women in CYBERSECURITY
WiCyS
DENVER 2021

2021 WiCyS CONFERENCE

SEPTEMBER 8-10, 2021
DENVER, CO

#WiCyS2021

VIP SPONSORS:

OPTUM®

Raytheon Technologies

TABLE OF CONTENTS

BADGE PICK-UP HOURS

WEDNESDAY	**7:00am - 7:00pm**
THURSDAY	**7:00am - 6:00pm**
FRIDAY	**7:00am - 9:00am**

USE THE APP

BOOST YOUR EXPERIENCE

Haven't had a chance to explore yet? After downloading the Whova app to your mobile device, use your email address to sign in.

You can browse the agenda, view speakers and sponsors, connect with other attendees, and ask conference questions by messaging Rian Sondag.

APP CODE: SeeHerAsEqual2021

SOCIAL MEDIA CONTEST

Win Lodging & Registration to WiCyS 2022!

Enter the social media contest on Facebook, Twitter or Instagram! Use **#WiCyS2021** on a public page or on the WiCyS Facebook event wall to share pictures and stories of your time at the conference.

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

SNAPCHAT @ WiCyS

Use Our Custom Snapchat WiCyS Conference Filter!

Make sure your location services are on in your mobile device. Open Snapchat and take a picture Swipe left or right to see the custom **#WiCyS2021** filter.

WELCOME TO THE 8TH ANNUAL WiCyS CONFERENCE

Welcome to WiCyS 2021! It has been 30 months since we could gather as a community so this is especially exciting for all of us in the WiCyS organization as we miss being with our tribe. You are part of the outstanding community that makes WiCyS strong. The agenda is packed, so take advantage of all the WiCyS conference has to offer. Network with fellow like-minded individuals. Introduce yourself and believe in the power of the collective nature to advance in your career and pay it forward as well.

We all welcome you as your authentic selves, here to connect and collaborate while making steady progress on impacting diversity in cybersecurity. A warm and heartfelt thanks to all the hundreds of volunteers that helped make WiCyS 2021 possible and I look forward to meeting many of you over the next few days!

Janell Straach
WiCyS Conference Chair and Chair of the Board

WiCyS BOARD OF DIRECTORS

Dr. Ambareen Siraj
WiCyS Founder, Director/Cybersecurity Education, Research and Outreach Center; Professor/CS, Tennessee Tech

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

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

Jenn Henley
Vice President,
Infrastructure at Facebook

Prajakta Jagdale
Senior Manager, Information Security,
Palo Alto Networks

Diana Kelley
Founder and CTO,
Security Curve

Jay Koehler
Software Engineering Manager,
AI Services, Red Hat

Allison Miller
CISO and Senior Vice President,
UnitedHealth Group/OPTUM

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

Dr. Greg Shannon
Chief Scientist,
Carnegie Mellon University

Dr. Dawn M. Beyer
Senior Fellow
Lockheed Martin Space

2021 WiCyS CONFERENCE KEYNOTE SPEAKERS

Debora A. Plunkett, Cybersecurity Leader

"From Disruption to Opportunity Without Compromise"

Debora Plunkett is a cybersecurity leader with over 30 years of experience. A former Director of Information Assurance at the National Security Agency, she is Principal of Plunkett Associates LLC, a consulting business. She is also a Senior Fellow at Harvard's Belfer Center and a Professor of Cybersecurity at the University of Maryland. Ms. Plunkett serves on the corporate boards of CACI International, Nationwide Insurance and BlueVoyant. She is a founding member and chairman of the board of Defending Digital Campaigns, a non-profit entity focused on providing free or low-cost cybersecurity services to federal election campaigns.

Ms. Plunkett served on the National Security Council at the White House in the Administrations of Presidents Clinton and George W. Bush where she developed national cybersecurity policies and programs. She earned an undergraduate degree from Towson University, an MBA from Johns Hopkins University, and a Master of Science in National Security Strategy from the National War College.

Aimee Cardwell, UnitedHealth Group

"The Courage to Succeed: The Door is Open (For A Change)"

Aimee is the Chief Information Security Officer (CISO) for UnitedHealth Group, a Fortune 5 company. Aimee oversees a team of cybersecurity professionals who work to prevent cyber threats to the organization and uphold privacy and security requirements in IT Governance & Policy. She and the team also safeguard technology assets globally on behalf of members, patients, providers, partners and colleagues.

With 25 years in the technology sector, including 10 years in financial services, she has focused on leading large IT organizations, developing technology strategy, establishing and enforcing governance, overseeing cybersecurity operations, and executing IT acquisitions. She is an inspirational leader who delivers strong results in customer experience, platform strategy, mobile, e-commerce and fintech. Prior to joining UnitedHealth Group, Aimee led Consumer Product Development Engineering at American Express, and held leadership roles at eBay, Expedia, and Netscape. In her spare time, Aimee explores the science, art, and meditative practice of cooking and serving food for those she loves.

Ashley Podhradsky, Dakota State University

Dr. Ashley Podhradsky is the Vice President of Research and Economic Development and Professor of Digital Forensics at Dakota State University. Ashley is also a board member of the First Bank and Trust Board of Directors. Ashley has been an invited speaker at several events and universities including The Pennsylvania State University, Bureau of Justice Affairs, Women in CyberSecurity, InfraGard, OSMOSIS Conference among others. Her research teams have received over 8.6 M in competitive grants and contracts.

Current awards include an NSF REU site, NSF NRT program and NSA GenCyber. In addition to her academic and professional work, she has a strong passion for increasing gender diversity in cybersecurity. She is the co-founder of CybHER™, an initiative to increase gender diversity in cybersecurity. Ashley was the recipient of the EmBe 2017 "Young Woman of Achievement", The 2017 Merrill Hunter Award for Excellence in Research, 2017 and 2018 New America Cybersecurity Fellow, and is a 2019 American Association for the Advancement of Science IF/THEN Ambassador.

2021 WiCyS CONFERENCE KEYNOTE SPEAKERS

Raytheon Technologies Keynote Panel

"Securing a Path for Success"

- ### Leslie Burns, Raytheon Technologies

Leslie Burns is the Executive Director, Information Security Strategy & Planning, responsible for leading the strategic planning and execution of information security and its transformation efforts for the enterprise. With a background in information technology, information security, and human resources, Leslie brings a broad and unique perspective to each of her roles. This perspective has enabled her to lead security transformations at several large, global companies. As part of the transformations, she has designed organizations, built diverse teams, and developed security leaders.

Prior to Raytheon Technologies, Leslie was most recently Vice President, Information Security Strategy and Business Operations at Thomson Reuters. Previously, she was a Principal at Booz Allen Hamilton, where she served as the Business Operations Leader for Booz Allen's Commercial business and Leader for its Cyber Business Advisory practice. Her experience also includes Senior Director, Information Security Strategy & Operations at Target and various leadership positions at General Electric. Leslie holds an MBA from New York University and a BS in Operations and Information Systems Management from Penn State University. She is a graduate of two GE leadership development programs, is Six Sigma certified, and a CISSP.

