WICYS CONFERENCE 2024

10th Anniversary

Women in Cybersecurity

WiCyS

NASHVILLE 2024

April 11-13 • Nashville, TN

10TH

Anniversary

#WiCyS2024

Bloomberg

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

FORTINET

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

Optum

RTX

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 associated with your conference registration 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.

https://whova.com/portal/wicys_202403/

CODE OF CONDUCT

WiCyS is committed to providing a safe and welcoming space for all. We will not tolerate behavior that doesn't adhere to the WiCyS code of conduct.

Report Unacceptable Behavior

Call: (720) 258-6281
Email: EAC@wicys.org

https://www.wicys.org/code-of-conduct/

SAFETY AND SECURITY

If you see any suspicious activity, experience or witness physical threats, or encounter an emergency, immediately take action:

Call 911
Call Security Personnel: (615) 458-5555

Due to the complexities of navigating the hotel facilities, please make sure to contact BOTH emergency numbers above.

CRISIS TEXT LINE

Text HOME to 741741 from anywhere in the United States, anytime. Crisis Text Line is here for any crisis (24/7). A live, trained Crisis Counselor receives the text and responds, all from our secure online platform. The volunteer Crisis Counselor will help you move from a hot moment to a cool moment.

Additional information can be found here: https://www.crisistextline.org

WIFI ACCESS CODE

SSID: WICYS-10

PASSWORD: CELEBRATE10!

CONFERENCE PHONE NUMBER

For urgent matters or non-medical/safety emergencies during the conference please call or text:

(720) 258-6281

TABLE OF CONTENTS

BADGE PICK-UP HOURS

Thursday 7:00am - 7:00pm

Friday 7:00am - 6:00pm

Saturday 7:00am - 9:00am

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. From community groups to career fairs, scholarships to speaking opportunities, and much much more – check out all the benefits below and see what's waiting for you!

https://www.wicys.org/benefits/

TO OUR LOCAL HOST THANK YOU!

The Cybersecurity Education, Research, and Outreach Center (CEROC) at Tennessee Tech

CEROC
Cybersecurity Education, Research and Outreach Center

WELCOME TO THE 10TH ANNIVERSARY WiCyS CONFERENCE

A Decade of WiCyS: Building and Sustaining a Community of Women in Cybersecurity Like No Other!

On April 11, 2014, Women in Cybersecurity (WiCyS) started its journey here in Nashville to celebrate the power of sisterhood in cyber. We saw and heard others like us. We found mentors, friends and role models among us. Most importantly, we stayed together over the years building relationships, careers and networks. By doing so, we successfully contributed to doubling women's representation in the cybersecurity field over the past decade from 11% to 24%.

As we commemorate the 10th anniversary of the WiCyS conference, I am filled with immense pride and gratitude for this vibrant and impactful community that is built on the unwavering commitments of women and allies dedicated to lifting themselves and others around them.

Cybersecurity is not just a career; it's a calling for societal impact in a time when modern technology drives almost every aspect of our lives. Without a cyber workforce at play, human society cannot coexist with technology. Now more than ever, diversity in the cyber workforce is critical because differences are our greatest assets to address complex multi-faceted problems.

The WiCyS conference was born out of a common sense to empower ALL diverse minds at a time of critical shortage of cybersecurity professionals – a vision fueled by a 2013 National Science Foundation grant originally managed by Tennessee Tech University and, since then, nurtured by countless passionate souls. The WiCyS conference could not have sustained and turned into the WiCyS Global Non-Profit organization without the support from its three founding partners: Cisco, Facebook and Palo Alto Networks. We are forever grateful for their crucial support at a very critical juncture. I must express my utmost eternal gratitude to my dear friend and confidant, Dr. Janell Straach, who has been by my side most of this journey and has led the organization with her admirable resolve.

I extend my heartfelt appreciation to the WiCyS Board, whose invaluable guidance propels the organization to thrive; to WiCyS Strategic Partners, who enable us every day to make a difference together; to the incredible committed WiCyS team led by our Executive Director Lynn Dohm, whose dedication and passion for this community is unwavering; and most importantly, to ALL of YOU, the WiCyS community! Our success story is woven from threads of comradery, collaboration and compassion. Together, as members of the WiCyS community, we champion the cause of women in cybersecurity.

To each one of you joining us this year on this milestone anniversary, let's collaborate to achieve a gender-balanced, robust and skilled cybersecurity workforce in the coming years. Let us envision a near future where the persistent shortage of cybersecurity professionals disappears, with women fearlessly at the forefront of this field.

Thank you for being part of this remarkable journey, whether you joined a decade ago or days ago. Here's to another decade of WiCyS – a decade of impact, inclusion and excellence.

With gratitude and much anticipation,

Dr. Ambareen Siraj
WiCyS Founder

FOUNDING PARTNERS

CISCO FACEBOOK paloalto® NETWORKS

WiCyS ORGANIZATION

BOARD OF DIRECTORS

Dr. Ambareen Siraj
NSF (Siraj is serving in her personal capacity)
Founder, WiCyS

Dr. Janell Straach
Chair of the Board, WiCyS
Faculty, Rice University

Dr. Costis Toregas
Treasurer, WiCyS
Director, Cyber Security and Privacy Research Institute, George Washington University

Dr. Dawn M. Beyer
Senior Fellow,
Lockheed Martin Space

Valerie Jane Chua
Tech Campus Manager, Silicon Valley,
JPMorgan Chase & Co.

Prajakta Jagdale
Director, Information Security,
Palo Alto Networks

Diana Kelley
Founder and CTO,
SecurityCurve

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

Allison Miller
Chief Information Security Officer and
Senior Vice President,
UnitedHealth Group/Optum

Sarah Morales
Senior Program Manager,
Privacy, Safety & Security Engineering, Google

Noureen Njoroge
Director of Global Cyber Threat Intelligence,
Nike, Inc.

Dr. Greg Shannon
Chief Cybersecurity Scientist,
Idaho National Laboratory
Chief Science Officer, Cybersecurity Manufacturing Innovation Institute

STAFF

Lynn Dohm
Executive Director

Michele Tomasic
Deputy Director

Mary Jane Partain
Program Director

Peter Baldwin
vCFO - Chief Financial Officer

Morgan Garland
Operational Manager

Colleen Huber
Marketing Manager

Jaclyn Justice
Professional Affiliate Manager

Cameron Mitchell
External Relations Manager

Quiana Oates
Program Manager

Quintana Patterson
Cybersecurity and Technology Manager

Myriam Saint Jean
Financial Manager

Adaeze Udoh
Program Coordinator

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 to learn more about strategic partnerships!

FLOWCODE PRIVACY.FLOWCODE.COM

https://www.wicys.org/support/strategic-partnerships/

2024 WiCyS CONFERENCE KEYNOTE SPEAKERS

Cybersecurity and Infrastructure Security Agency (CISA) Keynote:

Lisa Einstein

Senior Advisor for Artificial Intelligence and Executive Director of the Cybersecurity and Infrastructure Security Agency's Cybersecurity Advisory Committee, CISA

"Embodying Trustworthiness: Lessons from AI for Women in Cybersecurity"

Lisa Einstein serves as a Senior Advisor for Artificial Intelligence and Executive Director of the Cybersecurity and Infrastructure Security Agency's Cybersecurity Advisory Committee. She was Stanford's first dual master's degree recipient in computer science (AI specialization) and international policy (cyber policy and security specialization). While at Stanford, she led H.R. McMaster's research team on emerging technologies and geopolitics and conducted research on trust and safety engineering, AI-augmented education, and algorithmic decision support tools for humanitarian evacuations. Previously, Lisa taught physics to over 600 students as a Peace Corps Volunteer in rural Guinea. She received her BA from Princeton in physics and dance and danced professionally for several years, including with Camille A. Brown and Dancers.

Fortinet Keynote:

Kimberly Becan

Senior Director of Product Marketing-FortiGate and Network Operations, Fortinet

"From Code to Command: Navigating the Journey from Network Systems Programmer to Product Marketing Leader in Cybersecurity"

Kimberly leads the Network Firewall and Network Operations solutions of the Fortinet Security Fabric. She drives products and solutions to improve operational efficiency for Network, Security, and IT leaders with unified network and security management to ease the deployment and adoption of modern security technologies such as NGFW, Secure SD-WAN, and ZTNA. NGFW and unified management are essential to decrease security risks by ensuring consistent policies across the enterprise at scale while ensuring the best end-user digital experience.Before joining Fortinet, Kimberly held various positions leading product marketing, product development, solutions engineering, and customer success teams in network and security solutions, providing strong leadership and a creative approach for cross-functional success.

National Security Agency (NSA) Keynote:

Morgan Adamski

Director, Cybersecurity Collaboration Center, National Security Agency (NSA)

"Bringing Unique Perspectives to National Security"

Ms. Morgan Adamski is the Director of NSA's Cybersecurity Collaboration Center, responsible for scaling intel-driven cybersecurity through open, collaborative partnerships with interagency industry and international partners. By changing culture and challenging the status quo, her unconventional leadership style helps promote cyber best practices and guidance to harden billions of endpoints against nation-state cyber threats. For more than a decade, Ms. Adamski has worked across NSA's offensive and defensive missions. She has led offensive cyber mission planning, executed operations against some of the Agency's hardest intelligence targets, served as Senior Advisor to the Deputy Assistant Secretary for Defense (DASD) for Cyber Policy, and helped stand up the NSA Cybersecurity Directorate. As an advocate for women in cyber, she has continually stressed the importance of more diversity in the cyber community to make a difference. Awards: CAMI Award 2023, Billington Cyber Public-Private Partnership Collaboration Award 2022, Cyberscoop 50 Award for Government Leadership 2023.

2024 WiCyS CONFERENCE

KEYNOTE SPEAKERS

RTX Keynote:

Esmeralda Iyescas

Software Developer, Collins Aerospace

"From WiCyS Student to RTX Leader: My Career Journey"

Esmeralda Iyescas serves as a software developer at Collins Aerospace. As part of the RTX Digital Leadership Development Program, she has rotated through various digital technology departments throughout the RTX family, including Enterprise Architecture at Pratt and Whitney as well as Cyber Threat Intelligence at Raytheon. Esmeralda was actually recruited to join the RTX family as a recent graduate after an interview at WiCyS! Prior to joining Collins, Esmeralda completed her Bachelors of Science in IT from Florida International University, where she also gained a certificate in Global Cybersecurity Policies, and attained an Associates Degree in Computer Information Systems from Miami Dade College. She plans to pursue her masters degree in the Fall of 2024.

Keynote:

Deborah Frincke

Associate Labs Director, Sandia National Laboratories

"10th Anniversary Keynote"

As the National Security Programs Associate Labs Director for Sandia National Laboratories, Deborah Frincke manages Strategic Partnership projects for the U.S. Department of Defense and other federal departments and agencies, Strategic Intelligence Partnership Projects for the U.S. Intelligence Community, and programs for the U.S. Department of Energy Office of Intelligence and Counterintelligence. Deborah served at the National Security Agency from 2011 to 2020 in three capacities, most recently Director of Research, NSA Science Advisor, and Member of the Board of Directors. Deborah also served as Associate Laboratory Director at Oak Ridge National Laboratory (ORNL) for National Security Science (2020-2021), chief scientist of cybersecurity research at Pacific Northwest National Laboratory from 2004 to 2011, cofounder of TriGeo Network Security, and was a full professor at the University of Idaho. Deborah currently serves on the U.S. Strategic Command (USSTRATCOM) Strategic Advisor Group and was appointed by President Biden as a member of the National Quantum Initiative Advisory Committee.

SOCIAL MEDIA

CONNECT WITH THE WICYS COMMUNITY ON SOCIAL MEDIA

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

https://twitter.com/WiCySorg

https://www.facebook.com/wicys

https://www.instagram.com/wicysorg/

https://www.youtube.com/@WomeninCyberSecurityWiCySorg

THANK YOU TO OUR 2024 CONFERENCE SPONSORS

VIP SPONSORS

Bloomberg
Cybersecurity & Infrastructure Security Agency CISA
FORTINET
National Security Agency United States of America
Optum
RTX

PREMIUM SPONSORS

aws
Carnegie Mellon University Software Engineering Institute
cisco
Deloitte.
DeVry University
Ford
Google
LOCKHEED MARTIN
Microsoft
Naval Information Warfare Center PACIFIC
okta
SentinelOne
Southwest
Vanguard
verizon
Walmart
workday.

DIAMOND SPONSORS

Adobe
American Airlines
AON
BANK OF AMERICA
Brown Brothers Harriman
CHECK POINT
CROWDSTRIKE
CSSIA National Support Center for Systems Security and Information Assurance
DAKOTA STATE UNIVERSITY
ECS
GRAINGER
Huntington Bank
IBM
MITRE
MOTOROLA SOLUTIONS
Oak Ridge National Laboratory
paloalto NETWORKS
RICE UNIVERSITY
Sandia National Laboratories
servicenow
CERIC Cybersecurity Education, Research and Outreach Center
TikTok
The University of Rhode Island
CYBERSECURITY SERVICE U.S. DEPARTMENT OF HOMELAND SECURITY
wayfair
ZEBRA

PLATINUM SPONSORS

AMERICAN EXPRESS
asurion
Capital One
CHAMPLAIN COLLEGE
corelight
DELL Technologies
ENVESTNET
EY
FIU FLORIDA INTERNATIONAL UNIVERSITY
INL Idaho National Laboratory
MORGANFRANKLIN CONSULTING A Tetra Tech Company
Nestlé Information Technology
NC PaCE North Carolina Partnership for Cybersecurity Excellence
NuHarbor SECURITY
Pacific Northwest NATIONAL LABORATORY
proofpoint.
PROTECT AI
RIT Department of Cybersecurity
SANS
SecurityRisk ADVISORS
Swift
tenable
TOYOTA
UCCS University of Colorado Colorado Springs
W UNIVERSITY of WASHINGTON TACOMA
VS&Co

GOLD SPONSORS

ACTIVISION.
ARISTOCRAT
BATTELLE
Carnegie Mellon University Information Networking Institute
FANDUEL
INFOSEC
ISC2
JOHNS HOPKINS SCHOOL of ADVANCED INTERNATIONAL STUDIES
KEYFACTOR
CYBER SOLUTIONS
MIT LINCOLN LABORATORY
NCYTE CENTER
NICE NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION
NREL Transforming ENERGY
Northeastern University Khoury College of Computer Sciences
OLD DOMINION UNIVERSITY
SEALINGTECH
SPECTEROPS
TU TOWSON UNIVERSITY
TRAIL OF BITS
W UNIVERSITY of WASHINGTON | BOTHELL MASTER OF SCIENCE IN CYBERSECURITY ENGINEERING
Wentworth INSTITUTE OF TECHNOLOGY
WPI

SILVER SPONSORS

BILLINGTON CyberSecurity
Black Girls In CYBER
Last Mile Education Fund
Phylum
PUBLIC SECTOR NETWORK
RIDER UNIVERSITY
School of Information Technology Experience Collaborate | Innovate | Apply

10TH ANNIVERSARY SPONSORS - 2014 & 2024

asurion
Carnegie Mellon University Information Networking Institute
CHAMPLAIN COLLEGE
Google
IBM
LOCKHEED MARTIN
Microsoft
MIT LINCOLN LABORATORY
CERIC Cybersecurity Education, Research and Outreach Center

Bloomberg

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.

INTERNSHIP AND FULL-TIME ROLES

Bloomberg.com/careers

Make it happen here.

THANK YOU TO OUR 2024 WiCyS COMMITTEES

CONFERENCE PROGRAM CHAIR

Ambareen Siraj
NSF (Siraj is serving in her personal capacity)
Founder, WiCyS

CONFERENCE GENERAL CHAIR

Janell Straach
Chair of the Board, WiCyS
Faculty, Rice University

PROGRAM CO-LEADS

Pat Mccain
WiCyS **(Lead)**

Smriti Bhatt

Priyam Biswas
Intel

Chutima Boonthum-Denecke
Hampton University

Jennifer Cheung

Meg Layton
Children's National Hospital

Angel Liu
Confluent

Elena Peterson
Pacific Northwest National Laboratory

Elizabeth Rasnick
University of West Florida

Awalin Sopan
Workday

Bich Vu
MIT Lincoln Laboratory

PROGRAM

Ridhima Agarwal
JPMorgan Chase & Co.

Saja Alqurashi
Colorado State University

Safwa Ameer
MITRE Corporatiaon

Rutuben Ataliya
AWS Security

Deborah Barnes
Cradlepoint

Basma Basem
Microsoft

Shuvra Chakraborty
Temple University

Christina Chapple

Angela Clark
University of South Alabama

Diara Dankert
ConnectWise

Mai Ensmann
Cyber Florida: The Florida Center for Cybersecurity

Bill Gardner
Marshall University

Jessa Gegax
Surescripts

Keerthi Sameera Immanni

Nicole King
SentinelOne

Cindy Kishoyian
Verizon

Danielle Kissel
US Army, Army Retirement Services

Tanvi Kolte
LinkedIn

Chris Lemmon
Secure Yeti

Jen Miller-Osborn
Netwitness Firstwatch

Omoshalewa Muhammed
FORVIS

Laura Elena Navarro Cobos

Laxima Niure Kandel
Embry-Riddle Aeronautical University

Prathibha Muraleedhara
Stanley Black & Decker

Collins Okafor
WiCyS Houston Affiliate

Kalyani Pawar

Ana Pease

Trista Polaski
Carnegie Mellon University: Software Engineering Institute

Sneha Rangari
Visa Technology and Operations

Katie Riesing

Stephanie Scheuermann
Ford Motor Company

Jillian Seabrook
MIT Lincoln Laboratory

Amy Starzynski Coddens
Universities of Wisconsin Administration

Heather Stoner
Optum

Cindy Sutherland

Brittney Swearinger
Cisco

Junia Valente
Toyota Tsusho Systems, US, Inc.

Jaidie Vargas
Lockheed Martin

THANK YOU TO OUR 2024 WiCyS COMMITTEES

SCHOLARSHIP

Janell Straach
WiCyS **(Lead)**

Gretchen Bliss
University of Colorado Colorado Springs

Kristine Christensen
Moraine Valley Community College

Ramona Codreanu
University of Michigan

Joe Eastman
Champlain College

Maria Fanelle
MITRE

Marcie Friedman
Norfolk Southern

Esther Goldstein
Salesforce

Deepti Gupta
Texas A&M University-Central Texas

Amy Justice
Randstad North America

Rachael Klamo
Optum

Pushpa Kumar
University of Texas at Dallas

Aleise McGowan
The University of Southern Mississippi

Angela Pena
Dell Technologies

Penelope Rozhkova
Accenture

Samantha Shields
CISA

Angela Sims-Ceja
Aurora Water – City Of Aurora

Miranda Skar
Aon/Gotham Digital Science

Shannon Strum
Stripe

Mary Wallingsford
Anne Arundel Community College

Stella Whyte
River State University

CAREER FAIR

Pat McCain
WiCyS **(Lead)**

Tara Lewis
Collin College (Frisco)

CAREER GROWTH HUB PLANNING

Andrea Frost
Dell Technologies **(Lead)**

Julia Costin
Cyber Qubits

Terri Johnson-Akse
University of Colorado Colorado Springs

Michelle Lindblom
SecureMatter

CAREER GROWTH HUB OPERATIONS

Kimberly Bertschy
Wal-Mart

Devi Bhattacharya
University at Albany – State University of New York

Jason Craig

Sharon Mireku
Independent Contractor

Heather Ricciuto
IBM

Merle Rodriguez

Erica Smith

THANK YOU TO OUR 2024 WiCyS COMMITTEES

OPERATIONS & LOGISTICS

Lynn Dohm
WiCyS **(Lead)**

Peter Baldwin
WiCyS

Tia Debord
Times 10 Association Strategies

Patty Duffy
GlobauxSource

Morgan Garland
WiCyS

Jennifer Haisten
Times 10 Association Strategies

Colleen Huber
WiCyS

Kimberly Hutcherson
GlobauxSource

Jaclyn Justice
WiCyS

Quiana Oates
WiCyS

Patti Palacios
GlobauxSource

Quintana Patterson
WiCyS

Myriam Saint Jean
WiCyS

Tara Sparacino
Carnegie Mellon University: Software Engineering Institute/CERT

Michele Tomasic
WiCyS

Adaeze Udoh
WiCyS

POSTER

Chutima Boonthum-Denecke
Hampton University **(Lead)**

Amani Altarawneh
Tennessee Tech University

Smriti Bhatt
Purdue University

RETAIL STORE

Mary Jane Partain
WiCyS **(Lead)**

Reethee Ghafoor
WiCyS

Mia Partain
WiCyS

Myriam Saint Jean
WiCyS

SOCIAL MEDIA AND PR

Aditi Chaudhry
Two Sigma

Chelsea Conard
Massachusetts Institute Of Technology

Midori Connolly

Abigail Phillips
Nelly Group

Alina Thai
Georgetown University

VOLUNTEER

Cameron Mitchell
WiCyS **(Lead)**

Brooke Beyer
Lockheed Martin

Jamie Glenn
Carnegie Mellon University: Software Engineering Institute/CERT

Tricia McMahon
County of San Diego

2024 WiCyS SCHEDULE AT A GLANCE

THURSDAY		
7:00am - 7:00pm	Badge Pick-Up	Delta BCD Lobby
9:00am - 10:30am	**INVITE ONLY:** Leadership Breakfast and Symposium	Delta D
11:00am - 2:00pm	Headshots	Canal D
11:00am - 7:00pm	WiCyS Store Open	Delta C
12:00pm - 1:30pm	**INVITE ONLY:** Senior Leader Luncheon	Old Hickory
12:30pm - 1:30pm	First Timer's Panel	Delta D
12:30pm - 1:30pm	Recruiters Session	Bayou CD
12:30pm - 7:00pm	Capture The Flag (CTF) Mentoring Available	Delta A Lobby
1:30pm - 4:30pm	Career Fair Setup by Sponsors	Ryman B 1-2
2:00pm - 6:00pm	Career Growth Hub Open	Canal DE
2:00pm - 4:00pm	Workshop Series	Various Rooms
2:00pm - 2:45pm	Presentation Sessions	Bayou E
3:00pm - 3:45pm	Presentation Sessions	Bayou E
4:00pm - 4:30pm	Break	Delta BCD
4:00pm - 7:00pm	Poster Session Check-In	Delta BCD Lobby
4:30pm - 6:30pm	Workshop Series	Various Rooms
4:30pm - 5:15pm	Presentation Sessions	Bayou E
5:30pm - 6:15pm	Presentation Sessions	Bayou E
6:30pm - 7:15pm	Federal Scholarship Information and Networking Session	Bayou E
7:30pm - 9:30pm	Socials	Governor's Ballroom & Delta D
7:30pm - 8:15pm	Educators/Scientists - Meetup with Federal Funding Agencies	Bayou E

PICK-UP & PURCHASE WiCyS GEAR

VISIT DELTA C FOR THE WICYS STORE

THURSDAY: 11:00am - 7:00pm

FRIDAY: 9:45am - 6:00pm
(closed 12:00pm - 12:30pm for lunch)

SATURDAY: 10:00am - 1:00pm

The WiCyS 2024 conference store will support the WiCyS conference scholarship fund. We thank you for your ongoing support and for wearing your WiCyS pride while paying it forward to more women in cybersecurity.

FRIDAY		
7:00am - 6:00pm	Badge Pick-Up	Delta BCD Lobby
7:00am - 8:00am	Breakfast Available for Scholarship Recipients	Canal Lobby
7:00am - 8:15am	**INVITE ONLY:** Early Career Breakfast	Delta B
7:00am - 8:15am	**INVITE ONLY:** Mid Career Breakfast	Delta D
7:00am - 8:15am	**INVITE ONLY:** Male Allyship Breakfast	Bayou AB
7:00am - 8:30am	Poster Session Check-In	Delta BCD Lobby
8:00am - 9:00am	Career Fair Setup by Sponsors	Ryman B 1-2
8:30am - 9:45am	Conference Opening and Keynote (doors open 8:15am)	Delta A
9:45am - 6:00pm	WiCyS Store Open (closed 12:00 - 12:30pm for lunch)	Delta C
9:45am - 11:45am	Career Fair Open	Ryman B 1-2
9:45am - 11:45am	Capture The Flag (CTF) Mentoring Available	Delta A Lobby
9:45am - 11:45am	Career Growth Hub Open	Canal DE
9:45am - 11:00am	Student Poster Session and Networking Refreshment Break	Delta BCD Lobby
11:00am - 11:45am	Presentation Sessions	Various Rooms
11:00am - 11:45am	Student Chapter Leader Meetup	Delta D
12:00pm - 1:45pm	Keynote, Lunch and Networking (must be seated by 12:10pm to eat)	Delta A
1:55pm - 5:30pm	Career Fair Open	Ryman B 1-2
1:55pm - 5:30pm	Capture The Flag (CTF) Mentoring Available	Delta A Lobby
1:55pm - 5:30pm	Career Growth Hub Open	Canal DE
1:55pm - 2:40pm	Presentation Sessions	Various Rooms
1:55pm - 2:40pm	Affiliate Leader MeetUp	Delta D
2:45pm - 3:15pm	Break with Refreshments in Career Fair	Ryman B 1-2
2:50pm - 4:40pm	Workshop Series	Various Rooms
2:50pm - 3:40pm	Presentation Sessions	Various Rooms
3:50pm - 4:40pm	Presentation Sessions	Various Rooms
4:45pm - 5:30pm	Birds of a Feather	Various Rooms
6:00pm - 7:45pm	Keynote, Dinner and Networking (must be seated by 6:10pm to eat)	Delta A
8:30 pm - Midnight	CTF After Dark Party	Delta A Lobby

2024 WiCyS SCHEDULE AT A GLANCE

SATURDAY		
7:00am - 9:00am	Badge Pick-Up	Delta BCD Lobby
7:00am - 8:15am	**INVITE ONLY:** Military Breakfast	Bayou E
7:00am - 8:00am	Breakfast Available for Scholarship Recipients	Canal Lobby
7:00am - 5:00pm	Luggage Storage Available	Delta C
8:30am - 9:30am	Keynote (doors open 8:15am)	Delta A
9:30am - 10:00am	Group Picture and Break with Refreshments	TBD
10:00am - 1:00pm	WiCyS Store Open	Delta C
10:00am - 10:45am	Presentation Sessions	Various Rooms
10:00am - 10:45am	Lightning Talks	Delta D
11:00am - 11:45am	Presentation Sessions	Various Rooms
11:00am - 11:45am	Lightning Talks	Delta D
12:00pm - 12:45pm	Panels	Various Rooms
12:45pm - 2:00pm	Lunch, Closing Remarks and Awards (must be seated by 1:00pm to eat)	Delta A
2:00pm - 2:30pm	Travel Stipend Verification (Only for Stipend Awardees)	Delta BCD Lobby
2:30pm - 4:30pm	Workshop Series	Various Rooms

CPES & CEUS

GIAC, ISC2 and WiCyS CPEs and CompTIA CEUs are available for designated sessions. Reference the agenda or session descriptions to identify the sessions that qualify.

After attending the full session, locate the WiCyS volunteer at the back of the room to scan the QR code or to have your badge scanned.

You must complete this step before leaving the session. There will be no credit given after the session is over.

You will receive an email by May which will include information on submitting to CompTIA, GIAC and ISC2 to receive your CPEs/CEUs.

WICYS COMMUNITIES

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 below to learn more about WiCyS Professional Affiliates.

https://www.wicys.org/initiatives/affiliate-and-industry/

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

https://www.wicys.org/initiatives/student-chapters/

PROGRAM PARTICIPATION
TRACKS AND SESSIONS

● **TECHNICAL SKILL BUILDING TRACK**
Technical skill development in all areas of cybersecurity.

