of intricacies that are new to enterprise security teams and require quite different approaches. The challenge becomes how and where to start. The answer is complex and depends on many factors, including organizational maturity, size, budget, etc. However, despite varying factors, there are several OT security controls, including asset management, network segmentation, secure configuration, and more, that can be leveraged and prioritized to help answer this question. Whether these controls are taken as-is or customized, completed together or tackled one at a time, having a framework and starting point is one of the first steps to securing OT. This presentation will introduce some of these controls and dig deeper into what they mean, how to leverage them and, of course, how to prioritize which to do first. The best approach for an organization may vary; therefore, multiple examples will be shared, including how to start with one control versus how to tackle them all together. Regardless of the audience's experience with OT, this talk will provide ideas and ways to either start or further enhance the security of their OT environments.

## Diversity is a Result of Inclusive Cultures

Deidre Diamond, *CyberSN and Secure Diversity*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, BEST PRACTICES, SMART ABOUT "SMART" THINGS**

**CPE CREDITS: 1**

An advanced society requires complex human interactions. Teamwork skills are needed at a greater scale than ever before. This means emotional intelligence or "EQ skills" need strengthening. Developing EQ starts with the desire to learn combined with the right tools to do so! This talk centers on a nine-piece framework, the Standards of Inclusive Behavior, to help participants create inclusive cultures that will result in diverse workplaces. The presenter will explore how each of the nine standards for interactions impact professional environments and how to use this framework to create equality and diversity of thought. Security, privacy, economic well-being and mental health depend on the ability to engage others positively, yet this is a skill that employers rarely teach. When establishing a baseline of standards for human interactions that are framed through the window of cybersecurity, teams and organizations can excel because expectations are clear and fair.

# 2022 WiCyS CONFERENCE PRESENTATION SESSIONS

## Federated Learning for Enabling Secure Smart Communities: Current Technologies, Challenges and Future Directions

**Smriti Bhatt**, *Purdue University*; **Deepti Gupta**, *University of Texas at San Antonio*

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, LOOKING AHEAD, SMART ABOUT "SMART" THINGS**

**CPE CREDITS: 1**

The Internet of Things (IoT) has become increasingly ubiquitous in enabling smart homes, hospitals and industries. It utilizes cloud-enabled IoT (CE-IoT) architecture to provide smart ecosystem services using smart sensors, wearable devices, medical devices, and leverages existing cloud services to sense environmental parameters, users' vital parameters, monitor specific conditions, and generate multivariate data for enabling smart communities of the future. In this domain, the security of various entities, users and privacy of data are major concerns. There is a large amount of data generated, shared and transmitted between various entities in this ecosystem. Mostly, this large amount of data is analyzed in centralized architectures for data analysis. However, there are various security threats associated with centralized architectures for smart communities. Therefore, there is a need for decentralized architecture based on federated learning for securing smart communities of the future. In this presentation, they will focus on specific use cases of smart communities, such as Industrial IoT and remote patient monitoring, and utilizing federated learning for identifying security issues in these application domains. They will primarily discuss secure authorization, access and communication control, and anomalies detection and mitigation for enhancing security and data privacy in smart ecosystems. They also will present current technologies (e.g., digital twins, edge cloudlet computing, communication protocols – MQTT, CoAp, cloud IoT platforms, etc.) with real-world use cases, challenges toward enabling such secure smart ecosystems, and future research directions and avenues to solve these challenges. This topic aligns with the WiCyS 2022 theme and should spark discussions toward enabling secure smart connected ecosystems of the future.

## Let Them In: How Cyber Deception and Adversary Engagement Leads to Better Defense

**Gabby Raymond**, *The MITRE Corporation*

**TRACK: BEST PRACTICES**

**CPE CREDITS: 1**

The classic cybersecurity paradigm is that defenders must be 100% successful in their defense to keep adversaries at bay. But what happens when they are let in? By choosing what facts and fictions are presented to an adversary in an environment someone crafted, defenders can find, understand and affect adversary behaviors in real time. Safely engaging threats leads to better understand an adversary's goals. To do this, create high fidelity, synthetic environments tailored to a specific

adversary with documents, browser artifacts and other litter. These environments can either be left as a dangle or self-infected with malware. Observing an adversary in situ can provide organizations with actionable cyberthreat intelligence. Decreasing the value adversaries derive from operations can occur by carefully passing misinformation and disrupting the use of gained information by creating plausible deniability for intrusions. By negatively impacting an adversary's operational capabilities, a defender can reduce their motivation to operate. The goal is to shift the asymmetric advantage away from the adversary and toward the defender. For 10+ years, MITRE has been engaged in denial, deception and adversary engagement operations for internal defense and research purposes. This talk will give an overview of what they've learned and built, and where they see the field growing.

## MEMBERSHIP BENEFITS

### Amplify Your Network. Amplify Your Portfolio. Amplify Your Career.

Enjoy year-round benefits of engagement with a unique and powerful community of peers in academia, research, industry, and government.

Share ideas, best practices, experiences and more with thousands of women in cybersecurity!



Scan the code with your mobile phone camera to check out all the benefits!

# 2022 WiCyS CONFERENCE

## BIRDS OF A FEATHER

### BIRDS OF A FEATHER

Friday • 4:45 pm - 5:30 pm

#### Cybersecurity Academic Integration Through Outreach

Joan Labay-Marquez, *University of the Incarnate Word*

#### TRACK: BEST PRACTICES

This Birds-of-a-Feather session will discuss how to integrate cybersecurity awareness through outreach programs that include additional degree programs within the institution to support a department's CAE-CD application for designation as a National Center of Academic Excellence in Cybersecurity. Presenters will discuss CAE-CDE program eligibility requirements and demonstrate how to incorporate a cybersecurity awareness community outreach program with a service-learning focus to support the submission of an application for the Program of Study validation component, part one of a two-part process for designation. The CAE-CDE Program is open to current regionally accredited four-year colleges and graduate-level universities; its goal is to promote and support quality academic programs of higher learning that help produce the nation's cyber workforce.

#### Why Are There so Many aaS(es) in the Cloud?

Atia Ibrahim, *Optum*

#### TRACK: TODAY'S TECHNOLOGY AND CHALLENGES

Cloud technology is everywhere and on everyone's mind. The presenter decided to get into the cloud only five years ago. In that short period of time, the cloud has changed its shapes, and the pandemic helped it grow into cumulonimbus. The presenter had to change their 20 years of data center security mindset and use experience to support a current position as cloud security architect. This session will help remove some common mysteries and fears about cloud and help beginners in cybersecurity get a better understanding of cloud security. Discussions will revolve around how cloud security is different than data center security, why things in the cloud have aaS (as a Service) attached to them, and how aaS(es) play a role in cloud security. Examples will be provided on aaS(es) that impact daily lives. Netflix - is it a SaaS or PaaS? Conversation will be encouraged to remove the mystery about the cloud and cloud security.

#### I've Got a New Attitude - Staying Motivated, Inspired and Focused in a Cybersecurity Role

Jerry Hache and Marti Mondragon, *Palo Alto Networks*

#### TRACKS: BEST PRACTICES, CAREER DEVELOPMENT

Everyone faces challenges and encounters obstacles throughout their careers. Managing conflicting schedules, juggling priorities, trying to maintain work-life integration, and meeting the unique demands of a cybersecurity-related career can seem overwhelming. Past experiences already have provided people with many tools needed to successfully

overcome challenges posed by their career path. Learn how to identify those tools and continue to add to the list of tools in future endeavors/experiences. This session will talk about avoiding burnout and stress as well as managing it when it does occur. Join this informal, interactive discussion as presenters share their experiences, insights and secrets for creating a new attitude that will help lead more effectively and focus clearly on the tasks at hand and spark inspiration!

#### What Strategies Work To Make You Stay

Meg Layton, *Children's National Hospital*

#### TRACKS: BEST PRACTICES, CAREER DEVELOPMENT

This is an interactive discussion with women in the workforce. A number of studies have shown that while interacting with the pipeline get women into cybersecurity, many women are opting out at later points in their careers. This is meant to be an exploratory session to discover what organizations are doing to help keep women engaged throughout their careers, and what organizations should avoid as they look to diversify their workforce. (ISC)2 research reports that there isn't much difference between what men and women cybersecurity professionals value about their jobs, sharing workplace values, priorities and aspirations. Yet, women at senior levels or who have stayed in their careers can be a rarity. This session will talk about strategies that have made participants stay, the well-intentioned organizations that maybe do not have strategies that work, and how to make sure one's career is around for as long as it's wanted. Everyone has lists of what works, what doesn't and where things can improve.

#### Cultivating Women as Leaders - The Role of Allyship

Kip Bates, *University of California, Santa Barbara*; Reema Moussa, *University of Southern California, Gould School of Law*

#### TRACK: BEST PRACTICES

Everyone has heard the stats -- with only 25% representation, there simply aren't enough women in cybersecurity. Another dominant problem often overlooked is women's retention and leadership in cyber, which contributes significantly to the disparity between the prevalence of women and men in the cybersecurity field. Join Reema Moussa and Kip Bates for this roundtable discussion on the importance of male allyship in fostering women's leadership in the cybersecurity sphere. In this Birds-of-a-Feather session, participants will be encouraged to discuss their experiences and perspectives on how to instill in their organizations the mission of promoting women in cybersecurity and how it isn't solely a women's issue but a priority for everyone in the cybersecurity field.

# 2022 WiCyS CONFERENCE PANEL SESSIONS

## PANEL SESSIONS

**Friday • 12:00 pm - 12:45 pm**

### **It Takes Many Sailors to Move this Ship: Populating the Cybersecurity Workforce with Talent From Diverse Backgrounds**

**Joanna Grama**, *Vantage Technology Consulting Group*;  
**Jennifer Pacenza**, *REN-ISAC*; **Amy Starzynski Coddens**,  
*Indiana University Bloomington / REN-ISAC*

#### **TRACK: BEST PRACTICES**

The term cybersecurity conjures up visions of hoodie-wearing hackers in dark rooms or funky crime lab assistants who magically find the missing piece of evidence with a tap of a few buttons. In reality, securing networks, devices and data adequately and sufficiently requires much more than a single, mythical hacker. The smart, efficient and innovative security team is multidimensional and professionally diverse. Creating this kind of team requires more than information technology experts; it requires policy experts, business analysts, communicators, event coordinators, grant writers, and, of course, the engineers, system administrators, networkers, and lab assistants with their magical evidence-finding skills. This session will be led by former lawyers, educators and writers whose career paths all took the strange yet rewarding turn toward cybersecurity. Through an open conversation, participants will come away with a better understanding around how various backgrounds and professional experiences can benefit a cybersecurity organization. The session will enable attendees to understand the professional diversity needed to create smart, adaptive security teams; fulfill organizational needs and goals; and encourage career satisfaction and employee retention.

### **The Power of Six: Creating Cyber Experiences and Building a Talent Workforce Pathway for Women and Underrepresented Students**

**Laura Freeman**, *Virginia Tech National Security Institute*;  
**Sharon Hamilton and Lauren Provost**, *Norwich University*;  
**Linda Riedel**, *The Citadel*

#### **TRACK: BEST PRACTICES**

In 2017, six universities joined together (Power of Six) to establish a pilot program to demonstrate their ability to develop cybersecurity talent pathways for women and underrepresented students for civilian and military positions in the Department of Defense (DoD). Norwich University, University of North Georgia, The Citadel, Texas A&M, Virginia Tech and Virginia Military Institute share a common identity as senior military colleges but had never previously teamed up to create and fund academic, experiential and research opportunities for cybersecurity students. In 2018, the Power of Six built bipartisan federal support of senators and congresspersons to insert language in the 2019 National Defense Authorization Act to establish DoD Cyber Institutes.

In 2019, the Power of Six built the support for authorizations to fund this pilot effort to help fill the cybersecurity workforce gap. Using a common framework - the Cyber Leader Development Program - the "Power of Six" just successfully completed their first pilot program year! Panel focus: The DoD Cyber Institute team is excited to share their pilot program insights, lessons learned and strategies with other universities and community colleges interested in developing similar cybersecurity opportunities for women and underrepresented students.

### **The Skills Gap Wish List: Students, Industry and Academia**

**Dr. Brandy Harris, Pam Rowland, Niya Patterson, and Irene Vallalabos** *Grand Canyon University*; **Tamyria Williams**, *TWC CORE Consulting, LLC*

#### **TRACK: BEST PRACTICES**

"I wish you knew..." This conversation started at the 2021 WiCyS conference with industry partners sharing the gaps they have experienced when hiring students as interns or new hires. Students also have been asking, "What can I do to prepare myself for a career that will set me apart?" Academia is eager to help fill the skills gap and educate students to be prepared professionals. This panel will discuss specific needs, strategies and opportunities for student success. **INDUSTRY** - this is the time to share with academia and students the key skills and knowledge needed to fill the gaps seen in new hires and interns. **ACADEMIA** - this is the time to hear from students and industry on how to better prepare students for success. **STUDENTS** - share what to do and learn how to set themselves apart and become better prepared for a career in this exciting field. Together, key takeaways will be produced that can be shared with the entire community. Students will walk away with creative ideas on how to position themselves for success. Industry will provide specific ways that students can prepare for the field and make connections with some of the brightest and most engaged students. Academia will take away strategies as the conduit between students and industry.