- ### Alexandra Heckler, Collins Aerospace

As Chief Information Security Officer at Collins Aerospace, Alexandra leads a diverse team of cyber strategy and defense professionals to protect the company's digital infrastructure, operational technology and hosted services. Her team is focused on mitigating cyber threats, addressing global cyber compliance risk, and fostering a company-wide security culture. Prior to joining Collins, Alexandra spent 10 years at Booz Allen, a technology and management consulting firm. She led the company's Commercial Aerospace and Automotive practices, building and overseeing multi-disciplinary teams to advise C-level clients on cybersecurity and digital transformation initiatives. Her work centered on helping manufacturers manage the convergence of cyber risk across their increasingly complex business ecosystem, including IT, OT and connected products. She also supported technology, innovation and risk analysis initiatives across U.S. government clients. Alexandra helped lead Booz Allen's Women in Cyber—a company-wide initiative to attract, develop and retain female cyber talent—and was a key contributor to the firm's partnership with the Executive Women's Forum. She also served as Finance and Audit Chair on the Executive Committee of the newly-founded Space-ISAC. Alexandra holds a B.S. in Foreign Service with an Honors Certificate in International Business Diplomacy, and a M.A. in Communication, Culture and Technology from Georgetown University.

- ### Tina Oberai, Raytheon Intelligence & Space

Tina Oberai began her cybersecurity career at Raytheon and has held various roles throughout her 19-year career with the company. In her current role, Tina serves as a technical advisor to Raytheon programs providing guidance on customer cybersecurity requirements in order to enable successful contract execution, ensure a compliant cybersecurity posture and mitigate risk to our customers and our company. She works with cross-functional Raytheon stakeholders to review new US and International cybersecurity regulations to assess the impact to our company and drive strategic approaches to ensure compliance and continuously improve the company's cybersecurity practices, policies and standards. Tina has also served as a Cybersecurity Engineer on several Raytheon programs developing, designing and implementing secure, compliant network solutions and information systems for DoD customers.

Tina earned her Bachelor of Science degree in Computer Engineering from the University of Florida and is a Certified Information Systems Security Professional (CISSP) and Information Systems Security Engineering Professional (ISSEP). Since receiving her CISSP in 2007, Tina has taught multiple CISSP prep courses for Raytheon employees and local high-school students.

THANK YOU TO OUR 2021 CONFERENCE SPONSORS

VIP SPONSORS

- OPTUM
- Raytheon Technologies

PREMIUM SPONSORS

- Adobe
- cisco
- Google
- mastercard
- National Security Agency United States of America
- SentinelOne

DIAMOND SPONSORS

- AFCS Air Force Civilian Service
- AON Empower Results
- Carnegie Mellon University Software Engineering Institute
- CEROC Cybersecurity Education, Research and Outreach Center
- CSSIA National Support Center for Systems Security and Information Assurance
- Deloitte.
- IBM
- praetorian
- RICE
- salesforce
- verizon
- VISA
- Walmart
- workday.

PLATINUM SPONSORS

- aws
- American Express
- Arete
- asurion
- Bank of America
- Capitol Technology University
- Central Intelligence Agency
- Cleveland Clinic
- COALFIRE
- Comerica Bank
- cruise
- CYAI Cybersecurity Youth Apprenticeship Initiative CYAI2024.org
- www.cybher.org
- Defense Intelligence Agency United States of America
- U.S. Department of Homeland Security
- ECS
- elastic
- f5
- Goldman Sachs
- Idaho National Laboratories
- Lockheed Martin
- ManTech International Corporation
- Lincoln Laboratory Massachusetts Institute of Technology
- MorganFranklin Consulting A Vaco Company
- Northeastern University Khoury College of Computer Sciences
- paloalto networks
- RIT Golisano College of Computing and Information Sciences Department of Computing Security
- SHIFT5
- Square
- STARBUCKS
- str
- UCCS University of Colorado Colorado Springs
- ZEBRA

GOLD SPONSORS

- ARMOR
- Charter Communications
- CROWDSTRIKE
- DARKOWL
- EY Building a better working world
- flatiron.
- FIU Florida International University
- FORTINET
- Georgia Tech Research Institute
- HS Haystack Solutions
- Indiana University Cybersecurity
- JPMorgan Chase & Co.
- MITRE
- NYU Tandon
- NordVPN
- Pacific Northwest National Laboratory
- PrivacySwan Consulting
- P&G
- Sandia National Labs
- SANS Technology Institute
- SecurityRisk Advisors
- Security University
- SOPHOS
- CARBONITE an opentext company | WEBROOT an opentext company

SILVER SPONSORS

- Carnegie Mellon University Information Networking Institute
- ENVESTNET
- FIREEYE
- Purdue University
- 1865 Rider University
- S2 Stage 2 Security
- tenable
- Two Sigma

COMMUNITY COLLABORATORS

- Black Girls Hack
- Black Girls In Cyber
- CSA cloud security alliance
- CyberCorps Defending America's Cyberspace
- Cybersecurity Collaboration Forum
- Cyber Security Summit
- The Diana Initiative
- DiversityComm
- FIU Florida International University
- International Consortium of Minority Cybersecurity Professionals
- 75 Years IEEE Computer Society
- IEEE Symposium on Security and Privacy
- (ISC)²
- iSAW Foundation
- Last Mile Education Fund
- national center for women & information technology
- National Collegiate Cyber Defense Competition
- SecureWorld
- Sightline Security
- Tech Inclusion
- WITI women in technology international build. empower. inspire.

OPTUM®

Janani P.
Director of IT
Devoted Wife & Mother

Take your purpose to new levels.

150K
team members collaborating worldwide

222M
people in our consumer database

100K+
physicians & health care locations served

$3.5B
spent yearly on technology & innovation

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

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

Apply here: workatoptum.com

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

THANK YOU TO OUR 2021 WiCyS COMMITTEES

CONFERENCE PROGRAM CHAIR

Dr. Ambareen Siraj
WiCyS Founder, Director/Cybersecurity Education, Research and Outreach Center; Professor/CS, Tennessee Tech

CONFERENCE GENERAL CHAIR

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

PROGRAM

Celeste Matarazzo
Co-Chair
Cyber Defenders Program Manager, Lawrence Livermore National Laboratory

Ashley Podhradsky
Co-Chair
Interim Vice President of Research, Dakota State University

Chutima Boonthum-Denecke
Co-Chair
Professor of Computer Science
Director, Information Assurance and Cyber Security Center, Hampton University

Jennifer Cheung
Co-Chair
Research Scientist, NIWC Pacific

Mona-Lisa Pinkney
Co-Chair
Sr. Director, Cybersecurity Governance, Risk, Compliance, Engagement and Geographies, Nike, INC.

Aisha Ali-Gombe
Assistant Professor, Towson University

Amani Altarawneh
Graduate Assistant, Ph.D. Candidate, University of Tennessee at Chattanooga

Arpita Biswas
Incidence Response Lead, Databricks Inc.