● **EDUCATION & WORKFORCE DEVELOPMENT TRACK**
All levels of cybersecurity education and training programs.

● **RESEARCH & INNOVATION TRACK**
Includes research, entrepreneurship, and trends in emerging technologies.

● **CAREER ADVANCEMENT TRACK**
Includes hiring, leadership, career development/growth, internships and apprenticeship.

● **COMMUNITY ECOSYSTEM & OUTREACH TRACK**
Includes collaborations/partnerships and diversity, equality, inclusion & accessibility (DEIA) efforts.

CPE CREDITS: GIAC, ISC2 AND WiCyS

CEUS: CompTIA

* *Each colored dot represents a session track. Reference the colored dots throughout the agenda and session descriptions to identify each session's corresponding track(s).*

TECHNICAL PRESENTATIONS

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

WORKSHOPS

Workshops are 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.***

BIRDS OF A FEATHER (BoaF)

Birds of a Feather are informal discussion sessions moderated by the facilitator on just about any topic related to cybersecurity that elicit participant discussions. The facilitator leads the discussion with active participation from the audience. 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 discussion.

PANELS

Panels provide opportunities to discuss a current relevant topic in cybersecurity. In addition to the moderator, there can be up to 3 panelists. ***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 their choice. Runners-up receive prizes as well.

2024 WiCyS SCHEDULE
THURSDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 7:00pm	Badge Pick-Up	Delta BCD Lobby
9:00am - 10:30am	INVITE ONLY: Leadership Breakfast and Symposium	Delta D
11:00am - 2:00pm	Headshots - Sponsored by Ford Motor Company	Canal D
11:00am - 7:00pm	WiCyS Store Open	Delta C
12:00pm - 1:30pm	INVITE ONLY: Senior Leader Luncheon - Sponsored by Bloomberg	Old Hickory
12:30pm - 1:30pm	**First Timers Panel | Navigating Your First WiCyS Conference** *Elizabeth Hawthorne, Morgan Adamski, Deborah Kariuki, Shannon McHale, Ossie Munroe and Warren Proctor* Track(s): ● CPE Credits: 1	Delta D
12:30pm - 1:30pm	**Recruiters Session | Rethinking Recruiting: Effective Hiring Practices to Close the Skills Gap** *Audra Streetman and Lillian Teng* Track(s): ● ● CPE Credits: 1	Bayou CD
12:30pm - 7:00pm	Capture The Flag (CTF) Mentoring Available	Delta A Lobby
1:30pm - 4:30pm	Career Fair Setup by Sponsors	Ryman Hall B 1-2
2:00pm - 6:00pm	Career Growth Hub Open	Canal DE
2:00pm - 4:00pm	Workshop Series	
	The Beginner's Guide to Secure Code Reviews *Rita Law, Mary DuBard and FNU Prashasti* Track(s): ● CPE Credits: 2	Bayou AB
	Architectural Thinking for Security *Snezhana Dubrovskaya and Nikki Robinson* Track(s): ● ● ● CPE Credits: 2	Bayou CD
	OSINT Unveiled: Techniques and Tools for Effective Information Gathering *Katie Shuck, Cynthia Hetherington, Arica Kulm and Ashley Podhrasky* Track(s): ● ● CPE Credits: 2	Canal ABC
	The Weaponization of Misinformation: Fortifying Your Mind in the Face of Fake News *Madison Fox* Track(s): ● ● CPE Credits: 2	Delta B
	The Cultural Intelligence Code for Diverse Leadership *Loren Rosario-Maldonado* Track(s): ● CPE Credits: 2	Delta D
2:00pm - 2:45pm	Presentation Sessions	
	Gs, Cs, and P's - Exploring Certifications and Career Paths in Cyber *Midori Connolly* Track(s): ● CPE Credits: 1	Bayou E
3:00pm - 3:45pm	Presentation Sessions	
	Navigating the Career Journey *Pinal Patel, Jerusha Sejera and Michelle Kababik* Track(s): ●	Bayou E

2024 WiCyS SCHEDULE

THURSDAY AGENDA

TIME	DESCRIPTION	LOCATION
4:00pm - 4:30pm	Break	Delta BCD Lobby
4:00pm - 7:00pm	Poster Session Check-In	Delta BCD Lobby
4:30pm - 6:30pm	Workshop Series	
	The Malware Challenge: Stepping Up Your Triage Game *Alessandra Perotti* Track(s): ● CPE Credits: 2 CEUs: 2	Bayou AB
	Shift Left Security: Walk the Talk or Lose $10.5 Trillion! *Michelle Wan and Priya Nath* Track(s): ● CPE Credits: 2	Bayou CD
	The Best Defense is a Rusty Offense *Diane Stephens* Track(s): ● ● ● CPE Credits: 2 CEUs: 2	Canal ABC
	Introducing ThreatGPT: The Malicious Sibling of ChatGPT *Kshitiz Aryal, Lopamudra Praharaj and Maanak Gupta* Track(s): ● ● CPE Credits: 2	Delta B
	SANS Executive Cybersecurity Exercise *Michael Barcomb and Christopher Wilkes* Track(s): ● ● CPE Credits: 2 CEUs: 2	Delta D
4:30pm - 5:15pm	Presentation Sessions	
	Networking for Introverts in Cybersecurity *Paula Biggs and Rebecca Granger* Track(s): ● CPE Credits: 1	Bayou E
5:30pm - 6:15pm	Presentation Sessions	
	An Interviewee's Secret Sauce *Chandler Jackson* Track(s): ● CPE Credits: 1	Bayou E
6:30pm - 7:15pm	**Federal Scholarship Information and Networking Session** *Ashley Greeley and Laura Knowles* Track(s): ●	Bayou E
7:30pm - 9:30pm	Socials	Governor's Ballroom & Delta D
7:30pm - 8:15pm	**Educators/Scientists - Meetup with Federal Funding Agencies** *Sheikh Ghafoor, Ashley Greeley, Karen Karavanic and Akhirah Padilla* Track(s): ● ●	Bayou E

GO YOUR OWN WAY at NSA

Tech careers can take many paths, and at NSA, the choice is yours. Mai has gone from a signals analyst to a sought-after technical leader who seized every growth opportunity along the way - even a stint in Congress.

Join NSA for:

- **Advancement Opportunities**
- **Tuition Assistance**
- **External Assignments**

SCAN OR VISIT
TO **APPLY NOW!**

IntelligenceCareers.gov/NSA

NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA

NSA Careers

Mai T-J.

Technical Director, Cryptographic Portfolio Integration & Engineering

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

2024 WiCyS SCHEDULE
FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 6:00pm	Badge Pick-Up	Delta BCD Lobby
7:00am - 8:00am	Breafast Available for Scholarship Recipients	Canal Lobby
7:00am - 8:15am	INVITE ONLY: Early Career Breakfast - Sponsored by DeVry University	Delta B
7:00am - 8:15am	INVITE ONLY: Mid Career Breakfast - Sponsored by ServiceNow	Delta D
7:00am - 8:15am	INVITE ONLY: Male Allyship Breakfast - Sponsored by Bloomberg	Bayou AB
7:00am - 8:30am	Poster Session Check-In	Delta BCD Lobby
8:00am - 9:00am	Career Fair Setup by Sponsors	Ryman Hall B 1-2
8:30am - 9:45am	Conference Opening and Keynote (doors open at 8:15am) *Coffee Available Before and During Keynote Cybersecurity and Infrastructure Security Agency (CISA) Keynote: Embodying Trustworthiness: Lessons from AI for Women in Cybersecurity *Lisa Einstein, CISA* **Featured Speakers:** *Ann Johnson, Microsoft; Ebony Smith, Walmart*	Delta A
9:45am - 6:00pm	WiCyS Store Open (closed 12:00 - 12:30pm for lunch)	Delta C
9:45am - 11:45am	Career Fair Open	Ryman Hall B 1-2
9:45am - 11:45am	Capture The Flag (CTF) Mentoring Available	Delta A Lobby
9:45am - 11:45am	Career Growth Hub Open	Canal DE
9:45am - 11:00am	Student Poster Session & Networking Refreshment Break	Delta BCD Lobby
11:00am - 11:45am	Presentation Sessions	
	The Psychology of Belonging: Insights from the People Hacker *Jenny Radcliffe and Tashya Denose* Track(s): 🟢 CPE Credits: 1	Bayou AB
	Accelerating Incident Response Through Automation *Meghan Donohoe and Susan Paskey* Track(s): 🔵 🟠 CPE Credits: 1	Bayou CD
	Ascending to the C-Suite: Achieving the Mid-Level to Executive Transition *Zabrina McIntyre, Michelle Wagner and Barbara Mooneyhan* Track(s): 🟢 CPE Credits: 1	Bayou E
	Flipping the Script: Unleashing the Power of Flipper Zero in Cybersecurity *Mimi Vertrees* Track(s): 🔵 🟠 CPE Credits: 1	Canal ABC
	The Stealthiest Industrial Revolution *Megan Moloney* Track(s): 🟠 CPE Credits: 1	Delta B
11:00am - 11:45am	Student Chapter Leader Meetup *Quiana Oates* Track(s): 🔵	Delta D

2024 WiCyS SCHEDULE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
12:00pm - 1:45pm	**Keynote, Lunch, and Networking** (must be seated by 12:10pm to eat, Keynote starts at 12:30pm) **Fortinet Keynote:** From Code to Command: Navigating the Journey from Network Systems Programmer to Product Marketing Leader in Cybersecurity *Kimberly Becan, Fortinet* **National Security Agency (NSA) Keynote:** Bringing Unique Perspectives to National Security *Morgan Adamski, NSA* **Featured Speakers:** *Robyn Frye, Workday; Diane Tracy, Vanguard; Divya Ghatak, SentinelOne*	Delta A
1:55pm - 5:30pm	Career Fair Open	Ryman Hall B 1-2
1:55pm - 5:30pm	Capture The Flag (CTF) Mentoring Available	Delta A Lobby
1:55pm - 5:30pm	Career Growth Hub Open	Canal DE
1:55pm - 2:40pm	Presentation Sessions	
	Cloud Detection Engineering: Sleuthing in the Mist *Lydia Graslie* Track(s): ● CPE Credits: 1	Bayou AB
	Awareness Alone Won't Save Us: Why Human-Centered Design is Key to Cybersecurity *Rachel Russo Gaiser and Norah Maki* Track(s): ● CPE Credits: 1	Bayou CD
	Unlocking the Potential: LLM and ChatGPT Applications for Cybersecurity Careers and Beyond *Laura Malave* Track(s): ● ● CPE Credits: 1	Bayou E
	The Little ERG That Could: Building a Women in Cybersecurity Group from Scratch *Shir Butbul and Amelia Fisher* Track(s): ● CPE Credits: 1	Canal ABC
	Using AI to Ethically and Safely Boost Your Security Career *Caitlin Buckshaw* Track(s): ● CPE Credits: 1	Delta B
1:55pm - 2:40pm	Affiliate Leader Meetup *Jaclyn Justice* Track(s): ●	Delta D
2:45pm - 3:15pm	Break with Refreshments in Career Fair	Ryman Hall B 1-2

2024 WiCyS SCHEDULE
FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
2:50pm - 4:40pm	Workshop Series	
	Impact! How Targeted State Laws Affect Cybersecurity and Individuals in the Industry *Quintana Patterson* Track(s): ● ● CPE Credits: 2	Bayou AB
	Quantitative Cybersecurity Metrics *Lily Yeoh and Angel Liu* Track(s): ● CPE Credits: 2	Bayou CD
	Navigating Imposter Syndrome in the Face of Mental and Physical Disabilities *Elaine Harrison-Neukirch* Track(s): ● CPE Credits: 2	Delta B
	Choose Your Own Adventure: How Would You Handle a Ransomware Attack? *Megan Kaczanowski and Chloe Potsklan* Track(s): ● CPE Credits: 2 CEUs: 2	Delta D
2:50pm - 3:40pm	Presentation Sessions	
	Rising above the Flame: Confronting Burnout and Reinforcing Your Personal Boundaries *Ashley Smyk* Track(s): ● CPE Credits: 1	Bayou E
	Ecosystem Approach to Build an Inclusive and Dynamic Cyber Workforce *Seeyew Mo* Track(s): ● ●	Canal ABC
3:50pm - 4:40pm	Presentation Sessions	
	Reaching the Plateau of Productivity: Empowering Second Career Women in Cybersecurity *Joanna Grama and Carolyn Ellis* Track(s): ● CPE Credits: 1	Bayou E
	Federal Initiatives in Support of Cybersecurity Ecosystems *Toni Benson, Lynne Clark, Ashley Greeley, Marian Merritt and Carolyn Renick* Track(s): ● ●	Canal ABC

CAREER GROWTH HUB

The WiCyS Career Growth Hub is a place for resume review, mock-interview guidance and professional headshots.

Headshots Sponsored by:

Ford

Located in Canal DE

Thursday • 11:00am - 2:00pm
(Headshots Only)

Thursday • 2:00pm - 6:00pm

Friday • 9:45am - 11:45am & 1:55pm - 5:30pm

2024 WiCyS SCHEDULE
FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
4:45pm - 5:30pm	**Birds of a Feather**	
	Changing the Pace of Cyber: Live Long and Prosper [in Pursuit of Digital Trust and Security] *Anastasiya Rutus* **Track(s):** ●●●	Bayou AB
	Governing with Robots: What Does an AI-Enabled GRC Future Look Like? *Heather Holliday* **Track(s):** ●●	Bayou CD
	Recipe for Resilience: Blending Cross-Functional Talents in the Cybersecurity Kitchen *Saskia Hoffmann* **Track(s):** ●●	Canal ABC
	Overcoming Microaggressions and Shattering Stereotypes as Women in Security *Bri Frost* **Track(s):** ●	Delta B
	Green Cybersecurity *Iris Ye* **Track(s):** ●●●	Delta D
6:00pm - 7:45pm	**Keynote, Dinner, and Networking** **(must be seated by 6:10pm to eat, Keynote starts at 6:30pm)** **RTX Keynote: From WiCyS Student to RTX Leader: My Career Journey** *Esmeralda lyescas, Collins Aerospace* **Featured Speakers:** *Carly Jackson, NIWC Pacific; Nicole Becher, Google; Jaidie Vargas, Lockheed Martin*	Delta A
8:30pm - Midnight	**CTF After Dark Party**	Delta A Lobby

NCL @ WiCyS CAPTURE THE FLAG (CTF) COMPETITION

OFFERED BY: NATIONAL CYBER LEAGUE (NCL)

The WiCyS 2024 Conference Capture the Flag (CTF) competition is offered by WiCyS strategic partner National Cyber League (NCL). All conference registrants (students and non-students) were invited to register and compete in this virtual capture the flag competition, taking on realistic, industry skill-based challenges designed to test and build participants' hands-on cybersecurity skills.

The CTF kicks off on **Thursday, April 11 at 12:30pm** and ends on **Friday, April 12 at midnight**. CTF coaching is available in Delta A Lobby, so participants can get help with challenges and meet other CTF players as well as the NCL team. To wrap up the event, there also will be a CTF After Dark Party with plenty of swag, snacks and fun shenanigans for all participants. **Winners will be announced during the closing remarks and awards ceremony on April 13**. There will be leaderboards for students and non-students with prizes awarded to top players.

CTF Mentoring: Delta A Lobby
Thursday • 12:30pm - 7:00pm
Friday • 9:45am - 11:45am and 1:55pm - 5:30pm

CTF After Dark Party: Delta A Lobby
Friday • 8:30pm - Midnight

2024 WiCyS SCHEDULE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 9:00am	Badge Pick-Up	Delta BCD Lobby
7:00am - 8:15am	INVITE ONLY: Military Breakfast - Sponsored by Bloomberg and Optum	Bayou E
7:00am - 8:00am	Breafast Available for Scholarship Recipients	Canal Lobby
7:00am - 5:00pm	Luggage Storage Available	Delta C
8:30am - 9:30am	**Keynote** (doors open at 8:15am) *Coffee Available Before and During Keynote **Keynote:** 10th Anniversary Keynote *Dr. Frincke, Sandia National Laboratories* **Featured Speakers:** *Laketta Hawkins, Cisco; Rutu Vijaysinh Ataliya, Amazon Web Services; Carrie Mills, Southwest Airlines; Ayesha Khalid, Mastercard*	Delta A
9:30am - 10:00am	Group Picture and Break with Refreshments	TBD
10:00am - 1:00pm	WiCyS Store Open	Delta C
10:00am - 10:45am	Presentation Sessions	
	AI Detectives: The Vanguard of Social Media Forensics *Daniela Villalobos and Renata Uribe* Track(s): ● CPE Credits: 1	Bayou AB
	Build a Cybersecurity Clinic: Enhance Community Cybersecurity and Train Cyber Leaders *Francesca Lockhart and Kareem Chavez-Escobedo* Track(s): ● ● ● CPE Credits: 1	Bayou CD
	Your APIs Called, And They Told Me Your House is Haunted *Abigail Ojeda* Track(s): ● ● CPE Credits: 1	Canal ABC
	ICS Purple Team: Cybersecurity in Industrial Control Systems *Darla Montgomery and Haley Kim* Track(s): ● ● CPE Credits: 1	Delta B
10:00am - 10:45am	Lightning Talks (all talks are in the same room) ● ● ● ● ●	Delta D
	Cyber for Swifties: How Swiftie Nation Could Be Great Intelligence Analysts *Meghan Martinez*	
	Phishing 2.0: The Rise of Artificial Intelligence *Rachel Kang*	
	Technically, You Are Technical *Shannon McHale*	
	Who Ya Gonna Call? *Debby Briggs*	
	The Role of Cyber Competitions in Cultivating Next Gen Cybersecurity Talent *Jingdi Zeng*	
	Cybersecurity for Social Good *Bella Gomez*	
	A Quick Dive Into the New WiCyS Member Portal *Quintana Patterson*	

2024 WiCyS SCHEDULE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
11:00am - 11:45am	**Presentation Sessions**	
	Culturally Responsive Cybersecurity Assessment *Petra Robinson and Jenny Daugherty* **Track(s):** ● ● **CPE Credits: 1**	Bayou AB
	Building an Internship Program with Universities and Businesses in Your Community *Ann Jones* **Track(s):** ● ● ● **CPE Credits: 1**	Bayou CD
	Cyber-Securing Vehicles: Advanced Intrusion Detection Systems for Automotive Cyber Defense *Linxi Zhang* **Track(s):** ● ● **CPE Credits: 1**	Canal ABC
	Digital Footprint Unveiled: Understanding Public Data *Lily Lee* **Track(s):** ● **CPE Credits: 1**	Delta B
11:00am - 11:45am	**Lightning Talks (all talks are in the same room)** ● ● ● ● ●	Delta D
	Who Can Teach High School Cybersecurity? Good High School Teachers! *Moriah Walker*	
	The Privacy Paradox: Can People Stay Hidden in Plain Sight? *Caitlin Sarian*	
	Disney Villains Unleashed: A Cybersecurity Tale *Alissa Butcher*	
	Prompting Success: Using AI for Cybersecurity Education and Research *Paige Zaleppa*	
	Don't Listen to the Naysayers! *Tracey Ristich*	
	You Are the CEO of ME: Intentional Behaviors Yield Results *Jigisha Pardanani*	
	Extending Reach: Growing the WiCyS Community One Affiliate At a Time *Jaclyn Justice*	
	Managing and Mobilizing WiCyS Student Chapters *Quiana Oates*	

MILITARY BREAKFAST

TOGETHER. WE SERVE.

The Military Breakfast will honor our veterans, those currently serving, military spouses, and those on active duty who are attending WiCyS 2024.

Sponsored by:

Bloomberg Optum

Located in Bayou E

Saturday • 7:00am - 8:15am

This event is by invitation only and not open to all attendees!

RSVP is required.

2024 WiCyS SCHEDULE

SATURDAY AGENDA

TIME	DESCRIPTION	LOCATION
12:00pm - 12:45pm	**Panels**	
	Don't Be a Victim of Gender Washing *Dawn Armstrong, Leilia MacNeil and Kristen Rodriguez* **Track(s):** ●● **CPE Credits: 1**	Bayou AB
	From the Roots Up: Growing the Next Generation of Cyber Professionals with Apprenticeships *Abigail Allen, Donna Woods and Tobi West* **Track(s):** ●●● **CPE Credits: 1**	Bayou CD
	The Evolution of Cybersecurity Careers in Defending Against Physical Threats *Kelly Murray, Lisa Beury-Russo and Ryan Donaghy* **Track(s):** ● **CPE Credits: 1**	Canal ABC
	Cyber Sheroes: The Women Commanding AI's Evolution *Prajakta Jagdale, May Wang, Christina Papadimitriou and Nicole Nichols* **Track(s):** ●●● **CPE Credits: 1**	Delta B
	Navigating the New Normal: Women in Cybersecurity Adapting to Hybrid Work Environments *Jennifer Cox, Jessie Jamieson, Sasmita Panda, Khensani Carter and Muta Mashack* **Track(s):** ● **CPE Credits: 1**	Delta D
12:45pm - 2:00pm	**Lunch, Closing Remarks, and Awards** **(must be seated by 1:00pm to eat)**	Delta A
2:00pm - 2:30pm	Travel Stipend Verification (only for stipend awardees)	Delta BCD Lobby
2:30pm - 4:30pm	**Workshop Series**	
	Quantum Frontier: Bridging Quantum Information Science and Cybersecurity *Muhammad Ismail, Hanna Terletska and David Leathers* **Track(s):** ●●● **CPE Credits: 2**	Bayou AB
	Shall We Play A Game? Using Cyber Table Tops for Threat Hunting Tracks *Jaidie Vargas, Suzanne Dove, Yasmeen Natzle and Deirdre Peters* **Track(s):** ●● **CPE Credits: 2**	Bayou CD
	Discovering Vulnerabilities with Automated Fuzz Testing *Kainaat Singh* **Track(s):** ● **CPE Credits: 2**	Canal ABC
	Optimizing DFIR in Public Cloud: AWS, Azure and GCP *Dalal Alharthi* **Track(s):** ● **CPE Credits: 2**	Delta B
	Cybersecurity Prompt Engineering: Strategic Approach to Bolster Digital Defense *Adebunmi Odefunso* **Track(s):** ●●● **CPE Credits: 2**	Delta D

2024 WiCyS CONFERENCE PRE-CONFERENCE SESSIONS

SESSION KEY

- ● TECHNICAL SKILL BUILDING TRACK
- ● EDUCATION & WORKFORCE DEVELOPMENT TRACK
- ● RESEARCH & INNOVATION TRACK
- ● CAREER ADVANCEMENT TRACK
- ● COMMUNITY ECOSYSTEM & OUTREACH TRACK

PRE-CONFERENCE SESSIONS

THURSDAY • 12:30PM - 1:30PM

First Timers Panel | Navigating Your First WiCyS Conference

Speaker(s): *Elizabeth Hawthorne, Morgan Adamski, Deborah Kariuki, Shannon McHale, Ossie Munroe and Warren Proctor*

Room: Delta D **Track(s):** ●

Level: Beginner **CPE Credits: 1**

First time at the WiCyS conference? Not sure what to expect and how to navigate? No problem! Come and hear from others who have been in that situation and hear their stories. Panelists from various backgrounds and interests will share their experiences of what they found useful, what resonated most with them and, most importantly, tips on how to get the most out of this experience as a first-time WiCyS conference attendee.

PRE-CONFERENCE SESSIONS

THURSDAY • 12:30PM - 1:30PM

Recruiters Session | Rethinking Recruiting: Effective Hiring Practices to Close the Skills Gap

Speaker(s): *Audra Streetman and Lillian Teng*

Room: Bayou CD **Track(s):** ● ●

Level: Beginner **CPE Credits: 1**

Cybersecurity does not have a hiring problem, it has a recruiting problem. If the industry continues to shun nontraditional candidates instead of recognizing them as an untapped resource, it will never fill the hiring gap fast enough to defeat adversaries. This talk will demonstrate how career changers from a variety of backgrounds, including the humanities, can play a valuable role in an organization's cybersecurity strategy. Attendees will hear how a hiring manager drafted an entry-level job advertisement that went viral on TikTok. The talk also will feature a journalist who applied to that job posting and made the switch from local TV news to cybersecurity. In addition to life experience, career changers bring their own superpowers to a team, such as project management, communication and critical thinking. In order to fill vacancies and diversify the applicant pool, recruiters need to broaden their hiring criteria and consider candidates with aptitude and potential.

EARLY CAREER BREAKFAST

The Early Career Breakfast is a place for early career professionals to meet up, make connections, talk about the challenges faced by the new generation of cyber talent and brainstorm ideas to help encourage and engage other early professionals.

Sponsored by:

DeVry University

Located in Delta B

Friday • 7:00am - 8:15am

This event is by invitation only and not open to all attendees!

RSVP is required.

2024 WiCyS CONFERENCE MEETUPS

THURSDAY MEETUPS

THURSDAY • 6:30PM - 7:15PM

Federal Scholarship Information and Networking Session

Speaker(s): *Ashley Greeley and Laura Knowles*

Room: Bayou E **Track(s):** 🟢

Level: Intermediate/Advanced

Join this session to learn about various federal scholarships in cybersecurity and meet students participating in these types of programs. Learn about these programs and network with peers, alum, faculty and federal employers.

THURSDAY • 7:30PM - 8:15PM

Educators/Scientists - Meetup with Federal Funding Agencies

Speaker(s): *Sheikh Ghafoor, Ashley Greeley, Karen Karavanic and Akhirah Padilla*

Room: Bayou E **Track(s):** 🔵 🟠

Level: Intermediate/Advanced

For educators and scientists, this session provides information and opportunities for conversations with program directors/managers at various funding agencies such as NSF and NSA about potential grant opportunities related to cybersecurity.

FRIDAY MEETUPS

FRIDAY • 11:00AM - 11:45AM

Student Chapter Leader Meetup

Speaker(s): *Quiana Oates*

Room: Delta D **Track(s):** ●

Level: Beginner

Join this session to learn about starting, running and maintaining a student chapter on campus. Current chapter leaders will share their experiences, discuss challenges, and address the issues that commonly arise as a student chapter officer. Bring lots of questions with ideas and help each other succeed in promoting women in cybersecurity at their campuses.

FRIDAY • 1:55PM - 2:40PM

Affiliate Leader Meetup

Speaker(s): *Jaclyn Justice*

Room: Delta D **Track(s):** ●

Level: Beginner

Come engage with leadership from various affiliates as they form a freestyle discussion group to share ideas for strategies, best practices, social media and more! Already part of an established affiliate? Bring ideas and grow stronger together! Interested in forming an affiliate? Bring questions and take advantage of the expertise in the room!

SENIOR LEADER LUNCHEON

The Senior Leader Lunch is a place for senior level professionals to meet up, make connections, talk about the challenges and opportunities unique to cybersecurity leaders and brainstorm how to help increase the representation of women in cybersecurity.

Sponsored by:

Bloomberg

Located in Old Hickory

Thursday • 12:00pm - 1:30pm

This event is by invitation only and not open to all attendees!

RSVP is required.