# 2022 WiCyS CONFERENCE PANEL SESSIONS

## You've Got This: Stories of Career Pivots and How to Successfully Start a Cyber Career

**Jennifer Bate**, *Deloitte*; **Jennifer Cheung**, *NWIC Pacific*; **Meghan Jacquot**, *Recorded Future*; **Ashley Richardson-Sequeira**, *Palo Alto Networks*; **Alma Maria Rinasz**, *Bug Bounty Services*

### TRACK: CAREER DEVELOPMENT

A panel of four women, none of whom started in cybersecurity, who successfully pivoted to the industry will be moderated by another cyber professional who has a story to share after a long career gap and return to the field. Emphasis and care were given to put together a diverse panel with a variety of backgrounds, experiences and belief in #ShareTheMic. Two panelists are veterans and two are BIPOC. Each panelist has her own story, but they have common threads of collaboration, curiosity and determination. Questions will be carefully crafted to deliver a nuanced perspective to the audience. The hope is that conference attendees have takeaways regarding representation (they can see themselves in the panel) as well as concrete ideas for how to pivot (if applicable), start in cyber and be successful in the industry. The panel will end with a question and answer session as well as networking to get to know the panelists. All panelists are involved in WiCyS and encourage women in tech and cybersecurity, so part of the panel's focus will be to encourage attendees that they can be successful wherever they are in their journey.

## The Amazing Race – Coordinating Cyber Vulnerability Disclosure

**Cheri Caddy**, *U.S. Department of Energy*; **Lindsey Cerkovnik**, *Department of Homeland Security*; **Melissa Vice**, *DOD Cyber Crime Center (DC3)*

### TRACK: BEST PRACTICES

The white hats all around the globe want to find significant cyber vulnerabilities, and take action, before the black hats. The U.S. government is making significant investments in finding key technical vulnerabilities. That's actually the easy part. The bigger challenge is what happens after discovery – working with manufacturers on technical mitigations; assessing potential impact; working with impacted system owners in the public and private sectors; getting the word out about cyber vulnerabilities to entities who can take action; and publicly disclosing vulnerability information. This is a complicated dance that requires coordination among many internal and external stakeholders. This is an amazing race against time. This panel features “thought leaders” from three federal departments – Department of Energy, Department of Homeland Security and Department of Defense - Air Force – who are deeply involved in the cyber vulnerability discovery and disclosure mission, community coordination, and building the processes needed to realize national outcomes, specifically, increasing the resilience of interdependent critical infrastructure. Cyber vulnerability disclosure is a significant current challenge as well as an emerging area of focus while developing innovative methods

for cyber vulnerability discovery. As the U.S. government drives toward a whole-of-government, enterprise approach to innovative smart solutions for the challenges on the horizon and new opportunities arise for existing leadership and newcomers to cybersecurity. This multi-sector talk will touch on best practices for institutional/academic research and development, cyber supply chain risk management for the Defense Industrial Base (DIB) and Energy Sector Industrial Base, and priorities for implementing the innovative technology required to solve tomorrow's challenges today.

## WICYS COMMUNITIES

Visit the WiCyS Professional Affiliate and Student Chapter community tables at the conference to learn about the growing networks of like-minded individuals within WiCyS in your region or school!

### Professional Affiliate Community

No matter who, or where you are, WiCyS provides you with the resources to connect, mentor, learn from and encourage other members. Interested in forming a new WiCyS Affiliate or associating with an existing one?

Scan the code to learn more about WiCyS Professional Affiliates.



### Student Chapter Community

WiCyS Student Chapter members gain access to industry and academic leaders who are eager to help them succeed. Student Chapter leaders also receive prioritized opportunities for WiCyS initiatives. Come together with your school's community of students in cybersecurity and start a WiCyS Student Chapter or join an existing one!

Scan the code to find details on how to start a student chapter or to view a list of current chapters.





# 2022 WiCyS CONFERENCE LIGHTNING TALKS

## LIGHTNING TALKS

**Saturday • 10:00 am - 10:45 am**

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES,  
LOOKING AHEAD, BEST PRACTICES, CAREER  
DEVELOPMENT**

**CPE CREDITS: 1**

### **Economics and Ethics Behind Successful Free and Open Source Security Projects**

**Olivia Gallucci, Rochester Institute of Technology**

Many organizations use Free and Open Source Software (FOSS) to build products and implement procedures. Yet, there is a lack of understanding, acknowledgment and support of the FOSS community in the cybersecurity industry, creating gaps in security knowledge. This presentation by Olivia Gallucci and professor Stephen Jacobs explores the relationship between FOSS and closed-source vulnerabilities, FOSS lifecycles, and FOSS security trends in projects including and excluding Freedom 3 (i.e., the ability to redistribute modified programs). It also examines the social workings and economic development behind successful FOSS projects and communities. The goal of this research was to document the history of FOSS projects, illustrate how organizations use FOSS projects, and determine effective security practices. The research highlights the importance of FOSS in cybersecurity, including things like documentation, collaboration and human rights. Research methods include an extensive reading of published research, journal articles, statistics, CVEs, and press articles on security threats and mitigations.

### **Rust - Trust or Bust?**

**Diane Stephens, University of North Georgia, University of Georgia**

Rust is a new memory-safe programming language rapidly gaining momentum. What began as a research project at Mozilla is now part of the production Firefox browser and credited with significant performance improvements of the popular browser. Anyone who has used any of the following: Dropbox, Coursera, Cloudflare, OpenEthereum, Braintree, npm or Samsung SmartThings has used Rust in production. Rewriting the Linux kernel in Rust is getting serious consideration. Three compelling reasons to consider a switch to Rust is safety, speed and fearless concurrency. Memory safety problems that lead to security vulnerabilities in software are resolved at compile time through Rust's ownership and lifetime models. Every reference in Rust has a lifetime that prevents invalid references and enables concurrency without race conditions. There is no garbage collection because there are no references to clean up. With traditional memory vulnerabilities eliminated at compile time, Rust offers extremely fast runtime performance. It performs faster and is safer than C. Despite the benefits of safe and efficient code, Rust looks different from other programming languages and therefore has a reputation for

being difficult to learn and frustrating to compile. This talk will make sense of some oddities in Rust code, show how to avoid compilation headaches by understanding the ownership and lifetime models, demonstrate how it achieves memory safety, and assess what a transition to Rust might look like.

### **The Malware Did It!**

**Modhuparna Manna, Louisiana State University**

Imagine teaching 12-year-old kids and suddenly the computer starts showing indecent photographs. Should the teacher be charged? What if the instructor has no clue where they came from? This exact scenario happened with Julie Amero on Jan. 5, 2007, while she was teaching school kids. It turns out she had nothing to do with the pictures shown. Instead, the NewDotNet spyware was responsible for downloading inappropriate photos on her computer. This is a typical case of Trojan defense, where the accused appeals that malware is responsible for a crime they are being held responsible for. Sometimes, the defendants are speaking the truth while in other cases, the culprits blame malware for a crime they have committed. In this presentation, attendees will learn about Trojan defense and the challenges faced by forensic experts in cases due to the sophistication of modern malware. The presentation will conclude with a discussion on file-less and memory-only malware and the role modern memory forensic techniques play in identifying actual Trojan defense cases.

### **The Peanut Butter and Jelly Sandwich of Cyber Offense and Defense**

**Breanna H. and Laura L.**

The idea of blending cyber offense and cyber defense together sounds great. Though seemingly easy, like making and enjoying a peanut butter and jelly sandwich, there's something so different yet incredibly beneficial about merging these two completely diverse and opposite flavors of cyber ingredients together. At the same time, it may not be for everyone's palate. The emerging trend of blue and red teaming (a.k.a. purple teaming) sounds easy, but oftentimes can be far more challenging than meets the eye from a technical standpoint as well as a diversity and inclusion perspective. Systemic culture divides, old-fashion ideals, turf wars, a lack of leadership and resourcing, and the enormous knowledge transfer and access to critical information are just a few of the issues that can either help or hurt an organization's ability to purple team and make forward progress with this rightfully named coalition of the willing.

# 2022 WiCyS CONFERENCE LIGHTNING TALKS

## Hosting WiCyS Conference: Cleveland Inside Story

Shilpa Kedar, *Cleveland State University*; Gordan Taylor, *Destination Cleveland*

Hosting WiCyS can have a positive economic impact on local industry and the host city beyond the actual dates of the conference. Cleveland State University (WiCyS 2022 Local Host) and Destination Cleveland, the region's destination marketing and management organization, have partnered with other local public, private and nonprofit organizations to maximize the potential for talent attraction, development and retention through engagement opportunities that invite attendees' home to Cleveland and engage the local community in the mission of WiCyS.

## LIGHTNING TALKS

**Saturday • 11:00 am - 11:45 am**

**TRACKS: TODAY'S TECHNOLOGY AND CHALLENGES, LOOKING AHEAD, BEST PRACTICES, CAREER DEVELOPMENT**

**CPE CREDITS: 1**

### Ditch the Dichotomy: Embrace the Rainbow

Kaitlyn Bestenheider, *RSM US, LLP*

While new to the field, novice cyber professionals are constantly taught in dichotomies: Red Team vs. Blue Team. Black Hat vs. White Hat. These dichotomies divide people and are not truly reflective of the various roles and mindsets it takes to address the robust cybersecurity landscape. Using basic color theory and the NIST NICE Framework, Kaitlyn will present a better model to show the full spectrum of career options within the cybersecurity rainbow.

### Importance of Personal Gender Pronouns in and Out of the Workplace

Ruchira Pokhriyal, *Amazon Web Services*

If a person has never had to worry about which pronoun others use, the idea of gender pronouns might not seem important to them. This is where the gap of inclusion lies, that everyone needs to work on. The idea for this talk is to promote inclusion by enabling conversations about people's gender pronouns, to make more people aware that they can't always "guess" someone's gender pronouns just by looking at them. A society consists of people who are transgender, nonbinary or gender nonconforming and may choose to use pronouns that don't conform to binary male/female gender categorizations. Building gender inclusiveness in the workplace is an important step toward respecting diversity and equity. Educating more people about respecting an individual's pronouns will bring awareness to something that many people might not have thought about before and teach them why using correct personal gender pronouns is an important part of people's identity, which needs to be respected.

### TrustTalk with TikTok

Sydney Ng, *TikTok*

Today, everything is just one tap away. One thumbprint, one face scan, and one password can be used to unlock everything from social media accounts to electronic devices and even the front doors of homes! This current digital age integrates lives tightly with identity. If stolen or compromised, every aspect of one's daily lives could suffer irreparable damages. With one billion active users, TikTok is one of the leading platforms for short-form video content, and they are making it a mission to keep the identities of each and every creator and viewer safe. To keep this app up and running, they have millions of physical and virtual machines that process trillions of workloads, each of which can contain personal and sensitive user information.

## WICYS CODE OF CONDUCT

The WiCyS Code of Conduct applies to all events, platforms or WiCyS program attendees, speakers, sponsors, partners, vendors, facilities staff, volunteers, committee members, WiCyS members, and board members.



Scan the code with your mobile phone camera to view the full WiCyS Code of Conduct.

# 2022 WiCyS CONFERENCE LIGHTNING TALKS

How do they keep all this confidential data secure and ensure their applications have not been breached while preventing malicious attackers from disguising themselves as internal actors? TikTok has built a Zero Trust Framework that manages all of this (and more)! It assumes all external and internal processes cannot be trusted until they have successfully verified their identity, ensuring that everything within the domain remains protected. Zero Trust is the new industry approach for managing cryptographic identities and has already been adopted by Facebook, Google and many other companies. Come learn more about how TikTok's Zero Trust Network is revolutionizing the way they prevent service-level attacks and keep user information safe.

## The Top Reasons Why Employees Hate Internal Phishing Programs and What You Can Do About It

**Ashley Rose**, *Living Security*

One of the most tried and true methods for companies to gauge their cybersecurity and discover vulnerabilities in their networks is conducting phishing penetration tests. They provide valuable data and are an important part of enterprise security, but most employees hate them, and sometimes with good reason. Think of the incident in December 2020 when GoDaddy.com sent employees an email offering them a holiday bonus that turned out to be a phishing test. Tactics like this erode trust and make it impossible to build the positive security culture that every company should strive for. Given that phishing tests do routinely help cybersecurity professionals spot gaps in their security and shore up defenses, it's important to find a balance between keeping the enterprise secure and maintaining positive employee morale surrounding cybersecurity training. This session will break down top mistakes companies make when implementing a phishing simulation program that erodes employee trust and the key steps to building a culture that generates proven, lasting change in behavior.