Kristine Christensen
Director, Faculty Development Professor, Computer Information Systems, Moraine Valley Community College

Joshua Fallon
Network Defense Analyst, Software Engineering Institute

Esther Goldstein
Software Engineer, Data Security, Salesforce

Ashley Greeley
Cyber Professional, DoD

Erye Hernandez
Senior Security Engineer, Google

Ahmed Ibrahim
Teaching Assistant Professor, University of Pittsburgh

Michelle Lindblom
Security Awareness Manager, Salesforce

Magnolia McShane
Security & Threat Intelligence Consultant, Little Owl Security

Renita Murimi
Associate Professor of Cybersecurity, University of Dallas

Anita Nikolich
Research Scientist, School of Information Sciences, UIUC

Holly Parrish
Threat Operations Specialist, Arctic Wolf

Jan Pearce
Professor and Chair, Computer and Information Science, Berea College

Elena Peterson
Senior Cyber Security Researcher, Pacific Northwest National Laboratory

Anca Pop
Information Security Consultant, 365 Striker

Heather Ricciuto
Academic & Talent Outreach Program Manager, IBM

Angie Sawaya
Security & Privacy Compliance Manager, IBM Enterprise Technology & Security

Anita Siassios
WiCyS Australia Affiliate

Sara Young
Program Manager, Digital Security & Risk Management, Microsoft

Chuan Yue
Associate Professor, Colorado School of Mines

OPERATIONS AND LOGISTICS

Lynn Dohm
Executive Director, WiCyS

Peter Baldwin
vCFO, WiCyS

Morgan Garland
Operations Manager, WiCyS

Colleen Huber
Senior Creative Director, The Nelly Group

Lana Richardson
Community Care Manager, WiCyS

Jessica Robinson
vCISO, WiCyS, Founder, Pure Point International

Rian Sondag
Events Manager, WiCyS

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

THANK YOU TO OUR 2021 WiCyS COMMITTEES

WiCyS COLORADO CONFERENCE SUPPORT CONSORTIUM (WCCSC)

Gretchen Bliss
Lead
Director Cybersecurity Programs, University of Colorado Colorado Springs

Steve Fulton
Coleman Richardson Chair, Computer Science, USAFA

Nina Amey
Department Chair, Arapahoe Community College

Anastasia Biggs
Professor, Colorado Technical University

Bob Bowles
Director of the Center for Information Assurance Studies, Regis University

Nathan Chung
Senior Consultant, Microsoft

Lt Col Adrian de Freitas
Deputy Department Head, Computer and Cyber Science, US Air Force Academy

Terri Johnson
Department Chair
Computer Networking & Cybersecurity
Pikes Peak Community College

Heather Lawrence
Student, University of Colorado Colorado Springs

Dan Manson
Professor, Cal Poly Pomona

Marian Merritt
Lead for Industry Engagement, NIST/NICE

Joe Murdock
Business School Faculty, University of Colorado Denver

Ij Olawale
Student, University of Colorado Colorado Springs

Katrina Rosemond
Student, University of Colorado Colorado Springs

Patrice Siravo
Director of Commercial Cybersecurity, System High Corporation

Rhonda Spradling
Corporate Communications, AMERGINT Technologies

Yanyan Zhuang
Assistant Professor, University of Colorado Colorado Springs

SCHOLARSHIP

Shade Adeleke
Associate Professor and Cybersecurity Coordinator, Prince George's Community College

Jacquelyn Blanchard
Chief Cyber Architect, Lockheed Martin; Vice President, BSidesCharm

Gretchen Bliss
Director Cybersecurity Programs, University of Colorado Colorado Springs

Stacie Bohanan
Principal Research Scientist, University of Alabama in Huntsville

Eric Chan-Tin
Assistant Professor, Loyola University Chicago

Mandy Galante
Cybersecurity Education Specialist, NJ Cybersecurity & Communications Integration Cell

Elizabeth K. Hawthorne
Lecturer and Graduate Program Director of Cybersecurity, Rider University

Pushpa Kumar
Associate Professor of Instruction, The University of Texas at Dallas

Sarah Morales
Security Engineering Outreach Program Manager, Google

Noureen Njoroge
Director of Cyber Threat Intel, Nike, INC.

Jacqueline Ore
Career Success Lead, Cybersecurity, Fullstack Academy

Angela Sims Ceja
Water Technical Operations Superintendent, City of Aurora, Aurora Water Department

Hannah Tun
Lead Security Engineer, OmniSOC

SOCIAL MEDIA & PR

Maddie Witt
Lead
Social Media Specialist, WiCyS

Aditi Chaudhry
Lead
Cybersecurity Engineer, Two Sigma

Midori Connolly
Customer Success Manager, Yubico

Colleen Huber
Senior Creative Director, The Nelly Group

Drenusha Salihu
Linux System Administrator, BVM

Rian Sondag
Events Manager, WiCyS

Alina Thai
Threat Intelligence Analyst, Allstate

THANK YOU TO OUR 2021 WiCyS COMMITTEES

CAREER VILLAGE

Andrea Frost
Lead
Senior Software Security Engineer, Dell EMC

Kim Huynh
Security Program Manager, Research and Threat Intelligence at Microsoft

Terri Johnson
Department Chair, Pikes Peak Community College

Michelle Lindblom
Security Awareness Manager, Salesforce

CAREER FAIR

Mary Jane Partain
Career Fair Concierge Director, University of Texas-Dallas

Patrice Siravo
Director of Commercial Cybersecurity, System High Corporation

POSTER

Chutima Boonthum-Denecke
Professor of Computer Science
Director, Information Assurance and Cyber Security Center,
Hampton University

Susan Jeziorowski
Applied Cybersecurity Engineer,
MITRE

VOLUNTEER COORDINATION

Cameron Mitchell
Carnegie Mellon University - Software Engineering Institute

STUDENT CHAPTER LEADS

Vitaly Ford
WiCyS Chapter Coordinator
Assistant Professor,
Arcadia University

Pauline Mosley
Assistant Professor,
Pace University

PROFESSIONAL AFFILIATE LEADS

Lynn Dohm
Executive Director,
WiCyS

Lana Richardson
Community Care Manager,
WiCyS

RESOURCES COMITTEE

Lisa Ellrodt
Lead
Faculty Advisor, Pace University

Sri Bhamidipati
Technical Staff, Verizon Wireless

Madeline Estey
Student, Kent Place School

Maxine Franks
Application Security Agent, University Of Nevada Las Vegas

Meghan Jacquot
Risk Assessment Cybersecurity Engineering, Cyber Future Foundation

Catherine Miri
Student, Savio High School

Catherine Wairachu
Ait Security And Assurance, Towson University

Anna Yap
Project Manager, Index Analytics LLC

LEADERSHIP SUMMIT WORKING GROUPS

ADVANCEMENT

Champion: Jenn Henley, *Facebook*
Student Intern: Shannon McHale, *Rochester Institute of Technology*