Google

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

Security Engineering

2024 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

THURSDAY • 2:00PM - 4:00PM

The Beginner's Guide to Secure Code Reviews

Speaker(s): *Rita Law, Mary DuBard and FNU Prashasti*

Room: Bayou AB **Track(s):** ●

Level: Beginner **CPE Credits: 2**

In this workshop, we will provide an overview of when secure code reviews (SCRs) are useful, examples of common vulnerabilities in code, and how to use a risk-based approach to SCRs that utilizes the context of the code as well as scanning tools. The presenters will pull from their combined experiences in pentesting, education counseling, and internal application security to provide real-life examples. At the end, attendees will have the chance to use their new skills by performing a review on an open-source repository of their choice or code prepared by presenters. Attendees will walk away from this workshop confident in their ability to securely review code no matter their experience with the language. Today, many companies rely on automated static analysis tools to detect vulnerabilities in code. While they can be useful, scans may lack necessary insight, causing some vulnerabilities to be overlooked. This drives a need for more security engineers to perform manual secure code reviews in concert with scans. Secure code reviews could be reviews of an entire repository, a pull request, new code addition or validation of scanner findings. A risk-based approach to SCRs will take into account the review type, the context of the application and any specific security concerns. Although a manual code review may seem challenging at first, even a general familiarity of programming combined with minimal research can help beginners start reviewing in a language they are less familiar with. **(Laptops Preferred)**

Architectural Thinking for Security

Speaker(s): *Snezhana Dubrovskaya and Nikki Robinson*

Room: Bayou CD **Track(s):** ● ● ●

Level: Intermediate/Advanced **CPE Credits: 2**

This learning session delves into the intricacies of architectural patterns and automation, shedding light on the evolving role of architects in recent years. This transformation has led architects to become increasingly hands-on, blurring the lines between traditional architecture and engineering. The session begins by exploring the layers of architectural decision-making. It will start by looking at the top layer of enterprise security architecture, which provides a foundational context, offering insight into the building blocks of an organization, such as security domains and capabilities. However, it doesn't provide the precise context for individual solutions, it serves as a starting point like a blueprint. Moving to the conceptual layer, more context is introduced but it still falls short of describing the connections and interactions between various security capabilities. As the session progresses, it delves into solution architecture, focusing on understanding system boundaries involving human and nonhuman actors and their interactions. This understanding serves as the driving force for the development of other architectural artifacts. The session culminates in the creation of a security architecture pattern. This process commences with requirements identification followed by the adoption of patterns that meet these requirements. A preliminary solution is devised, akin to a strawman proposal, and threat modeling is conducted. Iteration and discussion with fellow architects are essential to refining the solution until it reaches an acceptable state, which will be done in smaller groups. **(Laptops Required)**

OSINT Unveiled: Techniques and Tools for Effective Information Gathering

Speaker(s): *Katie Shuck, Cynthia Hetherington, Arica Kulm and Ashley Podhrasky*

Room: Canal ABC **Track(s):** ● ●

Level: Beginner **CPE Credits: 2**

In an era where information equates to power, open source intelligence (OSINT) has become a critical skill set for analysts, investigators and cybersecurity professionals. This is a comprehensive training program designed to equip participants with the ability to efficiently discover, analyze and utilize publicly available information for intelligence purposes. This program demystifies the expansive world of OSINT, guiding attendees through the ethical and legal frameworks that govern its use. Participants will gain hands-on experience with cutting-edge tools and techniques for sourcing data from the internet, social media platforms, public government records and more. Emphasizing a blend of theory and practice, the course modules cover everything from advanced search engine capabilities to the intricate utilization of social media analysis tools.Throughout the training, participants will engage in real-world scenarios and simulations, fostering a deep understanding of how to apply OSINT methodologies in various contexts, including corporate security, law enforcement and risk management. The curriculum is structured to enhance critical thinking and

2024 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

decision-making skills, enabling practitioners to craft an informed narrative from disparate data points. “”OSINT Unveiled”” is not merely a technical walkthrough but a transformational journey into the art of extracting actionable intelligence from a sea of data. Attendees will possess the confidence and acumen to conduct OSINT investigations, construct a comprehensive intelligence picture, and anticipate security challenges in an increasingly transparent world. **(Laptops Required)**

The Weaponization of Misinformation: Fortifying Your Mind in the Face of Fake News

Speaker(s): *Madison Fox*

Room: Delta B **Track(s):** 🔵🟠

Level: Beginner **CPE Credits: 2**

This workshop will examine the progression of misinformation and disinformation throughout history, bringing attendees up to speed on the current state of fake news on the internet. While it is not a new concept, the emergence of artificial intelligence and machine learning has created a newfound sense of urgency to address these operations. Cyber professionals often discuss how the human layer is the most vulnerable and most difficult to protect. As bad actors leverage increasingly sophisticated technologies in their campaigns to dismantle the truth, the public is at risk of living in a false reality in their minds. When those who seek to cause harm control the perception of the world and current events, individuals can be used as pawns to advance narratives and efforts against their targets. Participants will be supplied with armaments of cyber defense to better protect themselves and those around them. This workshop will emphasize why preparation is key to protecting not just the digital landscape but also the one that people live in everyday. Participants will experience this preparation firsthand by creating a security awareness program based on a selected disinformation threat vector. From there, the programs will be put to the test against simulated attacks on a mock company that participants will be tasked to protect. **(Laptops Preferred)**

The Cultural Intelligence Code for Diverse Leadership

Speaker(s): *Loren Rosario-Maldonado*

Room: Delta D **Track(s):** 🟢

Level: Intermediate/Advanced **CPE Credits: 2**

Leading a diverse team encompassing various dimensions of diversity is a complex yet rewarding endeavor. This session aims to equip female leaders in tech with the knowledge and skills to effectively lead and harness the power of diversity within their teams. Through interactive discussions, case studies and practical exercises, participants will gain insights into the importance of inclusive leadership and learn strategies to create an inclusive work environment where all team members can thrive. They also will explore the unique challenges and opportunities that arise from diverse perspectives and develop techniques to leverage them for enhanced creativity, innovation and overall team performance. **(No Laptops Needed)**

2024 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

THURSDAY • 4:30PM - 6:30PM

The Malware Challenge: Stepping Up Your Triage Game

Speaker(s): *Alessandra Perotti*

Room: Bayou AB **Track(s):** ●

Level: Beginner **CPE Credits: 2** **CEUs: 2**

What does a malicious file look like? And how can an analyst understand whether a file is malicious or benign? These days, triage skills are crucial not only for malware researchers and hunters but also for security operations center (SOC) analysts and people who want to follow the incident response career path. From understanding the import address table and looking at entropy levels to examining strings, this hands-on, interactive workshop will guide participants through triaging some potentially malicious files by performing static properties and behavioral analysis with freely available tools, and it will explain how to determine whether a file is malicious or not while giving participants a chance to exercise their analysis skills on real-world malware samples. **(Laptops Preferred)**

Shift Left Security: Walk the Talk or Lose $10.5 Trillion!

Speaker(s): *Michelle Wan and Priya Nath*

Room: Bayou CD **Track(s):** ●

Level: Beginner **CPE Credits: 2**

Damage from cyberattacks is predicted to cost the world $10.5 trillion annually by 2025. Research shows it can be significantly less expensive to fix problems in the design phase than in production. It should be no surprise that shift left security and development security operations (DevSecOps) are both trending in the industry. These two ideas promote baking security in from the beginning rather than bolting it on at the end of the software development life cycle and integrating security at every stage. However, DevSecOps adoption is still low, and culture is cited as the number one barrier to progress as successful adoption requires close collaboration between security, development and operations functions. It's time to walk the talk! The goal of this workshop is to have participants walk away with knowledge of shift left security and DevSecOps practices, hands-on experience with security techniques and tools, and understanding the importance of baking security in from the beginning. This fun and engaging workshop is suitable for participants of all levels. A series of short presentations and group activities/games offer attendees the opportunity to learn how to create a data flow diagram, perform threat modeling using STRIDE methodology, identify vulnerabilities with static analysis tools, and evaluate risks and countermeasures. Participants will leave feeling inspired to promote a security mindset and lead change in their organizations. Participants will need to bring their own laptops but are not required to install any additional software or hardware. **(Laptops Required)**

The Best Defense is a Rusty Offense

Speaker(s): *Diane Stephens*

Room: Canal ABC **Track(s):** ●●●

Level: Intermediate/Advanced **CPE Credits: 1** **CEUs: 1**

Memory safety issues have plagued the software industry for over a decade and have consistently accounted for more than 65% of all software vulnerabilities. The problem stems from the use of languages such as C and C++ that allow developers to write fast code. Unfortunately, that code can be prone to memory bugs. Consider the analogy of a white board as dynamic memory. As software runs, it writes bits and bytes constantly on the whiteboard. Languages such as C/C++ don't spend time cleaning the whiteboard. The program should clean the whiteboard, wiping bits and bytes when they are no longer needed. This strategy is efficient but not safe. If the program leaves data on the board, a hacker can grab it. If a program scribbles over something, it can crash the system. Languages such as Java employ an automated cleaning service, a garbage collector, to enforce memory safety, but garbage collectors are expensive and slow. The Rust language provides a new model for memory safety that doesn't add cost or reduce speed. Rust programs must follow strict rules for writing on the whiteboard or they won't compile. These rules can be confusing and frustrating to programmers. This talk will make sense of the rules and explain Rust's novel memory safety concepts - ownership and borrowing. A new visualization tool - RustLive - will be demonstrated that clarifies the memory model. Attendees will understand why leaders from government, academia and industry have recommended a switch to Rust. **(Laptops Required)**

2024 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

Introducing ThreatGPT: The Malicious Sibling of ChatGPT

Speaker(s): *Kshitiz Aryal, Lopamudra Praharaj and Maanak Gupta*

Room: Delta B **Track(s):** ● ●

Level: Beginner **CPE Credits: 2**

The evolution of artificial intelligence (AI) and machine learning (ML) has led to digital transformations in the last decade. The latest frontiers in AI technology have arrived as generative AI (GenAI). While GenAI technologies such as ChatGPT have become the focal point of recent discussions, there is still a lack of awareness among the general public regarding safe usage practices. Students, practitioners and cyber stakeholders need to be aware of both the bright and dark side of the technology to ensure its ethical use. People have yet to understand GenAI, a new technology, and its cyber implications, comprehensively. However, as the technology continues to grow, new ways of using GenAI in cyber defence and attack are evolving, and it's critical to keep up with them to create a secure digital space. The workshop's objective is to impart knowledge about GenAI technology, like ChatGPT, and offer a hands-on experience to comprehend its cybersecurity implications. It will serve as a critical step in comprehending the operations of these tools, pinpointing their optimal use cases, acknowledging their constraints, and laying the foundation for secure and responsible usage – a timely requirement. The workshop is designed to bridge the gap between cybersecurity professionals and GenAI technology, fostering the benefit of both offensive and defensive security efforts. Practitioners at all experience levels can easily grasp and derive value from the workshop, enhancing their capabilities to address cybersecurity challenges effectively. **(Laptops Preferred)**

SANS Executive Cybersecurity Exercise

Speaker(s): *Michael Barcomb and Christopher Wilkes*

Room: Delta D **Track(s):** ● ●

Level: Intermediate/Advanced **CPE Credits: 2** **CEUs: 2**

The Executive Cyber Exercise drops attendees inside a simulated cyber event, helping them understand in a very real way what it takes to respond to a cyber incident from a strategic perspective. The simulated exercise will emphasize the importance of a well-practiced cyber crisis plan and the leadership skills required to deal with today's threats. The facilitators will use real-world experience and industry best practices to expose areas for improvement in their crisis response plans within a safe environment. This session involves a primary facilitator and multiple secondary SANS employees to successfully deliver the exercise. **(No Laptops Needed)**

MID-CAREER BREAKFAST

The Mid-Career Breakfast is a place for mid-career professionals to meet up, make connections, talk about the challenges faced by mid-career cyber talent and brainstorm ideas to help encourage and engage other mid-career professionals.

Sponsored by:

servicenow

Located in Delta D

Friday • 7:00am - 8:15am

This event is by invitation only and not open to all attendees!

RSVP is required.

2024 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

FRIDAY • 2:50PM - 4:40PM

Impact! How Targeted State Laws Affect Cybersecurity and Individuals in the Industry

Speaker(s): *Quintana Patterson*

Room: Bayou AB **Track(s):** ●●

Level: Beginner **CPE Credits: 2**

The workshop will discuss some of the state laws either passed or still under consideration and how those laws have, will or can impact the cybersecurity industry. **(No Laptops Needed)**

Quantitative Cybersecurity Metrics

Speaker(s): *Lily Yeoh and Angel Liu*

Room: Bayou CD **Track(s):** ●

Level: Intermediate/Advanced **CPE Credits: 2**

The workshop will provide an overview of how to design, implement, monitor and report on cybersecurity metrics for a risk management program. The workshop will cover the difference between and value of qualitative versus quantitative risk metrics. The presenter also will provide insight and value proposition for the implementation of cybersecurity metrics as well as provide real-world examples of quantitative metrics required and evaluated by auditors for cybersecurity/information security and compliance. The workshop will have a tabletop exercise for teams to define cybersecurity metrics. **(No Laptops Needed)**

Navigating Imposter Syndrome in the Face of Mental and Physical Disabilities

Speaker(s): *Elaine Harrison-Neukirch*

Room: Delta B **Track(s):** ●

Level: Beginner **CPE Credits: 2**

This workshop explores how mental and physical challenges can contribute to imposter syndrome. It delves into the unique challenges faced by individuals grappling with imposter feelings that may be related to their mental and physical disabilities whether they already suffer from imposter syndrome or the seeds have just been planted. Participants will discuss their symptoms and the impact of imposter syndrome, providing insights into how these feelings manifest differently for those with disabilities. Strategies for coping with imposter syndrome, including fostering self-compassion, setting realistic goals, and creating supportive environments, will be highlighted. By addressing the distinct dynamics of imposter syndrome in the realm of disabilities, this talk aims to empower individuals to recognize, navigate and overcome imposter feelings, fostering a more inclusive and supportive community for all. **(No Laptops Needed)**

Choose Your Own Adventure: How Would You Handle a Ransomware Attack?

Speaker(s): *Megan Kaczanowski and Chloe Potsklan*

Room: Delta D **Track(s):** ●

Level: Beginner **CPE Credits: 2** **CEUs: 2**

A tabletop exercise is a common way for organizations to test their incident response plans. It typically includes executives, security team members and anyone who might be called upon in a real incident. An incident leader (usually the head of the incident response team) will walk participants through a compromise scenario and test both participants and the incident response process. These exercises help stakeholders across the business understand different consequences of cyberattacks and prepare for a real attack. Most security professionals will participate in (or run) a tabletop exercise at some point in their career, but given that these types of exercises are run infrequently (perhaps once a year), it can be difficult to gain experience participating in them. The workshop will walk through high-level best practices for participating in tabletop exercises then dive into a “choose your own adventure” style game which mimics a simplified table-top exercise where players take on roles ranging from system administrator to CEO and work together to determine the best way to respond to a ransomware incident. Participants will leave with an understanding of how and when tabletop exercises are used and how they can most effectively participate in them. **(No Laptops Needed)**

2024 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

WORKSHOP SERIES

SATURDAY • 2:30PM - 4:30PM

Quantum Frontier: Bridging Quantum Information Science and Cybersecurity

Speaker(s): *Muhammad Ismail, Hanna Terletska and David Leathers*

Room: Bayou AB **Track(s):** ● ● ●

Level: Beginner **CPE Credits: 2**

In a world where data security is paramount, quantum information science (QIS) is emerging as the frontier of safeguarding digital realms. Welcome to this interactive workshop that demystifies the transformative power of quantum in the world of cybersecurity. The journey begins with an engaging video game developed by the presentation team to introduce the fundamentals of QIS, setting the stage for what is to come. Then participants will dive into the heart of QIS during a hands-on session, where attendees will explore the intricacies of single and multiple quantum bit (qubit) systems, quantum gates, measurements and the mysterious concept of quantum entanglement. The excitement does not stop there. Next, the session will venture into the application of QIS in cybersecurity with a focus on the quantum one-time pad (QOTP) and quantum key distribution (QKD) using the BB84 protocol. Learn how quantum technology can safeguard data like never before. The approach is hands-on, as attendees harness the power of Qiskit, an open-source framework for working with noisy quantum computers, and qasm_simulator to implement and run examples and protocols. Get ready to create keys based on qubits, secure data and navigate the quantum frontier of cybersecurity. "Quantum Frontier" is a gateway to a new era of cybersecurity. Join this interactive workshop to explore the quantum realm and gain valuable insights into securing the future of digital information. The journey starts here! **(Laptops Preferred)**

Shall We Play A Game? Using Cyber Table Tops for Threat Hunting Tracks

Speaker(s): *Jaidie Vargas, Suzanne Dove, Yasmeen Natzle and Deirdre Peters*

Room: Bayou CD **Track(s):** ● ●

Level: Intermediate/Advanced **CPE Credits: 2**

Train like one fights; fight like one trains! In this workshop, presenters will discuss War Games and how CTTs drive cyber resiliency. All critical infrastructure systems must be able to withstand cyberattacks, faults and failures, and continue to carry out mission essential functions. In this two hour hands-on workshop, participants will break into different groups, and each team will have purple, red and blue team contributors. Everyone will follow the Department of Defense CTT guidebook and other industry frameworks. Instructors will propose a system to each group, such as a critical infrastructure or a satellite. Attendees will learn how to use the CTT process for their systems, apply open-source threat briefings, and provide relevant info to secure systems against today's threats. **(Laptops Preferred)**

Discovering Vulnerabilities with Automated Fuzz Testing

Speaker(s): *Kainaat Singh*

Room: Canal ABC **Track(s):** ●

Level: Beginner **CPE Credits: 2**

Manually reviewing code bases with thousands of lines of code is impractical and requires the help of automated testing. This workshop will introduce participants to the concept of discovering vulnerabilities through a popular automated methodology called fuzzing. It refers to the process of discovering vulnerabilities by repeatedly running random inputs against a target software and observing unforeseen behavior. The first part will cover the different vulnerability discovery methodologies. The second part will cover the concept of fuzzing, its different methods and the fuzzer types. The third part will be a practical session where attendees learn the procedure of setting up a publicly available fuzzer, writing their own test harness, carrying out a fuzzing campaign and interpreting the results. This workshop is a foundational course providing participants with the fundamentals of the fuzzing process and working knowledge of using a fuzzer. Participants should have a basic understanding of low-level programming languages such as C or C++. Participants should bring laptops with Linux installed (can be in a virtual machine or WSL too), at least 20GB of free hard disk space with at least 8GB of RAM. **(Laptops Required)**

2024 WiCyS CONFERENCE
WORKSHOP DESCRIPTIONS

Optimizing DFIR in Public Cloud: AWS, Azure and GCP

Speaker(s): *Dalal Alharthi*

Room: Delta B **Track(s):** 🔵

Level: Intermediate/Advanced **CPE Credits: 2**

In today's ever-evolving cybersecurity landscape, the migration to cloud environments introduces both opportunities and challenges. Envision this scenario: an organization is in the midst of a cloud migration when it becomes the target of a sophisticated cyberattack. The incident response team starts opting for containment by shutting down the affected virtual machine (VM). While containment is achieved, a critical question emerges: How can the team effectively conduct digital forensics on this VM when essential forensic data may have been lost during the shutdown? This workshop aims to address this question and, more broadly, to enhance and optimize cloud digital forensics and incident response (DFIR) processes. The presenter will address industry best practices while shedding light on academic research in this domain. Key takeaways include a comparative analysis of AWS, Azure and GCP services and their capabilities in supporting DFIR processes, a proposed flowchart of cloud digital forensics and a customizable incident response runbook. Hands-on work will include exercises on the following items in AWS, Azure and GCP: (1) Writing, testing and automating incident response runbooks; (2) designing and implementing an isolation security policy to contain security breaches; (3) Leveraging query languages, such as the Search Processing Language and Resource Query Language; (4) Taking snapshots of infected VMs; (5) Ways to demonstrate a valid chain of custody (CoC) for digital evidence in response to legal requests. This workshop directly aligns with certifications such as AWS Certified Security - Specialty, Microsoft Certified: Azure Security Engineer, and Google Cloud Professional Cloud Security Engineer. **(Laptops Preferred)**

Cybersecurity Prompt Engineering: Strategic Approach to Bolster Digital Defense

Speaker(s): *Adebunmi Odefunso*

Room: Delta D **Track(s):** 🔵🟠🟢

Level: Intermediate/Advanced **CPE Credits: 2**

The rising popularity of generative AI has significantly impacted the world of technology since OpenAI announced ChatGPT, prompting engineers to harness this technology for enhancing their work. Cybersecurity engineers and, sadly, threat actors are not left behind in this exploration. However, a common challenge lies in understanding and effectively implementing prompt engineering to achieve optimal results. This workshop aims to provide a deep dive into the fundamentals of prompt engineering, exploring various approaches that can elevate their capabilities in leveraging generative AI. The success of prompt engineering hinges on the quality of prompts used. Mastering this art leads to superior outcomes. In this workshop, participants will explore the primary approaches to prompting, enabling attendees to choose the most suitable one for their specific cybersecurity tasks. These approaches include n-shot prompting, chain-of-thought prompting and generated knowledge prompting. By delving into these methodologies, attendees will gain a comprehensive understanding of how to craft precise and effective prompts. They also will examine specific-use cases such as scripting, security education and awareness, policy development, incidence response, etc. Throughout the workshop, participants will receive hands-on guidance on how to seamlessly integrate prompt engineering into their cybersecurity workflows. The workshop also will address potential pitfalls and offer best practices for mitigating common issues associated with prompt engineering. By the end of this workshop, equipped with a strong foundation in prompt engineering techniques, participants will be able to enhance their cybersecurity strategies, improve threat detection, and bolster their organization's security posture. **(Laptops Required)**

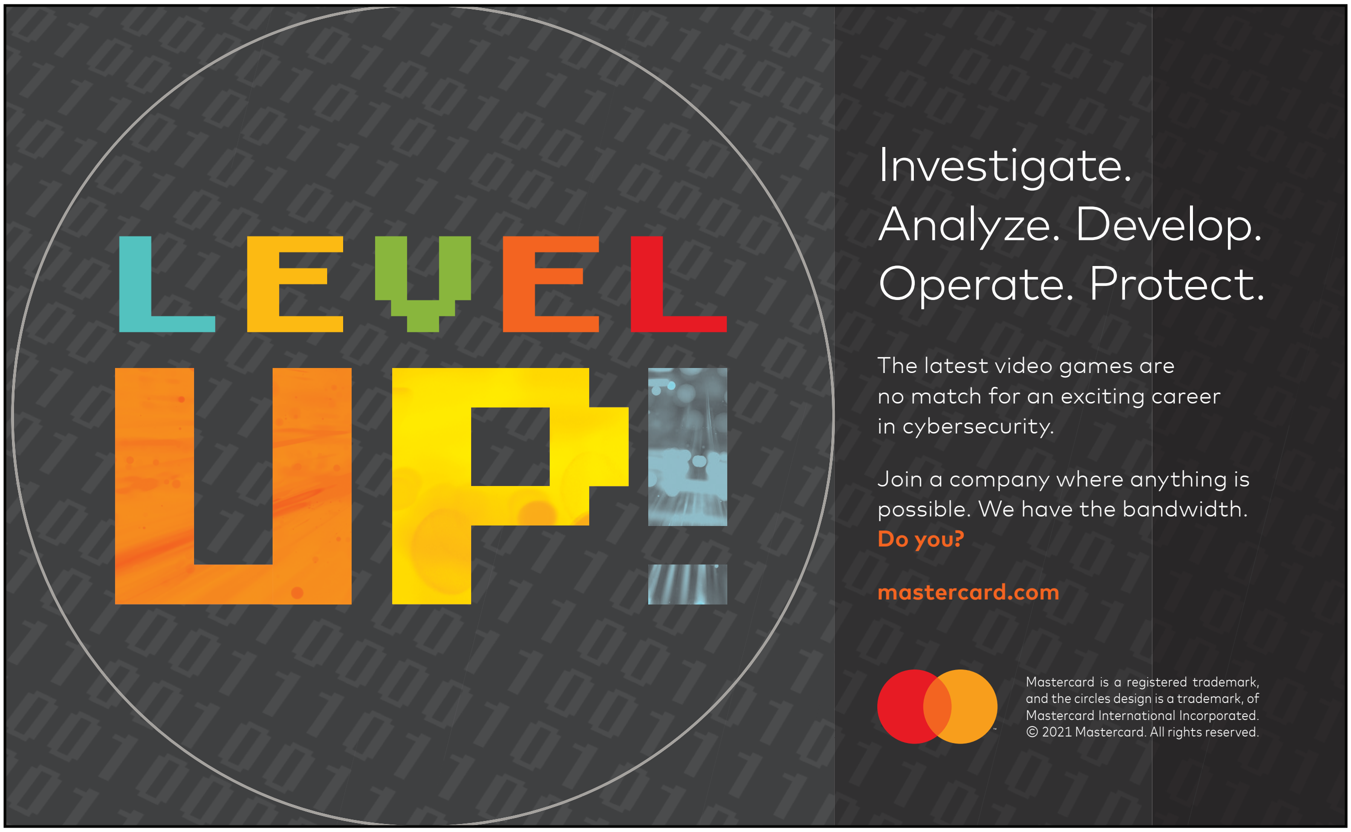
WiCyS UPCOMING EVENTS

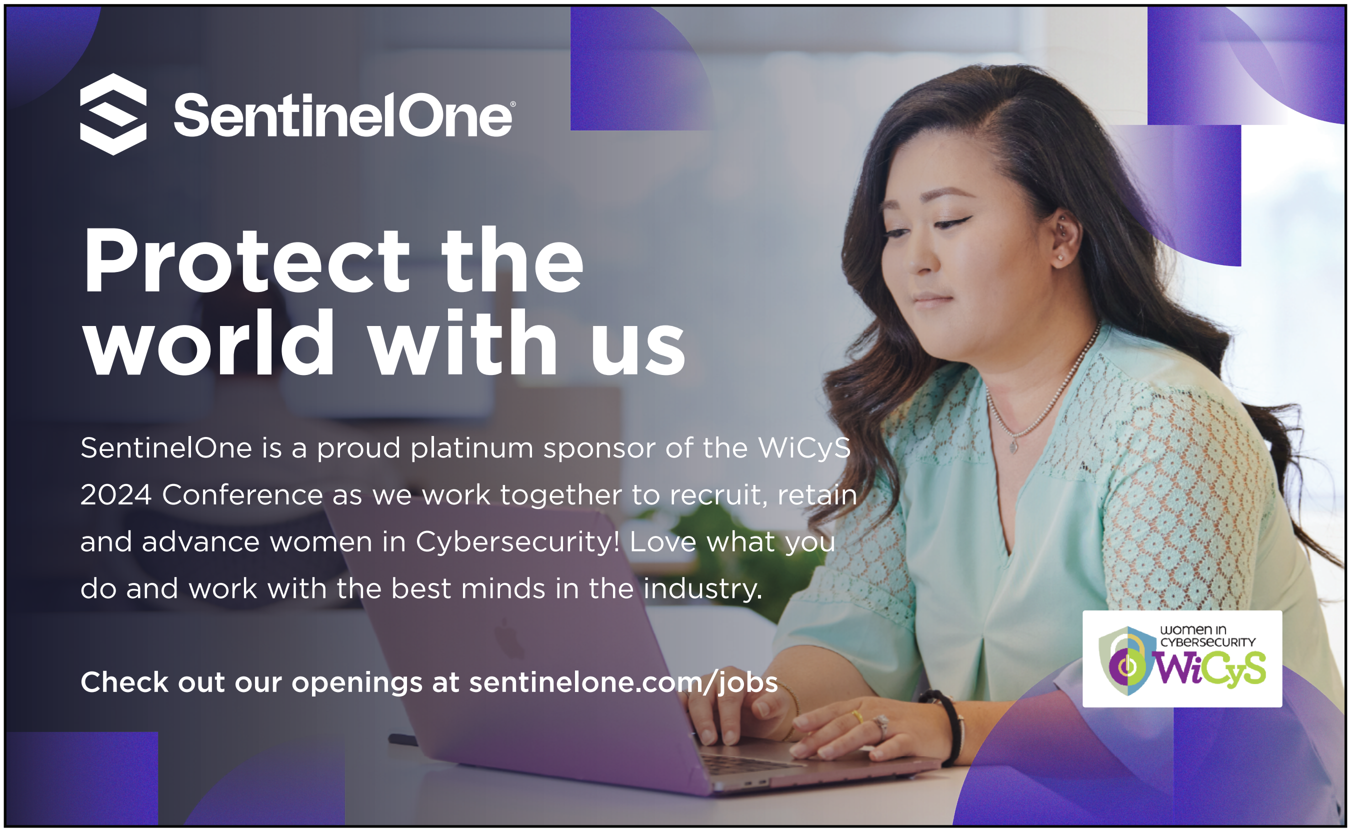
Check out the WiCyS event calendar!