## Developing a Corporate-Wide and Global Women in Cyber Affinity Group

**MacKenzie Cavanagh**, *GE Gas Power*

Many global companies over the past two years have enhanced efforts to increase diversity and inclusion within the technology and engineering space. GE is a company that historically has supported many of its minority employees through affinity networks such as the Women's Network and the African American Forum. However, there still remains a gap in many functions that would support women in technology and specifically women in cybersecurity. At the beginning of 2021, an effort was started amongst a group of women leaders at GE to start a group dedicated to women in cybersecurity at GE by supporting them through three important pillars - connections, impact and mentoring. This group combined the many divisions in GE (Gas Power, Aviation, Healthcare, Corporate) and from all over the world to come together for knowledge sharing and mentorship. This talk will highlight

the journey to starting this group; from sending their first representative to WiCyS in Denver 2021 to having a speaker at WiCyS 2022, and for future plans for increased recruiting.

## Leaders - Stop Performance Review Panic!

**Pam Rowland**, *Grand Canyon University*

Strengths, weaknesses, feedback, goals. These words combined with "performance review" can conjure up panic in employees. The cybersecurity warriors on a team often find performance reviews intimidating and unnerving. This lightning talk will suggest five questions to alleviate the panic and provide a valuable conversation for a business and its employee. In a field where there is plenty of data pointing to a shortage in cybersecurity talent, retaining employees is imperative. Twenty years of performance reviews on the employee side and now on the supervisory side provides some entertaining anecdotes of panic at the review. Employees have some of the best ideas, but using the traditional methods by which performance reviews are conducted will not yield valuable insight. Stop the panic and calm the waters. These five questions will change the way a business conducts reviews.

## Data Provenance Defense Strategies for GPS Spoofing in Autonomous Vehicles

**Lalitha Donga**, *Rochester Institute of Technology*

Autonomous vehicles are transforming transportation systems, allowing travel from place-to-place without requiring human drivers. They use vehicle-to-vehicle (V2V) mechanisms to share data with other cars and vehicle-to-infrastructure (V2I) mechanisms to share data with road infrastructures. Although such connectivity helps vehicles gain full situational awareness to make smarter decisions on the road, it also introduces several critical security risks. Sensors -- laser, radar, camera, Global Positioning System (GPS), and light detection and ranging (LiDAR) -- permit autonomous vehicles to acquire information about their environment to permit safe navigation. However, these sensors generate around 25 GB of data per hour. According to AAA, an average American spends around 17,600 minutes driving annually, and so a single autonomous vehicle could potentially generate around 300 TB of data annually. Even though autonomous vehicles have several potential benefits, the vast amount of data they possess makes them a likely target for a variety of security attacks. GPS spoofing is one attack on authentic data where an attacker sends a counterfeit signal to override the actual GPS satellite signal. Such inauthentic GPS data can cause cars to crash or get directed elsewhere for malicious purposes. Effective defense strategies are needed to combat GPS spoofing to improve the safety of autonomous vehicles. Current defense strategies for GPS spoofing are mainly effective on simpler attacks, but their effectiveness against more complex attacks is unknown. Data provenance (authenticating the origin of data over time) is a promising approach that could ensure the data used by autonomous vehicles is not just from a trusted source but also has not been maliciously modified in transit.

# 2022 WiCyS CONFERENCE

# STUDENT POSTERS

## STUDENT POSTERS

Friday • 9:45 am - 11:00 am

### 1. A Dark Web Pharma Framework For A More Efficient Investigation Of Dark Web Covid-19 Vaccine Products

Francisca Afua Opoku-Boateng, *Dakota State University*

The COVID-19 pandemic has restructured the demand for goods and services worldwide. The combination of a public health emergency, economic distress and misinformation-driven panic have pushed customers and vendors toward a shadow economy. More specifically, this global pandemic has sparked a booming COVID-19 black market on the dark web – a sinister complement to the internet- where illegal goods and services are both advertised and sold. Criminals and scammers have patronized and exploited the deep dark web section of the internet to engage in several criminal activities. The dark web is a segment of the World Wide Web and driven by financial gains. As COVID-19 cases increase, the demand for mitigation and curative products like personnel protective equipment (PPE), vaccines and other solutions have driven the illicit markets and organized criminal activities. Although several research studies have been conducted around the dark web and its markets as well as investigating it, these studies have not leveraged the open-source intelligence and its associated tools for investigating COVID-19 vaccines on it. Neither do these researchers present any tool to aid the pharmaceutical industry during investigations on their products, specifically COVID-19 vaccines that are being procured on the dark web. As it becomes more recognized by normal web users during this pandemic, how to perform cybercrime investigations in the dark web turn into a challenge for manufacturers, investigators and law enforcement officers. Due to this, this research is working to (1) understand the dark web in general, and the impact its markets have on the pharmaceutical industry during the time of this pandemic; (2) comprehend the demand and supply of various COVID-19 vaccine products that are procured on the dark web; and (3) ultimately create a dark web pharmaceutical investigative framework, which can be utilized by the pharmaceutical industry, manufacturers, investigative analysts and law enforcement to better understand and navigate that space appropriately as they investigate illicit activities or cybercrimes. The proposed framework will be in the form of a methodology with four phases/steps. This framework will be explored by pharmaceutical investigators and be built upon the known Justine Nordine OSINT framework template -- a web-based tool developed by Justine Nordine, primarily in the JavaScript programming language. The research will apply a qualitative research method approach (the grounded theory tagging and thematic analysis) to evaluate the proposed framework. Ultimately, the research findings will serve as a reference paper and contribute significantly to the pharmaceutical investigators' community as well as both the OSINT and dark web investigative communities. The document will help all parties understand what is being researched in this area and provide them with necessary information to highlight

some challenges and even solutions discussed throughout the research.

### 2. A Hybrid Approach Toward Efficient and Accurate Intrusion Detection for In-Vehicle Networks

Linxi Zhang and Di Ma, *University of Michigan, Dearborn*

With recent advancements in the automotive world and the introduction of autonomous vehicles, automotive security has become a real and important issue. As modern vehicles built with tens of electronic control units (ECU) are connected to in-vehicle networks, the controller area network (CAN) has become a target of cyberattacks. The anomaly-based intrusion detection system (IDS) is considered one effective approach to secure CAN and detect malicious attacks. Currently, there are two primary approaches used for intrusion detection: Rule-based and machine learning-based. Rule-based approach is efficient but limited in detection accuracy while machine learning-based detection has comparably higher detection accuracy but higher computation cost at the same time. In this paper, we propose a novel hybrid IDS that combines the benefits of both rule-based and machine learning-based approaches. More specifically, we use machine learning to achieve a high detection rate while keeping the low computational requirement by offsetting the detection with a rule-based component. Our experiments with CAN traces were collected from four different vehicle models that demonstrate the effectiveness and efficiency of the proposed hybrid IDS.

### 3. An Exploration of Security Concerns Surrounding Cloud-Based Electronic Health Records

Gargi Nandy and Deanna House, *University of Nebraska*

Adoption of electronic health records (EHR) and the need for anytime access have driven many providers to move to cloud environments. The utilization of cloud providers for EHR storage and access provides more flexibility for healthcare providers, patients and medical facilities. EHR were created with the intent to collaborate amongst providers, patients, labs or other trusted parties involved in a patient's care. These health records include medical history, immunization records, test results, insurance provider details, social security number, treatment history and other sensitive personal health information. Cloud computing is an emerging technology because of its adaptability, domain compatibility and better service use. It is gaining popularity among healthcare industries due to low costs and "pay-as-you-go" features. The burden of on-premise hardware and infrastructure needs is placed on a cloud provider with benefits of high performance and computational capabilities realized by users. Despite clear benefits, the security risks and vulnerabilities are great. They include data breaches, malicious insider attacks, accidents, privilege abuse, IP attacks, API and browser vulnerabilities, and denial of service (DoS/DDoS) attacks. There are challenges working with the vast amount of healthcare data and making sure it remains secure and private. Many health data incidents



# 2022 WiCyS CONFERENCE STUDENT POSTERS

happen, which justifies a need for research in this area to combine both healthcare and security perspectives. We explore research and reports on healthcare cloud-based data leakage, data breaches and information-related security incidents and categorize them into external and internal attacks. We provide insight into the root cause of these attacks to determine where gaps may exist. The research helps us provide key areas to focus mitigation efforts on and predict better risk assessment and risk management strategies to understand vulnerabilities.

## 4. At What Age Should a Child Start Learning About Cybersecurity?

**Georgia Tyner, SUNY Empire State College**

A, B, Cybersecurity...How early can a child start learning about cybersecurity? From the first time a child uses a cellphone, tablet or computer, they should be protected from cyberthreats. If their device is protected, that child is encountering cybersecurity. What should they know, when should they know it, and can they learn about cybersecurity at an early age? What is the best way for them to learn? In this paper, I will research what age children begin to learn about cybersecurity. I will research what type of cybersecurity education currently exists, online, in-person, through books, e-books, comic books or games, for children in pre-K to high school. I will look at the types of cybersecurity education and the success rate of the path of a cybersecurity career, if it has been around long enough to claim influence. There are many reasons we would want our children to know about cybersecurity. It could be a fruitful career, and the knowledge can protect them from predators, malware and malicious ads, to name a few. If parents don't understand cybersecurity basics, how can they teach their children? What help is out there? In this research, I will use systematic literature review as a research method as well as review existing programs and their effectiveness.

## 5. Building Detections for Fileless Ransomware Using Machine Learning and Binary Visualization

**Sylvia Azumah and Nelly Elsayed, University of Cincinnati**

The continued evolution and diversification of ransomware has established various threats that have become severe problems for businesses and organizations. As ransomware has become an increasingly used technique by threat actors to compromise systems with the aim of extracting more ransom, there is an ever-increasing need to develop better mitigation techniques to detect and block them before they occur. According to a SonicWall report, ransomware attacks rose by 62% worldwide and 158% in North America alone between 2019 and 2020. Statistical projections predict an increase in these metrics, considering the threat landscape grows exponentially with more institutions gravitating toward a remote workforce situation. Conventional detection methods, such as signature-based solutions used by antivirus and other traditional endpoint solutions, are ineffective at detecting modern ransomware tactics. This is primarily due to a novel

mode of carrying deploying malware known as "Fileless" malware. It involves deploying malware payloads with the malicious code embedded in native scripting languages or written straight into memory using administrative tools such as PowerShell and WMI. Since these payloads are not written to a disk, traditional solutions are often left in the dark about these executions. Studies have established that these attacks are 10 times more likely to succeed than file-based ones. What makes Fileless malware so insidious is also responsible for making them so prolific and effective. Machine learning algorithms over the years have expanded with great results in cybersecurity and more applications. Currently, security defenses available to mitigate the attacks are ineffective, hence bringing forth the development of novel techniques. This study focuses on introducing a novel approach for creating detections for Fileless malware using a combination of machine learning and binary visualization. The proposed method will investigate the malware and efficiently detect malicious payload to minimize the rate of ransomware.

## 6. Comparative Analysis on IoT Memory Images Generated Using Hardware and Software Acquisition

**Ramyapandian Vijayakanthan and Aisha Ali-Gombe, Towson University; Irfan Ahmed, Virginia Commonwealth University**

In recent years, memory analysis has become a crucial building block for incident response, cybercrime investigation, security and privacy analysis. This research work provides a comparative evaluation of IoT memory acquisition methods. The overarching objective is to explore the pros and cons of the acquisition methods and, by extension, their reliability and accuracy in memory forensics. Our research develops modular and dynamic testbeds using different sensors and hardware settings from which we will build the corpus of IoT memory images. We leverage free and open-source IoT applications to develop apps such as a smart thermostat, smart hygrometer, smart lock, smart garage, smart game app monitor, smart breath detector, smart geo-location tracker, smart check-in, smart water quality detector, smart plant pot monitor, etc. Next, for each app built and executed in our testbed, we utilize two memory acquisition methods: JTAG for hardware and LiME for software to acquire the memory image during each execution. Finally, in the analysis phase, we explore the similarities and differences between each set of memory images collected from the same app. Our evaluation performs a comparative analysis of the 50 memory image sets (25 generated using hardware and 25 using software) in terms of their bit-pattern using distance measure, image size, recovered strings, code and the remnant of in-memory data structures.



# 2022 WiCyS CONFERENCE STUDENT POSTERS

## 7. Detecting Polyglot Files Using Binary Classification with Machine Learning

Mary Adkisson, *Tennessee Tech University*

Malware is software designed to intentionally harm computer systems. Common methods of malware delivery rely on the system user to click a link or open an email attachment. While malware protection tools exist for detecting malicious files, one file type, a polyglot, can evade basic detection. A polyglot is a file that can be interpreted as more than one file type. Basic polyglots have nested extensions, allowing them to spoof detectors that only scan the file type descriptor (.exe, .jpg, etc.). More sophisticated polyglots take advantage of magic numbers, which, if present, are usually located at the beginning of the file and use a unique signature. Certain command line tools look at magic numbers to determine file type. However, malicious data can be stored after and around magic signatures, and such data might not start at the first byte of the file. Therefore, neither of these methods are sufficient for accurately detecting file type. In this project, we scanned the entire contents of a file before making a decision about type. We used binary classification with various machine-learning algorithms to understand how to assign a label to a given file input. The input we used was a combination of single-type files and benign polyglots. We compared the accuracy and speed of five classification models for training and testing: Random Forest, Support Vector Classification, Stochastic Gradient Descent, Gradient Boosting and Catboosting. Using our collection of 9,574 files, we ran these models in the range of 0.112- 492 seconds, with an accuracy range of 91.2%- 100%, depending on the algorithm. Our results showed that the optimal classification algorithm was Random Forest: it trained in 1.09 seconds and was 100% accurate. By successfully labeling files, we can improve security in file downloads and malware scanners.