PIPELINE

Champion: Prajakta Jagdale, *Palo Alto Networks*
Student Intern: Maggie Van Nortwick, *Northeastern University*

INCLUSION

Champion: Diana Kelley, *Microsoft*
Student Intern: Maleesha Perera, *University at Albany*

TRANSITIONING/RETURNING

Champion: Dr. Dawn Beyer, *Lockheed Martin*
Student Intern: Shaina Munoz-Rivera, *University of Puerto Rico*

THANK YOU TO OUR 2021 WiCyS COMMITTEES

MISSION SUPPORT TEAM

Dawn Beyer
Senior Fellow, Lockheed Martin

Susan Bullwinkel
Director, Business Delivery Enablement, Enterprise Information Security, Optum

Valerie Jane Chua
Program Manager, Security Learning & Awareness, Facebook

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

Allie Decrastro
Program Manager, Global Enablement, AWS

Mariana Gardinali
Software Engineer, Cisco

Divya Ghatak
Chief People Officer, SentinelOne

Jenn Henley
Vice President, Infrastructure, Facebook

Tracey Hilton
Senior Program Manager, Facebook

Ann Johnson
Corporate Vice President, Microsoft

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

Val Miller
Growth Strategies, Security Events, AWS

Cameron Mitchell
Operations Coordinator, Carnegie Mellon University- SEI

Sarah Morales
Outreach Program Manager, Security And Privacy, Google

Katrina Mouquin
Security Architect, Bloomberg

Jodi Schaubschlager
Director, Information Security, Optum

Ashley Smyk
Principal Technical Program Manager, AWS

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

Noelle Warburton
Director, Security and Trust Communications,Cisco

Dasha Zenkovich
Marketing Manager, Microsoft

RACIAL EQUITY

Jessica Robinson
Lead
vCISO, WiCyS, Founder, Pure Point International

Kelli Hudson
Associate, Capability Architect, Booz Allen Hamilton

Sofia Martinez
Steam Facilitator, Illinois Tech Amp/ Co-Terminal Undergrad

Alyssa Miller
Application Security Advocate, Snyk

Jennifer Munoz
Student, Indiana University

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

Quintana Patterson
Compliance And Security Analyst, University Of Colorado

Mona-Lisa Pinkney
Senior Director, Governance, Risk, Compliance & Engagement Management, Corporate Information Security, Nike, Inc.

MENTOR/MENTEE

Archana Ramamoorthy
Lead
Director, Cloud Security Product Manager, Google

Susan Bullwinkel
Director, Business Delivery Enablement, Enterprise Information Security, Optum

Cat Goodfellow
Director, Continuous Monitoring & Improvement, Cyber Development & Engineering EIS, UnitedHealth Group

Joanna Grama
Associate Vice President, Vantage Technology Consulting Group

Deborah Kariuki
Faculty, Computer Science Ed, UMBC

Karen Nemani
President, WiCyS Ontario Affiliate

Lauren Provost
Ethical Hacker, Author, Computer Science Professor, Simmons University

Julie Sparks
Security Engineer, Cloudflare

PROGRAM PARTICIPATION
TRACKS AND SESSIONS

CURRENT TECHNOLOGY AND CHALLENGES TRACK

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

LOOKING AHEAD TRACK

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

BEST PRACTICES TRACK

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

CAREER DEVELOPMENT TRACK

Leadership, advancement, and transition.

PRESENTATIONS

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

WORKSHOPS

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

BIRDS OF A FEATHER (BoaF)

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

LIGHTNING TALKS

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

PANELS

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

POSTERS

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

2021 WiCyS SCHEDULE AT A GLANCE

TIME	DESCRIPTION	LOCATION
WEDNESDAY		
7:00am - 7:00pm	Badge Pick-Up	Aurora 3
9:00am - 3:30pm	Leadership Summit (By Invite Only)	Various Rooms
12:00pm - 1:30pm	Senior Leadership Luncheon (By Invite Only)	Aurora B
12:30pm - 1:30pm	First Timer's Guide to WiCyS	Summit 6
12:30pm - 1:30pm	Recruiters Session	Summit 7
12:30pm - 7:00pm	CTF Coaching	Aurora D
2:00pm - 4:00pm	Workshop Series	Various Rooms
2:00pm - 7:00pm	Career Village Open	Willow Lake 1-2-3-4-5
4:00pm - 7:00pm	Poster Session Check-In	EH 3 PreFunc.
4:30pm - 6:30pm	Workshop Series	Various Rooms
6:30pm - 7:30pm	Student Scholarship Recipient Dinner	Crest 3-4-5
7:00pm - 8:00pm	Educators Funding 1-on-1	Summit 3
7:00pm - 8:00pm	WiCyS 2022 Call for Participation Information	Summit 5
7:00pm-9:00pm	Raytheon Technologies Mentoring Social	Homestead 1-4
8:00pm - 9:00pm	Federal Scholarship (SFS/ DoD) Scholars Meetup and Information Session	Summit 3

TIME	DESCRIPTION	LOCATION
FRIDAY		
7:00am - 9:00am	Badge Pick-Up	Aurora 3
7:00am - 10:00am	Shared Interview Space	Homestead 1
7:30am - 8:30am	Breakfast Available for Students & Fellowship Recipients	Corridor next to Aurora A-B-C
8:00am - 5:00pm	Luggage Storage avaiable	Aurora D
8:45am - 9:45am	Keynote	Aurora A-B-C
9:45am - 10:15am	Group Picture	EH3 or Outside
10:15am - 11:00am	Presentation Sessions	Various Rooms
10:15am - 11:00am	Affiliate MeetUp	Summit 2-3
11:15am - 12:00pm	Presentation Sessions	Various Rooms
11:15am - 12:00pm	Student Chapter MeetUp	Summit 2-3
12:00pm - 12:45pm	Panel Sessions	Various Rooms
12:45pm - 2:00pm	Lunch, Closing Remarks	Aurora A-B-C
2:00pm - 2:30pm	Travel Stipend Verification	Outside of Aurora ABC
2:30pm - 4:30pm	Workshop Series	Various Rooms

TIME	DESCRIPTION	LOCATION
THURSDAY		
7:00am - 6:00pm	Badge Pick-Up	Aurora 3
7:00am - 8:00am	Breakfast Available for Students & Fellowship Recipients	Corridor next to Aurora A-B-C
7:00am - 8:00am	Military and Veteran Group Breakfast	Summit 4-5
7:00am - 8:30am	Poster Session Check-In	EH 3 PreFunc.
7:00am - 7:00pm	Shared Interview Space	Homestead 1
8:30am - 9:45am	Conference Opening, and Keynote	Aurora A-B-C
9:45am - 11:45am	Career Fair / Village Open	Aurora EH 3/ Willow Lake 1-2-3-4-5
9:45am - 11:45am	CTF Coaching	Aurora D
9:45am - 11:00am	Student Poster Session	EH 3 PreFunc.
11:00am - 11:45am	Presentation Sessions	Various Rooms
11:00am - 11:45am	Lightning Talks	Summit 8-9
11:45am - 1:45pm	Lunch and Keynote	Aurora A-B-C
1:55pm - 2:40pm	Presentation Sessions	Various Rooms
1:55pm - 2:40pm	Lightning Talks	Summit 8-9
1:55pm - 5:30pm	Career Fair / Village Open	Aurora EH 3/ Willow Lake 1-2-3-4-5
1:55pm - 5:30pm	CTF Coaching	Aurora D
2:40pm - 4:40pm	Workshop Series	Various Rooms
4:45pm - 5:30pm	Birds of a Feather	Various Rooms
6:00pm - 7:45pm	Dinner and Keynote	Aurora A-B-C
8:30pm - 9:30pm	WiCyS Racial Equity Committee Meet and Greet	Aurora D PreFunction
8:30pm - Midnight	CTF Coaching	Aurora D
9:00pm - Midnight	CTF After Dark Party	Aurora D