Learn about upcoming training programs, webinars, Affiliate events, Student Chapter initiatives and more.

Scan the code to learn more about upcoming events!

https://www.wicys.org/events/


LEVEL
UP!



2024 WiCyS CONFERENCE
PRESENTATION SESSIONS

SESSION KEY

● TECHNICAL SKILL BUILDING TRACK

● EDUCATION & WORKFORCE DEVELOPMENT TRACK

● RESEARCH & INNOVATION TRACK

● CAREER ADVANCEMENT TRACK

● COMMUNITY ECOSYSTEM & OUTREACH TRACK

PRESENTATION SESSION

THURSDAY • 2:00PM - 2:45PM

Gs, Cs, and P's - Exploring Certifications and Career Paths in Cyber

Speaker(s): *Midori Connolly*

Room: Bayou E **Track(s):** ●

Level: Beginner **CPE Credits: 1**

Does it seem like every day there's a new certification? Still unsure about what path to take in a cyber career and what certifications can help get there? Ever wonder if certifications are needed at all?This session will help organize and target the seemingly endless industry certifications. Learn from five women in five different segments of cyber about the education/certification they found to be the most relevant in obtaining their current positions.

PRESENTATION SESSION

THURSDAY • 3:00PM - 3:45PM

Navigating the Career Journey

Speaker(s): *Pinal Patel, Jerusha Sejera and Michelle Kababik*

Room: Bayou E **Track(s):** ●

Level: Intermediate/Advanced

Join senior leaders from Verizon's Cyber Defense, Network Security and Cyber Recruitment teams as they dive deeper into the multitude of paths on which a cyber career could take you. This talk will highlight personal stories of overcoming challenges in not only work and life, while navigating creating meaningful careers, as well as discussions on how to not only stay the course in your own journey, but reach new heights.

MALE ALLYSHIP BREAKFAST

The Male Allyship Breakfast is a place for WiCyS male allies to learn actionable steps to become powerful advocates for women in cybersecurity. Guided by Melinda Briana Epler, TED speaker and author of "How to Be an Ally," this dynamic workshop will equip participants with specific allyship actions, insights from research and examples, engaging discussions, and provide an opportunity to foster inclusion.

Sponsored by:

Bloomberg

Located in Bayou AB

Friday • 7:00am - 8:15am

This event is by invitation only and not open to all attendees!

RSVP is required.

2024 WiCyS CONFERENCE
PRESENTATION SESSIONS

PRESENTATION SESSION

THURSDAY • 4:30PM - 5:15PM

Networking for Introverts in Cybersecurity

Speaker(s): *Paula Biggs and Rebecca Granger*

Room: Bayou E **Track(s):** 🟢

Level: Beginner **CPE Credits: 1**

Hate networking (with people)? It is important to understand that face-to-face interactions and interpersonal communication skills are critical to the success of career endeavors. As an introvert, it can be difficult to navigate the complexities of today’s job market and know where to start to gain the “”soft”” skills and abilities that are beyond what is in technical books. It requires deliberate effort to get out of your comfort zone and talk to strangers in order to elevate yourself to the path to success. In this presentation, learn from professionals who have networked their way into the cybersecurity industry and hear words of wisdom on how to overcome mental blocks while learning valuable networking skills to propel a cybersecurity, or any, career. We will go over tips to calm anxiety when you have to “”people”” and discuss things the introverted can do to prepare when they are confronted with professional social situations that will help enhance career and personal goals. Attendees can expect to use these tools the moment they step out the door: leveraging the best aspects of personality type, where to start a network, preparing for small talk, developing elevator pitches, how to talk to strangers, and how to network at large events. There is always more to learn, and a list of resources about effective networking will be provided to attendees.

PRESENTATION SESSION

THURSDAY • 5:30PM - 6:15PM

An Interviewee’s Secret Sauce

Speaker(s): *Chandler Jackson*

Room: Bayou E **Track(s):** 🟢

Level: Beginner **CPE Credits: 1**

Even four years later, the COVID-19 pandemic significantly impacted everyday human interaction, including aspects like home life, relationships and the workplace. As people transition back to the office, there’s an opportunity to enhance communication skills. For young professionals embarking on their career journey, securing internships and new roles can be a challenge. Effective communication, soft skills and understanding emotional intelligence are essential for standing out in interviews and building a successful career in cybersecurity. Join this session to explore the five components of emotional intelligence and key interpersonal communication skills to help achieve career goals.

PRESENTATION SESSION

FRIDAY • 11:00AM - 11:45AM

The Psychology of Belonging: Insights from the People Hacker

Speaker(s): *Jenny Radcliffe and Tashya Denose*

Room: Bayou AB **Track(s):** 🟢

Level: Beginner **CPE Credits: 1**

The women of cybersecurity have a story to tell, and this presentation is here to help tell it. Perseverance is paramount for the women of this industry, and many still face the battle of proving they belong here. In this session, the hosts of a female-driven podcast centered on belonging in cyber will record a live episode with a globally recognized expert in the art of people hacking and social engineering. Together, they will explore the pivotal role of perseverance in shaping a remarkable career and day-to-day life. The presenter’s extroverted and fiercely independent spirit routinely propels her into positions of authority, yet she, too, faces moments when she yearns for another to share the reins. Discover how she navigates this intricate balance and continues to thrive in an industry where resilience and determination are the pillars of success. Beyond that, uncover the pivotal role perseverance has played in individual careers, reinforcing the undeniable truth that everyone belongs here, exactly as they are.

2024 WiCyS CONFERENCE PRESENTATION SESSIONS

Accelerating Incident Response Through Automation

Speaker(s): *Meghan Donohoe and Susan Paskey*

Room: Bayou CD **Track(s):** ● ●

Level: Intermediate/Advanced **CPE Credits: 1**

As the complexity of incident response continues to grow, security professionals face challenges that impede efficiency and contribute to burnout. This issue is particularly prevalent in the field of incident response, where responders are constantly juggling the need to swiftly track down elusive threats while adhering to tight time constraints. Everyone has seen colleagues run out of steam from the pressures of working one high-priority incident after another and understands why this issue is endemic to the profession; and everyone has probably wondered how to move past these issues. This is where automation enters the conversation. Through a comprehensive case study that puts the process of responding to Duo MFA fraud reports under the microscope, the audience will see the impact of automation on the incident lifecycle and the investigator's role. Unlike other presentations that focus solely on automating the detection stage, this case study includes multiple phases of incident response. Developers will learn more about flexible coding practices and the fast-paced environment of an incident response event while responders will gain insights into the advantages of automation from a hands-on perspective. Everyone will be inspired to explore and embrace automation as a means to accelerate incident response.

Ascending to the C-Suite: Achieving the Mid-Level to Executive Transition

Speaker(s): *Zabrina McIntyre, Michelle Wagner and Barbara Mooneyhan*

Room: Bayou E **Track(s):** ●

Level: Intermediate/Advanced **CPE Credits: 1**

Successfully transitioning from mid-level to an executive role demands a strategic evolution of skills and perspectives. This distinguished panel of women, who made that transition, will delve into the transformative journey, uncovering the critical distinctions in skill sets required to ascend to an executive position. Mid-level professionals often find themselves at a pivotal juncture, aiming to bridge the gap between their current capabilities and the enhanced skillset essential for executive leadership. The session will explore the nuanced differentials that pave the way for making that leap. The discussion will spotlight distinct competencies crucial for aspiring executives, including, but not limited to, refined strategic thinking, advanced decision-making abilities, adept communication and an expanded understanding of holistic business operations. The seasoned executives on the panel will share insights based on their years of personal experiences. Participants will gain a deeper understanding of the skills that differentiate mid-level managers from their executive counterparts. The session will not only highlight the necessary skill upgrades but also will provide actionable guidance for professionals aspiring to make this leap. Join this insightful and dynamic talk to learn effective strategies for skill development, acquire a comprehensive understanding of what it takes to successfully transition from a mid-level role to an executive position, and what participants who are currently in mid-level of their career journey can do now to set themselves up for executive consideration.

Flipping the Script: Unleashing the Power of Flipper Zero in Cybersecurity

Speaker(s): *Mimi Vertrees*

Room: Canal ABC **Track(s):** ● ●

Level: Beginner **CPE Credits: 1**

Join as presenters explore the realm of cybersecurity through the revolutionary Flipper Zero. This presentation is crafted for individuals at every stage of their cybersecurity journey, from students to seasoned professionals and career changers. It'll begin with an overview of the Flipper Zero, an all-in-one hacking gadget, and its diverse capabilities. While delving into its features, participants will see how this user-friendly hacking tool serves as a gateway to hardware hacking, exposing essential tools for red teaming scenarios. Delve into vulnerabilities with concrete examples that the Flipper Zero can exploit. Explore different attack vectors through real-world demonstrations. Witness a live demonstration of Flipper Zero's real-world attack capabilities. Learn the emulation process to understand the tool's potential fully. Understand the impact of security breaches on businesses and how Flipper Zero can prevent them. It's not just a tool; it's an educational companion, defending against emerging threats like RFID attacks. Whether a student taking first steps, an early-career professional navigating cybersecurity intricacies or a seasoned executive seeking fresh insights, this presentation is for everyone. Don't miss this unparalleled opportunity to unlock the future of cybersecurity with Flipper Zero. This presentation is a must-attend event, promising to reshape the cybersecurity perspective.

2024 WiCyS CONFERENCE PRESENTATION SESSIONS

The Stealthiest Industrial Revolution

Speaker(s): *Megan Moloney*

Room: Delta B **Track(s):** ●

Level: Intermediate/Advanced **CPE Credits: 1**

Digital technology is accelerating at an unprecedented pace. While many innovations move the needle in specific industries, only a few have driven significant technical, socio-economic and cultural change. These moments in history are marked as industrial revolutions, and they are coming faster and faster. This session will discuss the theory that society is already entering the Fifth Industrial Revolution, which will be anchored in artificial intelligence and quantum computing. Presenters will explore how this differs from the Fourth Industrial Revolution and what it may mean for the tech workforce and society as a whole.

PRESENTATION SESSION

FRIDAY • 1:55PM - 2:40PM

Cloud Detection Engineering: Sleuthing in the Mist

Speaker(s): *Lydia Graslie*

Room: Bayou AB **Track(s):** ●

Level: Intermediate/Advanced **CPE Credits: 1**

Cloud platforms provide unique challenges when it comes to developing accurate and actionable detections, especially Azure and Microsoft 365. The complexity, rapid iteration and shared responsibility model of cloud platforms frequently result in extensive obfuscation of the inner workings, making it difficult for end-user detection engineers to make informed decisions about what to detect on. This presentation will walk through lessons learned on Microsoft cloud detection engineering and recommend some best practices for other users seeking to create cloud detections.

Awareness Alone Won't Save Us: Why Human-Centered Design is Key to Cybersecurity

Speaker(s): *Rachel Russo and Norah Maki*

Room: Bayou CD **Track(s):** ●

Level: Beginner **CPE Credits: 1**

What if people could improve cybersecurity outcomes by designing systems to nudge users to make more security-conscious decisions as they interact with these systems?

It's time to augment the traditional human behavior change approach with human-centered design. The importance of cybersecurity education and awareness is undeniable, but simply educating users without providing built-in behavioral incentives has not been and will not be the best cybersecurity risk-reduction method. It is possible to reduce the dangers associated with human error and make cybersecurity more effective and sustainable by using human-centered design as a first layer of defense.

Unlocking the Potential: LLM and ChatGPT Applications for Cybersecurity Careers and Beyond

Speaker(s): *Laura Malave*

Room: Bayou E **Track(s):** ●●

Level: Beginner **CPE Credits: 1**

In the fast-paced world of cybersecurity, staying at the forefront of the field is a constant challenge. This workshop offers an immersive experience into the world of large language models (LLM), with a focus on ChatGPT, and how they can be harnessed to propel one's cybersecurity career to new heights. This session is designed to empower attendees with practical skills and insights to navigate the dynamic cybersecurity landscape effectively. Through a series of interactive hands-on activities, participants will learn how to leverage LLMs for various aspects of their cybersecurity careers, including job interviews, resume and cover letter optimization, company research, certification preparation and real-world applications. Key Session Highlights: 1. Resume and Cover Letter Transformation: Discover how ChatGPT can help craft compelling and tailored resumes and cover letters that grab the attention of recruiters and hiring managers. 2. Job Interview Success: Learn to ace cybersecurity interviews by practicing with ChatGPT-generated questions, answers and tips. 3. Company Research and Competitive Analysis: Uncover the potential of LLMs for in-depth company research, allowing better understanding of prospective employers and their security needs. 4. Certification Journey: Find out how ChatGPT can assist in studying for industry certifications by providing explanations, resources and clarification of complex concepts. 5. Applications of ChatGPT in Cybersecurity: Explore hands-on applications of ChatGPT such as threat intelligence analysis, automated report generation and security chatbot development.

2024 WiCyS CONFERENCE
PRESENTATION SESSIONS

The Little ERG That Could: Building a Women in Cybersecurity Group from Scratch

Speaker(s): *Shir Butbul and Amelia Fisher*

Room: Canal ABC **Track(s):** ●

Level: Beginner **CPE Credits: 1**

Did you know women make up only 24% of the overall cybersecurity workforce? At smaller companies, this can be even more prevalent, leading to feelings of isolation and a general lack of belonging. Sparking change with an employee resource group (ERG) can feel like a daunting challenge, but the impact is worthwhile. This talk details one ERG's experience from ideation to realization and provides a game plan for women and allies looking to make a difference. When Women in Cybersecurity ERG was launched, there were only three women in the 30-person company. Three months later, this number doubled. The impact was not only about numbers, it was the ability to foster a culture of allyship, belonging and empowerment. Attendees will learn: 1. How to start and maintain a women in security group regardless of industry, company size or role 2. The importance of executive awareness and a top-down approach 3. How to utilize the ERG to create a sense of community and build relationships 4. How to use the ERG to give back to the cybersecurity community.

Using AI to Ethically and Safely Boost Your Security Career

Speaker(s): *Caitlin Buckshaw*

Room: Delta B **Track(s):** ●

Level: Beginner **CPE Credits: 1**

Product security is a vast landscape of various languages, frameworks, tools, infrastructure and other technologies. Without decades of experience, how can one succeed in this rapidly moving realm? The answer, and what this talk will cover, is with the safe and ethical assistance of artificial intelligence.

PRESENTATION SESSION

FRIDAY • 2:50PM - 3:40PM

Rising above the Flame: Confronting Burnout and Reinforcing Your Personal Boundaries

Speaker(s): *Ashley Smyk*

Room: Bayou E **Track(s):** ●

Level: Beginner **CPE Credits: 1**

In an era where the demand for cybersecurity professionals is continually mounting, women, in particular, face unique challenges requiring resilience and adaptability. As a cybersecurity professional who has personally struggled with burnout and setting personal boundaries, the presenter understands the detrimental effects it can have on professional growth and overall well-being. This presentation aims to shed light on the omnipresent issue of burnout, importance of mental health, and provide practical strategies for setting personal boundaries in the workplace.

Ecosystem Approach to Build an Inclusive and Dynamic Cyber Workforce

Speaker(s): *Seeyew Mo*

Room: Canal ABC **Track(s):** ●●

Level: Intermediate/Advanced

An inclusive and dynamic workforce is necessary for innovation, but how can society get there? In this session, converse with representatives from the White House Office of the National Cyber Director to explore how an ecosystem approach to workforce development and education can break down the barriers facing underrepresented communities, fuel more collaboration, and ultimately boost innovation that benefits everyone. Whether representing industry, academia or government, everyone needs all hands on deck!

2024 WiCyS CONFERENCE PRESENTATION SESSIONS

PRESENTATION SESSION

FRIDAY • 3:50PM - 4:40PM

Federal Initiatives in Support of Cybersecurity Ecosystems

Speaker(s): *Toni Benson, Lynne Clark, Ashley Greeley, Marian Merritt and Carolyn Renick*

Room: Canal ABC **Track(s):** ●●

Level: Intermediate/Advanced

Join this session to learn about existing and future federal initiatives underway to prepare, grow and sustain cybersecurity education and workforce development efforts toward building robust cybersecurity ecosystems. Representatives from the U.S. Department of Labor, National Security Agency, Cybersecurity and Infrastructure Security Agency and NIST/NICE in the U.S. Department of Commerce will provide an overview of program priorities, grant programs, workshops, webinars, conferences, apprenticeship and internship opportunities, professional development options, resources and other activities. Through an open and interactive conversation, participants will gain a better understanding of the plethora of federal cybersecurity education and workforce development opportunities and how academia and industry can collaborate with various government programs to build a whole-of-nation approach.

Reaching the Plateau of Productivity: Empowering Second Career Women in Cybersecurity

Speaker(s): *Joanna Grama and Carolyn Ellis*

Room: Bayou E **Track(s):** ●

Level: Intermediate/Advanced **CPE Credits: 1**

(ISC)2, a leading cybersecurity professional organization, conducts a yearly cybersecurity workforce survey. The 2022 report estimates the global cybersecurity workforce gap has grown more than twice as much as the overall workforce. With an abundance of jobs, it is no wonder that more people are considering careers in cybersecurity. Women considering a second career in cybersecurity have an advantage, they bring their past experiences, professionalism and a multi-disciplinary perspective into their new roles. But what other skills and attributes does a second-career woman need to thrive in cybersecurity? Using the Gartner Hype Cycle as a storytelling device, the presenters will share their career transition stories. The presenters of this session are female cybersecurity professionals with over 26 years of combined experience in cybersecurity development and leadership. They will highlight the essential attributes, such as communication, collaboration, adaptability, problem-solving skills, work ethic and a commitment to lifelong learning that second-career women should cultivate to thrive in the cybersecurity field. From the Peak of Inflated Expectations, through the Trough of Disillusionment and up the Slope of Enlightenment, the presenters will share tips, techniques and tools that anyone can use to advance their careers in cybersecurity and reach the Plateau of Productivity.

PRESENTATION SESSION

SATURDAY • 10:00AM - 10:45AM

AI Detectives: The Vanguard of Social Media Forensics

Speaker(s): *Daniela Villalobos and Renata Uribe*

Room: Bayou AB **Track(s):** ●

Level: Intermediate/Advanced **CPE Credits: 1**

In the rapidly changing world of cybersecurity, artificial intelligence (AI) is becoming a key player in social media investigations. This session reveals how AI is changing digital forensic investigations. It will start with an interesting case study, backed by important statistics that show how AI is becoming more and more essential in cybersecurity. The discussion moves on to review how language models can analyze social media data, showing they are capable of finding false information, understanding people's feelings and identifying trends. Then, the focus will be directed to the practical uses of AI, such as finding cyberbullying, uncovering fake profiles and tracing where viral content comes from. Future trends and the expanding role of AI in forensics will be studied, inviting dialogue on upcoming research avenues poised to advance AI utilization in the field. Attendees will leave with actionable insights and foresight into forthcoming technological advances, ready to apply these learnings to complex cybersecurity challenges. This discussion will not only impart knowledge but also provide strategic takeaways for professionals at the forefront of cybersecurity, fostering a deeper comprehension of AI's potential to innovate and secure a digital future.

2024 WiCyS CONFERENCE

PRESENTATION SESSIONS

Build a Cybersecurity Clinic: Enhance Community Cybersecurity and Train Cyber Leaders Beginner

Speaker(s): *Francesca Lockhart and Kareem Chavez-Escobedo*

Room: Bayou CD **Track(s):** ●●●

Level: Beginner **CPE Credits: 1**

What is a cybersecurity clinic? Why should someone build one? What is taught? How can one draw an interdisciplinary and diverse student group? Who does the clinic serve? This session is intended to answer these questions and more by providing a comprehensive how-to guide for developing and launching a cybersecurity clinic at a local school, college, community college or university. Attendees need not be employed at an educational institution to attend; clinic champions and leaders come from all sectors and fields. The audience will be exposed to the growing cybersecurity clinic movement in the U.S. and best practices for the establishment, scalability and long-term success of clinics. The presentation will be co-presented with a current cybersecurity clinic student who will tell her clinic story and explain concrete steps attendees can take to recruit new audiences of students and clients to participate in cybersecurity capacity building in the local community. Join in this mission to develop the cybersecurity workforce while simultaneously fostering cyber resilience in small organizations of all types in a growing number of U.S. states!

Your APIs Called, And They Told Me Your House is Haunted

Speaker(s): *Abigail Ojeda*

Room: Canal ABC **Track(s):** ●●

Level: Intermediate/Advanced **CPE Credits: 1**

Applications are constantly built and deployed for significant business functions that connect the globe. As a result, developers are building exponentially more application programming interfaces (API), which are actively transmitting critical data. While a robust web application firewall (WAF) might keep out the known bad actors, current and emerging API attack types are anything but obvious. Instead, organizations are haunted by shadow APIs, exposed APIs, secretly compromised partner APIs, zombie APIs and more, which can be exploited in ghost-like low-and-slow attacks. The good news is organizations don't have to be haunted by these challenges. This presentation offers a proactive approach to having necessary conversations about API security within an organization — from developers to executives. Join this session to learn about current API attack types and how they align to the 2023 OWASP API Top 10 list.

Understand recent API attack use cases, explore the resulting compliance mandates like PCI DSS 4.0, and analyze how the cybersecurity industry has learned to prevent these types of attacks using AI/ML strategies. Finally, gain an analysis of the relatively new API security industry and how to contextualize it in a larger security strategy.

ICS Purple Team: Cybersecurity in Industrial Control Systems

Speaker(s): *Darla Montgomery and Haley Kim*

Room: Delta B **Track(s):** ●●

Level: Intermediate/Advanced **CPE Credits: 1**

Critical infrastructure is the heart of a thriving society, and it is under daily attack from nation state actors. Critical infrastructure includes electrical grids, water treatment stations and healthcare networks, and relies on operational technology (OT) systems. OT is an umbrella term that industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems fall under. The threat is so serious that in the U.S., the president issued Executive Order 13636: Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience. This presentation will portray how a defense industrial base secures itself against these dangerous cyber threats. It will showcase the experiences of a women-led cybersecurity team in their defense of critical infrastructure for the defense industry. It will broadly examine the OT-specific cybersecurity landscape and the unique challenges it presents. The presentation will include a demonstration of the tools, tactics and procedures used by a purple team to proactively remediate OT cybersecurity vulnerabilities. Participants will learn technical skills through an in-depth examination of the team's successful mitigations against real-world threats. The presentation also will highlight the merits of a culture of empowerment and touch on how cybersecurity teams may foster this culture. The presenters will be the women who founded this unique team and the lead information systems security engineer responsible for day-to-day cybersecurity operations.

2024 WiCyS CONFERENCE PRESENTATION SESSIONS

PRESENTATION SESSION

SATURDAY • 11:00AM - 11:45AM

Culturally Responsive Cybersecurity Assessment

Speaker(s): *Petra Robinson and Jenny Daugherty*

Room: Bayou AB **Track(s):** ●●

Level: Intermediate/Advanced **CPE Credits: 1**

Privilege comes in a myriad of forms and can be invisible to those who have it. In education, efforts that aspire to level the field are termed “culturally responsive.” Considering cybersecurity workforce needs and the desire to achieve educational equity, it is essential to broaden the focus on culturally relevant pedagogy to include a laser-type focus on the equity of assessments. This presentation will describe the process of designing cybersecurity assessments concerned with addressing culture, context and inclusiveness and are accessible to all learners. The Assessment Resources in Cybersecurity project, funded by the National Science Foundation, is developing valid and reliable assessment items to determine what students know about data and network security. Using an evidence-centered design approach, a key step in the process is convening a sensitivity panel to review and revise the items through a culturally responsive assessment framework. In this presentation, details of the sensitivity panel review process, the evaluation rubric, sample problematic items and solutions to revising the items will be shared. A discussion on lessons learned will be facilitated to highlight how this approach can increase awareness about the historical, social, cultural, political and economic contexts which can build in bias and deficit views into assessments. As such, these shared lessons can promote social justice while supporting curriculum change and accountability for creating more meaningful, inclusive and equitable cybersecurity education curriculum and assessment.

Building an Internship Program with Universities and Businesses in Your Community

Speaker(s): *Ann Jones*

Room: Bayou CD **Track(s):** ●●●

Level: Beginner **CPE Credits: 1**

In the Cybersecurity workforce, people face many challenges in recruiting and maintaining staff. Cybersecurity is one of the hardest positions to fill in any organization. Due to the lack of skill sets and the challenging salaries being offered, creating a robust cybersecurity internship program is a way to bridge this gap. Over the last five years, this internship model has had a focus on creating partnerships with the local universities and businesses in the area to come together to build a solid cybersecurity structure for students and local businesses. The robust internship program is not only a benefit to the students but also has allowed businesses to keep talent in the community, gaining years of intern experience and setting them up for success when graduating in cybersecurity. The impact on the STEM programs has allowed businesses to be reimbursed for student internships up to $5,000 every quarter through the grants given by the governor’s office. Embracing communities to solve a problem everyone is faced with has resulted in a positive experience for everyone.

Cyber-Securing Vehicles: Advanced Intrusion Detection Systems for Automotive Cyber Defense

Speaker(s): *Linxi Zhang*

Room: Canal ABC **Track(s):** ●●

Level: Intermediate/Advanced **CPE Credits: 1**

The advancement of vehicle technology brings with it a pressing need for dependable cybersecurity measures. This presentation focuses on developing a sophisticated intrusion detection system (IDS) framework that applies machine learning (ML) and binarized neural networks (BNN) to safeguard against cyber threats in the automotive domain. Traditional IDS approaches, which are largely rule-based, struggle to keep pace with the sophistication of modern cyberattacks within vehicle networks. The proposed solution addresses these shortcomings by integrating responsive ML algorithms and streamlined BNN models, resulting in more accurate threat detection with fewer incorrect alerts. The innovative IDS framework combines rule-based systems’ precision with the dynamic learning capability of ML, providing a dual-layer of defense that can effectively identify both established and emerging cyber threats. BNN serve as an efficient method for on-board systems constrained by limited computational capacity. The integration of such advanced technologies aims to bolster vehicular cybersecurity, preserving the integrity of automotive communication networks. Throughout this presentation, they will dissect the process of designing and implementing this novel IDS, highlighting its practical implications for real-world scenarios. They will discuss the design challenges, outline deployment methodologies, and offer practical guidance for automotive industry stakeholders and cybersecurity experts. This presentation will serve as both a technical exposition and a strategic guide for reinforcing automotive cyber defense in an era of increasingly connected vehicles.

2024 WiCyS CONFERENCE PRESENTATION SESSIONS

Digital Footprint Unveiled: Understanding Public Data

Speaker(s): *Lily Lee*

Room: Delta B **Track(s):** ●

Level: Beginner **CPE Credits: 1**

In a world where data contains a treasure trove of information, it's crucial to unravel the mysteries of one's digital footprint. Join this session for an eye-opening journey through the complex realm of public data in an exploration that will leave attendees informed and empowered. The session will dive into the nuances that distinguish open, public and personal data; the secrets of how public data is amassed; unveil the players in the data-driven marketplace – those who share, sell and purchase information; gain insight into the hazards posed by unscrupulous actors and unethical practices that threaten the privacy and security of public data; the surveillance that often operates just beneath the surface of online activities; and confront potential risks lurking within the vast data landscape of public data. But fear not; this session will conclude with best practices for safeguarding public data and equip attendees with the knowledge and tools to defend an online presence and make informed decisions in the digital age.