## 8. Developing Defects in Privacy: The Challenge of Engineering Privacy in iOS App Groups

Maryam Aldairi, *University of Pittsburgh*; Arjun Brar, Akanksha Bubber, Hanan Hibshi and Kuixi Song, *Carnegie Mellon University*; Daniel Votipka, *Tufts University*; Marjan Salamati-Pour, *Penn State University*

The iOS file system uses sandboxes to prevent information leakage between applications (apps). App group containers (app groups) are part of an iOS sandboxing feature that allow developers to establish a shared container between apps. Although the intent behind app groups is to facilitate app development and improve the user experience when interacting with multiple apps, this design choice raises privacy concerns. An app could gain access to user information from another one in the same app group, even if a user did not urposefully allow cross-application sharing. Furthermore, if a developer does not sufficiently protect the information in all apps in the group, third-party libraries included in one app could introduce unforeseen privacy leakages. Our research investigates the potential iOS data leakage threat from app

groups and presents empirical evidence that developers are most likely unaware of the leakage threat. We inspect the top 200 free apps on the iOS U.S. app store to assess the adoption of groups. We evaluate our threat model through a case study where we analyze Facebook and Google iOS application families and a proof-of-concept iOS app group. We also present findings from a user study involving viewpoints from mobile app developers and end-users to measure the differences between their understanding of data sharing and privacy. Our results show there are no current restrictions or enforcement mechanisms protecting data shared across app groups. As we identify in our case study, this allows apps to gain implicit access to sensitive data. In addition, developers are unaware of the privacy risks of app group sharing, and therefore are unlikely to take necessary mitigation steps. The user study shows the different privacy perspectives and expectations between developers and end-users. We propose possible mitigation approaches and provide recommendations and guidelines to help mobile app developers avoid unforeseen privacy concerns and remain in compliance with data-sharing laws and regulations.

## 9. Exploring Side Channel Data for Detecting Malicious Software

Rebecca Clark and J. Todd McDonald, *University of South Alabama*; Lee Hively, *Oak Ridge Nat'l Lab (Retired)*

Rootkits are pernicious types of malware with administrative-level privileges that obtain access or control of a computer system. They often hide themselves effectively against detection mechanisms because they have the ability to alter system data and essentially lie to an end user. Side channel data such as CPU power and temperature, however, are outside the scope of a rootkit to alter. In this research, we use CPU power analyzed by a nonlinear phase space algorithm to detect rootkit execution. We collect CPU power measurements with a Data Acquisition System (DAQ) while test computers are in various states of activity (normal, stressed and manually controlled) and in either infected or uninfected states. We also compare results of our novel nonlinear phase space approach to common machine learning algorithms used in similar research. We train our algorithm using various phase space graph features that identify optimal threshold levels for graph dissimilarity and the optimal successive occurrences above threshold that produce the best detection accuracy. Our initial results demonstrate that certain rootkits can be detected through our phase space algorithm using low-frequency power signatures.

# 2022 WiCyS CONFERENCE STUDENT POSTERS

## 10. Forensic Analysis of Alternative Conservative Social Media Platforms

Hailey Johnson and Karl Volk, *University of New Haven*

Alternative social media platforms have grown in popularity, and can foster extremist behavior and encourage dangerous actions. This was demonstrated in the US Capitol attack on January 6th, 2021, where the spreading of false information and extremist ideologies through applications such as Parler, MeWe, and TheDonald inspired riots. While some of these applications have suffered due to the attack, many individuals continue to actively use them. Since several of the more popular conservative alternative social media applications are fairly new, a mass forensic analysis of them and the identification of important artifacts has not been conducted. This project discusses the forensic investigation of multiple alternative social media applications. The applications examined include Parler, MeWe, Clouthub, Wimkin, Minds (Minds Mobile and Minds Chat), Safechat, 2nd1st, and Gettr. The mobile devices used in this research were a Samsung Galaxy S6 (Android 7), and an iPhone 6S (iOS 14.4.2). The applications were downloaded and accounts were created. The methodology included a testing phase which consisted of testing basic user functionalities to generate data while capturing network traffic, and the analysis phase in which the authors meticulously analyzed information stored by the applications and identified artifacts. The results demonstrated that data stored from the account registration, such as the user's email, username, hashed password, first and last name, follower and following count, could be seen. Other information related to the interactions between the two phones including text, images, and videos posted on the feed, profile pictures, and private message content in plain text were discovered. Multiple artifacts were found from each application on both phones, and are discussed in depth. In the continuing tool development phase, the important artifacts identified are incorporated in a python script, which displays a preview and report of the artifacts found and the information stored.

## 11. Fuzzing the Intel Graphics Driver Using Syzkaller and kAFL: A Comparative Analysis

Kainaat Singh, *University of Bonn, Germany*

Kernel-space vulnerabilities can lead to privilege escalation or kernel rootkits to gain persistence and, therefore, it is important to keep the kernel code secure. Device drivers make up more than 60% of the kernel source code. As most of the drivers are executing in the supervisor mode, they need to be trustworthy. In general purpose computing on graphics processing units (GPU), the highly parallel nature of the GPUs is leveraged. This massive parallelism is achieved by exploiting thousands of core applications like financial, encryption, big data and bitcoin mining. GPUs also are made available by cloud computing service providers in a virtualized environment for customers who do not want to buy expensive hardware. Even though applications are running sensitive data through the GPU, not much effort has been made toward securing the graphics subsystem. One interesting problem is validating the graphics

device drivers, as most of them are running with supervisor privileges and interacting with several untrusted user-space applications. A current popular method for software validation is an automated testing process called fuzzing. Fuzzing refers to the process of discovering vulnerabilities by repeatedly running random inputs against a target software and looking for unforeseen behavior. This poster will present the first ever research at finding a coverage-guided fuzzing solution for the Intel i915 Linux graphics driver in cooperation with Intel Corporation for large-scale driver validation. The aim was to find a solution that overcomes the challenges of fuzzing the i915 graphics driver. First, the different Intel device virtualization configurations to fuzz the driver were explored. To choose a suitable fuzzer for the solution, a comparative analysis was performed between the two most promising fuzzers -- Syzkaller and Kernel AFL (kAFL) -- on real hardware. Lastly, a qualitative analysis of the tested fuzzing solutions based on defined criteria is provided.

## 12. Graph Neural Networks for Hardware Security

Rozhin Yasaei and Mohammad Al Faruque, *University of California Irvine*

The time to market pressure and resource constraints has pushed system on a chip (SoC) designers toward using third-party CAD tools and intellectual property (IP) cores and outsourcing design, fabrication and testing worldwide. The globalization of the semiconductor industry has raised the risk of insertion of hardware trojans (HT) by rogue entities. Consequently, HT detection has become one of the significant hardware security concerns. To ensure the trustworthiness of SoC design, it is essential to ascertain the authenticity of 3 PIPs in the early stages of design flow because removing them would be expensive later. Detecting a few lines of HT design in a large industrial-strength IP with one thousand lines of RTL code is extremely challenging, and any work that requires manual review is error-prone, time-consuming and unscalable. Despite numerous HT detection methods proposed in the literature, the problem still exists because as the designers develop a new defense mechanism against the existing HTs, the attackers design new HTs to evade detection. The existing solutions for trojan detection have several shortcomings: Reliance on golden-chip, unable to identify unknown HTs, burden the designer with a manual review of code, unable to guarantee HT detection, limited detection scope to some specific type of HTs, being unscalable or too complex. To overcome these limitations, we propose a novel golden reference-free pre-silicon HT detection method that learns the circuit behavior and identifies the HTs due to malicious behavior. We model the hardware design as its intrinsic representation, the graph and, for the first time, we leverage a state-of-the-art machine learning technique -- graph neural networks -- to learn the behavior of the circuit. The results indicate that our method discovers HTs, even the unknown ones that the current state-of-art fails to detect, with 97% recall (true positive rate) in 21.1ms, faster than other methods. Our methodology has a

# 2022 WiCyS CONFERENCE STUDENT POSTERS

novel perspective toward the hardware security problem and introduces a powerful tool using graph learning techniques to model hardware design behavior.

## 13. Identification of Clear Text Data Obfuscated Within Active File Slack

Claire Wills, *University of South Alabama*

Obfuscating text on a hard drive can be done by utilizing the slack space of files. Text can be inserted into the area between the end of the file itself and the cluster it is stored in but stay hidden from traditional methods of viewing files. If the hard drive is large, how does a digital forensics expert know where to look to find text that has been obfuscated using this technique? Searching through a large hard drive could take up a substantial amount of time that the expert possibly could not justify (Renaud et al., 2021). If the digital forensics expert lacks the knowledge on how to properly search a hard drive for obfuscated text using this method, how will the text be located and identified (Horsman & Sunde, 2020)? To address this, we propose an algorithm that will scan the slack space in a drive for text that otherwise would be missed due to error or time restraints. Based on the success of the algorithm, a tool could be created to use hard drive metadata to find text hidden in the slack space and report the findings back to the digital forensics' expert.

## 14. Intrusion Prediction-Aware Moving Target Defense for Smart Farming

Kristin Barrett, Tajah Clark and Dr. Jagruti Sahoo, *South Carolina State University*

Smart farming is a recent technology that has gained significant momentum due to its enormous advantages, including increased agricultural yield, higher operational efficiency and lower cost. It uses Internet of Things (IoT) devices such as pH probes and moisture sensors that track various farm parameters and provide farmers with real-time updates on the health of the farm. However, a multitude of factors, including static footprint, resource limitation and high volume of data make the IoT devices vulnerable to cyberattacks. Malicious actions such as unauthorized access and modification of the on-field parameters (e.g., soil pH and moisture) will degrade the performance of smart farming applications. Moving target defense (MTD) is a defense scheme that can certainly ensure the resiliency of the smart farming systems against diverse cyberattacks. It introduces dynamicity to the attack surface of the IoT devices by shuffling configuration parameters such as IP addresses, port numbers and protocols. A critical challenge is to determine the appropriate shuffling sequence in a way that prevents the attackers from discovering the systems. In this work, we propose an MTD scheme that uses a port shuffling method to protect the vulnerable services running on IoT devices. We model the reconnaissance activities of the attackers as a time series and estimate the number of scanned ports using the exponentially weighted moving average method. On detecting intrusions, i.e., port scans, we

observe the first few ports and use this knowledge along with the estimated number of them to find the safe pool that can be used for generating new port numbers for the vulnerable services. Through our evaluation, we conclude that the proposed MTD scheme improves resiliency and reduces the mean response time.

## 15. Is a Significant Demographic Left Out of the Equation? An Overview of Possible Inequitable Access to Cybersecurity Educational Programs in the United States

Johanna Jacob, *The University of Texas at San Antonio*

Cybersecurity skills shortages have reached widespread proportions. The consensus in the science, technology, engineering and mathematics (STEM) community is that there is a lack of an established pathway in K-12 education that would help students gain an interest in cybersecurity and related careers. Though cybersecurity education is offered in K-12 across the United States through various means such as camps, clubs, competitions and coursework, there is an uneven access for students to engage in these activities. Middle and high school populations include teachers and educators who are in smaller and lower income school districts and often less exposed to the multifarious initiatives in cybersecurity. This inequity gap is further enhanced by the lack of sufficient funding for rural school districts, which translates to a lack of quality educational resources, highly qualified teachers, strong STEM programs, and extracurricular opportunities that can help improve low-income students' educational achievements. Recent studies point out that, "Lower levels of knowledge are reported among classroom teachers, in public schools, and in communities without cybersecurity resources such as cybersecurity companies, organizations that employ cybersecurity specialists, and Universities that offer cybersecurity programs and/or conduct cybersecurity research." In this regard, we analyze and study the deterrents to equitable access to cybersecurity education in the U.S. by considering CyberPatriot as a case study. The CyberPatriot National Youth Cyber Education Program is a globally acclaimed program in existence since 2009. Created in the U.S., its sole purpose and design is to inspire students toward careers in cybersecurity or other STEM disciplines critical to our nation's future. In the 2018-19 season, there were 6,387 registered teams and over 32,000 competitors spanning thousands of schools across the U.S. Using initial data provided by CyberPatriot, we provide an overview of the analysis of the participation demographics across all U.S. states along with data obtained from the U.S. Department of Education. We also point out some indicators that contribute to significant trends observed from the participation metrics. Finally, we introduce a survey-based methodology catered to teachers, mentors and trainers from schools that participated in CyberPatriot to obtain more complete and current data to more accurately analyze student participation and interest, teacher training, public/private partnerships, demographics for schools and

# 2022 WiCyS CONFERENCE STUDENT POSTERS

school districts, available STEM programs and access to cybersecurity programs, and educator knowledge. Results of the data analysis help understand potential factors along with challenges presented for rural schooling (Title-I schools), thereby suggesting urgent and a comprehensive need to boost student interest and pave the way for substantial growth in cybersecurity education in the K-12 avenue across the U.S.