PICK UP AND PURCHASE WiCyS GEAR

Visit Aurora Registration

WEDNESDAY 11:00am - 7:00pm

THURSDAY 9:30am - 6:00pm

FRIDAY 7:00am - Sellout

2021 WiCyS SCHEDULE

WEDNESDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 7:00pm	Badge Pick-Up	Aurora 3
9:00am - 3:30pm	Leadership Summit (Invite Only)	Aurora C; Summit 2-5
11:00am - 7:00pm	WiCyS Store Open	Aurora Registration
12:00pm - 1:30pm	Senior Leadership Luncheon (Invite Only)	Aurora B
12:30pm - 1:30pm	**First Timer's Guide to WiCyS Conference** **Kaitlyn Carroll,** *Tennessee Technological University;* **Elizabeth K. Hawthorne,** *Rider University;* **Susan Jeziorowski,** *MITRE;* **Lynne Miller,** *Raytheon;* **Susanne Wetzel,** *Stevens Institute of Technology*	Summit 6
12:30pm - 1:30pm	**Strategic Engagement with WiCyS Community for Hiring!** **Dr. Ambareen Siraj,** *CEROC, WiCyS*; **Lynn Dohm,** *WiCyS*	Summit 7
12:30pm - 7:00pm	CTF Coaching	Aurora D
2:00pm - 7:00pm	Career Village Open	Willow Lake 1-2-3-4-5
2:00pm - 4:00pm	**Workshop Series** (4 Concurrent)	
	Red Team/Blue Team: How to Think Like a Hacker **Marcelle Lee, Mari Galloway, Lisa Jiggetts and Vanessa Redman,** *Women's Society of Cyberjutsu*	Summit 2-3
	The Hitchhiker's Guide to the Home Network: Analyzing IoT Traffic **Maria Melchiorre, Alicia Ouyang, Kim Gavin, and Christopher Morris,** *Systems and Technology Research (STR)*	Summit 8-9
	Hacking Unconscious Biases for a More Inclusive Work Environment **Elena Peterson,** *Pacific Northwest National Laboratory;* **Manisha Kanodia,** *UC San Diego;* **Laura Murphy,** *IBM in support of Kyndryl;* **Deveeshree Nayak,** *University of Washington*	Summit 6-7
	A Close Look into WiCyS Veteran Apprenticeship Program **Martha Laughman,** *Smoothstack;* **Dr. Ambareen Siraj,** *CEROC, WiCyS;* **Lynn Dohm,** *WiCyS*	Summit 4-5
4:00pm - 4:30pm	Break	
4:00pm - 7:00pm	Poster Session Check-In	EH 3 PreFunction
4:30pm - 6:30pm	**Workshop Series** (4 Concurrent)	
	Artificial Intelligence Assisted Malware Analysis **Maanak Gupta,** *Tennessee Tech University;* **Mahmoud Abdelsalam,** *Manhattan College;* **Sudip Mittal,** *University of North Carolina at Wilmington*	Summit 8-9
	Both Sides of a CTF: Compete and Create **Hugrun Hannesdottir, Sara Schwarz Iglesias and Dianelys Soto-Cruz,** *Carnegie Mellon University*	Summit 6-7
	Simulating Supply Chain Breaches with Arena **Elizabeth Rasnick and Chris Kadlec,** *Georgia Southern University*	Summit 4-5
	Measuring the Invisible: How Inclusion Impacts Employee Satisfaction and Company Performance (Invite Only) **Paolo Gaudiano,** *Aleria*	

2021 WiCyS SCHEDULE
WEDNESDAY AGENDA

TIME	DESCRIPTION	LOCATION
6:30pm - 7:30pm	Student Scholarship Recipient Dinner	Crest 3-4-5
7:00pm - 8:00pm	Educators Funding 1-on-1	Summit 3
7:00pm - 8:00pm	WiCyS 2022 Call for Participation Information Session	Summit 5
7:00pm - 9:00pm	Raytheon Technologies Mentoring Social	Homestead 1-4
8:00pm - 9:00pm	Federal Scholarship (SFS/DoD) Scholars Meetup and Information Session	Summit 3

JOB BOARD++

CYBERSECURITY EXCLUSIVE

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

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

2021 WiCyS SCHEDULE

THURSDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 6:00pm	Badge Pick-Up	Aurora 3
7:00am - 8:00am	Breakfast for Students and Fellowship Recipients	Corridor next to Aurora A-B-C
7:00am - 8:00am	Military and Veteran Group Breakfast	Summit 4-5
7:00am - 8:30am	Poster Session Check-In	EH 3 PreFunction
7:00am - 7:00pm	Shared Interview Space	Homestead 1
8:30am - 9:45am	**Conference Opening, and Keynote** (doors open at 8:15am) **Keynote Introduction: Divya Ghatak,** *SentinelOne* **Keynote: "From Disruption to Opportunity Without Compromise"** **Debora A. Plunkett**, *Cybersecurity Leader*	Aurora A-B-C
9:30am - 6:00pm	WiCyS Store Open	Aurora Registration
9:45am - 10:15am	Refreshment Break	Aurora B
9:45am - 11:00am	Student Poster Session & Networking Break	EH 3 PreFunction
9:45am - 11:45am	Career Fair and Career Village Open	Aurora EH 3, Willow Lake 1-2-3-4-5
9:45am - 11:45am	CTF Coaching	Aurora D
11:00am - 11:45am	**Presentation Sessions** (3 Concurrent)	
	PASTA and OCTIVE and STRIDE, Oh My! Bringing Threat Modeling Out of the Woods **Alyssa Miller,** *S&P Global*	Summit 2-3
	You've Got a Degree, You've Got Credentials, How Do You Get a Job in Cybersecurity? **Ronda Henning,** *L3Harris Technologies*	Summit 6-7
	Understanding the Phenomenon of Vulnerability Chaining Blindness **Dr. Nikki Robinson,** *IBM*	Summit 4-5
11:00am - 11:45am	**Lightning Talks** (all talks are in the same room)	Summit 8-9
	Community Crowd Sourcing for WiCyS Cybersecurity Resource Library **Meghan Jacquot,** *WiCyS Resource Committee*	
	A Strategic Approach to IoT Security: How an Organization Can Work Toward a Secure Future **M'Kaila Clark,** *Empire State College*	
	Effectiveness of Threat Mitigation in Layers of the Open Systems Interconnection Model **Olivia A. Gallucci and Sylvia Perez-Hardy,** *Rochester Institute of Technology*	
	A Department of Defense Conference on Re-Entry for Women Veterans into Cybersecurity Careers **Rachelle Heller,** *George Washington University;* **Costis Toregas,** *George Washington University and WiCyS Board Member*	
	Demystifying Cyber Risk Metrics and Reporting **Priya Mouli,** *LTI- Larsen and Toubro Infotech*	
	The Future of Ethical Hacking **Lauren Provost,** *Norwich University*	
	Unmasking Cyber Command's Protections for the 2020 Election **Diana Parr,** *SAIC*	
	Last Mile Education Fund: Investing in the Next Generation of Tech Talent **Ruthe Farmer,** *Last Mile Education Fund*	