Special Thanks

WICYS STRATEGIC PARTNERS

Tier 1

Akamai, amazon, AT&T Cybersecurity, Bloomberg, Carnegie Mellon University Software Engineering Institute, cisco, Ford
Google, LOCKHEED MARTIN, Microsoft, Optum, Sandia National Laboratories, SentinelOne

Tier 2

accenture, Adobe, DeVry University, intel, JPMorgan Chase & Co.
McKESSON, MITRE, MOTOROLA SOLUTIONS, NAVY FEDERAL Credit Union, workday.

Tier 3

American Airlines, AON, ARCTIC WOLF, Arete, ARISTOCRAT, CYBERSECURITY SERVICE, DELL Technologies, Edward Jones
ENVESTNET, flatiron, FORTINET, HAYSTACK SOLUTIONS, IBM, ISC2, HUNTRESS, leidos, LIGHTHOUSE LABS
LinkedIn, Nissan Information Technology, OAK RIDGE National Laboratory, paloalto, PayPal, salesforce, SANS, servicenow.
StoneX, tenable, TikTok, TREND, UC San Diego, Vanguard, wayfair

WICYS FOUNDING PARTNERS

cisco, FACEBOOK, paloalto

Southwest

We ♥ Cybersecurity, too.

Scan or visit **swa.is/wicys** to join an airline that can take your career to new heights.

U.S. ARMY CYBER COMMAND

U.S. Army Cyber Command has 16,500 uniformed and civilian professionals working together to defend the Army's networks and conduct cyber operations around the globe. They rapidly develop and deploy cyberspace capabilities to equip our force for the future fight against a resilient, adaptive adversary.

FUTURE CAREERS →

https://tinyurl.com/27cbbyff

2024 WiCyS CONFERENCE BIRDS OF A FEATHER

SESSION KEY

- ● TECHNICAL SKILL BUILDING TRACK
- ● EDUCATION & WORKFORCE DEVELOPMENT TRACK
- ● RESEARCH & INNOVATION TRACK
- ● CAREER ADVANCEMENT TRACK
- ● COMMUNITY ECOSYSTEM & OUTREACH TRACK

BIRDS OF A FEATHER

FRIDAY • 4:45PM - 5:30PM

Changing the Pace of Cyber: Live Long and Prosper [in Pursuit of Digital Trust and Security]

Speaker(s): *Anastasiya Rutus*

Room: Bayou AB **Track(s):** ● ● ●

Level: Intermediate/Advanced

In these tech-filled lives, trust and security are vital. From sleep tracking and surgeries to autonomous cars and drone management in geopolitical conflicts, a secure digital environment is key. So are the people hired to establish and maintain the guardrails. While cybersecurity professionals work day and night on ensuring humans can safely explore these new worlds, they carry a hidden burden: burnout. An alarming 83% of cybersecurity professionals recently admitted to making errors directly linked to burnout resulting in cyber breaches. This problem is exacerbated by the taboo on safely speaking up about stress levels at work. Around 34% of workers in the U.S. do not feel safe reporting stress because they think it would be interpreted as a lack of interest or unwillingness to do the assigned task. In this Birds-of-a-Feather session, presenters will explore transformational strategies that can change the pace of the cyber industry. Join this interactive discussion to discover practical tools you can apply in work and life for a more sustainable balance. You deserve to live long and prosper in a resilient world where burnout is a trend of the past not a recurring nightmare.

Governing with Robots: What Does an AI-Enabled GRC Future Look Like?

Speaker(s): *Heather Holliday*

Room: Bayou CD **Track(s):** ● ●

Level: Intermediate/Advanced

You've seen the headlines with artificial intelligence (AI) making a big splash in the news. Even lawyers have been (in)famous for their (mis)use of AI. Surely, there is a future in governing with robots, but with all this bad press what does an AI-enabled governance, risk and compliance (GRC) future look like? The goal of this session is to create a new design for GRC, which is responsibly and safely enabled by AI. There will be small groups to generate ideas for developing an AI-enabled GRC program that enables and enhances cybersecurity practices. Participants will discuss ideas about how to address the pain points and pitfalls of AI as well as how to engage reluctant leaders and get their support for an AI-enabled GRC program.

WiCyS MENTORSHIP

Become a WiCyS 24' Mentor

Are you interested in becoming a mentor for the WiCyS 2024 mentorship program? The next WiCyS mentorship cycle will launch in Fall 2024.

Scan the code to receive more information.

2024 WiCyS CONFERENCE BIRDS OF A FEATHER

Recipe for Resilience: Blending Cross-Functional Talents in the Cybersecurity Kitchen

Speaker(s): *Saskia Hoffmann*

Room: Canal ABC **Track(s):** 🟢🔵

Level: Beginner

In the ever-evolving realm of cybersecurity, silos are out and collaboration is in. “Recipe for Resilience” serves as a deep-dive discussion into the art of relationship building across different company teams, emphasizing its critical role before, during and after cyber incidents. This session will explore effective strategies like security champions programs and security partners, especially vital for smaller security teams. Participants will share experiences, learning how to proactively weave security into their corporate fabric. The takeaway? Security is a team sport, and this session is an invitation to discover how others are nurturing the relationships that create a resilient, cyber secure organization.

Overcoming Microaggressions and Shattering Stereotypes as Women in Security

Speaker(s): *Bri Frost*

Room: Delta B **Track(s):** 🟢

Level: Beginner

The world of cybersecurity presents a vast amount of career opportunities, but as women in a male-dominated industry, it also presents many challenges. Women cyber professionals often encounter subtle yet pervasive microaggressions that can undermine their confidence and career progression. It’s ok to push back! But how do you do that in a professional yet assertive manner? Learn how to ensure your opinions are being heard and your technical abilities seen rather than being questioned because of gender bias. This session will facilitate a candid dialogue among women in cybersecurity as well as share experiences and success stories with stereotype-driven bias. Walk away with actionable strategies to challenge microaggressions and reshape perceptions around stereotypes.

Green Cybersecurity

Speaker(s): *Iris Ye*

Room: Delta D **Track(s):** 🔵🟠🔵

Level: Intermediate/Advanced

This session is an open forum for discussing the implementation and considerations related to sustainable security infrastructure within the rapidly evolving realm of renewable energy technologies. Sustainability of cybersecurity is not just led by technical feasibility but also environmental well being. This session will focus on exploring how businesses can embark on the journey of green cybersecurity, considering environmental, social and governance factors and the growing reliance on renewable energy sources. As the renewables sector undergoes rapid expansion, and with renewables accounting for a significant proportion of new power capacity globally, the discussion will center on the critical need for cyber resilience in renewable energy technologies. The conversation aims to gather insights and inspire collaborative thinking among participants to address emerging challenges and trends in the green cybersecurity domain.

2024 WiCyS CONFERENCE
PANEL SESSIONS

SESSION KEY

- ● TECHNICAL SKILL BUILDING TRACK
- ● EDUCATION & WORKFORCE DEVELOPMENT TRACK
- ● RESEARCH & INNOVATION TRACK
- ● CAREER ADVANCEMENT TRACK
- ● COMMUNITY ECOSYSTEM & OUTREACH TRACK

PANEL SESSIONS

SATURDAY • 12:00PM - 12:45PM

Cyber Sheroes: The Women Commanding AI's Evolution

Speaker(s): *Prajakta Jagdale, May Wang, Christina Papadimitriou and Nicole Nichols*

Room: Delta B **Track(s):** ● ● ●

Level: Intermediate/Advanced **CPE Credits: 1**

"Cyber Sheroes" convene a vanguard of women whose technical expertise is revolutionizing AI in cybersecurity. This panel delves into their pioneering work, from leveraging machine learning for intrusion detection to utilizing neural networks for real-time threat analysis. Panelists will demystify AI's role in identifying and neutralizing sophisticated cyber threats, sharing insights on building resilient, self-improving systems capable of anticipating hacker maneuvers. Attendees will engage with the technical narratives behind crafting AI algorithms that safeguard critical infrastructure without infringing on privacy. Discussions will pivot around the practicalities of training AI under rigorous ethical constraints and the implementation of quantum-resistant AI models to fortify cybersecurity in the approaching quantum computing era. This compact session aims to celebrate technical innovation led by women, inspiring a diverse future for AI-driven cybersecurity solutions that are as ethical as they are advanced. "Cyber Sheroes" is not merely an acknowledgment of women's impact in AI but a forward-looking dialogue on the integral, technical contributions they continue to make in securing a digital world.

From the Roots Up: Growing the Next Generation of Cyber Professionals with Apprenticeships

Speaker(s): *Abigail Allen, Donna Woods and Tobi West*

Room: Bayou CD **Track(s):** ● ● ●

Level: Intermediate/Advanced **CPE Credits: 1**

On July 19, 2022, at the National Cyber Workforce and Education Summit, the administration gathered cabinet secretaries and major companies to discuss ways to improve pathways into this critical sector and announced the start of its 120-day Cybersecurity Apprenticeship Sprint, an initiative run by the U.S. Department of Labor in coordination with the White House Office of the National Cyber Director and departments of Commerce, Homeland Security, Defense and other federal agencies. This effort has once again demonstrated overwhelming potential and success in promoting registered apprenticeships. The work of the Sprint resulted in over 7,000 apprentices getting hired, over 1,000 of whom were from the private sector. Of these private sector apprentices, 42% were people of color and 32% were female. Prior to the Sprint, 27% of all cybersecurity apprentices were people of color and 28% women, which reflects the impact of this Sprint and the power of the public and private sectors working together and partnering with community-based organizations to reach diverse populations. This panel presentation, hosted by three female subject matter experts in their field, will focus on how employers and educators can recreate these results using registered apprenticeships. The audience will hear from two programs, the first being implemented at the K-12 level and focusing on pre-apprenticeships, and then a registered apprenticeship program at the community college level.

2024 WiCyS CONFERENCE PANEL SESSIONS

Don’t Be a Victim of Gender Washing

Speaker(s): *Dawn Armstrong, Leilia MacNeil and Kristen Rodriguez*

Room: Bayou AB	**Track(s):** ● ●
Level: Intermediate/Advanced	**CPE Credits: 1**

Despite the growing demand for cybersecurity professionals, women continue to face significant barriers when entering and advancing within this field. This panel, consisting of women in all stages of their careers, will address the multi-faceted challenges women encounter, ranging from securing employment to progressing in their careers in cybersecurity. They will explore pragmatic strategies for marketing oneself with a keen focus on the optimization of resumes to neutralize gender bias. By analyzing the subtleties in language and presentation that can inadvertently reveal gender, they want to equip candidates with the tools to mitigate unconscious bias and emphasize skills and qualifications. Panelists will provide their experiences with bias in the workplace, in career advancement, and examples of how language changes in their resume increased the number of interviews. The panel will delve into the critical role of mentorship in both personal and professional growth. They will discuss how being a mentor and seeking mentorship can forge pathways to empowerment, skill enhancement and networking opportunities. The concept of sponsorship also will be discussed as a proactive counterpart to mentorship, advocating for active support in career advancement. If time permits, the moderator will invite panelists to discuss job seeking strategies, how to stay organized in a job search, and the value of a cover letter and thank you note.

The Evolution of Cybersecurity Careers in Defending Against Physical Threats

Speaker(s): *Kelly Murray, Lisa Beury-Russo and Ryan Donaghy*

Room: Canal ABC	**Track(s):** ●
Level: Beginner	**CPE Credits: 1**

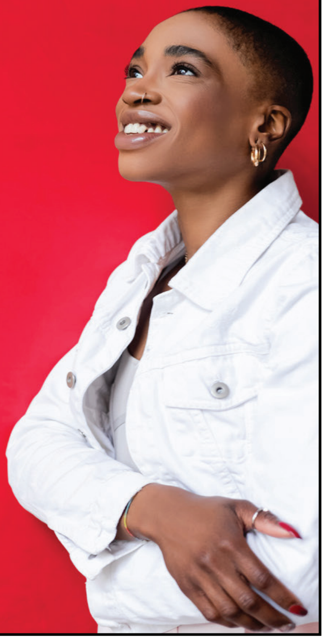
Artificial intelligence. Election security. Terrorism. The big issues that make primetime news and front-page headlines also are some of the fastest growing opportunities for those seeking a career in cybersecurity. But what does it actually mean to work on these hot-button topics every day? Tackling today’s global threats require innovative thinking, technical analysis, strategic planning and lots of practice. Three public-sector executives at the forefront of combating these threats will explain the integral role cybersecurity professionals play in anti-terrorism efforts, critical infrastructure protection, and preparing for the opportunities and challenges of tomorrow as well as how they’re driving the evolution of cybersecurity roles in areas where the playbook is still being written. Attendees will learn what the panelists are seeing in the landscape of emerging cyber threats, vulnerabilities, attack vectors and response procedures across the nation. They will learn about the essential skills beyond engineering and programming needed to excel in this field, including project management, talent acquisition and retention, technical writing and team leadership, and how all of these skills can build a team of creative thinkers ready to solve complex and unprecedented challenges to national security.

Navigating the New Normal: Women in Cybersecurity Adapting to Hybrid Work Environments

Speaker(s): *Jennifer Cox, Jessie Jamieson, Sasmita Panda, Khensani Carter and Muta Mashack*

Room: Delta D	**Track(s):** ●
Level: Intermediate/Advanced	**CPE Credits: 1**

In today’s rapidly evolving world, the lines between personal and professional lives are blurring like never before, giving rise to the era of hybrid work. As people embrace this new normal, it is crucial to explore how it impacts various facets of everyday lives, particularly the realm of cybersecurity. In this panel discussion, the presenters will delve into the multifaceted challenges and opportunities women in the cybersecurity field face as they transition into this hybrid work paradigm. This session aims to foster an engaging dialogue among experts, practitioners and attendees, shedding light on the unique experiences of women in cybersecurity. It will examine the implications of hybrid work on gender dynamics, career progression, work-life balance and the cybersecurity landscape. The diverse panel will share their personal journeys, insights and strategies for thriving in this evolving landscape while also addressing the broader societal and industry-level implications. Some topics will include balancing remote and in-office work for career advancement; nurturing a supportive work culture that promotes diversity and inclusion in cybersecurity; leveraging technology to secure remote work environments and data; strategies for professional development and networking in a hybrid world; and adapting to evolving cyberthreats in the context of remote work.



2024 WiCyS CONFERENCE LIGHTNING TALKS

SESSION KEY

- ● TECHNICAL SKILL BUILDING TRACK
- ● EDUCATION & WORKFORCE DEVELOPMENT TRACK
- ● RESEARCH & INNOVATION TRACK
- ● CAREER ADVANCEMENT TRACK
- ● COMMUNITY ECOSYSTEM & OUTREACH TRACK

LIGHTNING TALKS

SATURDAY • 10:00AM - 10:45AM

All Lightning Talks are in Delta D

Tracks: ●●●●●

Level: Beginner & Intermediate/Advanced

Cyber for Swifties: How Swiftie Nation Could Be Great Intelligence Analysts

Speaker(s): *Meghan Martinez*

Taylor Swift is a cultural phenomenon, particularly for women of all ages. The lengths that "Swifties" go to to piece together all the Easter eggs she leaves in her lyrics and music videos could put true investigators and analysts to shame. What if cybersecurity folks met Swifties where they are at and show them how their powers could be used in the cyber industry?

Phishing 2.0: The Rise of Artificial Intelligence

Speaker(s): *Rachel Kang*

In the ever-growing landscape of cyber threats, phishing continues to be one of the most reliable social engineering tactics attackers leverage to target individuals and enterprises. However, as daily lives become more intertwined with artificial intelligence platforms and similar emerging technologies, how do people protect themselves when bots are now replacing the role of the human scammer? Because many social engineering attacks are still limited by the need for a human element to facilitate rapport with victims, cybercriminals have begun weaponizing advanced artificial intelligence tools to broaden the reach of their phishing campaigns, rendering preventative efforts to identify and contain such attacks more difficult. This talk will explore how advanced artificial intelligence has been incorporated into the latest phishing campaigns over the last few years. Attendees will gain a better understanding of the emerging threat associated with AI-enabled phishing and what this means for the future of cyber threat landscapes.

Technically, You Are Technical

Speaker(s): *Shannon McHale*

Who is doubting their technical abilities? Well, knock it off! Are others doubting an individual's technical abilities? Not after this talk! Who wants to enhance their technical skills but do not know how? This talk will show participants! Throughout their careers, women often contend with the pervasive stereotype of being deemed nontechnical or less technical. This label can deeply influence self-perception, leading to a burdensome sense of imposter syndrome.

Join this presentation where presenters will walk attendees through a structured approach to becoming technically experienced, comprising four essential steps. They'll emphasize the significance of building confidence in one's technical skills and provide practical tools to cultivate identity as a technical expert. Lastly, they'll explore effective tactics for showcasing technical abilities, ensuring that others recognize one's capabilities. Everyone is technical and capable! Let's make sure everyone knows it!

2024 WiCyS CONFERENCE LIGHTNING TALKS

Who Ya Gonna Call?

Speaker(s): *Debby Briggs*

Organizations become victims of cybercrimes on a daily basis. It's only a matter of time before a familiar organization will need to report an incident to law enforcement. When that happens, where should someone start? Reporting requirements vary based on jurisdiction and the severity of the crime, but it's important that an organization knows how to develop a relationship with its local law enforcement officers if it does become a victim of a cybercrime. Enterprises might be reluctant to report cybercrimes due to concerns about the time and financial resources it can require, along with the belief that it may not lead to a successful recovery for their business. However, according to recent guidance from the U.S. Department of Justice, cybercrimes should be reported to law enforcement at either the local, state, federal or international level. In this lightning talk, the presenter will discuss the importance of reporting a cyberattack to law enforcement, and how organizations can address and report specific cybercrimes such as DDoS attacks, social engineering attacks or ransomware attacks. Additionally, the audience will understand how organizations can initiate contact with law enforcement and how the cybercrime might be dealt with (such as tracking down cybercriminals). Emphasis will be on the importance of building trust and maintaining an ongoing relationship with law enforcement to ensure an organization has support if it becomes a victim of a cyberattack.

The Role of Cyber Competitions in Cultivating Next Gen Cybersecurity Talent

Speaker(s): *Jingdi Zeng*

Practical experiences, such as internships, apprenticeships and cooperative education programs, have long been invaluable for recent graduates and career changers to pursue full-time employment. Recently, cybersecurity competitions have emerged as a powerful complement to these traditional pathways, offering participants a distinctive advantage in the competitive job market. The accelerated growth of cloud technologies has streamlined the logistics of hosting such competitions, significantly reducing the complexities associated with the provision and maintenance of hardware and software resources. This, coupled with well-defined cybersecurity work roles in standards such as the National Initiative for Cybersecurity Education (NICE) framework, has enabled the design of competition scenarios that closely reflect and validate the practical skills required by employers. Drawing on her experience mentoring students in various cybersecurity competitions, the presenter will identify the elements that contribute to the success of these events. The discussion will then seek collective experiences and perspectives of attendees. The aim of this presentation is to foster a dialogue that will help shape a shared vision for the future role of cybersecurity competitions in the continuum of cyber education and workforce preparedness.

Cybersecurity for Social Good

Speaker(s): *Bella Gomez*

The world is more digitally connected than ever. Technology has the power to change and improve lives. But, it also has the power to do extensive damage and harm vulnerable communities that need protection and are at risk of cyberthreats. In 2015, the UN identified 17 Sustainable Development Goals (SDGs) to be achieved by 2030 – ranging from eradicating poverty to fighting for a more just and peaceful world while navigating vast global issues. Digital technologies, particularly the combination of artificial intelligence and data science, can facilitate efforts to achieve SDGs. The power of using technology for social good in recent endeavors from data-driven urban systems for sustainable smart city development to AI models that can help detect malnutrition using photographs of individuals living in a given area has been witnessed. So where does cybersecurity come in? It creates the space for people to think about how to collaborate across public and private sectors and work to ensure that research and data collected by groundbreaking nonprofit organizations are protecting the communities they work so hard to assist. Global threats require global thinking and responses. How do people define technology for social good? Who's responsibility is it to ensure that technology continues to help, not harm, at-risk communities? How can cybersecurity create positive impacts in developing regions of the world? These ideas will guide a lightning talk to encourage individuals to consider the ways in which their passions for cybersecurity can be used for social good.

A Quick Dive Into the NEW WiCyS Member Portal

Speaker(s): *Quintana Patterson*

Who has interacted with the new WiCyS member portal? A game changer indeed. This unique portal is designed specifically for WiCyS members for all things WiCyS. With improved navigation, enhanced security features and interest groups for everyone, the new system will elevate the WiCyS experience and reenergize community engagement. Learn how to join, connect with different interest groups, request a new interest group, make announcements, and connect with the WiCyS community members wherever they are across the globe!

2024 WiCyS CONFERENCE
LIGHTNING TALKS

LIGHTNING TALKS

SATURDAY • 11:00AM - 11:45AM

All Lightning Talks are in Delta D

Tracks: ●●●●●

Level: Beginner & Intermediate/Advanced

Who Can Teach High School Cybersecurity? Good High School Teachers!

Speaker(s): *Moriah Walker*

More cybersecurity professionals are needed across the country. Cybersecurity educators also are needed in the K-12 space. Unfortunately, most states do not have a license for cyber education or related programs, and most cyber professionals are not willing to teach in a public school, so where are people to teach students at a high school level? They already work in education. Typically, the best cyber teachers are really good educators who are willing to learn cyber.

The Privacy Paradox: Can People Stay Hidden in Plain Sight?

Speaker(s): *Caitlin Sarian*

This lightning talk addresses the critical intersection of personal privacy and technological advancement, raising the question of whether true privacy is attainable in a world where technology's capabilities are ever-increasing. It scrutinizes the tradeoffs individuals make, often unconsciously, between convenience and privacy in the digital domain. The discussion orbits around three pivotal themes: the integration of privacy by design, the balancing act between regulation and innovation, and the pursuit of anonymity in an interconnected ecosystem. A fourth dimension is added to consider the corporate responsibility in educating users about privacy settings and transparency in data collection practices. The aim is to incite a conversation on how privacy can be preserved and reimagined amidst incessant change.

Disney Villains Unleashed: A Cybersecurity Tale

Speaker(s): *Alissa Butcher*

Ever wonder if Disney villains could be lurking in the world of cybersecurity, posing the greatest digital threats? Come reimagine these iconic villains as metaphors for diverse cyber threats. Just as the villains plot and scheme in the Disney world, cyber threats exhibit their unique characteristics and strategies in the digital landscape. Join this captivating journey to unveil the concealed dangers that parallel these infamous villains and empower attendees to fortify their organization's defenses against the cunning schemes. Uncover amazing mysteries and real-life tales from Ursula's tentacles of malware to Scar's betrayal as an insider threat. Explore the untold stories and discover strategies to guard a digital kingdom against these lurking dangers. Join the presenters as they unmask the digital adversaries, enhancing cybersecurity safeguards while preserving trust and confidentiality. Don't miss this unique talk!

Prompting Success: Using AI for Cybersecurity Education and Research

Speaker(s): *Paige Zaleppa*

In this lightning talk, the presenter will discuss how gaining a fundamental understanding of prompt engineering has improved utilization of AI for research and learning as a PhD student in information technology. Prompt engineering is defined as the process of structuring text so it can easily be interpreted by generative AI models. Acquiring proficiency in this essential skill has become crucial for students, educators and researchers, considering the rise in AI adoption over the past two years. Since the beginning of 2023, the presenter has learned different prompting techniques such as zero-shot, few-shot and chain-of-thought. Employing these techniques has enhanced their ability to quickly grasp new concepts, brainstorm potential research questions and build an understanding around various topics in cybersecurity. As a result, they experienced an increase in the efficiency and quality of reading comprehension and writing, which has directly impacted learning and research. The presenter will share their experiences using prompt engineering to inspire others to embark on their path to success!

2024 WiCyS CONFERENCE LIGHTNING TALKS

Don’t Listen to the Naysayers!

Speaker(s): *Tracey Ristich*

This presentation explores the applicability of Arnold Schwarzenegger’s six rules of success to the field of cybersecurity, offering valuable insights for individuals seeking to establish themselves in this industry. Schwarzenegger’s rules, when adapted, provide a roadmap to help professionals remain resilient and focused on their goals, even in the face of setbacks and adversity.

You Are the CEO of ME: Intentional Behaviors Yield Results

Speaker(s): *Jigisha Pardanani*

You Are the CEO of ME can achieve PROVEN results for people who are intentional in exhibiting certain behaviors with consistency. By doing so, an individual’s career will naturally progress to where they want it to go. In this session, presenters will deconstruct how to advance one’s career by sharing a set of established behaviors that will get people where they want to go. This session will also include relatable, real-life examples, highlighting lessons learned and strategies. After attending this session, you will have the strategy and tools to map out how to get to the next level in your career.

Extending Reach: Growing the WiCyS Community One Affiliate At a Time

Speaker(s): *Jaclyn Justice*

Hear the why and how of launching a WiCyS professional affiliate. The presenter will discuss the purpose of the affiliate initiative and give a brief overview of how the program works from launch to running a successful affiliate.

Managing and Mobilizing WiCyS Student Chapters

Speaker(s): *Quiana Oates*

Learn about creating and growing WiCyS Student Chapters. The presenters will brief attendees on the benefits of building such a supportive community at campuses of higher education; the process of how to start; the strategies to sustain; and ways to engage with the greater WiCyS community at large.

A DECADE OF EMPOWERMENT

From 2014 to 2024, these sponsors celebrate 10 years of WiCyS sponsorship!

asurion

Carnegie Mellon University Information Networking Institute

CHAMPLAIN COLLEGE

Google

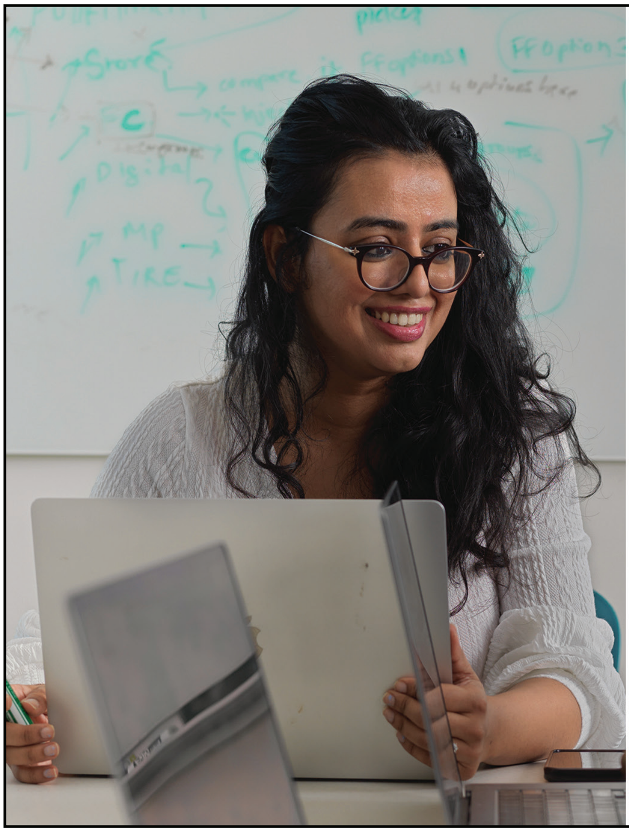
IBM

LOCKHEED MARTIN

Microsoft

MIT LINCOLN LABORATORY

CEROC Cybersecurity Education, Research and Outreach Center



2024 WiCyS CONFERENCE STUDENT POSTERS

STUDENT POSTERS

FRIDAY • 9:45AM - 11:00AM

1. Enhancing Privacy on HTTPS Traffic: A Novel Super Learner Attack and an Efficient Defense

Masoumeh Abolfathi, University of Colorado, Denver

Web privacy-enhancing technologies have evolved to protect against traffic analysis (TA) attacks, particularly website fingerprinting (WFP) attacks that compromise user privacy by revealing visited websites on encrypted connections. Leveraging recent advances in AI methods, the objective is to better understand privacy vulnerabilities of HTTPS traffic against ever-evolving TA attacks. As a novel contribution, this work proposes an HTTPS website fingerprinting attack model called Super Learner Attack (SLA), an ensemble of base learners to exploit the strengths and diminish the weaknesses of the individual base learners, including LogisticRegression, DecisionTreeClassifier, Gaussian Naive Bayes, KNeighborsClassifier, AdaboostClassifier, BaggingClassifier, RandomForestClassifier and ExtraTreeClassifier. The SLA aims to learn fusion weights in a data-adaptive manner to obtain the optimal combination of the base learners. Responding to the challenge of WFP attacks and in direct response to the SLA, this work proposes HTTPS Obfuscation Defender (HOD), a novel and highly effective defense strategy rooted in deception. This strategy disrupts classification by skillfully introducing fake packets into real flows, obfuscating patterns and disrupting classification. Unlike previous methods, this approach leverages adversarial example algorithms originally designed for image analysis to generate maximal obfuscation in encrypted HTTPS traffic. Experimental results demonstrate that the HOD significantly reduces the accuracy of website fingerprinting from 97.2% to 2.89%, even when an attacker attempts to adapt to the defense and retrain a classifier using defended traffic. HOD minimizes time and bandwidth impact, ensuring a practical and resource-efficient defense.