## 16. Mobile Application Security and Best Practices

**Alexa Freglette, Worcester Polytechnic Institute**

As mobile applications become more accessible via networks and the Cloud, the security required to protect a user's personally identifiable information drastically increases in importance. Mobile application security breaches are becoming more common as vulnerabilities increase. According to research conducted by analysts at Positive Technologies, high vulnerabilities were found in 38% of IOS and 43% of Android mobile applications (2019). It is crucial for the protection of users' data for developers to utilize a security-first approach, placing more emphasis on security when developing their applications. While building applications, it is critical for developers to run their code through complex security penetration testing which can simulate attacks that hackers might perform. Analysts can test for these breaches by using open-source security scanners such as ImmuniWeb® MobileSuite and Zed Attack Proxy. This project will examine mobile applications' common vulnerabilities, current means to solve these issues, and ways in which security can evolve to be more effective. The research will also advise best practices that companies should follow to enforce better mobile application security.

## 17. Offensive and Defensive Analysis of Behavioral Biometrics on Wearable Devices

**Sindhu Reddy Kalathur Gopal, University of Wyoming**

Smart wearables have become an integral part of our lives, and we use them daily. As a result, we are retaining most of our personal and private data on these devices. Due to the reliance on these items to store and process sensitive information, it is essential, and has become increasingly significant, to ensure secure access to these devices. Although widely used entry point authentication systems are in place to verify users' identity, they face several security challenges, such as session hijacks. In order to address these shortcomings, a behavioral biometrics-based active authentication system is proposed where users are verified by continuously using their behavioral patterns. However, the existing authentication systems require a user to perform certain predefined tasks in order to verify his/her identity, such as typing a fixed text, performing some arithmetic operations, identifying geometric shapes, etc. This becomes a major challenge when one needs to authenticate continuously or at a regular interval. Also, the existing models in the literature show the efficacy of the models where the training and testing samples come from the same emotional state. The performance of these models decreases drastically

when samples come from different emotional states. This makes it challenging to deploy the existing methods in a real-world continuous authentication system.

To address these limitations, we propose an enhanced, reliable and inexpensive continuous authentication system that (i) verifies the user's identity using their hand movements captured through inertial measurement units, a.k.a., micro-accelerometer and micro-gyroscope while they perform free-text typing on their desktop or laptop keyboard(s). (ii) The proposed model requires training on the user's hand movement patterns while they are in any of the emotional states and later authenticating them irrespective of the emotional state. We refer to this model as the emotion-invariant continuous authentication model. In this study, we developed three one-class SVM classifier-based authentication models and tested them using intra-emotional (trained and tested on the same emotion) and inter-emotional (trained on happy emotion and tested on sad emotion and vice versa) data. The results show that the model is as good as the emotion-aware authentication model in terms of authentication performance and is more efficient in terms of computational efficiency. The extensive feature analysis presented in the work introduces an optimal discriminative feature subset as a building block for the design of the proposed emotion-invariant continuous authentication model. A detailed experimental analysis is presented which shows our model, based on a one-class SVM classifier, could successfully authenticate the users in our experimental dataset with very low average error rates: (1) FAR and FRR values of 0.67% and 0.17%, respectively, when the model was trained on the happy emotion and tested on sad emotion (inter-emotional) data, (2) FAR and FRR values of approx 0.1% when trained and tested on the same emotion (intra-emotional) data.

## 18. PacMan: Maze Authentication Using Behavioral Biometrics

**Jessa Gegax, Adeline Reichert, Natasha Miller and Colton Roach, University of Wyoming**

Behavioral biometrics as a means of user authentication is a growing field in cybersecurity since it can individualize cognitive abilities that are more difficult to replicate for an impostor/attacker. Measuring someone's performance or keystroke patterns is an example of how a behavioral biometric can be used in conjunction with continuous authentication to better protect confidential information and prevent breaches. The objective for this research was to expand on this idea and use machine-learning tools to validate a user's identity based on how they solved a maze. A preliminary dataset of our team's performance was provided that attempted verification with two machine-learning classifiers: Mini rocket and cross correlation. These classifiers provided promising results and showed the possibility of being able to distinguish a genuine user from an impostor. However, further research is required to achieve higher accuracies that guarantee successful and secure authentication with a larger dataset.



# 2022 WiCyS CONFERENCE STUDENT POSTERS

## 19. Phishing Website Detection Using Deep Learning-Based Models

**May Almousa and Mohd Anwar**, *North Carolina A&T State University*

Phishing websites are fraudulent sites that appear legitimate and trick unsuspecting users into interacting with them, stealing their valuable information. Because phishing attacks are a leading cause of data breach, different solutions have been explored for cybersecurity management, including machine learning-based technical approaches. However, there is a gap in understanding how robust deep learning-based models together with hyperparameter optimization is for phishing website detection that is not overfitted to the training dataset. In this vein, this study pursues the task of developing parsimonious deep learning models and hyperparameter optimization to achieve high accuracy and reproducible results for phishing website detection. This paper demonstrates a systematic process of building detection models based on three-deep learning algorithm architectures (long short-term memory-based detection models, fully connected deep neural network-based detection models, and convolutional neural network-based detection models) that are built and evaluated using four publicly available phishing website datasets, achieving the best accuracy of 97.37%. We also compared two different optimization algorithms for hyperparameter optimization: Grid search and genetic, which contributed a 0.1% to 1% increase in accuracy.

## 20. Privacy Preserving Framework for Smart Grid

**Anna Volpova, Sumita Mishra and Gaurav Shivaji Wagh**, *Rochester Institute of Technology*

Smart grid functionalities, such as real-time grid monitoring and dynamic billing, require the collection of fine-grained smart metering data at frequent time intervals. However, a customer's privacy can be breached by deriving behavioral patterns from the granular metering data. Distributed aggregation-based privacy-preserving frameworks can provide the desired functionalities while keeping the framework lightweight for resource-constrained smart meters. Most of the distributed frameworks do not consider modification of metering data during transit. We propose a distributed privacy framework that employs features of a threshold secret sharing scheme (Shamir's) and secure multi-party computation (SMPC) to support integrity verification of metering data. Shamir's Secret Sharing is an algorithm based on polynomial interpolation over finite fields, an algebraic method of estimating unknown values in a gap between two known data points. SMPC is a technique that allows a set of parties to jointly compute an output while maintaining private inputs. The proposed framework is developed in a simulated environment under a malicious adversarial setting, where the assumption is that the metering data can be modified during the collection process. We demonstrate that our approach, with a built-in integrity check mechanism, can collect the smart metering data in a privacy-preserving manner and identify the meters subjected to modification of data.

## 21. Protecting Location-Set Privacy for Location-Based Services

**Neha Sharma, Krunal Mahant and Yidan Hu**, *Rochester Institute of Technology*

Deep penetration of internet-capable and location-aware mobile devices in people's everyday lives is driving the explosive growth in location-based services (LBS), where users submit their locations to a cloud service provider (CSP) to retrieve location-dependent information and personalized services. However, exposing accurate locations to a possible untrusted/unknown CSP has raised serious privacy concerns. To protect users' location privacy, a promising approach is to obfuscate a user's location before submission via a randomized perturbation mechanism achieving geo-indistinguishability. This is a formal notion of location privacy that allows users to protect their true locations while enjoying LBS with a bounded accuracy loss of results from the CSP. However, geo-indistinguishability is proposed based on the underlying assumption that the user only needs to submit a single location to enjoy LBS, which is not always true. In fact, it is common for a user to provide a set of locations to enjoy it, e.g., finding the nearest point of interest close to all frequently visited locations. To protect the privacy of a user with multiple locations, we propose a novel location privacy protection mechanism (LPPM), which not only provides a strong theoretical location privacy guarantee for the user with multiple locations but also improves accuracy of results from the CSP. Our key idea is twofold. First, we adopt Planar Laplace Mechanism, a typical location perturbation mechanism satisfying geo-indistinguishability, to perturb each location set for privacy protection. Second, we introduce an additional well-designed fake location into the set of perturbed spots to significantly reduce the overall noise introduced by the Planar Laplace Mechanism, thus improving the accuracy of results while ensuring the same level of location privacy. Simulation studies based on a real location dataset confirm the efficacy and efficiency of the proposed LPPM.

## 22. ROP on PLCs

**Adeen Ayub and Irfan Ahmed**, *Virginia Commonwealth University*, **Hyunguk Yoo**, *The University of New Orleans*

Programmable logic controllers (PLC) are critical components of industrial control systems. They directly control and monitor physical processes such as nuclear plants, oil and gas processing, power grid systems, etc. They run a control logic program that defines how an industrial process is controlled. Attackers target the control logic of a PLC to sabotage a physical process. PLCs come with firmware installed in order for them to function the way they should. Existing work has shown different networks as well as firmware-level attacks on PLCs. Most of them involve code injection attacks, which can be mitigated by making the memory non-executable. However, one exploitation technique that bypasses the aforementioned mitigation is return oriented programming (ROP). None of the existing literature focuses on ROP for PLCs. ROP is an



# 2022 WiCyS CONFERENCE STUDENT POSTERS

exploitation technique that allows an attacker to perform unintended operations by constructing a gadget chain from the application code. Since the attacker just changes the sequence of code operations of the application itself, she does not have to inject a new malicious code to launch her attack. In this work, we present ROP on PLCs, specifically the control logic. We use the existing control logic instructions in binary and construct gadget chains to disrupt the physical process being controlled. We test the attacks on different control logic programs written for different physical systems and confirm that our approach works successfully.

## 23. Route Agility and Deception Against Adversarial Traffic Analysis Attacks

Masoumeh Abolfathi, *University of Colorado Denver*

While encryption can protect network traffic against simple on-path eavesdropping attacks, it cannot prevent sophisticated traffic analysis (TA) attacks from inferring sensitive information about the encrypted traffic. TA attackers utilize machine-learning algorithms to decipher traffic patterns of a communication (e.g., a website visit) and then use these learned patterns to accurately identify similar communications (which website is being visited by a targeted user), even though packets are encrypted. This research presents a novel and effective defense approach to protect multipath networks against TA attacks. The proposed approach is based on two proactive defense paradigms: agility (route randomization) and deception (fake packet injection). The route randomization strategy distributes packets of a flow on multiple paths between a source and destination to restrict the amount of traffic that a TA adversary can collect from a flow. The deception strategy augments the randomization strategy by injecting dummy packets among the real packets of a flow on different paths. The focal research problem is to identify the optimal strategies for how real and fake packets must be distributed on multiple paths with different capacities to achieve maximum effectiveness against TA attacks. The problem is formalized as a zero-sum game, and it is shown that the water-filling distribution of real and fake packets provides an optimal defense solution. The theoretical and experimental studies demonstrate that the proposed approach can significantly degrade the accuracy of the TA attacks.

## 24. Security and Privacy Issues in Telemedicine: A Survey Study

Thuong Ho and Ankur Chattopadhyay, *Northern Kentucky University*

Technological advances have made a significant change in the way healthcare services can be received and delivered today. Telemedicine is a form of an online, virtual healthcare service that is convenient for people in context of time commitments, cost and limitations of in-person availability. However, it has to abide by the Health Insurance Portability and Accountability Act (HIPAA) rules to protect the integrity,

confidentiality and availability of patient records. Despite the benefits, the adoption of telemedicine remains challenged with technical constraints, including security and privacy issues that pose risks. To our knowledge, prior literature does not holistically survey a comprehensive list of security concerns in telemedicine and study the corresponding countermeasures to eliminate vulnerabilities in telemedicine systems. In this novel study, we surveyed existing research work in telemedicine and created a taxonomy framework that identifies potential vulnerabilities in telemedicine and the variety of threats (in the form of cybersecurity attacks) they pose. Previous literature shows only one case study [1] on threat modeling plus vulnerabilities in an experimental telemedicine system. Our detailed survey addresses this gap by providing a unique, in-depth understanding plus review of research literature, including overall security holes in telemedicine and their impacts on patient privacy. A taxonomized survey data collection analyzing vulnerability-based security risks identified in telemedicine and a review of possible remedies is our main research contribution. The first two defensive techniques currently being used are encryption and hash functions [2]. A one-time mutual authentication procedure should be established before sending data to a user using session key [3]. A robust authentication system, employing the following factors simultaneously, can be implemented (three-factor authentication): Password (something you know), smart-card or one-time-passcode (something you have) and biometric (something you are). Embedding biometric-based authentication can increase the difficulty of an interception attack to a certain degree, as it requires the participants to be physically present on screen at the point of authentication. However, use of biometric devices will require additional capital cost and involve a more complex user interface as well as user management. Combining two or more factor authentication is the most economical and practical way. Medical image watermarking and medical image authentication schemes can be used to prevent modification and fabrication. This mechanism must balance six basic security requirements, including imperceptibility or invisibility, robustness, capacity, complexity and reversibility because it is impossible to accomplish all requirements at the same time. These defensive techniques can be built into telemedicine systems to overcome security issues, but training for handling private data needs help at an organizational level to prevent information leakage. AI and blockchain technology innovations can be investigated for bolstering the defense layer in telemedicine services in real-time to potentially detect malicious activities and augment interoperability between different systems. To build trust by enhanced measures in telemedicine systems, biometric authentication methods, like facial recognition and other visual analytics, can be considered. Our review of existing literature indicates lack of research in application of biometrics in telemedicine for addressing present security risks.