2021 WiCyS SCHEDULE
THURSDAY AGENDA

TIME	DESCRIPTION	LOCATION
11:45am - 1:45pm	**Lunch, Networking, and Keynote** (must be seated by noon to eat) **Keynote Introductions: Ruchi Shah,** *Google* **and Morgan Adamski,** *NSA* **Keynote: "The Courage to Succeed: The Door is Open (For A Change)"** **Aimee Cardwell,** *Optum*	Aurora A-B-C
1:55pm - 2:40pm	**Presentation Sessions** (3 Concurrent)	
	A Framework for Identifying Host-Based Artifacts in Dark Web Investigations **Dr. Arica Kulm,** *Dakota State University*	Summit 2-3
	Do Developers Write SUPER Secure Code? **Mary Anne Waddick,** *Raytheon Technologies*	Summit 6-7
	Understanding Privacy through Computational Social Science over Twitter and Reddit **Jayati Dev,** *Indiana University Bloomington*	Summit 4-5
1:55pm - 2:40pm	**Lightning Talks** (all talks are in the same room)	Summit 8-9
	Improving Cybersecurity Field Preparedness by Gamification and Scenario-Based Activities **Molly Cooper,** *Ferris State University*	
	Highlights of Mainframe Security **Elizabeth Schweinsberg,** *US Digital Service*	
	Crowd-Sourced Vulnerability Disclosure Program Working to Keep the DOD "Left of Boom" **Melissa S. Vice,** *DoD Cyber Crime Center (DC3), VDP*	
	Communities Within WiCyS Community: Special Interest Groups **Rian Sondag,** *WiCyS*	
	2021 Executive Orders and What They Mean for the Software Supply Chain **Megan Moloney,** *Guidehouse, National Security Segment*	
	Identity Governance: How to Prevent Reputational Damage **Vidya Ganesh,** *Farmers Insurance*	
	Experience Leading a Deployed USMC Cyber Team **Svetla Walsh,** *United States Marine Corps*	
	NICE Workforce Framework for Cybersecurity WiCyS Video Album **Dr. Ambareen Siraj,** *CEROC, WiCyS;* **Mimi Vertrees,** *Tennessee Technological University;* **Rian Sondag,** *WiCyS*	
1:55pm - 5:30pm	Career Fair and Career Village Open *(Break w/ Refreshments in Career Fair from 2:45pm - 3:15pm)*	Aurora EH 3, Willow Lake 1-2-3-4-5
1:55pm - 5:30pm	CTF Coaching	Aurora D