2. G-Code Forensics: Tracing Manipulation Attacks in FFF-Based 3D Printing

Hala Ali, Virginia Commonwealth University

3D printing, also known as additive manufacturing, is a revolutionary technology that creates physical objects by depositing material layer by layer. In FFF-based 3D printing, precise control of parameters like nozzle movement and filament extrusion rate ensures integrity of the printing object. G-code refers to the set of instructions that control the 3D printer's movements and actions during the printing process. A primary concern is filament attacks that might not make apparent changes to G-code, but they significantly affect the physical properties of the printed objects without any visible deformations. Hence, identifying whether a change is an attack or a standard printing requirement becomes challenging. This work presents a novel automated G-code analysis engine for detecting filament attacks, such as cavity and density variation attacks. They formally analyze malicious activities linked to filament attacks to extract relevant G-code features. The engine utilizes these features with Bi-LSTM to classify G-code programs to successfully distinguish benign G-code programs from various malicious ones with a detection accuracy of 93.89%.

3. ACPsGrpah: Automated Access Control Policy Specification Framework

Saja Alqurashi, Colorado State University

Security requirements of an organization are often expressed in natural languages. Access control policies (ACPs) are embedded in the security requirements. Security administrators manually extract ACPs, interpret them, and construct a formal access control model, which is later enforced by security mechanisms. However, ACPs in natural language are unstructured and ambiguous, and manually extracting ACPs from security requirements and translating them into enforceable policies is tedious, complex, expensive, labor-intensive and error-prone. Toward this end, this project proposes a practical framework to construct formal ACP specifications from natural language automatically. It is a novel framework that helps security administrators manage an organization's access policies. The experimental results are promising as they achieved, on average, an F1-score of 93% when identifying ACPs sentences and an F1-score of 96% when extracting policy attributes from natural language access control policies.

4. Sonic Defenses for Industrial Control Systems: Converting Memory to Audio Signals

Nehal Ameen, Virginia Commonwealth University

Programmable logic controllers (PLC) are a critical component of Industrial Control Systems (ICS). They are responsible for automating industrial physical processes for critical infrastructure, which makes them a major target for attackers. The field of ICS is constantly facing challenges in triaging such attacks. In this paper, WaveSleuth, a novel approach that leverages memory signals to conduct heartbeat checks that can help detect anomalies in a PLC's memory, is introduced. WaveSleuth extracts the memory periodically and converts the acquired raw memory data into audio signals that can

2024 WiCyS CONFERENCE STUDENT POSTERS

be utilized to represent unique patterns and characteristics of a system's memory signals, providing valuable insights into the system's state and operation. WaveSleuth then measures the DTW distance between each consecutive memory dump to determine whether the most recently acquired memory dump has been maliciously altered or not. The performance of WaveSleuth was evaluated on a fully functional physical process that emulates a four-floor elevator by executing three different successful attacks. Each attack targets a different region of the PLC's memory and alters it. Rigorous stress tests were conducted to demonstrate the footprint size detectable by WaveSleuth. It proved to be successful at detecting attacks with small footprints in less than one second each. WaveSleuth provides a lightweight technique to perform the first step required for triaging through digital forensic analysis of arbitrary memory images by translating high-dimensional binary data to simple audio signals that can be analyzed more easily, which can be invaluable in saving time and effort during incident response.

5. PLCs Bewitched! Attacking the Control Logic through Design Flaws

Adeen Ayub, Virginia Commonwealth University

In industrial control systems (ICS), programmable logic controllers (PLCs) govern critical infrastructures like nuclear plants and power grids. The escalating risk of remote attacks on PLC control logic necessitates robust intrusion detection systems (IDS). This poster reveals the inadequacy of standard IDS features, such as entropy, n-gram and decompilation in detecting binary control logic programs embedded within protocol message headers and payloads. A new approach is introduced, leveraging a previously overlooked PLC design feature — redundant address pins (RAP) that enable the injection of programmable malicious code (PMC) into control logic as an initial attack vector, eluding IDS scrutiny and executing with every scan cycle. Three distinctive attack methods — GizmoSplit, BuffWarp and EnigmaFlow — are presented. These methods seamlessly integrate control logic with network traffic through payload encoding, small-size payloads or sparse memory addressing, utilizing PMC for the execution of malicious control logic. GizmoSplit strategically divides control logic into gadgets, written to random memory locations, utilizing PMC to modify the stack for execution through return-oriented programming. BuffWarp employs a small-size buffer for periodic injection of malicious code with PMC moving buffer content to consecutive memory locations for execution. EnigmaFlow encodes control logic, sending it to an unused memory region, relying on PMC for decoding and execution. Evaluation results highlight the stealthiness and efficacy of these attacks, demonstrating their ability to bypass IDS relying on standard message header and payload features. This research emphasizes the imperative need for enhanced intrusion detection mechanisms tailored to control logic attacks exploiting PLC design vulnerabilities.

6. Efficient Candor: Transparency of IoT Device Presence and Capabilities

Isita Bagayatkar, University of California, Irvine

Widespread deployment of internet of things (IoT) devices in numerous settings triggers many security and privacy issues. These devices often are stealthy, and their presence and capabilities are unknown to nearby users. Stealthy sensing falls under the provisions of recent privacy regulations, such as GDPR and CCPA. To this end, this work is developing PAISA, a simple root of trust architecture for secure announcements of nearby IoT devices and their functionalities. PAISA is a compliance-based approach aiming to show that device manufacturers can easily support full transparency of their devices. PAISA guarantees secure operation even if the device is fully software-compromised. PAISA involves one or more IoT device(s), each with a trusted execution environment (TEE) and a user device (smartphone) that queries and receives information from the former. PAISA exchange is initiated by a user device broadcasting a request and all PAISA-compliant nearby devices responding with a secure announcement. An alternative model involves devices periodically and unilaterally broadcasting announcements to all currently present user devices. The two models (PULL and PUSH, respectively) have advantages and drawbacks. Both models of PAISA will be prototyped, experimented with and analyzed in performance and security.

2024 WiCyS CONFERENCE STUDENT POSTERS

7. A Forensic Analysis of Malware Written in Go

Jessica Berrios, University of New Haven

In response to escalating threats targeting corporate entities, an investigation is underway to scrutinize malware intricacies. The focus centers on the forensic analysis of Go-programmed ransomware, increasingly favored by malicious actors. The core of this inquiry delves into the comprehensive static analysis of RobbinHood ransomware, an adversarial agent that caused substantial disruptions in a targeted attack on Baltimore's governmental operations in 2019.
Using tools like Ghidra, Ida and strings, the code responsible for effecting encryption processes on the targeted computing environments was deconstructed. Dynamic analysis, a pivotal component of the investigative framework, involved executing a sample of RobbinHood ransomware within an isolated virtual environment, facilitating real-time capture of system logs and processes and providing nuanced insights. Findings from dynamic analysis unveiled the ransomware's operational dynamics with the encryption initiation mechanism systematically generating HTML files within directories housing user data. Notably, not all directories are subject to encryption with the default directory remaining impervious to the ransomware's effects. A recurrent observation pertains to the frequent occurrence of the cftmon.exe file in the process monitor, indicating the malware's proclivity for navigating the operating system through command prompt manipulations. Log analysis further elucidates the stepwise progression of the ransomware's operational sequences. While static analysis results undergo investigation, the overarching aim is to attain a nuanced understanding of the encryption methodologies employed, with a prospective focus on potential avenues for data recovery solutions. This research underscores the exigency of fortifying cybersecurity postures against evolving threats, particularly those leveraging the Go programming language.

8. Secure Address Resolution Protocol (S-ARP)

Aishwarya Channappaji, Northeastern University

Communication within a LAN network uses IP-over-Ethernet, and this communication is fostered using Address Resolution Protocol (ARP), which resolves the IP address to a hard coded MAC address of a device. Securing an internal network is crucial considering the weight of confidentiality it carries. However, this is vulnerable to many attacks and, ARP being one of the least secure protocols, contributes to most of these attacks. Exploiting the weakness in ARP, an attacker can gain access to the traffic simply by manipulating the ARP table and replacing the actual MAC address with that of the attacker. This would further let the attacker sniff the traffic and devise other higher layer attacks like DNS spoofing. Hence, securing ARP is of prime importance. The paper presents a secure version of ARP (S-ARP), which maintains a centralized ARP cache table rather than being host specific. Access to this table from each host is provided through secured key exchanges where each host has a public and private key pair and a trusted digital certificate trusted within the network. Whenever there is a new request, the host validates its identity using the certificate to the centralized server. Once verified, the centralized server keeps an entry of the IP and corresponding MAC in its system. This table can be accessed by other hosts by verifying its identity. This method can be done without the centralized server, however, multiple key exchanges amongst hosts can lead to performance overhead, which is reduced by maintaining centralized access with only one-time verification.

9. Using Side Channels to Detect Malicious Software with Machine-Learning Algorithms

Rebecca Clark, University of South Alabama

This poster highlights the critical importance of inclusive design in today's technologically driven world. With over one billion people living with disabilities globally, it's imperative that technology is designed to cater to diverse user needs, including factors such as age, language, culture, gender identity, and socioeconomic status. Inclusive design thinking involves centering the needs of marginalized communities throughout the design process, ensuring that technology is accessible and ethical. Attendees of this session will have the opportunity to learn about proven inclusive research methods, such as co-design sessions with disabled users, to better understand their needs and preferences. Additionally, they will uncover common exclusionary practices in tech design and develop strategies to prioritize inclusion throughout product development cycles. Capital One's approach to embedding inclusive design thinking into their products and processes serves as a blueprint for other organizations looking to make a positive impact. By sharing their insights and model, attendees can gain valuable insights into how to implement inclusive design practices effectively, ultimately gaining a competitive edge while promoting accessibility and equity. Overall, this session provides a valuable opportunity for attendees to learn about the importance of inclusive design, gain practical insights and strategies, and contribute to creating technology that benefits everyone.

2024 WiCyS CONFERENCE STUDENT POSTERS

10. Detection of Cyberbullying in GIF using AI

Pal Dave, North Carolina A&T State University

Cyberbullying is a well-known social issue, and it is escalating every day. Bullying does not just happen in person; it has taken over all social media. Cyberbullying can be done intentionally or unintentionally by the social media users. Someone can use social media as a platform to bully a victim. It can be unintentional because sometimes a user might not know what they are doing or how it can impact others. Mostly out of curiosity or without being concerned, users upload, share and write their views on social media, which can affect a community or a person mentally and emotionally. Due to the vigorous development of the internet, social media provides many different ways for users to express their opinions and exchange information. Cyberbullying occurs on social media using text messages, comments, sharing images and GIFs or stickers, as well as audio and video. Much research has been done to detect cyberbullying on textual data; some are available for images. Very few studies are available to detect cyberbullying on GIFs/stickers. First, hashtags related to cyberbullying using Twitter were extracted. These hashtags helped download GIF files using publicly available API GIPHY. Over 4100 GIFs were collected in total. Deep-learning pre-trained model VGG16 was used for the detection of cyberbullying. The deep-learning model achieved the accuracy of 97%. This work provides the GIF dataset for researchers working in this area.

11. Going Beyond Hacking with Encrypted and Verified Computation

Meron Demissie, University of Michigan

In today's world, where much personal information is held and used to drive services by organizations people may not trust, privacy is always at great risk. Privacy-enhanced technologies address these risks typically by giving data owners cryptographic-strength control over who can view and compute upon their data. Examples of such technologies include homomorphic encryption, multiparty computation and zero-knowledge proofs. Unfortunately, their programming complexity and performance overheads have necessarily limited their adoption. More performant and programmable solutions like trusted execution environments (TEEs) suffer from side channels within their implementation. In this poster is the first privacy-enhanced architectural instruction extension that supports both verified encrypted computation and safe data disclosures. The work implements a verified encrypted computation using a protected functional unit enclave that imbues the CPU with the ability to perform computation directly on encrypted personal data without any software or untrusted hardware having access to its plaintext or keys. It was built on the verified computation capability to provide safe data disclosures, where data owners can precisely specify what program values can be decrypted. In early experiments, they ran the privacy-enhanced VIP-Bench benchmarks and demonstrated that the proposed design slows native, unprotected computation approximately 1.6 times on average and is four to nine orders of magnitude faster than existing cryptographic approaches. Overall, preliminary results reveal that the design presents a compelling solution that combines the strong security of inefficient cryptography-based approaches and the high performance of more vulnerable TEEs.

12. Human-AI Teaming for Cyber Defense

Yinuo Du, Carnegie Mellon University

Autonomous agents powered by artificial intelligence (AI) are becoming more prevalent and capable in their abilities to collaborate with humans on interdependent tasks as teammates. Agents designed according to the principles of human cognition may capture human-like behavior. They may be better human collaborators than complex models that rely on large amounts of data. However, there is limited empirical work to test the impact of cognitive agents on teamwork. In this study, the effectiveness of two types of autonomous agents are compared: those that rely on simple heuristics to perform complex reasoning (heuristic-based) and those that rely on episodic memory to determine their collaborative actions (instance-based) with a random agent. The case of Human-AI cyber protection teams is used, leveraging the Input-Mediator-Output-Input model to systematically evaluate how the skill, knowledge and type of AI teammate impacts the team's interaction and outcomes. The skilled agents have a significant positive impact on the team monitoring and backup process and task performance compared to the random teammate. Instance-based agents are subjectively rated as more biased and less trustworthy than heuristic-based agents. It also was found that humans become more reactive to losses when paired with instance-based teammates than when paired with heuristic-based teammates. These novel findings are helpful in informing the intricacies involved in building effective AI teammates to collaborate with humans in complex adversarial tasks.

2024 WiCyS CONFERENCE STUDENT POSTERS

13. Privacy Preserving Publish for Electronic Health Records

Yu Duan, University of California, Irvine

We address the challenge of generating publishable electronic health records (EHR) based on authentic datasets containing personal information. Our chosen solution involves the integration of synthetic data into real datasets to modify the overall dataset's privacy level while preserving its utility. To achieve this, a generic framework was developed with the simultaneous goals of ensuring privacy, utility and similarity. The framework comprises three essential components: a synthesis module, a multi-filter module and a valid buffer. The quantification of privacy in the framework utilizes k-anonymity, and the synthesis module employs a generative model. The multi-filter module includes privacy, similarity and utility filters while the valid buffer serves as storage for valid synthetic data.The experimentation involves three EHR datasets with variations in disease, population and data size, employing tabular generative adversarial models. The results demonstrate the effectiveness, efficiency and generality of the proposed framework. Additionally, detailed evaluations for each round of implementation are presented, including the final round showcasing the framework's performance with various metrics from different perspectives. In conclusion, the proposed method emerges not only as a robust framework for generating publishable tabular datasets with multiple objectives but also as a comprehensive and detailed evaluation infrastructure for data synthesizers.

14. Fake Online Review Detection Using Advanced Language Models

Neha Gautam, Carnegie Mellon University

Fake online reviews present a substantial challenge for e-commerce platforms and consumers, motivating this research. Distinguishing between human-generated and computer-generated fake reviews, the study relies on established datasets like Amazon English reviews and Chinese Restaurant reviews. Employing advanced language models, GPT 3.5 generates Chinese reviews and Google Generative AI Palm 2 creates English reviews. The detection model utilizes GPT-Neo, specifically GPT-Neo 125M, coupled with Youden's J Statistics to optimize classifier thresholds.The research successfully demonstrates the efficacy of these models in detecting fake reviews, showcasing high accuracy, precision and recall rates for both English and Chinese datasets. Notably, GPT-Neo 125M outperforms a baseline model, Gambetti et al., particularly in Chinese reviews. To enhance future detection accuracy, the study recommends diversifying the training dataset, addressing biases toward short positive reviews with limited colloquial language. The findings underscore the significance of leveraging advanced language models and statistical metrics for robust fake review detection, emphasizing the need for ongoing improvements in training data to ensure the reliability and accuracy of detection systems.

15. Exposing New Denial of Service Vulnerability in Connection Establishment of Wi-Fi Systems

Naureen Hoque, Rochester Institute of Technology

To establish a secure Wi-Fi connection, several unprotected management frames are exchanged during a connection establishment (CE) phase between an access point and a station before they mutually authenticate each other and start a protected session. It is, therefore, possible for an adversary to spoof elements of those unprotected frames at the physical or MAC layers, facilitating additional attacks. In this work, it is the first to formally model and analyze this CE phase based on the latest IEEE 802.11 standard and, accordingly, expose a new denial of service (DoS) vulnerability. To validate the identified DoS vulnerability in the Wi-Fi CE phase, it is tested against the latest wpa supplicant daemon, showing that an adversary can stealthily prevent a station from connecting to a preferred AP for up to 90 minutes, likely more. The formal analysis and testbed validation codes were released to the community after it was responsibly disclosed to the Wi-Fi Alliance.

16. Toward a Lightweight Security Framework Using Blockchain and Machine Learning

Shereen Ismail, University of North Dakota

Cyberattacks pose a significant challenge to the security of internet of things (IoT) sensor networks, necessitating the development of robust countermeasures tailored to their unique characteristics and limitations. Various prevention and detection techniques have been proposed to mitigate these attacks. In this paper, an integrated security framework using blockchain (BC) and machine learning (ML) is proposed to protect IoT sensor networks. The framework consists of two modules: a BC prevention module and an ML detection module. The BC prevention module has two lightweight mechanisms: identity management and trust management. Identity management employs a lightweight smart contract (SC) to manage the node registration and authentication, ensuring that unauthorized entities are prohibited from engaging in any tasks while trust management uses a lightweight SC responsible for maintaining trust and credibility between sensor nodes throughout the network's lifetime and

2024 WiCyS CONFERENCE STUDENT POSTERS

tracking historical node behaviors. Consensus and transaction validation are achieved through a verifiable byzantine fault tolerance mechanism to ensure network reliability and integrity. The ML detection module uses LightGBM algorithm to classify malicious nodes and notify the BC network if it must make decisions to mitigate their impacts. The performance of several off-the-shelf ML algorithms were investigated, including Logistic Regression, Complement Naive Bayes, Nearest Centroid and Stacking, using the WSN-DS dataset. LightGBM is selected following a detailed comparative analysis conducted using accuracy, precision, recall, F1-score, processing time, training time, prediction time, computational complexity and Matthews Correlation Coefficient (MCC) evaluation metrics.

17. Unlocking VR Security: Identifying Vulnerabilities and Fortifying with Behavioral Biometrics

Sindhu Reddy Kalathur Gopal, University of Wyoming

The typing activity on VR devices is believed to be resistant to direct observation attacks since virtual screens in an immersive environment are not directly visible to others present in physical proximity. The presented video-based side channel attack, Hidden Reality (HR), shows that although a virtual screen in VR devices is not in direct sight of adversaries, indirect observations might get exploited to steal users' private information. The HR uses video clips of users' hand gestures while they type on the virtual screen to decipher the typed text in various key entry scenarios on VR devices including typed pins and passwords. Experimental analysis performed on a large corpus of 368 video clips shows that HR can successfully decipher an average of over 75% of the text inputs. High success rates of the attack model led to conducting a user study to understand the user's behavior and perception of security in VR. The analysis showed that over 95% of users were not aware of any security threats on VR devices and believed the immersive environments to be secure from digital attacks. In response to pressing security threats, the proposal is for HM-Auth, user-authentication system that harnesses users' intrinsic hand movement signatures captured by IMUs while entering passwords on VR devices. Rigorous testing conducted with 33 participants' data demonstrates HM-Auth's effectiveness, achieving high intra-user and low inter-user similarity scores, leveraging Siamese networks. Experiment results underscore HM-Auth's potential as a promising and secure authentication approach when compared to traditional knowledge and physiological-based authentication systems in VR devices.

18. Analyzing and Modeling Risks in the OSS Debian Supply Chain Through Network Propagation

Sahithi Kasim, Purdue University

Cybersecurity attacks, such as the solarwind attack, occur due to vulnerabilities in open-source software (OSS) supply chains. When developers reuse packages across different technical and social boundaries, they create complex hidden, socially bound technical structures of OSS supply chains that pose inherent risks. Packages depend on each other due to hidden build dependencies that are distinct from functional dependencies in the source code, making it difficult for the average developer to discern the risks associated with changes to certain packages. Such changes can propagate risks to other packages, making them vulnerable to attacks. Although there have been many studies on OSS, this study is one of the first to use network science methods to analyze the risks associated with OSS supply chains. The study aims to identify the position of a package in a network and how its centrality and coreness evolve over time. The results show that various measures yield varied results, indicating that different packages carry varying risks. There also are numerous underlying relationships between interdependencies and source packages that contribute to the risks.

19. Developing a More Robust Code Vulnerability Detecting Model

Marina Katoh, University of Tulsa

In order to minimize the number of vulnerabilities in software, several ML-based vulnerability detecting models have been introduced in recent years. While these models have shown to have a significant accuracy in detecting vulnerabilities in a given code, very little research has been conducted regarding the vulnerabilities these very models may have. In this poster, a set of tests are proposed that can be used to assess the robustness of vulnerability detecting models. Within this system, various transformations are applied to a given input code without changing its original functionality. For this study, a test on three state-of-the-art models was conducted and successfully decreased the accuracy of their vulnerability predictions by a significant amount. This indicates that the adversarial transformation can cause a vulnerability detector to misclassify a vulnerable code as invulnerable and vice versa. By better understanding the weaknesses of these models, more robust models that are defensive against malicious attacks can be developed.

2024 WiCyS CONFERENCE STUDENT POSTERS

20. Using Reinforcement Learning to Perform Vulnerability Analysis on a Simulated 5G Network

Katie Ketner, U.S. Naval Academy

Reinforcement learning is a machine-learning technique in which an agent learns by interacting with its environment through trial and error. For this project, the environment is a simulated 5G network built with modeling software, and the agent's goal is to find the most optimal attack vector or a way to compromise the network. The agent's behavior is directed by a reward calculation, which determines the positive or negative reward an agent receives after each action depending on how effective the action was at advancing the agent's progress toward its goal. For this specific application, the reward calculation factors in the attack vector's impact on confidentiality, integrity and availability. The reinforcement learning database is built using tactics and techniques from the MITRE 5G Hierarchy of Threats (FiGHT) framework. The MITRE FiGHT framework is a remodeling of the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK) framework and focuses on assessing the confidentiality, integrity and availability of 5G networks, weapon systems and networked devices. This project builds on previous research, applying reinforcement learning to defensive penetration testing but is unique in that it is focused on applying reinforcement learning for an offensive objective. 5G networks are a unique challenge to secure due to their emergence, applicability and scalability and will no doubt continue to be an issue to tackle in the coming years.

21. Empowering Cybersecurity Education: Designing a Capture the Flag Platform Using Kubernetes

Thea Kjeldsmark, University of California, Irvine

The potential of Capture the Flag (CTF) platforms is often confined by the issue of accessibility and complex setup. Most platforms are either closed-source or complicated to configure, which can be frustrating and time-consuming for organizers. This research addresses these issues by exploring the feasibility of designing a user-friendly and high-performing CTF platform that utilizes a container orchestration tool to manage users and challenges. The proposed Haaukernetes is an open-source CTF platform that uses Kubernetes, a container orchestration tool, to improve setup and container management while still maintaining high availability and security. Haaukernetes is designed by first outlining the advantages of choosing Kubernetes. Then, the different CTF concepts are mapped to Kubernetes concepts to provide a foundation for the architecture and design choices. Since CTF challenges involve vulnerable applications, network policies that isolate users are tested and examined. Different setup methods are discussed and conclude that Kubernetes provides additional flexibility, allowing various distribution methods. To understand the performance of Haaukernetes, performance tests were conducted, which indicate that the memory usage scales linearly with the number of users, demonstrating the platform's ability to handle increased user loads efficiently. Based on the architecture and results, Haaukernetes is compared to the open-source CTF platform Haaukins, which differs in not using a container orchestration tool. While Haaukernetes and Haaukins offer similar user functionalities, using Kubernetes allows the ability to add additional features and significantly reduce setup time and codebase complexity, which can empower more organizers to set up CTF events.

22. Exploring the Efficacy of DL Techniques for IoT IDS Using Vision Transformers

Beryl Lekaram and Samah Mansour, Grand Valley State University

Intrusion detection systems (IDS) play a crucial role in safeguarding networks from cyberattacks by identifying and analyzing malicious activities. Traditional machine-learning approaches have limitations in handling complex network traffic data, leading to suboptimal performance in intrusion detection. This study proposes a novel vision intrusion detection model based on the vision transformer (ViT) architecture to address these challenges. The proposed model is evaluated on a public intrusion detection dataset, CICIOT2023, achieving an accuracy of 91.67% and a recall rate of 90.86%. The experimental results demonstrate the effectiveness of the proposed model in intrusion detection. These findings underscore the potential of ViT-based approaches for intrusion detection tasks and pave the way for further advancements in IDS capabilities.

23. Exploring the Prevalence of Deepfake Media Among Politically Active Accounts on X

Sathwika Manda, Carnegie Mellon University

The rapid spread of misinformation and the uptick of interest in AI-generated content on the internet, particularly in social media, has proven to be a growing problem in recent years. Artificially generated media has the potential for great harm in dangerous propaganda or misinformation campaigns. One realm where artificial media has been used quite a lot is in politics. With the recent scandals related

2024 WiCyS CONFERENCE STUDENT POSTERS

to misinformation campaigns and the upcoming election, this issue is particularly relevant. The aim of this work is to determine the prevalence of and trends in deepfake media, specifically for politically active accounts on X (formerly Twitter), which are accounts that interact with more political content in general than an average control user. To accomplish this, fake X accounts were created with fake users and varying demographic information that interacted with eight sub-areas in politics while recording each account engagement. Four control accounts also were maintained that mimicked a non-politically active user. A deepfake detection tool was run on all the media encountered and noted which posts were flagged as being deepfake media. Statistical tests were then performed to examine whether politically active users encounter more deepfakes than general users and whether there is a difference in engagement metrics such as likes and shares between deepfake and non-deepfake media. The findings suggested a statistically significant positive trend between politically active accounts and deepfake encounters but little insight into differences in engagement metrics between posts containing deepfake media and posts that did not.