# 2022 WiCyS CONFERENCE STUDENT POSTERS

## 25. Toward Detecting Anomalous User Behavior Using Hierarchical Federated Learning LSTM Approach

**Deepti Gupta**, *University of Texas at San Antonio*; **Olumide Kayode**, *Frostburg State University*; **Smriti Bhatt**, *Purdue University*; **Maanak Gupta**, *Tennessee Tech University*; **Ali Saman Tosun**, *University of North Carolina at Pembroke*

The Internet of Medical Things is becoming ubiquitous with a proliferation of smart medical devices and applications used in smart hospitals, smart home-based care and nursing homes. It utilizes smart medical devices and cloud computing services along with core Internet of Things technologies to sense patients' vital body parameters, monitor health conditions and generate multivariate data to support just-in-time health services. Mostly, this large amount of data is analyzed in centralized servers. Anomaly detection (AD) in a centralized healthcare ecosystem is often plagued by significant delays in response time with high performance overhead. Moreover, there are inherent privacy issues associated with sending patients' personal health data to a centralized server, which also may introduce several security threats to the AD model, such as the possibility of data poisoning. To overcome these issues with centralized AD models, we propose a federated learning (FL) based AD model that utilizes edge cloudlets to run models locally without sharing patients' data. Since existing FL approaches perform aggregation on a single server and restrict the scope of FL, we introduce a hierarchical FL that allows aggregation at different levels enabling multi-party collaboration. We introduce a novel disease-based grouping mechanism where different AD models are grouped based on specific types of diseases. Furthermore, we develop a new federated time distributed, long short-term memory approach to train the AD model. We present a remote patient monitoring use case to demonstrate our model, and illustrate a proof-of-concept implementation using digital twin and edge cloudlets.

## 26. U.S. Ransomware Analysis of Public Sector Infrastructure

**Tahlla Taylor**, *University of Texas Dallas*

Ransomware has been emerging as one of the leading threats in cybersecurity. Every year, hackers become more creative, and their targets remain unsuspecting. Over several years, hospitals, police stations, schools and other objects of public sector infrastructure have experienced an increase in attacks across the U.S. I present an exploratory analysis of over 1,800 ransomware cases in the U.S. from 2016 through the present. I classify these attacks according to their targets, locations and impact. I show that the severity of attacks range from no change in the organization (very low) to life-threatening (very high) depending on the type of attack and target. My analysis advances our understanding of the strategic considerations underlying this cybercrime, and I will present solutions to reduce ransomware attacks in this sector.

## 27. Understanding Student Privacy in K-12 Technology During COVID

**Katie Shuck**, *Dakota State University*

For several years, technology has been increasingly integrated into K-12 classrooms to engage students and create effective multidisciplinary learning environments. The onset of the COVID-19 pandemic drastically increased the adaptation of technology in K-12 classrooms as students moved to distance learning and schools had to quickly find ways to continue the students' education. Schools and classrooms adopted video conferencing tools, online learning platforms and games, connected classrooms, and more. Unfortunately, the rapid adoption of new technology was done to quickly pivot from in-person to online learning and student privacy and security was often an after-thought. This research project looks at student privacy incidents that occurred during the pandemic and analyzes the Privacy Policies of some of the most commonly used K-12 technologies used during the pandemic in order to quantify and classify student data collected and possible privacy harms. This project builds on research conducted by this researcher prior to the pandemic that analyzed K-12 technology used pre-pandemic.

## 28. Usable Privacy Approaches to Improving the Transparency of Conversational Interactions

**Karen Bonilla and Aqueasha Martin-Hammond**, *Indiana University-Purdue University Indianapolis*

The pervasiveness of voice search and intelligent voice assistants like Alexa and Google Home provide new opportunities to help individuals complete day-to-day tasks. However, previous studies show that some users have a lack of trust about data privacy practices and protections of these devices. Such worries concerning how and where confidential data is stored and managed on these devices is therefore cited as a deterrent to intelligent voice assistant use. In our initial studies of users' challenges and concerns about voice assistant devices, we learned that there were key scenarios that led to a lack of trust in the device's data privacy and protection measures. However, how do we design conversational dialogs that foster more trusting relationships with users? To understand how to address user concerns, we developed a series of scenarios with BotSociety informed by our prior studies to explore how to improve conversational interactions to make them more transparent for users. We conducted semi-structured interviews to first understand the background participants have with voice assistants, as well as their concerns. Then we presented the BotSociety scenarios, which reenact commonly mentioned concerning interactions users had with their voice assistant devices and co-explored with participants how we might help improve their trust. Initial findings from our interviews suggest that privacy concerning occurrences mentioned by users such as a device speaking out of turn, not correctly processing a query, and providing accurate information in general could potentially be resolved through improved voice detection/recognition

# 2022 WiCyS CONFERENCE STUDENT POSTERS

and conversational design. Our work contributes to the fields of human-computer interaction, conversational design and usable privacy focusing on improving transparency of voice-based interactions through design.

## 29. Where In The World is SHA-3?

Eliora Horst, *Loyola University of Chicago*

SHA-3 is the latest update to the family of hashing algorithm standards. Hashes are used to add integrity to the transfer of data throughout the electronic world. While it makes significant improvements to previous entries and developed a new internal structure that made collisions even more unlikely, this algorithm is in scarce use compared to its ancestors. This poster examines what makes SHA-3 so unique and analyses why it is not being integrated more into the current cybersecurity landscape. SHA-3 uses a Keccak sponge function internally to compute its hashes. This system completely deviates mathematically from previous SHA iterations, which significantly decreases the likelihood of collisions. It also was developed as a way to look ahead to future collision issues with SHA-2, which is currently in wide use across many applications. Because of the success of SHA-2, and the lack of any major flaws or known collisions, SHA-3 has not been adapted. SHA-3 also is generally slower than SHA-2 and requires more computational power to operate. However, many parts of the cybersecurity world are slow to update their standards. For example, many digital forensic tools still utilize MD5 and SHA-1 to validate their data, which poses a not insignificant risk to veracity of data in a court of law. SHA-3 lies at a crossroads, where it is a significant improvement upon SHA-2 in many ways. However, the urgency to implement it widely has not yet arisen, although the ever-expanding field of cybersecurity is rapidly approaching this turnover point.

## JOB BOARD++

### MEMBERS: GET THE WORD OUT

Activate your profile and upload your resume to the Job Board++. Then, scroll through the WiCyS strategic partner booths and start applying to internships, part-time, or full-time positions.

### RECRUITERS: GET EXCLUSIVE ACCESS

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

## THANK YOU

### Honoring those who served our community!

WiCyS gives thanks to all the monetary support donated to the Alan Paller Memorial Cyber Talent Emergency Fund, Kristina Spalding Scholarship Fund and James Summers Scholarship Fund.

These funds not only awarded WiCyS 2022 scholarships and fellowship awards to help members progress in the cybersecurity field, but memorialize three people who supported diversity, inclusion and women advancing in cybersecurity.



In memory of Alan Paller



In memory of Kristina Spalding



In memory of James Summers



**Amazon Web Services (AWS) is the world's most comprehensive and broadly adopted cloud platform, offering over 175 fully featured services from data centers globally.**

Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster. AWS Global Security Practice, Professional Services Organization is a global team of experts that can help Enterprise Customers realize their desired business outcomes when using the AWS Cloud.

**AWS Security** owns security for all services offered by AWS, including EC2 and S3. This creates a lot of different opportunities for cross-team collaboration and high visibility into the company. We dive deep into security technologies to innovate and provide our customers the best possible experience with every transaction that happens in the cloud. Our projects include building new authentication systems, enhancing cryptography, and conducting massive-scale audit analysis.

**AWS Professional Services** is responsible for assisting enterprise customers as they shift to the cloud by incorporating our services into their overall architecture. We work hand-in-hand with customer teams and AWS partners to provide deep expertise in the architecture, design, development, and implementation of cloud computing initiatives that result in real business outcomes. As part of our team, you'll accelerate the adoption of our products all while advocating for the success of our customers.

**Ready to build at AWS ?**

<https://aws.amazon.com/careers/security> | <https://www.amazon.jobs/en/teams/professional-services>

**Carnegie Mellon University**  
Software Engineering Institute

## Secure the Future of Cybersecurity

Meet our staff at **Booth 119**  
and join our effort in solving the  
nation's cybersecurity challenges.

**Apply today!**

Visit our website for more information.  
[sei.cmu.edu/careers](https://sei.cmu.edu/careers)







Discover what's possible.

# Security Careers at Cisco

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



# Deloitte.

Don't just write the code.  
Crack the code

Find your calling at Deloitte Cyber

Learn more  
[Deloitte.com/us/cyberjobs](https://deloitte.com/us/cyberjobs)



Copyright © 2022 Deloitte Development LLC. All rights reserved.





# WORLD-CLASS EXPERIENCES *without* THE WORLD-CLASS EGO

Join in at [THISISCLEVELAND.COM](http://THISISCLEVELAND.COM) | [#ThisisCLE](https://twitter.com/ThisisCLE)

@TheCLE    @ThisisCLE    [facebook.com/ThisisCleveland](https://facebook.com/ThisisCleveland)

## Wind + Cloud = Power

Connected machines, big data,  
and predictive analytics are  
propelling the next industrial era.

*Let us help you power your career  
and together we will power the world.*

[ge.com](http://ge.com)  
[gecareers.com](http://gecareers.com)





# Every day you're safer with Google

We keep more people safe online than anyone else in the world with products that are **secure by default**, **private by design** and **put users in control**.



If you are passionate about building systems that protect users and working at massive scale on a stunning array of technologies and challenges, then we'd love to meet you.

Find current opportunities with Security and Privacy teams [g.co/SecurityPrivacyEngJobs](https://g.co/SecurityPrivacyEngJobs)

 Security Engineering

# 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](https://mastercard.com)



Mastercard is a registered trademark, and the circles design is a trademark, of Mastercard International Incorporated. © 2021 Mastercard. All rights reserved.





## NSA CYBERSECURITY



- ✓ *Tackle the nation's hardest cybersecurity problems*
- ✓ *Collaborate across industry and government*
- ✓ *Disrupt malicious cyber activities at scale*
- ✓ *Work with the best and brightest*

Apply at [intelligencecareers.gov/NSA](https://intelligencecareers.gov/NSA) to join our team.

U.S. citizenship is required. NSA is an Equal Opportunity Employer.



# The Future of Cybersecurity Will be Determined by You

**Come Join Our Team**  
[sentinelone.com/careers](https://sentinelone.com/careers)



## The business of innovation is never business as usual

Innovative technology. Breakthrough science. The latest medical advances. AbbVie is a global biopharmaceutical company tackling the world's toughest health challenges

Learn more at [abbvie.com/careers](https://abbvie.com/careers)



abbvie

People. Passion. Possibilities.™

**AON**

## We Believe Businesses Thrive When People Flourish

Aon is proud to support WiCyS and their dedication to the success of technical women and diversity in cyber security.

Learn more: [aon.com/cyber-solutions](https://aon.com/cyber-solutions)



**BANK OF AMERICA** 



## We see things differently.

Bank of America Global Information Security is a proud supporter of WiCyS.

EOE/M/F/Vet/Disability © 2022 Bank of America Corporation.  
AR4G599 | DI-11519



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.

### Program Highlights:

- NSA Center of Academic Excellence – CDE
- First CyberCorp 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 Camp Program
- CTF, defense and offense competition teams
- **The place to be for cyber in Tennessee!**



1020 Stadium Drive • POB 5134 • PRSC 414 • Cookeville, TN 38505 • (931) 372-3519  
[ceroc@tntech.edu](mailto:ceroc@tntech.edu) • <http://www.tntech.edu/ceroc> • [@TNTechCEROC](https://twitter.com/TNTechCEROC)





## We're Hiring! Come Join Our Team

Check Point was recognized by Forbes as a 2021 Best Employer and Best Employer for Women!  
*Come join us. It's a great place to be.*

See what openings we have here:



**Billions of data points.  
Countless lines of code.  
Security vulnerabilities.**

How will you help shape CIA's digital future?

*An equal opportunity employer and a drug-free workforce.*




Because healthcare is the next frontier in tech



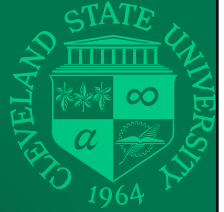
We invest in our caregivers, technologies, and processes to grow and run at optimal velocity. Join us, and you'll experience the difference of a culture where opportunities for personal development and the support to get there go hand-in-hand.

[clevelandclinic.jobs](https://clevelandclinic.jobs)

*Cleveland Clinic is pleased to be an equal employment employer: Women/Minorities/Veterans/Individuals with Disabilities*



**CLEVELAND STATE UNIVERSITY**  
engagecsu.com



**CYBERSECURITY PROGRAMS IN BUSINESS, ENGINEERING AND LAW COLLEGES.**

**TALK TO OUR STUDENTS AND FACULTY AT BOOTH 412.**



CSU is proud to lead the local host committee for the 2022 WiCyS Conference.