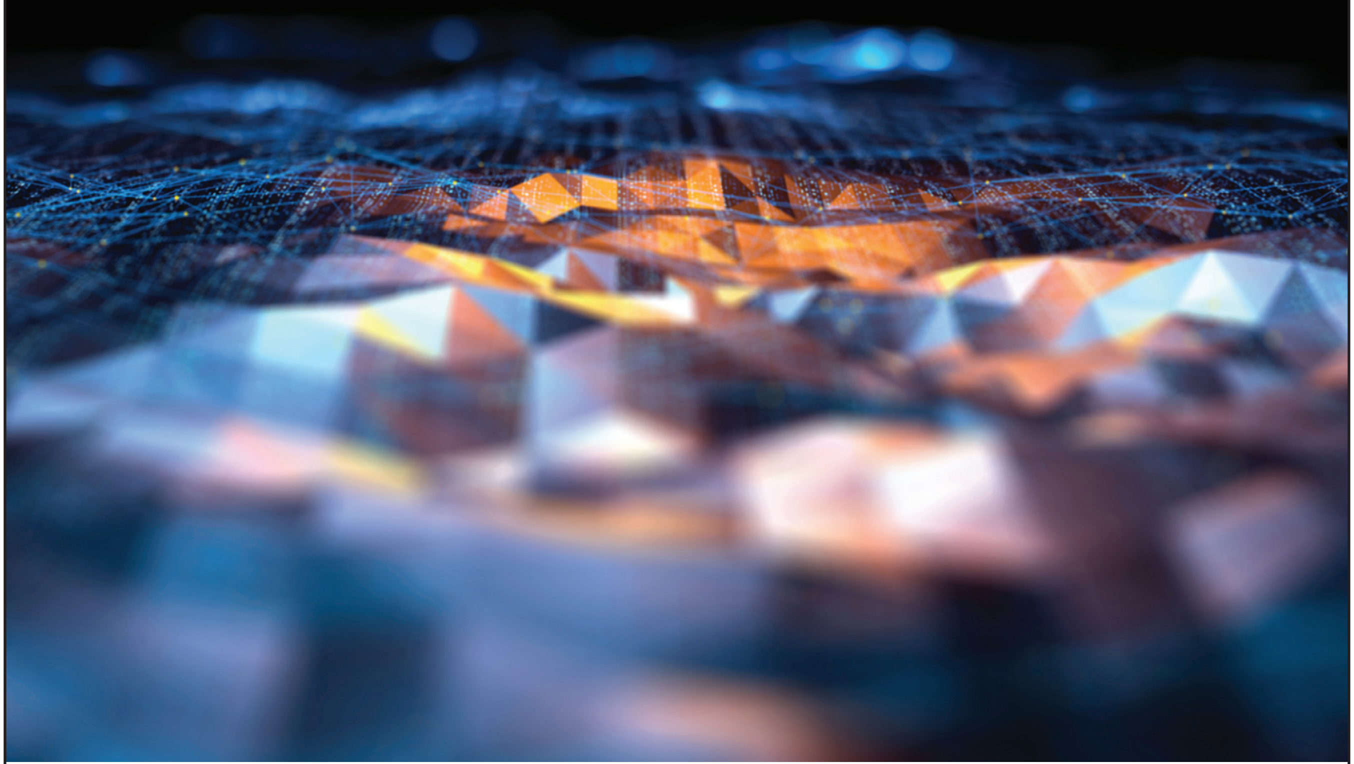
2021 WiCyS SCHEDULE
THURSDAY AGENDA

TIME	DESCRIPTION	LOCATION
2:40pm - 4:40pm	**Workshop Series** (4 Concurrent)	
	Leaders, Equity and Influence: Creating a Culture of Self-Accountability **Jessica Robinson, Kelli Hudson, Sofia Martinez, Alyssa Miller, Jennifer Munoz, Noureen Njoroge, Quintana Patterson, and Mona-Lisa Pinkney,** *WiCyS Racial Equity Committee*	Summit 2-3
	How to Show Work (in Documentation) to Auditors and Regulating Bodies **Krystal Gabel,** *Bank of the West*	Summit 4-5
	Personal Branding in Cybersecurity and Privacy **Barbra Mooneyhan,** *BrightInsight;* **Janice Reese,** *Network PDF Cloud*	Summit 8-9
	Build an Attack: Why Tabletop Exercises are for Everyone **Remi Cohen,** *F5;* **Sayako Quinlan,** *CrowdStrike*	Summit 6-7
4:45pm - 5:30pm	**Birds of Feather** (4 Concurrent)	
	Things We Wish We Knew Before Starting Our Careers in Cybersecurity **Maggie Marxen and Bailey Bercik,** *Microsoft*	Summit 6-7
	The Not-So-Well-Talked-About Topic: Fostering Allyship **Han Thazin (Hannah) Tun,** *OmniSOC, Indiana University;* **Amy Starzynski Coddens,** *REN-ISAC*	Summit 8-9
	Not Everyone Starts in Technology, Where Did Your Journey Start? **Dr. Kelley Misata,** *Sightline Security;* **Deborah Kariuki,** *University of Maryland Baltimore County (UMBC)*	Summit 2-3
	Fostering a Transparent Security Culture to Reduce Insider Threat **Chrysa Freeman,** *Code42*	Summit 4-5
6:00pm - 7:45pm	**Dinner, Networking, and Keynote** (must be seated by 6:15pm to eat) **Keynote Introduction:** **Shannon Lietz,** *Adobe* **Keynote:** **Ashley Podhradsky,** *Dakota State University*	Aurora A-B-C
8:30pm - 9:30pm	WiCyS Racial Equity Committee Meet and Greet	Aurora D PreFunc.
8:30pm - Midnight	CTF Coaching	Aurora D
9:00pm - Midnight	CTF After Dark Party	Aurora D

CAREER VILLAGE

Wednesday, 2:00pm - 7:00pm / Thursday, 9:45am - 11:45am & 1:55pm - 5:30pm
Located in Willow Lake 1-2-3-4-5

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



2021 WiCyS SCHEDULE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
7:00am - 9:00am	Badge Pick-Up	Aurora 3
7:00am - 10:00am	Shared Interview Space	Homestead 1
7:00am - Sell Out	WiCyS Store Open	Aurora Registration
8:00am - 5:00pm	Luggage Storage avaiable	Aurora D
7:30am - 8:30am	Breakfast Available for Students & Fellowship Recipients	Corridor next to Aurora A-B-C
8:45am - 9:45am	**Keynote** (doors open at 8:30am) **Keynote Introduction: Helen Patton,** *Cisco* **Keynote: "Securing a Path for Success"** **Leslie Burns, Alexandra Heckler, and Tina Oberai,** *Raytheon Technologies*	Adams Ballroom
9:45am - 10:15am	Group Picture / Break with Refreshments	EH3 or Outside
10:15am - 11:00am	**Presentation Sessions** (3 Concurrent)	
	Cybersecurity for Aviation Requires a Different Perspective **Amanda Buchanan,** *Raytheon Technologies*	Summit 4-5
	Hack the Farm Today; Own the Grid Tomorrow! **Mary Ann Hoppa,** *Norfolk State University*	Summit 6-7
	Above Our Heads - How Attackers are Leveraging the Cloud **Elif Kaya and Kim Huynh,** *Microsoft;* **Remi Cohen,** *F5*	Summit 8-9
10:15am - 11:00am	**Affiliate MeetUp**	Summit 2-3
11:15am - 12:00pm	**Presentation Sessions** (2 Concurrent)	
	How to Train Your Operator: Observations of a "Charming" Adversarial Group **Allison Wikoff,** *IBM X-Force*	Summit 6-7
	AI and Cybersecurity: What is Our Role? **Shafia Zubair,** *Morningstar*	Summit 8-9
11:15am - 12:00pm	**Student Chapter MeetUp**	Summit 2-3
12:00pm - 12:45pm	**Panel Sessions** (4 Concurrent)	
	Securing the Supply Chain: When Every Step is a New Weak Link **Bianca Steele and Jess Smith,** *Pacific Northwest National Laboratory;* **Bob Hanson,** *Lawrence Livermore National Laboratory;* **Greg Shannon,** *Cybersecurity Manufacturing Innovation Institute;* **Cheri Caddy,** *U.S. DOE*	Summit 2-3
	The New Threat Landscape in a Post Pandemic World **Priyam Biswas,** *Intel;* **Awalin Sopan,** *Sophos;* **Abhilasha Bhargav-Spantzel and Michele Myauo,** *Microsoft;* **Reshma Shahabuddin,** *Sophos*	Summit 4-5
	Acquire the Right Cybersecurity Competencies to Be More Prepared for a Job **Susanne Wetzel,** *Stevens Institute of Technology;* **Dr. Sharon R. Hamilton and Zoe Fowler,** *Norwich University;* **Karen Wetzel,** *National Initiative for Cybersecurity Education (NICE)*	Summit 6-7
	Overcoming Imposter Syndrome in Cybersecurity **Noureen Njoroge and Dr. Mona-Lisa Pinkney,** *Nike;* **Reena Madan,** *Verizon;* **Latisha Scarborough,** *Microsoft*	Summit 8-9

2021 WiCyS SCHEDULE

FRIDAY AGENDA

TIME	DESCRIPTION	LOCATION
12:45pm - 2:00pm	**Lunch, Closing Remarks, and Awards** (Must be seated by 1:00pm to eat) **Closing Remarks: Alissa "Dr. Jay" Abdullah, Mastercard**	Aurora A-B-C
2:00pm - 2:30pm	Travel Stipend Verification	Outside of Aurora A-B-C
2:30pm - 4:30pm	**Workshop Series** (3 Concurrent)	
	Fellowship of the RING: Experience Cybersecurity Curriculum and Resources for K-12 **Tania Williams, Jesse Hairston and Benjamin Cummins,** *The University of Alabama in Huntsville*	Summit 2-3
	Android Reverse Engineering **Aisha Ali-Gombe, Oluwasetemi Owoeye and Ramyapandian Vijayakanthan,** *Towson University*	Summit 4-5
	Threat Hunting Using MITRE ATT&CK for Inspiration **Lily Lee and John Stoner,** *Splunk Inc.*	Summit 8-9

MILITARY AND VETERAN BREAKFAST

TOGETHER. WE SERVE.