24. Identifying Bug Origins through Work Item Associations

Salome Perez, University of Nebraska-Lincoln

Several software engineering maintenance tasks require the ability to link a commit that introduced a bug with the commit that later fixed it. Existing approaches based on the original SZZ algorithm identify the potential commit that induced a bug when given a fixing commit as input. Inspired by prior work that introduced the notion of a work item as a logical grouping of commits, which could be a single unit of work toward addressing the implementation of an issue or feature, this work leverages the insight that a bug-inducing commit and its fix(es) represent a work item. In this context, the current understanding of how work items could impact the performance of SZZ-based algorithms that find the starting points of bugs is limited. To bridge this gap, a heuristic is proposed that, given an input commit, uses information from changed methods to identify related commits that form a work item with the input commit. Then a new variant of SZZ is built that leverages the work item-detecting heuristic to suggest bug-inducing commits. A manual evaluation is conducted to assess the accuracy of the heuristic in identifying work items and evaluating the approach on 821 repositories previously used to study the performance of SZZ. This evaluation shows an F1 score improvement ranging from 2% to 9%. The heuristic is then used to mine work item instances from different projects into a dataset that provides instances of work items related to JIRA labeled issues, grouped together based on an NLP-based scoring model.

25. MADEA: Malware Detection Architecture for IoT Using Traffic Analysis and Device Attestation

Renascence Tarafder Prapty, University of California, Irvine

Internet of things (IoT) devices are vulnerable to malware and require new mitigation techniques due to their limited resources. To this end, some prior work focused on periodic measurement of IoT devices via remote attestation (RA) while other efforts considered traffic analysis (TA) to identify suspicious or anomalous events in the network traffic that might indicate malware activities. Neither approach by itself is a complete solution: RA is costly if done frequently (it is unclear how to schedule it optimally) while TA merely raises suspicion of malware presence without confirming it. To solve this, MADEA was designed, the first system that blends RA and TA to offer a comprehensive approach to malware detection for the IoT ecosystem. Extensive experiments were performed with tens of typical smart home devices, their network traffic was analyzed and showed that IoT devices' traffic patterns are limited and predictable but also differ significantly from the patterns exhibited when malware is present. MADEA's design builds upon this key observation. TA builds profiles of expected packet traces during the benign operation of each device and then uses them to detect malware in network traffic in real-time. An anomaly detected by TA further triggers RA for the suspected device, which in turn confirms the presence or absence of malware on the device. MADEA achieves 100% true positive rate. It also outperforms other approaches with 160 times faster detection time and, for a 1.84-watt camera, it can save at least 26 watt hours of power yearly consumed for periodic malware detection.

2024 WiCyS CONFERENCE STUDENT POSTERS

26. Investigating User Photo Privacy Settings on Instagram: Two User Interview Studies

Katherine Garcia, Old Dominion University

Social networking services (SNS), such as Instagram and Facebook, are well known for their photo-sharing capabilities. However, the concern of photo privacy arises, such as who can view photos and which users are included in posts. While photo privacy settings on SNS provide some options for how users can share photos, their effectiveness is dependent upon users being aware of and understanding these settings. To better grasp users' understanding of these photo privacy settings, two studies were conducted, including structured interviews with Instagram users. In Study 1, 16 users were interviewed about their personal use of SNS, knowledge of Instagram, current privacy settings and perspectives on SNS privacy. Results showed that users who had multiple accounts were aware of more settings than those with a single Instagram account. In Study 2, another nine users were interviewed, all of whom had multiple Instagram accounts. The results were similar to Study 1 - users were aware of the majority of the privacy settings, especially the earlier features such as setting their account to public or private. Overall, conflict between users over a posted photo was uncommon. It was discovered that when users were unsure of their setting state, they assumed it was the default. However, the default settings on SNSs usually promote information sharing rather than privacy. These results suggest that SNS designers should make newer privacy settings intuitive and apparent to users and promote default photo-sharing settings that protect users' privacy.

27. Evidence of Cognitive Biases in CyberAttackers from An Empirical Study

Saeefa Rubaiyet Nowmi, University of Texas, El Paso

In this study, the work aimed to identify cognitive biases exhibited by cyberattackers in the study by Aggarwal et al (2021). Specifically, it was investigated whether attackers displayed a preference for targeting systems located in specific areas of the network as well as investigated any discernible behavioral patterns such as consistently attacking the same system in every round (Default Setting Bias) or persistently targeting a particular system despite previous failures (sunk-cost fallacy). The results show evidence for the default effect and sunk-cost fallacy in the decision-making processes of human attackers and suggest that they can have significant implications for the effectiveness of the cyber defense. This study provides valuable insights for the development of targeted interventions and countermeasures in cyber defense.

28. Leveraging Intelligence Intrusion Detection through XGBoost Algorithm

Shahrzad Sayyafzadeh, Florida A&M University

The escalating complexity of cyberthreats requires advanced intrusion detection systems that can proactively identify potential security breaches. This paper presents an innovative approach to intrusion detection using the XGBoost algorithm, a powerful machine-learning technique known for its robust performance in classification tasks. By leveraging XGBoost's gradient boosting framework, they aim to enhance the accuracy and efficiency of intrusion detection systems. They demonstrate the effectiveness of their approach in accurately detecting intrusion instances. The results underscore the potential of XGBoost as a reliable tool for building intelligent intrusion detection systems that can amplify network security and minimize the risk of cyberthreats.

29. Black Box Entropy Estimation

Svettlira Van Jakovich, Texas A&M University, College Station

Random numbers are essential in cryptographic systems to guarantee the security of sensitive information. However, research has demonstrated that some deployed systems may lack adequate randomness in their entropy source outputs, leading to potential compromises of cryptographic keys. This research investigates the importance of quantum security and high-quality entropy in cryptographic applications. It evaluates Qrypt's Quantum Entropy Service as a potential solution for addressing post-quantum cryptographic vulnerabilities. The research steps include exploring post-quantum cryptography, investigating NIST publications for entropy assessment best practices, examining approaches for generating randomness, assessing the entropy of Qrypt's Quantum Entropy Service, and evaluating the effectiveness of Qrypt's proposed solution.

2024 WiCyS CONFERENCE SPEAKER INDEX

KEYNOTE SPEAKERS

NAME	AFFILIATION	DATE AND TIME
Deborah Frincke	Sandia National Laboratories	Saturday Morning Keynote
Esmeralda lyescas	Collins Aerospace	Friday Dinner Keynote
Kimberly Becan	Fortinet	Friday Lunch Keynote
Lisa Einstein	Cybersecurity and Infrastructure Security Agency (CISA)	Friday Morning Keynote
Morgan Adamski	National Security Agency (NSA)	Friday Lunch Keynote

FEATURED SPEAKERS

NAME	AFFILIATION	DATE AND TIME
Rutu Vijaysinh Ataliya	Amazon Web Services	Saturday Morning Keynote
Nicole Becher	Google	Friday Dinner Keynote
Robyn Frye	Workday	Friday Lunch Keynote
Divya Ghatak	SentinelOne	Friday Lunch Keynote
Laketta Hawkins	Cisco	Saturday Morning Keynote
Carly Jackson	NIWC Pacific	Friday Dinner Keynote
Ann Johnson	Microsoft	Friday Morning Keynote
Ayesha Khalid	Mastercard	Saturday Morning Keynote
Carrie Mills	Southwest Airlines	Saturday Morning Keynote
Ebony Smith	Walmart	Friday Morning Keynote
Diane Tracy	Vanguard	Friday Lunch Keynote
Jaidie Vargas	Lockheed Martin	Friday Dinner Keynote

PROGRAM SPEAKERS

NAME	AFFILIATION	DATE AND TIME
Morgan Adamski	Cybersecurity Collaboration Center	Thursday, 12:30pm - 1:30pm
Dalal Alharthi	University of Arizona	Saturday, 2:30pm - 4:30pm
Abigail Allen	US Dept. of Labor, Office of Apprenticeship	Saturday, Noon - 12:45pm
Dawn Armstrong	HumanGood	Saturday, Noon - 12:45pm
Kshitiz Aryal	Tennessee Technological University	Thursday, 4:30pm - 6:30pm
Michael Barcomb	SANS Institute	Thursday, 4:30pm - 6:30pm
Toni Benson	Cybersecurity and Infrastructure Security Agency	Friday, 3:50pm - 4:40pm
Lisa Beury-Russo	Cybersecurity and Infrastructure Security Agency	Saturday, Noon - 12:45pm
Paula Biggs	Alliance Cyber	Thursday, 4:30pm - 5:15pm
Debby Briggs	Netscout Systems, Inc.	Saturday, 10:00am - 10:45am
Caitlin Buckshaw		Friday, 1:55pm - 2:40pm
Shir Butbul	Echelon Risk + Cyber	Friday, 1:55pm - 2:40pm
Alissa Butcher	Northwood University	Saturday, 11:00am - 11:45am
Khensani Carter	Tenable	Saturday, Noon - 12:45pm
Kareem Chavez-Escobedo	University of Texas, Austin	Saturday, 10:00am - 10:45am
Lynne Clark	NSA	Friday, 3:50pm - 4:40pm
Midori Connolly	Cyderes	Thursday, 2:00pm - 2:45pm
Jennifer Cox	Tenable	Saturday, Noon - 12:45pm
Jenny Daugherty	DARK Enterprises, Inc.	Saturday, 11:00am - 11:45am
Tashya Denose	Meta	Friday, 11:00am - 11:45am

2024 WiCyS CONFERENCE
SPEAKER INDEX

PROGRAM SPEAKERS

NAME	AFFILIATION	DATE AND TIME
Ryan Donaghy	Cybersecurity and Infrastructure Security Agency	Saturday, Noon - 12:45pm
Meghan Donohoe	Cisco	Friday, 11:00am - 11:45am
Suzanne Dove	Lockheed Martin	Saturday, 2:30pm - 4:30pm
Mary DuBard	New York Times	Thursday, 2:00pm - 4:00pm
Snezhana Dubrovskaya	IBM	Thursday, 2:00pm - 4:00pm
Carolyn Ellis	Arizona State University	Friday, 3:50pm - 4:40pm
Amelia Fisher	Echelon Risk + Cyber	Friday, 1:55pm - 2:40pm
Madison Fox	Cisco	Thursday, 2:00pm - 4:00pm
Bri Frost	Pluralsight	Friday, 4:45pm - 5:30pm
Sheikh Ghafoor	National Science Foundation	Thursday, 7:30pm - 8:15pm
Bella Gomez	Washington University, St. Louis	Saturday, 10:00am - 10:45am
Joanna Grama	Vantage Technology Consulting Group	Friday, 3:50pm - 4:40pm
Rebecca Granger	Alliance Cyber	Thursday, 4:30pm - 5:15pm
Lydia Graslie	Edward Jones	Friday, 1:55pm - 2:40pm
Ashley Greeley	Government	Thursday, 6:30pm - 7:15pm Thursday, 7:30pm - 8:15pm Friday, 3:50pm - 4:40pm
Maanak Gupta	Tennessee Technological University	Thursday, 4:30pm - 6:30pm
Elaine Harrison-Neukirch	Scythe	Friday, 2:50pm - 4:40pm
Elizabeth Hawthorne	Rider University	Thursday, 12:30pm - 1:30pm
Cynthia Hetherington	Hetherington Group	Thursday, 2:00pm - 4:00pm
Saskia Hoffmann		Friday, 4:45pm - 5:30pm
Heather Holliday	Holliday Communications	Friday, 4:45pm - 5:30pm
Muhammad Ismail	Tennessee Technological University	Saturday, 2:30pm - 4:30pm
Chandler Jackson	Amazon Web Services	Thursday, 5:30pm - 6:15pm
Prajakta Jagdale	Palo Alto Networks	Saturday, Noon - 12:45pm
Jessie Jamieson	Tenable	Saturday, Noon - 12:45pm
Ann Jones	Sentara Health	Saturday, 11:00am - 11:45am
Jaclyn Justice	Women in Cybersecurity (WiCyS)	Friday, 1:55pm - 2:40pm Saturday, 11:00am - 11:45am
Michelle Kababik	Verizon	Thursday, 3:00pm - 3:45pm
Megan Kaczanowski	Clear	Friday, 2:50pm - 4:40pm
Rachel Kang	Aon	Saturday, 10:00am - 10:45am
Karen Karavanic	National Science Foundation	Thursday, 7:30pm - 8:15pm
Deborah Kariuki	University of Maryland Baltimore County	Thursday, 12:30pm - 1:30pm
Haley Kim	Naval Facilities Engineering Systems Command	Saturday, 10:00am - 10:45am
Laura Knowles	OPM SFS	Thursday, 6:30pm - 7:15pm
Arica Kulm	Dakota State University	Thursday, 2:00pm - 4:00pm
Rita Law	Weight Watchers	Thursday, 2:00pm - 4:00pm
David Leathers	Tennessee Technological University	Saturday, 2:30pm - 4:30pm
Lily Lee	Splunk	Saturday, 11:00am - 11:45am
Angel Liu	Confluent	Friday, 2:50pm - 4:40pm
Francesca Lockhart	University of Texas, Austin	Saturday, 10:00am - 10:45am

2024 WiCyS CONFERENCE
SPEAKER INDEX

PROGRAM SPEAKERS

NAME	AFFILIATION	DATE AND TIME
Leilia MacNeil	Bank Iowa	Saturday, Noon - 12:45pm
Norah Maki	Cybersecurity and Infrastructure Security Agency	Friday, 1:55pm - 2:40pm
Laura Malave	St. Petersburg College	Friday, 1:55pm - 2:40pm
Meghan Martinez	CyberTrust Massachusetts	Saturday, 10:00am - 10:45am
Muta Mashack	Tenable	Saturday, Noon - 12:45pm
Shannon McHale	Google Public Sector	Thursday, 12:30pm - 1:30pm Saturday, 10:00am - 10:45am
Zabrina McIntyre	KPMG	Friday, 11:00am - 11:45am
Marian Merritt	NICE at NIST	Friday, 3:50pm - 4:40pm
Seeyew Mo	ONCD	Friday, 2:50pm - 3:40pm
Megan Moloney	Guidehouse	Friday, 11:00am - 11:45am
Darla Montgomery	Naval Facilities Engineering Systems Command	Saturday, 10:00am - 10:45am
Barbara Mooneyhan	Woebot Health	Friday, 11:00am - 11:45am
Ossie Munroe	Bloomberg	Thursday, 12:30pm - 1:30pm
Kelly Murray	Cybersecurity and Infrastructure Security Agency	Saturday, Noon - 12:45pm
Priya Nath	Workday	Thursday, 4:30pm - 6:30pm
Yasmeen Natzle	Lockheed Martin	Saturday, 2:30pm - 4:30pm
Nicole Nichols	Palo Alto Networks	Saturday, Noon - 12:45pm
Quiana Oates	Women in Cybersecurity (WiCyS)	Friday, 11:00am - 11:45am Saturday, 11:00am - 11:45am
Adebunmi Odefunso	Athenahealth Inc.	Saturday, 2:30pm - 4:30pm
Abigail Ojeda	Akamai Technologies	Saturday, 10:00am - 10:45am
Akhirah Padilla	NSA	Thursday, 7:30pm - 8:15pm
Sasmita Panda	Tenable	Saturday, Noon - 12:45pm
Christina Papadimitriou	Palo Alto Networks	Saturday, Noon - 12:45pm
Jigisha Pardanani	Ally	Saturday, 11:00am - 11:45am
Susan Paskey	Cisco	Friday, 11:00am - 11:45am
Pinal Patel	Verizon	Thursday, 3:00pm - 3:45pm
Quintana Patterson	Women in Cybersecurity (WiCyS)	Friday, 2:50pm - 4:40pm Saturday, 10:00am - 10:45am
Alessandra Perotti	CVS Health	Thursday, 4:30pm - 6:30pm
Deirdre Peters	Lockheed Martin	Saturday, 2:30pm - 4:30pm
Ashley Podhrasky	Dakota State University	Thursday, 2:00pm - 4:00pm
Chloe Potsklan	NBCUniversal	Friday, 2:50pm - 4:40pm
Lopamudra Praharaj	Tennessee Technological University	Thursday, 4:30pm - 6:30pm
FNU Prashasti	New York Times	Thursday, 2:00pm - 4:00pm
Warren Proctor	Tennessee Technological University	Thursday, 12:30pm - 1:30pm
Jenny Radcliffe	Human Factor Security Ltd	Friday, 11:00am - 11:45am
Carolyn Renick	U.S. Department of Labor, Veterans' Employment and Training Service	Friday, 3:50pm - 4:40pm
Tracey Ristich	The Diana Initiative	Saturday, 11:00am - 11:45am
Nikki Robinson	IBM	Thursday, 2:00pm - 4:00pm
Petra Robinson	Louisiana State University	Saturday, 11:00am - 11:45am

2024 WiCyS CONFERENCE SPEAKER INDEX

PROGRAM SPEAKERS

NAME	AFFILIATION	DATE AND TIME
Kristen Rodriguez	Mount San Antonio College	Saturday, Noon - 12:45pm
Loren Rosario-Maldonado	Cultura, Inc.	Thursday, 2:00pm - 4:00pm
Rachel Russo Gaiser	Cybersecurity and Infrastructure Security Agency	Friday, 1:55pm - 2:40pm
Anastasiya Rutus	You Deserve Rest LLC	Friday, 4:45pm - 5:30pm
Caitlin Sarian	Cybersecurity Girl	Saturday, 11:00am - 11:45am
Jerusha Sejera	Verizon	Thursday, 3:00pm - 3:45pm
Katie Shuck	State of South Dakota	Thursday, 2:00pm - 4:00pm
Kainaat Singh	Intel Corporation	Saturday, 2:30pm - 4:30pm
Ashley Smyk	AWS	Friday, 2:50pm - 3:40pm
Diane Stephens	University of Georgia	Thursday, 4:30pm - 6:30pm
Audra Streetman	Splunk	Thursday, 12:30pm - 1:30pm
Lillian Teng	Capital One	Thursday, 12:30pm - 1:30pm
Hanna Terletska	Middle Tennessee State University	Saturday, 2:30pm - 4:30pm
Renata Uribe	Echelon Risk + Cyber	Saturday, 10:00am - 10:45am
Jaidie Vargas	Lockheed Martin	Saturday, 2:30pm - 4:30pm
Mimi Vertrees	Tennessee Technological University	Friday, 11:00am - 11:45am
Daniela Villalobos	Echelon Risk + Cyber	Saturday, 10:00am - 10:45am
Michelle Wagner	DocuSign	Friday, 11:00am - 11:45am
Moriah Walker	Lakota Local Schools	Saturday, 11:00am - 11:45am
Michelle Wan	Workday	Thursday, 4:30pm - 6:30pm
May Wang	Palo Alto Networks	Saturday, Noon - 12:45pm
Tobi West	Coastline College	Saturday, Noon - 12:45pm
Christopher Wilkes	SANS Institute	Thursday, 4:30pm - 6:30pm
Donna Woods	Moreno Valley USD	Saturday, Noon - 12:45pm
Iris Ye	University of Michigan	Friday, 4:45pm - 5:30pm
Lily Yeoh	C1Risk	Friday, 2:50pm - 4:40pm
Paige Zaleppa	Towson University	Saturday, 11:00am - 11:45am
Jingdi Zeng	DeVry University	Saturday, 10:00am - 10:45am
Linxi Zhang	Central Michigan University	Saturday, 11:00am - 11:45am

Adobe

Learn how we help you build more trusted user experiences

Subscribe to our newsletter.

www.adobe.com/go/securitynews

AON

Cyber Security Consulting Roles

Digital Forensics, Incident Response, Penetration Testing, Security Advisory Services, and More

What We Do

At Aon we help clients manage the full lifecycle of their cyber journey and manage the total cost of risk for sustainable cyber resilience. We serve as trusted advisors in managing risk, helping clients make decisions with clarity and confidence in a complex risk environment. When security incidents happen, we are on the front lines, managing an organization's response to some of the most complex cyber breaches in the world.

Aon is the only team that has the scope and breadth of services to support clients in every area of the cyber lifecycle. We specialize in cyber risk management consulting in the areas of digital forensics, incident response, proactive risk advisory consulting, penetration testing, threat intelligence, investigations, and cyber insurance.

If you want to work on some of the highest profile, most challenging and sophisticated cases out there, we want to hear from you. The team works closely together to ensure learning, growth and career development. And we invest in you through mentorships, educational opportunities, as well as providing the ability to attend networking and security training conferences.

Join our team, visit jobs.aon.com/jobs and search "cyber" to apply today!

Digital Forensics and Incident Response

Solving cyber events

Respond to the incident, create an investigation strategy, contain the incident while preserving evidence, and confidently communicate with stakeholders.

Security Advisory

Identifying security weaknesses

Evaluate and remediate vulnerabilities, determine readiness to respond, and improve cyber resilience.

Testing

Illuminating system vulnerabilities

Leverage real-world testing and simulations to help clients better understand their weaknesses and strengthen their defenses.

Investigations and Intelligence

Using knowledge to empower

Help protect clients by applying traditional investigative techniques to the digital environment.

Quantification

Optimizing total cost of risk

Model cyber loss scenarios and stress test current insurance limits to enhance client risk financing strategies.

Cyber Insurance

Securing the future

Balance sheet protection from the financial impact of a cyber incident.

Open Roles

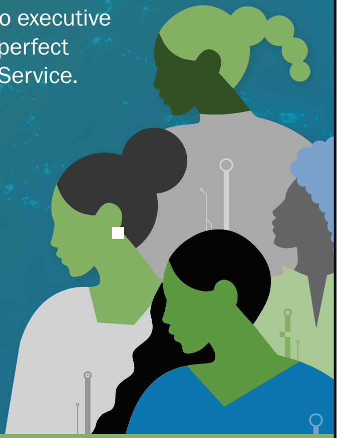
Aon is looking for cyber security professionals with the following skillsets and experience:

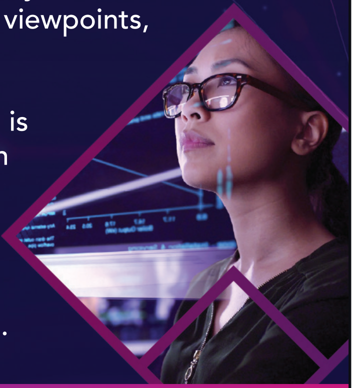
- Forensic computer analysts
- Penetration testers
- Incident responders
- IT security engineers
- Information security analysts
- Security architects
- Fraud examiners
- Security risk consultants
- Investigators
- Forensic accountants
- Governance and risk management professionals
- Privacy professionals
- Evidence technicians
- Brokers
- And more

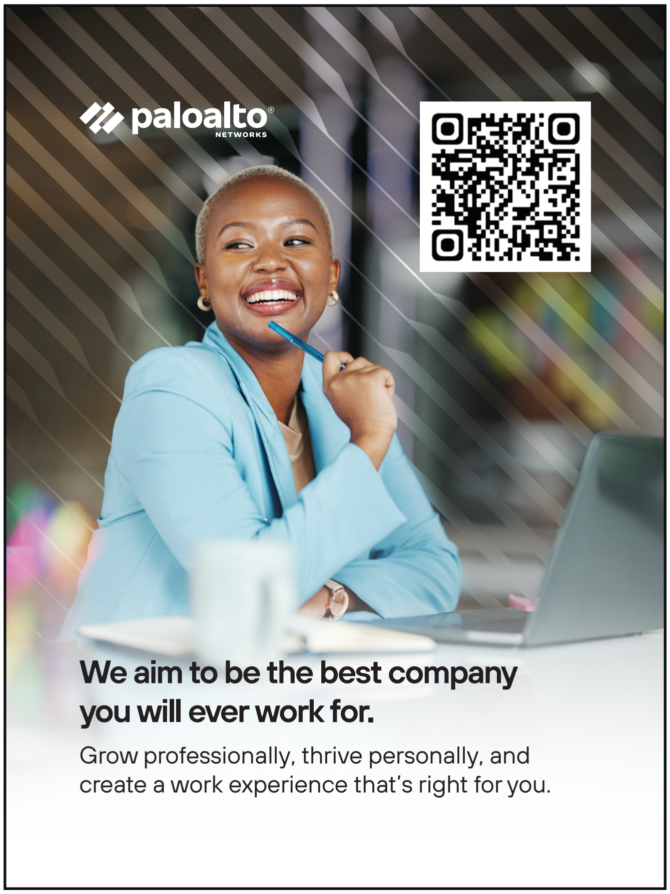
BANK OF AMERICA

BE A GAME CHANGER

We believe the next innovation
can come from you.







Being a leading retailer takes a leading Cybersecurity team.

The secret to delivering that one-of-a-kind Target magic? A safe and secure shopping experience where guests can discover all the joy Target has to offer. That's where our in-house team of industry-recognized cybersecurity experts comes in. They keep Target and our guests protected 24/7 against cybercriminals and fraudsters using industry-leading tools, a proactive threat intelligence program and Cyber Fusion Center to investigate and respond to threats so our guests can shop when and how they want — easily and securely.

Learn more & explore opportunities at tech.target.com.

CEROC

Cybersecurity Education, Research and Outreach Center

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

- NCAE-C Center of Academic Excellence –CyberDefense
- First and Largest CyberCorps SFS program in the State of TN
- Only DoD Cyber Scholarship (CySP) program in TN
- CyberEagles and WiCyS student cybersecurity clubs
- WiCyS Conference–Founding Institution and First Student Chapter
- GenCyber Camp and GenCyber on Wheels Programs
- Cyber Interest Groups in CTF, Defense, and Offensive Security

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

CEROC Info

CS Graduate Info

we're hiring

careers.tiktok.com

TikTok's Global Security Organization provides a comprehensive suite of shared services to protect our most critical assets by securing our people, processes, and technology. If you're looking for your next challenge, we'd love to hear from you!

THE UNIVERSITY OF RHODE ISLAND

SECURE YOUR CAREER

WITH A MASTERS IN CYBERSECURITY

Apply to the University of Rhode Island's Professional Science Masters Degree in Cybersecurity

- *Fully online & asynchronous*
- *Full and part-time options available*
- *Scholarships available*
- *National Center of Academic Excellence in Cybersecurity*

dfcsc.uri.edu/psm

wayfair

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.

ZEBRA

Build your edge. Build what's next.

Join a community of changemakers, innovators, and doers. Join Zebra.

We're Hiring!