**CSSIA**  
National Support Center for Systems  
Security and Information Assurance

The Center for Systems Security and Information Assurance (CSSIA) has instructed more than 2000 teachers and college faculty in cybersecurity related areas. CSSIA strives to bring the best and most current courses to you throughout the year and works with the National Science Foundation (NSF) Advanced Technology Education (ATE) grant programs and industry partners to define and organize these efforts. Visit our website to view our courses now!

[CSSIA.org](http://CSSIA.org)



**ECS**


**JOIN US  
IN BUILDING A  
BETTER CYBER TEAM**

We're currently hiring analysts,  
engineers, and more.

**Apply today!**  
[www.ecstech.com/cybersecurity-careers/](http://www.ecstech.com/cybersecurity-careers/)

**Individuality  
defines me.**

[ibm.com/careers](http://ibm.com/careers)



**IBM**

IBM and the IBM logo are trademarks of International Business Machines Corporation. Registered in many jurisdictions. Other trademarks and service marks are the property of IBM or other companies. A current list of IBM trademarks is available at [ibm.com/trademark](http://ibm.com/trademark). ©International Business Machines Corp. 2022. R00392



**intel.**

Security begins with Intel  
Together we can do impossible things

[intel.com/jobs](http://intel.com/jobs)

## Secure a bright future.

KeyBank is proud to sponsor the 2022 Women in Cybersecurity Conference. We are also proud to support diversity, equity, and inclusion in everything we do, striving to create a culture where every person feels included, valued, and empowered.

If you're looking for a great opportunity to showcase your technical expertise and help us build the bank of the future, we'd love to meet with you.

Come see us at the Career Fair, or visit [key.com/techjobs](https://key.com/techjobs) for current opportunities.



Key.com is a federally registered service mark of KeyCorp. ©2022 KeyCorp.  
KeyBank is Member FDIC. 211213-1361622



## HEALTHCARE IS ABOUT MORE THAN MEDICINE. IT'S ABOUT HOPE.

The MetroHealth System is redefining healthcare by going beyond medical treatment to improve the foundations of community health and well-being: access to affordable housing, a cleaner environment, economic opportunity and access to fresh food, convenient transportation, legal help and other services. That's why we're devoted to hope, health and humanity. Find out more at [metrohealth.org](https://metrohealth.org).



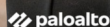
# WE ARE HIRING

- For our executive team, we raised the representation of women to 36%, an increase of 4.9% YoY.
- Since the beginning of 2020, 86% of our roles have included at least 2 diverse candidates at interviews prior to moving to offer.
- Our FLEXLocation offers increased remote and work-from-home opportunities. Both are concerns raised by women and people of color in the current job market.



**APPLY NOW**

[jobs.paloaltonetworks.com](https://jobs.paloaltonetworks.com)



MASTER OF COMPUTER SCIENCE | MASTER OF DATA SCIENCE

Transform your tech career with an online master's degree from top-ranked Rice University.



Visit [online.rice.edu](https://online.rice.edu) to access Rice's world-class, convenient masters degrees.

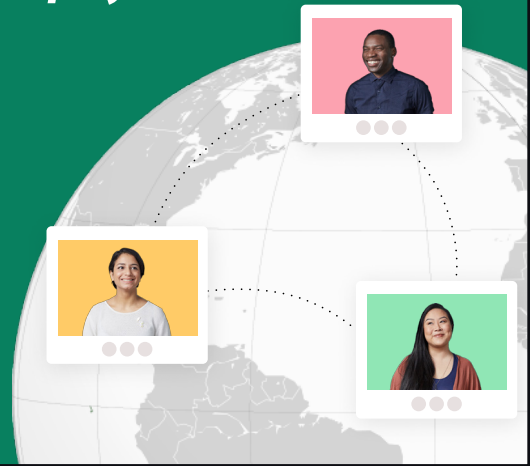


# It's more than just a job – it's an opportunity.

Sfdc.co/WiCyS2021



# Work with us in the fastest growing city- the internet.



## /\*\*We're hiring!

Are you ready to make an epic impact? Join our team of information security professionals working together to keep Walmart secure.

Apply today at [careers.walmart.com](https://careers.walmart.com)

& ; > # @ ^ ; > . / & . % ^ # % & ; > # @ ^ ; > . / & . % ^



# We support women in cybersecurity.

Come connect with the team that is building the largest platform for all things home!



To learn more about our opportunities in Cybersecurity & Privacy stop by our booth or scan the QR code to see our open positions.



**You have  
the talent.  
We have  
the power.**

**Move at the speed  
of technology.**

Joining the Verizon Cybersecurity team means you'll get to protect, defend and respond to cyber threats. You'll also be prepared to meet challenges at levels rarely encountered – all at a place where you can learn and grow.

**Explore career opportunities at  
[verizon.com/cybersecurity](https://www.verizon.com/cybersecurity)**



Verizon is an equal opportunity/disability/vet employer

# A workplace that works for women.

At Workday, we believe opportunity should be for everyone.

That's why we're cultivating a workplace that welcomes diverse perspectives and empowers women to succeed in whatever role they choose.

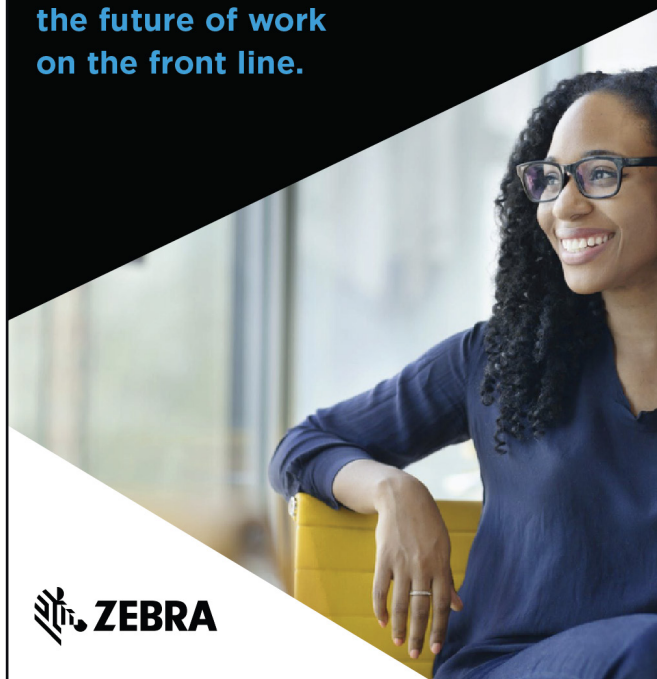
Come join a company where women are valued and where women lead: [workday.com/careers](https://workday.com/careers)

©2022 Workday, Inc. All rights reserved. Workday and the Workday logo are registered trademarks of Workday, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.



## Calling All Changemakers

Join us as we shape  
the future of work  
on the front line.



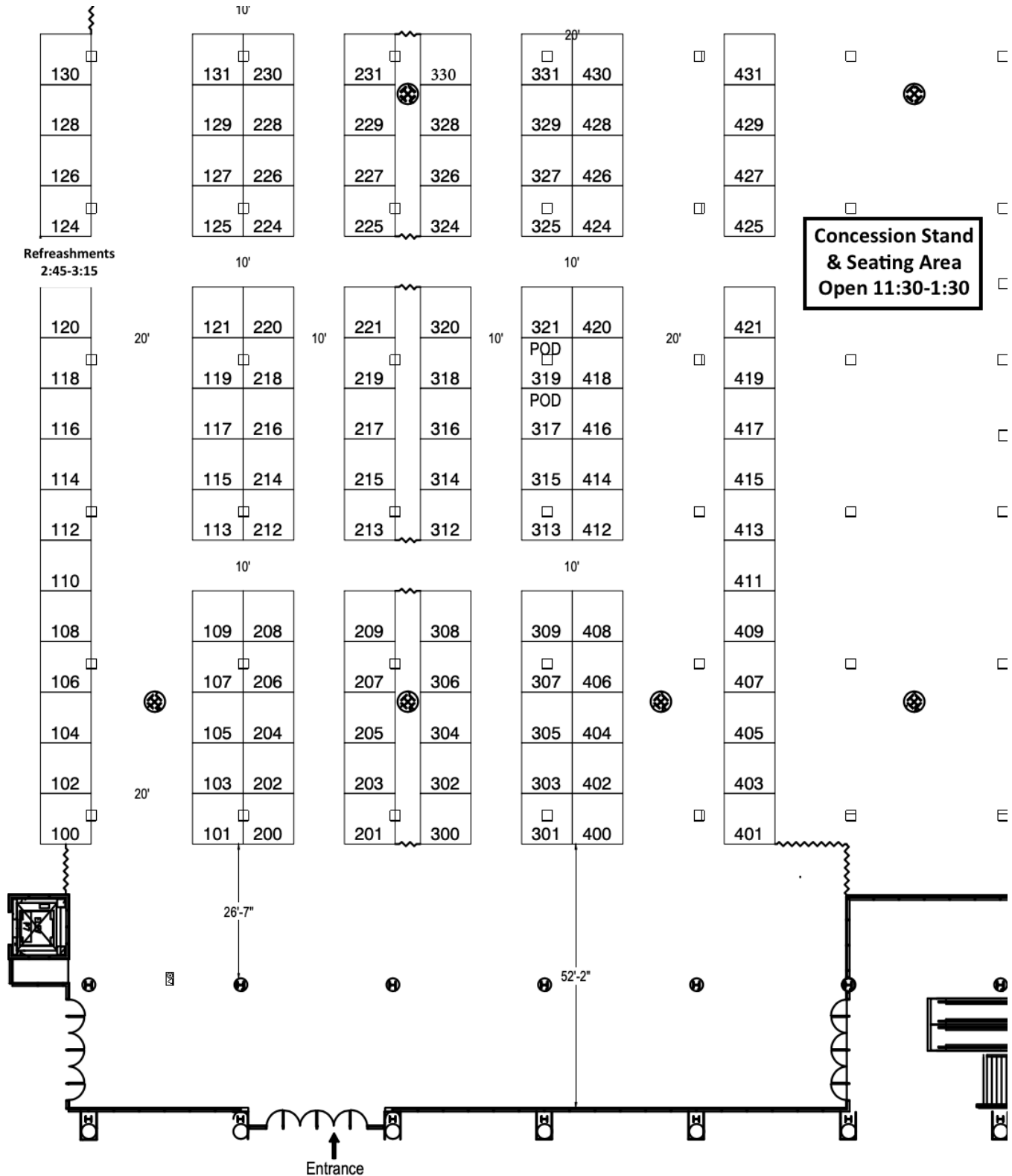
# VISIT THE CAREER FAIR

|  |         |  |         |
|--|---------|--|---------|
| A-LIGN . . . . .   | 106     | KeyBank . . . . .  | 420     |
| AbbVie . . . . .   | 312     | Keyfactor Inc. . . . .                                       | 431     |
| Amazon . . . . .   | 404     | Lockheed Martin . . . . .                                    | 212     |
| Amazon Web Services, Inc. . . . .  | 406/408 | Lutron Electronics . . . . .                                 | 321     |
| American Airlines . . . . .  | 128     | ManTech . . . . .  | 112     |
| American Express . . . . .   | 124     | Marshall University . . . . .                                | 320     |
| AON . . . . .  | 327     | Mastercard . . . . .   | 204/206 |
| Arctic Wolf . . . . .  | 325     | MetroHealth . . . . .  | 415     |
| Arista Networks . . . . .  | 217     | Microsoft . . . . .  | 126     |
| Asurion . . . . .  | 125     | MIT Lincoln Laboratory . . . . .                             | 305     |
| Binary Defense . . . . .   | 414     | MITRE . . . . .  | 226     |
| Bloomberg L.P. . . . .   | 200/202 | NASA . . . . .   | 309     |
| CAE in Cybersecurity National Center . . . . .   | 317 POD | National Security Agency (NSA) . . . . .                     | 300/302 |
| Capitol Technology University . . . . .  | 224     | NCyTE (Whatcom Community College) . . . . .                  | 227     |
| Carnegie Mellon University - Information Networking Inst. . . . .                        | 117     | New York University - Tandon School of Engineering . . . . . | 214     |
| Carnegie Mellon University - Software Engineering Inst. . . . .                          | 119/121 | NICE-NAT'L Initiative for Cybersecurity Education . . . . .  | 228     |
| Case Western Reserve University . . . . .  | 429     | Northeast Ohio CyberConsortium . . . . .                     | 413     |
| Center for Systems Sec. and Info. Assurance (CSSIA) . . . . .                            | 105     | Northeastern University Houry College of Comp. Sci. . . . .  | 324     |
| Central Intelligence Agency . . . . .  | 113     | Optum . . . . .  | 201/203 |
| CyberSecurity Education, Research and Outreach Center (CEROC) - Tennessee Tech . . . . . | 100     | Pacific Northwest National Laboratory . . . . .              | 230     |
| Charter Communications (Spectrum) . . . . .  | 225     | Palo Alto Networks . . . . .                                 | 401     |
| Check Point Software Technologies Inc. . . . .   | 207     | Peraton . . . . .  | 220     |
| Cleveland Clinic . . . . .   | 421     | Procter & Gamble . . . . .                                   | 430     |
| Cleveland Consortium Group/Cleveland State Univ. . . . .                                 | 412     | Progressive Insurance . . . . .                              | 102     |
| Commonwealth Cyber Initiative . . . . .  | 116     | Purdue University . . . . .                                  | 317-POD |
| Conquest Cyber . . . . .   | 316     | Raytheon . . . . .   | 219/221 |
| Cruise . . . . .   | 118     | Rider University . . . . .                                   | 319-POD |
| Cybersecurity & Infrastructure Security Agency-CISA . . . . .                            | 215     | Sandia National Labs . . . . .                               | 218     |
| Cybersecurity Youth Apprenticeship Initiative (CYAI) . . . . .                           | 318     | SANS Institute . . . . .                                     | 403     |
| CybHER at Dakota State University . . . . .  | 107     | Security Risk Advisors . . . . .                             | 307     |
| Deloitte . . . . .   | 101/103 | Securonix . . . . .  | 208     |
| Destination Cleveland. . . . .   | 409/411 | SentinelOne . . . . .  | 108/110 |
| ECS Federal. . . . .   | 104     | Sherwin-Williams Company, The . . . . .                      | 418     |
| Evolve Security. . . . .   | 426     | Shopify . . . . .  | 329     |
| EY . . . . .   | 424     | Southwest Airlines . . . . .                                 | 229     |
| Fastly . . . . .   | 129     | SpecterOps . . . . .   | 405     |
| Federal Reserve Bank of Cleveland . . . . .  | 425     | Splunk . . . . .   | 328     |
| Fortress Security Risk Management . . . . .  | 416     | Starbucks . . . . .  | 231     |
| GE Premium . . . . .   | 301/303 | Tenable, Inc. . . . .  | 317-POD |
| Georgia Tech Research Institute . . . . .  | 314     | Trend Micro . . . . .  | 428     |
| Goldman Sachs . . . . .  | 304     | Trusted Sec . . . . .  | 427     |
| Google . . . . .   | 400/402 | Two Six Technologies . . . . .                               | 407     |
| Grainger . . . . .   | 326     | University of Colorado Colorado Springs . . . . .            | 313     |
| Hyland . . . . .   | 417     | University of Colorado Dept of Computer Science . . . . .    | 114     |
| IBM . . . . .  | 209     | Verizon . . . . .  | 308     |
| Idaho National Laboratory . . . . .  | 306     | Walmart . . . . .  | 120     |
| Indiana University Cybersecurity . . . . .   | 127     | Wayfair . . . . .  | 205     |
| Information Security Summit . . . . .  | 319-POD | Wentworth Institute of Technology . . . . .                  | 315     |
| Intel Corporation . . . . .  | 213     | Westfield . . . . .  | 419     |
| ISC2 - Int'l Info Systems Security Cert Cons . . . . .                                   | 115     | Zebra Technologies . . . . .                                 | 109     |
| JPMorgan Chase & Co. . . . .   | 216     |  |         |

*Thank you to the additional sponsors that are not physically represented in the Career Fair listing.*



# VISIT THE CAREER FAIR



# EVENTS, PRIZES, TRAVEL AWARDS & SPECIAL ITEMS

## THANK YOU TO OUR SPONSORS

|   |  |
|---|--|
| <b>AbbVie</b>   | Headshots  |
| <b>Amazon</b>   | Scholarships & Travel Awards   |
| <b>AON</b>  | Scholarships & Travel Awards   |
| <b>AWS</b>  | Scholarships & Travel Awards   |
| <b>Bloomberg</b>  | Scholarships, Travel Awards, & Military Breakfast                                |
| <b>Carnegie Mellon University Software Engineering Institute</b>            | Selfie Station & Host of CTF   |
| <b>Cisco</b>  | Conference Bags, Scholarships & Travel Awards                                    |
| <b>Cleveland Consortium</b>   | Local Host   |
| <b>Cleveland State University</b>   | Local Host/Support, Printing, & Transportation                                   |
| <b>Dell</b>   | Scholarships & Travel Awards   |
| <b>Deloitte</b>   | Scholarships & Travel Awards   |
| <b>DoD C3E Community College Cyber Enrichment Program at Tennessee Tech</b> | Scholarships & Travel Awards   |
| <b>Flatiron</b>   | Scholarships & Travel Awards   |
| <b>GE</b>   | Scholarships & Travel Awards   |
| <b>Goldman Sachs</b>  | Scholarships & Travel Awards   |
| <b>Google</b>   | Scholarships & Travel Awards   |
| <b>Intel</b>  | Military Breakfast & Selfie Station  |
| <b>MasterCard</b>   | Scholarships & Travel Awards   |
| <b>Microsoft</b>  | Scholarships & Travel Awards   |
| <b>National Cybersecurity Training &amp; Education Center (NCyTE)</b>       | Scholarships & Travel Awards   |
| <b>NorthEast Ohio Cyber Consortium</b>                                      | Lanyards   |
| <b>Optum</b>  | Conference Shirts, Selfie Station, Scholarships & Travel Awards                  |
| <b>Oracle</b>   | Scholarships & Travel Awards   |
| <b>Protiviti</b>  | Scholarships & Travel Awards   |
| <b>Raytheon</b>   | Career Village Funding, Breaks, Military Breakfast, Scholarships & Travel Awards |
| <b>SalesForce</b>   | Scholarships & Travel Awards   |
| <b>Securonix</b>  | CTF After Dark Snacks  |
| <b>Sentinel One</b>   | Scholarships & Travel Awards   |
| <b>Sophos</b>   | Scholarships & Travel Awards   |
| <b>The Home Depot</b>   | Scholarships & Travel Awards   |
| <b>VISA</b>   | Scholarships & Travel Awards   |
| <b>Workday</b>  | Scholarships & Travel Awards   |
| <b>Zebra</b>  | Scholarships & Travel Awards   |

# 2022 WiCyS CONFERENCE VENUE MAPS

## HUNTINGTON CONVENTION CENTER



# 2022 WiCyS CONFERENCE VENUE MAPS

## WICyS LOCATION MAP

*Join in at [ThisisCLEVELAND.COM](https://www.thisiscleveland.com)*

**WiCyS**  
CLEVELAND 2022

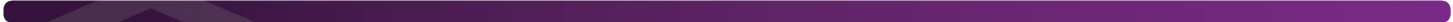
**WOMEN IN CYBERSECURITY**  
MARCH 17-19, 2022

**EVENT LOCATIONS**  
Huntington Convention Center of Cleveland  
Tower City / Public Square Station

**EVENT HOTELS**

- 1 Hilton Cleveland Downtown
- 2 Cleveland Marriott at Key Center
- 3 Drury Place Hotel
- 4 Westin Cleveland Downtown

**5 MINUTE WALK**



# 2022 WiCyS CONFERENCE VENUE MAPS

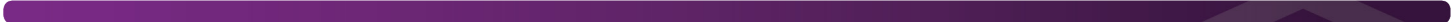
## DOWNTOWN CLEVELAND PARKING MAP

Get the map on your phone at [MAP.THISISCLEVELAND.COM](http://MAP.THISISCLEVELAND.COM)

Join in at **ThisisCLEVELAND.COM**

**PARKING**

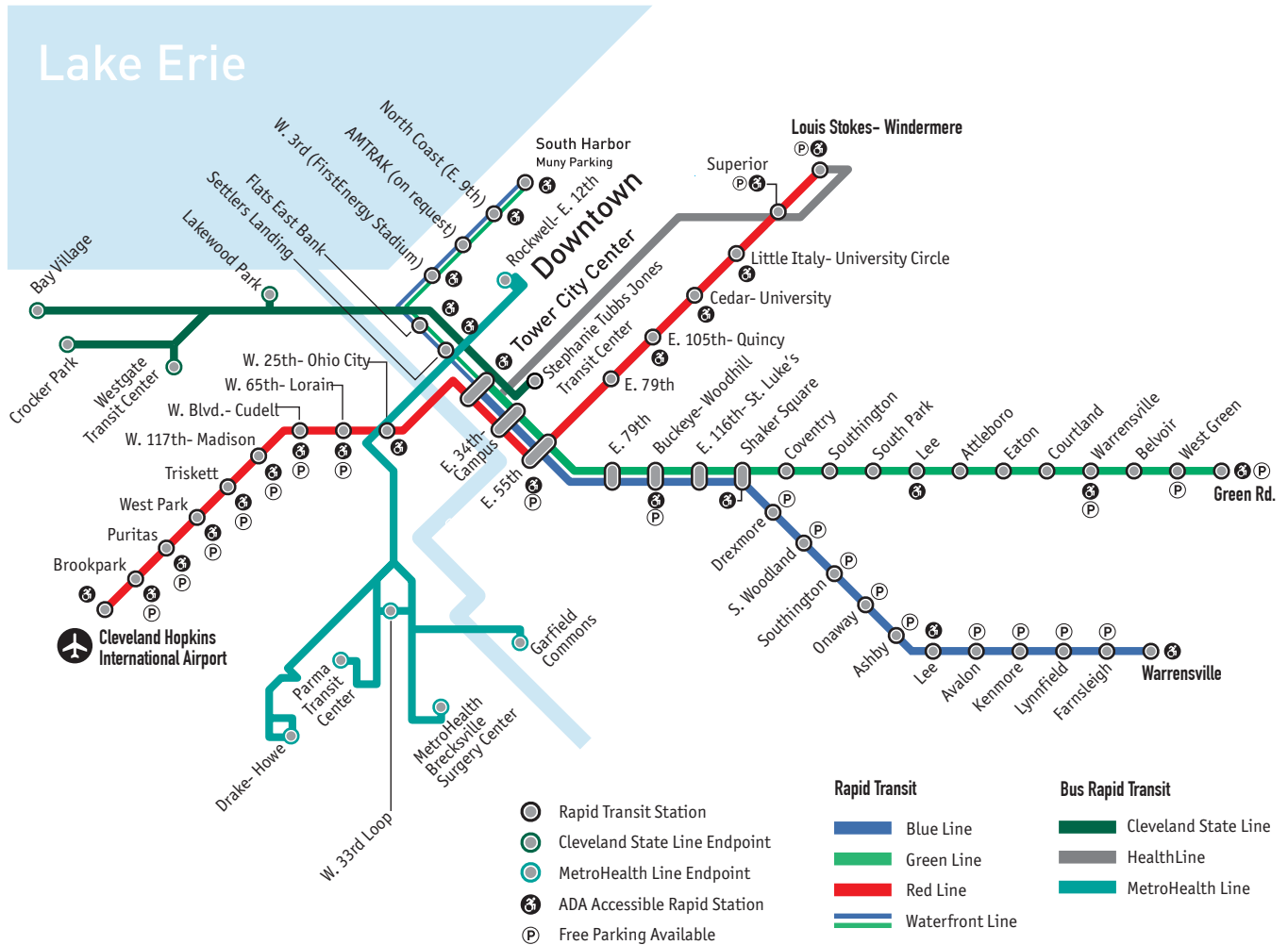
- 1 Huntington Park Garage, (connected),  
1141 West 3rd, 216-443-2141
- 2 Willard Park Garage,  
601 Lakeside Ave E, 216-664-2999
- 3 Memorial Plaza Garage,  
300 St Clair Ave NE, 216-664-1114
- 4 777 Rockwell Garage,  
777 Rockwell Ave, 216-472-1366
- 5 Cuyahoga County Courthouse Square Parking,  
310 West Lakeside Ave, 216-443-7007
- 6 LAZ Parking,  
1365 W 9th Street, 216-577-5414
- 7 North Point Parking Garage,  
1111 East 9th Street, 216-575-0355
- 8 North Coast Municipal Parking Lot,  
1500 S Marginal Rd, 216-664-2999
- 9 Katco Inc.,  
1180 Lakeside Ave E, 216-575-1532
- 10 One Cleveland Center Garage,  
1375 E 9th St, 216-621-6600
- 11 Oswald Center Garage,  
1100 Superior Ave E, 216-589-9050
- 12 55 Public Square Garage,  
W 3rd St/W St Clair Ave, 877-727-5452
- 13 Public Square West,  
226 W Superior Ave, 216-664-1114
- 14 Warehouse District-Lot 44,  
1426 W 3rd St, 216-621-0328
- 15 Warehouse District-Lot 46,  
1400 W 3rd St, 216-621-0328
- 16 200 Public Square Garage,  
320 Superior Ave, 216-589-9050
- 17 515 Euclid Garage,  
515 Euclid Ave, 216-771-5333
- 18 Euclid-Prospect Gateway Garage,  
740 Euclid Ave, 216-861-3021





# 2022 WiCyS CONFERENCE VENUE MAPS

## RAPID TRANSIT SYSTEM MAP



women in  
CYBERSECURITY

WiCyS



#SeeHerAsEqual



## **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](mailto:info@wicys.org).