View Zebra Technologies openings at www.zebra.com/careers

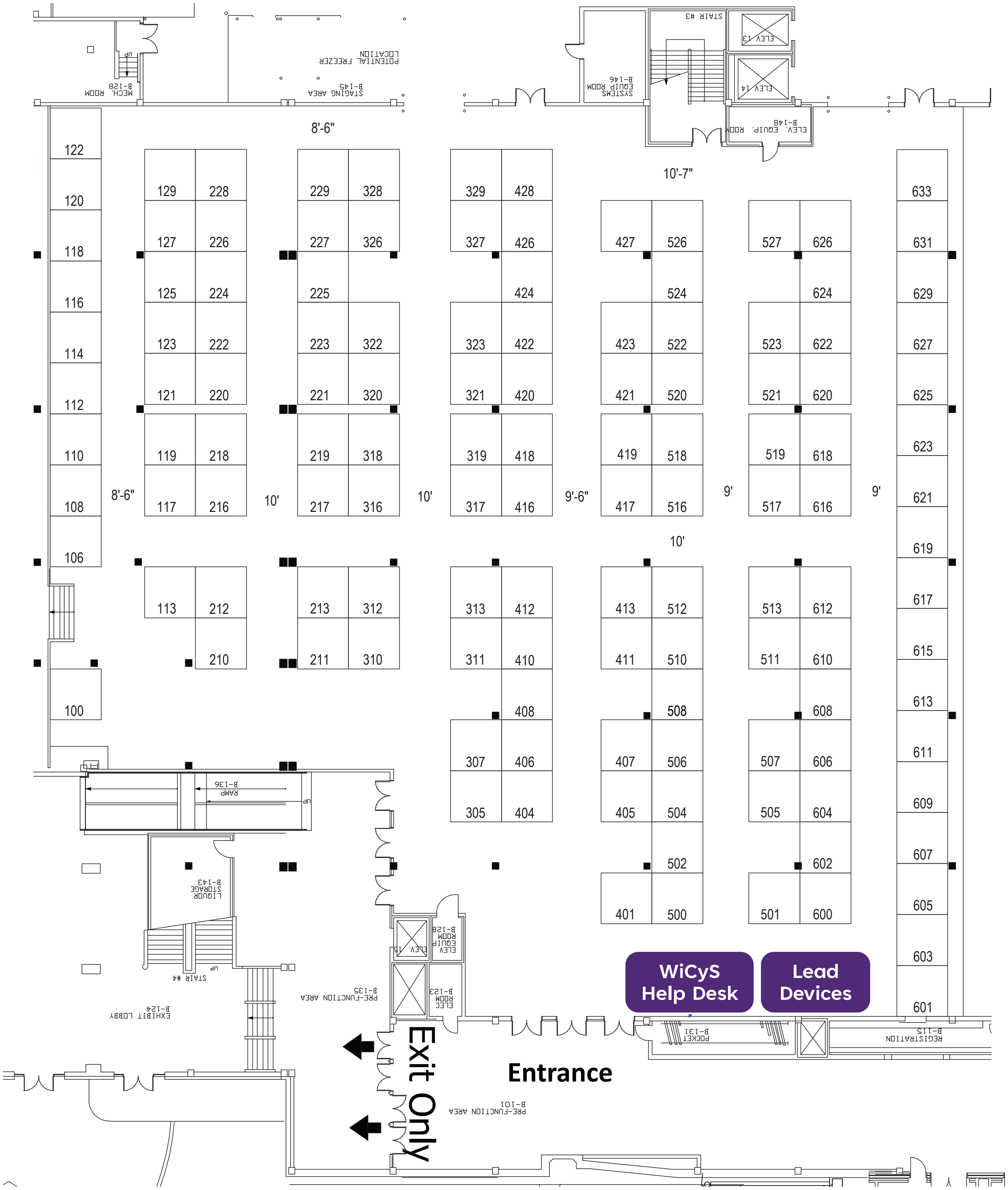
VISIT THE CAREER FAIR

ORGANIZATION	BOOTH #
Activision Publishing Inc	606
Adobe	613
Amazon Web Services	311/313
American Airlines	610
American Express	617
Aon Cyber Solutions	612
Aristocrat	219
Asurion	424
Bank of America	619
Battelle	618
Bloomberg	505/507
Brown Brothers Harriman & Co	No Booth
Capital One	No Booth
Carnegie Mellon University Information Networking Institute	321
Carnegie Mellon University Software Engineering Institute	317/319
Champlain College	621
Check Point Software Technologies, Inc.	412
Cybersecurity and Infrastructure Security Agency (CISA)	600/602
Cisco	511/513
Corelight	623
CrowdStrike, Inc.	519
Center for Systems Security and Information Assurance (CSSIA)	117
Dakota State University - CybHER	329
Dell Technologies	520
Deloitte Services LP	516/518
DeVry University	420/422
ECS Federal LLC	501
Envestnet Financial Technologies, Inc.	625
EY	223
FanDuel	627
Florida International University	522
Ford Motor Company	601/603
Fortinet	405/407
Google	210/212
Grainger	629
Haiku, Inc.	No Booth
Huntington National Bank	113
IBM	218
Idaho National Laboratory	631
Infosec	622
International Information Systems Security Certification Consortium (ISC2)	323
Johns Hopkins University School of Advanced International Studies (SAIS)	620
Keyfactor	225
L2 Cyber Solutions	624
Lockheed Martin	305/307
Mastercard	504/506
McDonald's	220
Microsoft	316/318
MIT Lincoln Laboratory	222
MITRE (The MITRE Corporation)	217
MorganFranklin Consulting	119
Motorola Solutions	421
National Renewable Energy Laboratory (NREL)	121
National Security Agency	211/213
NIWC Pacific	417/419
NCyTE Center at Whatcom Community College	221
Nestlé IT	106
NICE	524
North Carolina State University	108
Northeastern University Khoury College of Computer Sciences	426
NuHarbor Security, Inc.	428
Oak Ridge National Laboratory	328
Okta	609/611
Old Dominion Unversity	227
Optum	No Booth
Pacific Northwest National Laboratory	229
Palo Alto Networks	508
Phylum	No Booth
Proofpoint	224
Protect AI	110
Rider University	527 (POD)
Rochester Institute of Technology	114
RTX	500/502
Sandia National Labs	401
SANS Institute	326
Sealing Technologies, Inc.	123
Security Risk Advisors	125
SentinelOne	310/312
ServiceNow	616

VISIT THE CAREER FAIR

ORGANIZATION	BOOTH #
Southwest Airlines	416/418
SpecterOps	228
SWIFT	116
Target	112
Tenable	118
Tennessee Tech University - CEROC	615
TikTok	100
Towson University	427
Toyota	120
Trail of Bits	122
U.S. Army Cyber Command	521/523
U.S. Dept of Homeland Security Cybersecurity Service (DHS)	604
University of Cincinnati School of Information Technology	527 (POD)
University of Colorado, Colorado Springs	423
University of Rhode Island	608
University of Washington Bothell	626
University of Washington-Tacoma	605/607
Vanguard	411/413
Verizon	320/322
Victoria's Secret & Co	129
Walmart	510/512
Wayfair	No Booth
Wentworth Institute of Technology	127
Worcester Polytechnic Institute	226
Workday	408/410
Zebra Technologies	517

VISIT THE CAREER FAIR



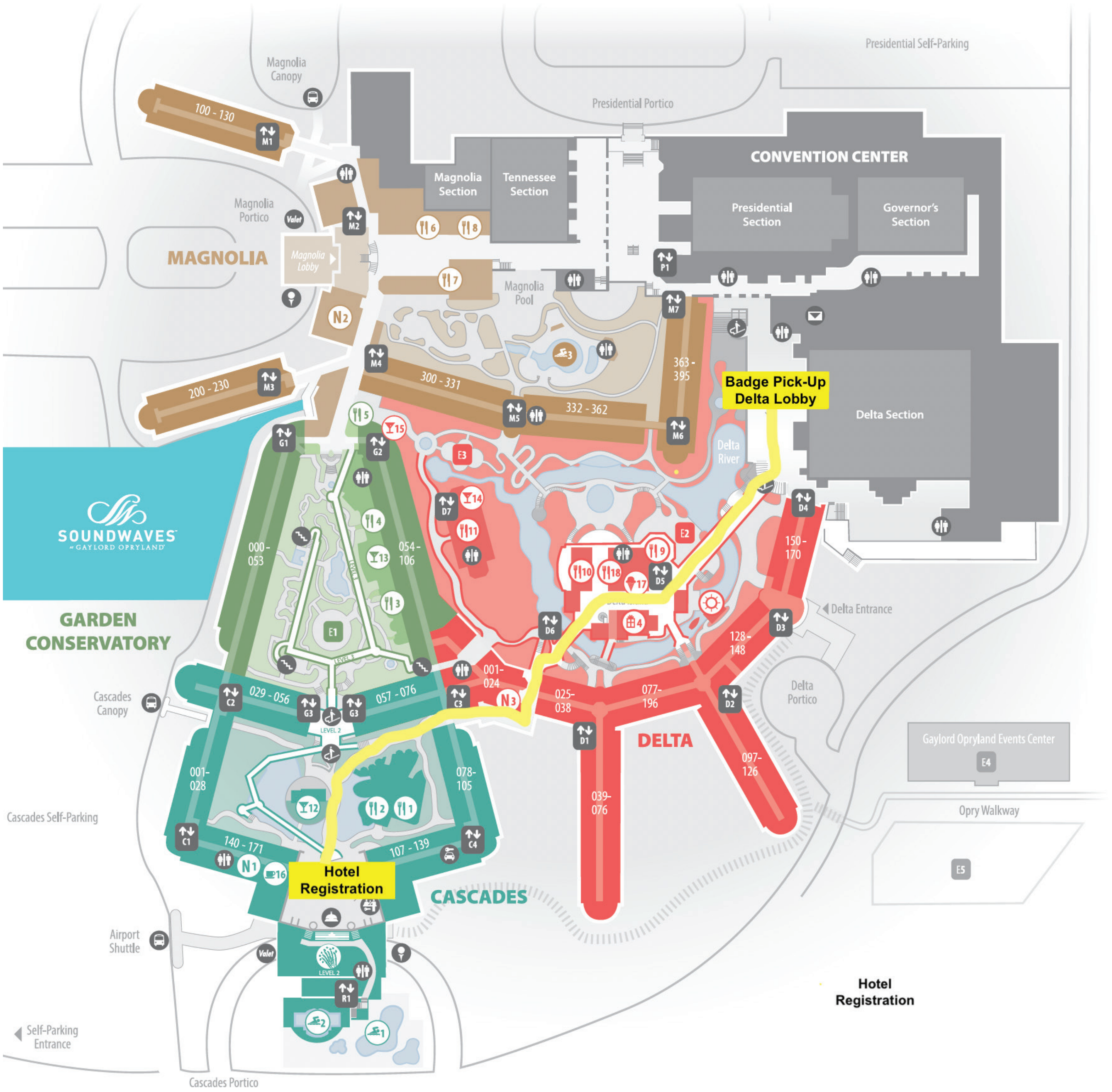
EVENTS, TRAVEL AWARDS & SPECIAL ITEMS

THANK YOU SPONSORS

ORGANIZATION	ITEM(S)
Amazon Web Services	Scholarships with Travel
Bloomberg	Male Allyship Breakfast, Military Breakfast, Senior Leader Luncheon, Selfie Station and Scholarships with Travel
Carnegie Mellon University Software Engineering Institute	Scholarships with Travel
Cisco	Conference Bag and Scholarships with Travel
Deloitte Services LP	Scholarships with Travel
DeVry University	Early Career Breakfast and Scholarships with Travel
Envestnet Financial Technologies, Inc.	Scholarship with Travel
Ford Motor Company	Headshots and Scholarships with Travel
Fortinet	Conference Shirt and Scholarships with Travel
Google	Scholarships with Travel
International Information Systems Security Certification Consortium (ISC2)	Scholarships with Travel
Lockheed Martin	Scholarships with Travel
Mastercard	Scholarships with Travel
Microsoft	Scholarships with Travel
Microsoft Philanthropies	Scholarships with Travel
MorganFranklin Consulting	Scholarship with Travel
NIWC Pacific	Scholarship with Travel
National Security Agency	Scholarships with Travel
National Cybersecurity Training and Education Center (NCyTE)	Scholarships with Travel
Okta	Scholarships with Travel
Optum	Friday Lunch, Military Breakfast and Scholarships with Travel
Phylum	Scholarships with Travel
RTX	Scholarships with Travel
Sealing Technologies, Inc.	Scholarships with Travel
SentinelOne	Lanyard and Scholarships with Travel
ServiceNow	Mid-Career Breakfast
Southwest Airlines	Scholarships with Travel
Target	Scholarships with Travel
TwoSigma	Scholarship with Travel
TZP Cares Foundation	Scholarships with Travel
Vanguard	Scholarships with Travel
Verizon	Scholarships with Travel
Walmart	Scholarships with Travel
Workday	Scholarships with Travel
Zebra Technologies	Scholarship with Travel

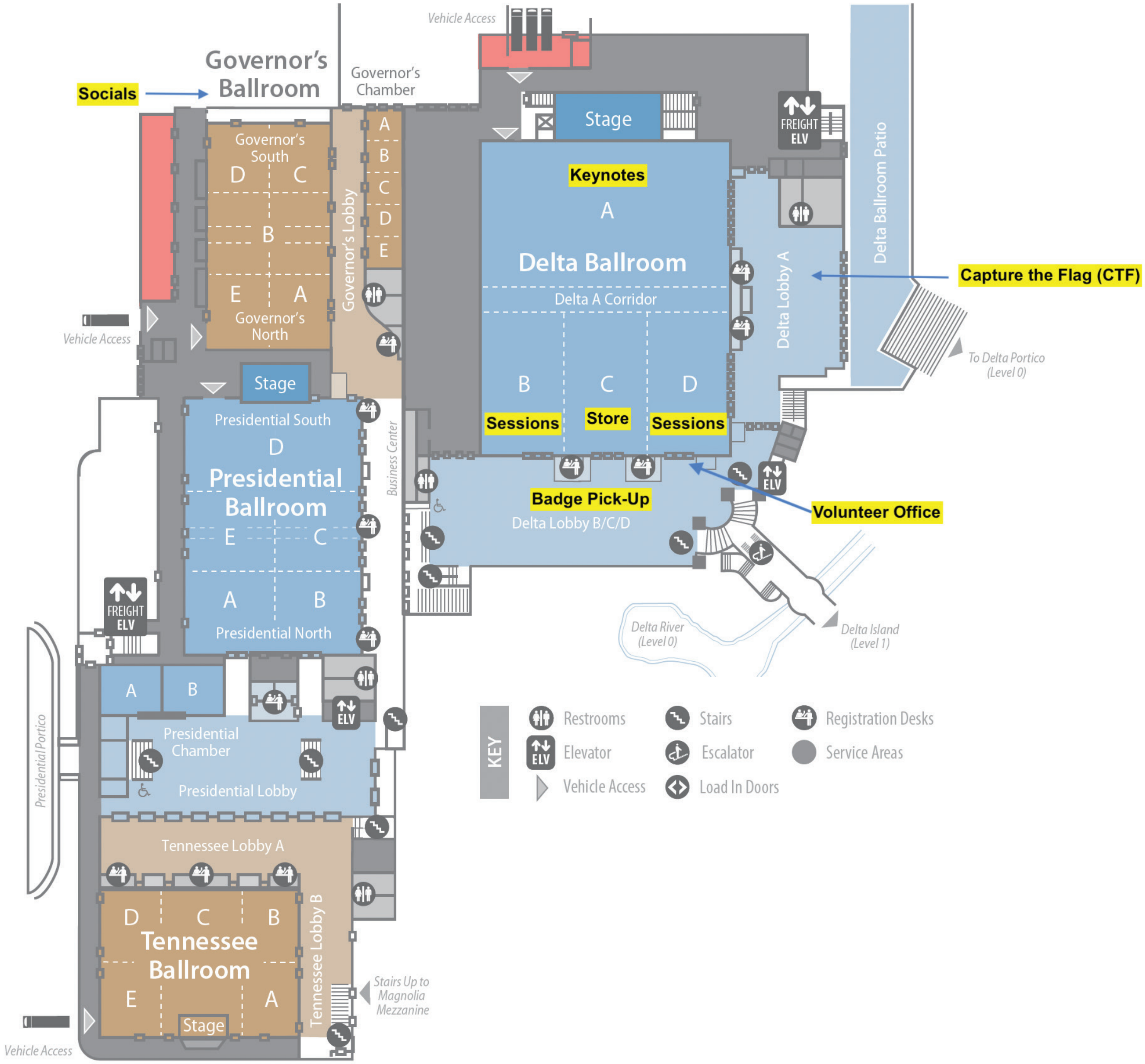
2024 WiCyS CONFERENCE VENUE MAPS

GAYLORD CONVENTION CENTER



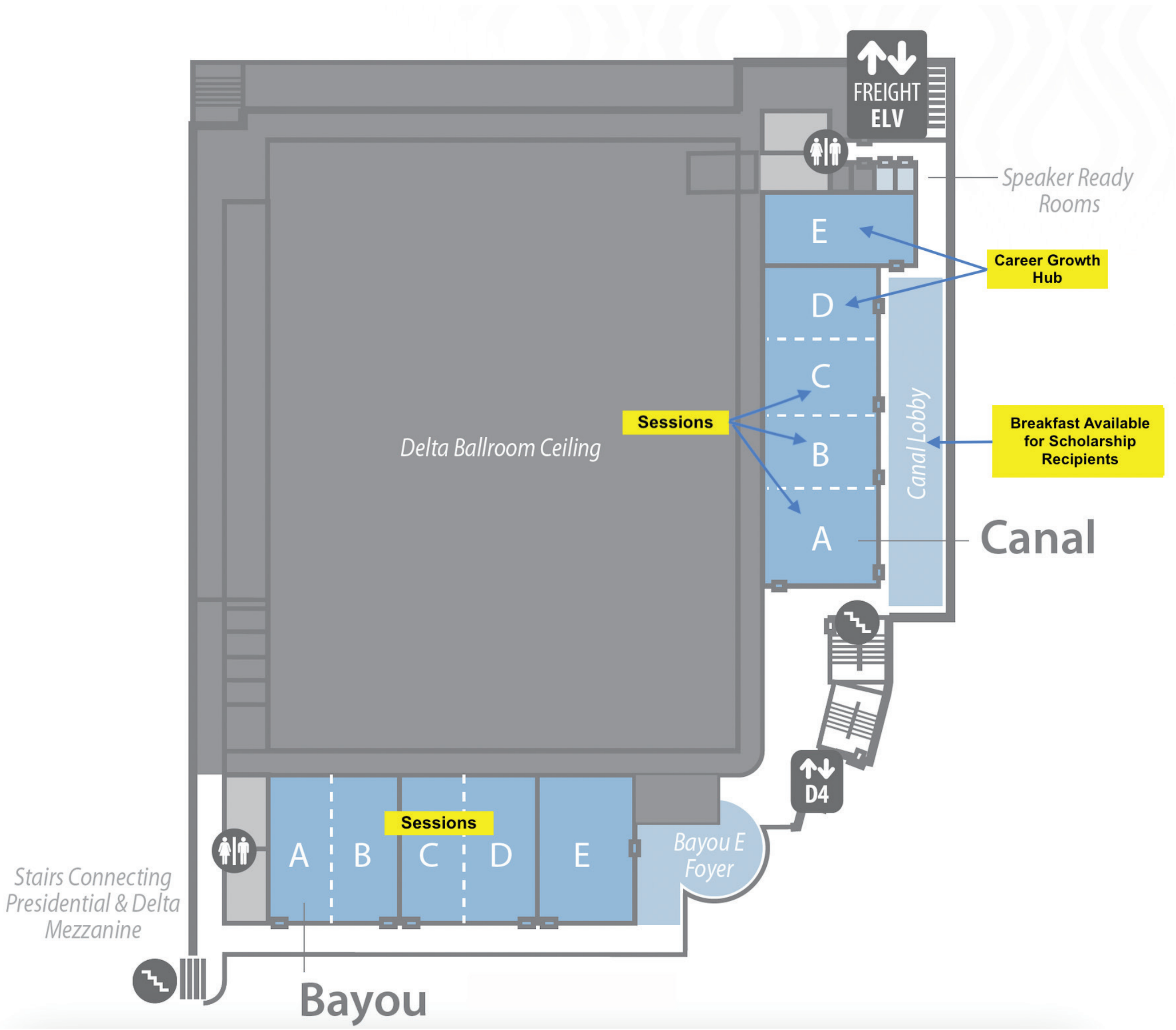
2024 WiCyS CONFERENCE VENUE MAPS

GAYLORD CONVENTION CENTER



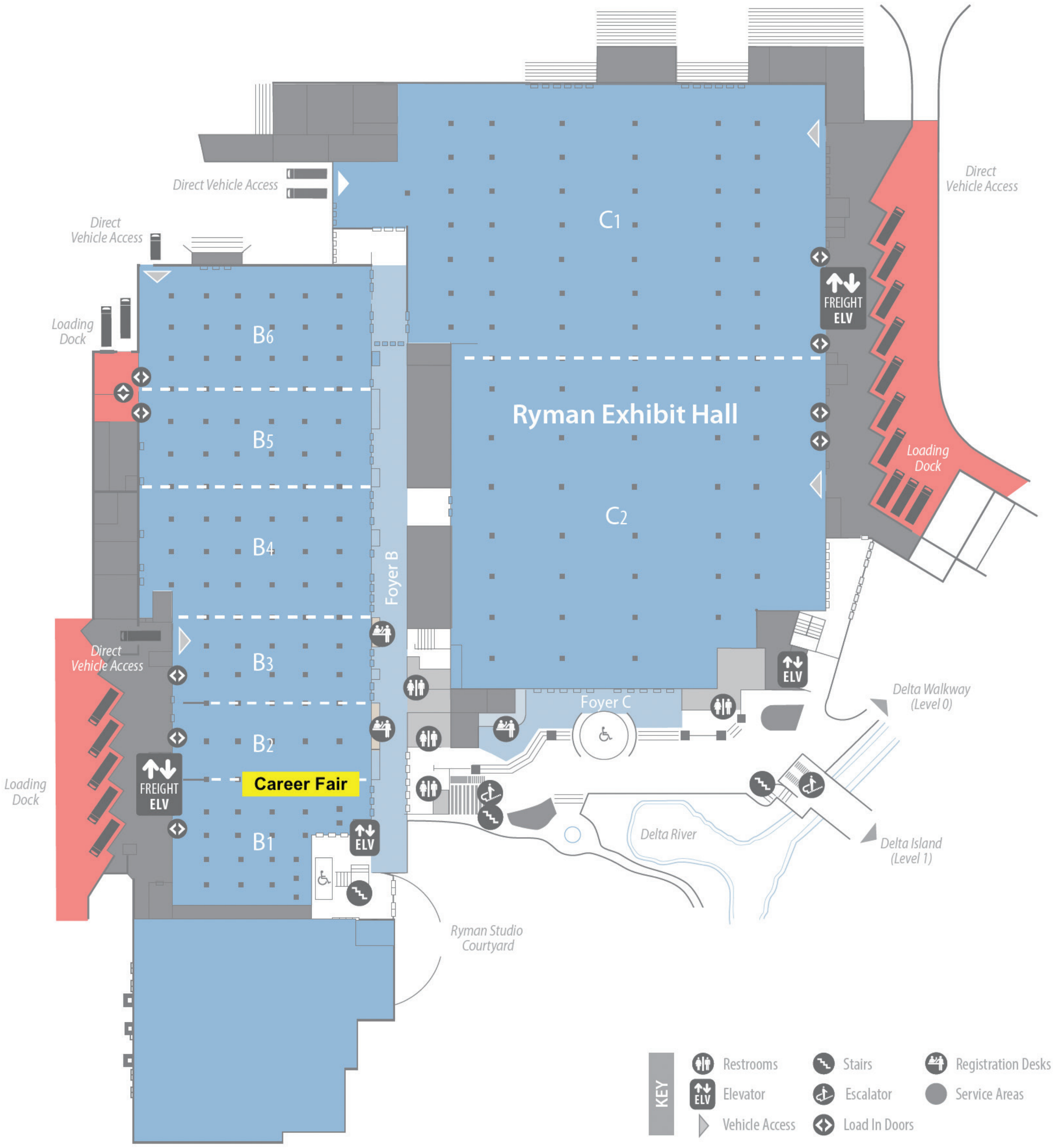
2024 WiCyS CONFERENCE VENUE MAPS

GAYLORD CONVENTION CENTER



2024 WiCyS CONFERENCE
VENUE MAPS

GAYLORD CONVENTION CENTER



2024 WiCyS CONFERENCE

NOTES

WORDS FROM CONFERENCE PROGRAM TITLES

Achieving
Cybersecurity
Results
Instagram
SANS
Cybersecurity
Individuals
Optimizing DFIR
Automation
Digital Footprint
Platform
HTTPS Traffic
Machine Learning
Cyber Sheroes
Fake News
Transparency
Sleuthing in the Mist
Best Defense
Strategic Approach
Women in Security
Secure Code Reviews
Cybersecurity
Hidden in Plain Sight
Human-AI
Personal Boundaries
Unleashing the Power
Belonging
AWS
Second Career
Resilience
Success
Cyber-Securing Vehicles
Challenge
Black Box Entropy Estimation
Success
Women
Weaponization of Misinformation
Cyber
GCP
Detection
Capture the Flag
Lightweight Security Framework
Governing
Table Tops
Cybersecurity
AI
Cybersecurity Education
Attacking the Control Logic
Privacy
APIs
Efficient Candor
Identifying
Choose Your Own Adventure
Work Item Associations
Cyber
Cultural Intelligence Code
Women
Automated Fuzz Testing
Information Gathering
XGBoost Algorithm
Tools
Build
Vulnerability Analysis
Hybrid
Effective
AI
Real Reflections
Evolution
Impact
Effective Hiring Practices
Safely
Cybersecurity
Reaching the Plateau
Industrial Control Systems
Targeted State Laws
Threat Hunting Tracks
Executive
Electronic Health Records
Device Attestation
Build
Engineering
Role
Confronting Burnout
Fortifying Your Mind
Tracing Manipulation Attacks
IoT
Enhancing Privacy
Support
Detect Malicious Software
Clinic
CEO
Accelerating
Secure
Cybersecurity
User Photo Privacy Settings
Shattering Stereotypes
Research
Careers
Malware Challenge
Walk the Talk
Train
Secret Sauce
Networking for Introverts
Exercise
Forensic Analysis
Advanced Language Models
Work Environments
Reinforcement Learning
Ecosystems
NEW WiCyS Member Portal
Certifications
Assessment
Cybersecurity Tale
Specification
Fortifying Behavior Biometrics
Cyber
Architectural Thinking
OSINT
Bolster
Simulated 5G Network
Efficient Defense
Stepping Up
Flipping the Script
Inclusive
Meetup
Apprenticeships
Service Vulnerability
Culturally Responsive
Commanding
Federal Initiatives
Microaggressions
Intrusion Detection Systems
FFF-Based 3D Printing
CyberAttackers
Understanding
Prompt
Machine Learning
S-ARP
VR Security
Automotive Cyber Defense
Game
Professionals
Wi-Fi Systems
Train
Digital Doppelgängers
Unlocking Potential
Bridging
Trust
Efficacy
Audio Signals
ChatGBT
Close the Skills Gap
Building
Overcoming
Shift Left Security
Key
Next Generation
Malware Written in Go
Digital
Duality
Identifying Vulnerabilities
Cybersecurity
Using Vision Transformers
Leveraging
Future
Defending Against Physical Threats
Discovering
Public Data
Crime-Intent Sentiment Detection
Protocol
Student Chapter
Flipper Zero
Intelligence Intrusion Detection
Great
Rethinking Recruiting
Ascending
Incident Response
Disney Villains
Exploring
Adapting
Artificial Intelligence
Reach
Talent
Imposter Syndrome
Careers
Career
Industrial Control Systems
Supply Chain
AI
Gender Washing
Cybersecurity
Cybersecurity
Digital Defense
Dive In
Revolution
Intelligence Analysts
Vulnerabilities
Virtual Visions
Rising Above
Attack
Empirical Study
Interviewee
Talents
OSS Debain
Ecosystem Approach
Maleware Detection
Phishing
Code Vulnerability
Enhance
Diverse Leadership
Algorithms
Social Good
Beginner's Guide
Dynamic
Cybersecurity
Randomware Attack
Behaviors
ChatGPT
Leader
Evolution
AI
Workforce
Vanguard
Leadership
Cybersecurity
LLM
Cybersecurity
Cybersecurity
Social Media
Roots
Military

women in
CYBERSECURITY
WiCyS

WiCyS.ORG

JOIN WiCyS IN SUPPORTING WOMEN IN CYBERSECURITY

Join Women in CyberSecurity (WiCyS) in its mission to help build a strong and gender-balanced cybersecurity workforce. Initiated in 2013 by Dr. Ambareen Siraj through a National Science Foundation (NSF) grant to Tennessee Tech University, WiCyS is now a non-profit organization with a global footprint offering many membership, sponsorship and collaboration benefits.

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