Thursday, 7:00am - 8:00am - Summit 4-5

The Military and Veteran Breakfast will honor our military and veteran WiCyS members with special recognition to our Veteran Assistance Program Fellowship Award recipients and the inaugural cohort of the WiCyS Veteran's Apprenticeship Program.

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

2021 WiCyS CONFERENCE
WORKSHOP DESCRIPTIONS

PRE-CONFERENCE SESSIONS
Wednesday • 12:30pm - 1:30pm

First Timer's Guide for WiCyS Conference

Kaitlyn Carroll, *Tennessee Technological University;* **Elizabeth K. Hawthorne,** *Rider University;* **Susan Jeziorowski,** *MITRE;* **Lynne Miller,** *Raytheon;* **Susanne Wetzel,** *Stevens Institute of Technology*

Attending a WiCyS conference for the first time can be both exciting and daunting. There is just so much to navigate in such little time! First timers attending the WiCyS conference should join this session. Panelists from various backgrounds and interests will share their experiences of what they found useful, what matters and, most importantly, how anyone can get the most out of this experience as a first-time WiCyS attendee.

Strategic Engagement with WiCyS Community for Hiring!

Dr. Ambareen Siraj, *CEROC, WiCyS*; **Lynn Dohm,** *WiCyS*

The WiCyS organization is proud to be a family of more than 5000 members in its community. If you are interested in recruitment from this diverse WiCyS community, join us to learn about the tools that the WiCyS organization has at your disposal. From our resume database and member community portal to career fairs and more, find out how you can be more engaged in meaningful ways yearlong. We also want to hear from you regarding recruitment: success stories, challenges, and ideas for us to work more effectively together.

PRE-CONFERENCE SESSIONS
Wednesday • 7:00pm - 8:00pm

WiCyS 2022 Call for Participation Information Session

WiCyS 2021 Program Committee

Interested in attending and presenting at the WiCyS 2022 conference? The WiCyS 2022 Call for Participation for speaking engagements will open on Wednesday, September 15th and is open to anyone interested. Join the WiCyS 2021 Program Committee to go over best practices when writing a presentation proposal abstract, tips and tricks for making your submission stand out, and get your questions answered.

1:1 FUNDING MEETUP

EDUCATORS FUNDING 1-ON-1

Wednesday, 7:00pm - 8:00pm, Summit 3

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

FEDERAL SCHOLARSHIP (SFS/DOD) SCHOLARS MEETUP AND INFORMATION SESSION

Wednesday, 8:00pm - 9:00pm, Summit 3

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

2021 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

WORKSHOP SERIES
Wednesday • 2:00 pm - 4:00 pm

Red Team/Blue Team: How to Think Like a Hacker

Marcelle Lee, Mari Galloway, Lisa Jiggetts and Vanessa Redman, *Women's Society of Cyberjutsu*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

In this hands-on workshop, the presenters will follow the steps of an attack from a red team perspective and consider how to remediate the actions for each phase from a blue team perspective. Participants can expect to increase their knowledge of the following: Five phases of an attack – Recon, scanning, gaining access, maintaining access, covering tracks; how to use Kali Linux to gain access to a remote host; how to defend against certain types of attacks; topics associated with the EC-Council CEH certification; and topics associated with the CompTIA PenTest+ certification. In a nod to cyber competitions, there will be flags planted throughout for participants to find.

The Hitchhiker's Guide to the Home Network: Analyzing IoT Traffic

Maria Melchiorre, Alicia Ouyang, Kim Gavin, and Christopher Morris, *Systems and Technology Research*

TRACK: BEST PRACTICES

This workshop is a crash course on creating and analyzing an Internet of Things (IoT) network. The presenters will demonstrate how to set up an IoT lab that mimics a modern home network, how to capture traffic between devices, and how to analyze and visualize this data. They also will discuss basic packet altering methods and how to expand this setup to test different cybersecurity scenarios (ex. Man in the Middle Attack). Participants will learn skills that can apply to their career and home network (all skill levels welcome). To start, the presenters will demonstrate how to set up a hardware lab of devices (ex. Raspberry Pi) in common home network configurations. They will focus on setting up IoT devices of different capability levels that allow for transmitting, receiving and capturing data. They will analyze the data pulled from this setup to later determine network behavior and security risks. Next, they will instruct attendees on how to login to devices in the IoT lab as well as how to start capturing network traffic. Participants will learn and use common packet capturing and network analysis tools (ex. nmap). To mimic common malicious cybersecurity scenarios, the presenters will demonstrate how to delete or alter packets traveling between devices. Finally, this presentation will use Python to complete basic analysis and visualization of captured network traffic.

Hacking Unconscious Biases for a More Inclusive Work Environment

Elena Peterson, *Pacific Northwest National Laboratory;* **Manisha Kanodia,** *UC San Diego;* **Laura Murphy,** *IBM in support of Kyndryl;* **Deveeshree Nayak,** *University of Washington*

TRACK: CAREER DEVELOPMENT

The WiCyS Inclusion Working Group will present an in-depth workshop on the issue of unconscious bias in hiring and career development in the cybersecurity workplace and the scientific basis for the need for diversity and inclusion. Many cyber-based companies are realizing the need to focus on diversity and inclusion and have started to create councils, boards, working groups, etc., to be more mindful of the issues and possibly affect change. However, there are many things individuals can do, based on science, to influence their workplaces and better understand how to create an inclusive culture. There also are ways of understanding whether a potential new employer has a culture of inclusion to help women select a workplace that will truly support their career development. This workshop will begin with a discussion of the definition, the need for inclusivity and assess the difference between diversity and inclusion. Participants will learn about the various cognitive biases that affect how women (and minorities) are treated in the cybersecurity field as well as how to recognize when those biases appear.

A Close Look into WiCyS Veteran Apprenticeship Program

Martha Laughman, *Smoothstack;* **Dr. Ambareen Siraj,** *CEROC, WiCyS;* **Lynn Dohm,** *WiCyS*

TRACK: CAREER DEVELOPMENT

Women veterans face challenges post-transition to civilian life and are at higher risk for unemployment post-separation. WiCyS is committed to women in cybersecurity's achievements and successes while providing the needed and necessary pipeline for the workforce. This leads WiCyS to help solve both the veteran transition dilemma and the nation's cybersecurity talent shortage with one program. At this workshop, presenters will discuss the WiCyS feeder program that aligns the military to industry using the cybersecurity apprenticeship pathway. The mission is to help veterans in the community find paths into cybersecurity careers after military service. In collaboration with SmoothStack, WiCyS is working with its strategic partners to provide DOL-certified apprenticeship opportunities to the veteran community for ultimate placement in partner organizations. Any organization that wants to find out how to be part of the solution should join this workshop where the program will be outlined in detail.

2021 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

WORKSHOP SERIES
Wednesday • 4:30 pm - 6:30 pm

Artificial Intelligence Assisted Malware Analysis

Maanak Gupta, *Tennessee Tech University;* **Mahmoud Abdelsalam,** *Manhattan College;* **Sudip Mittal,** *University of North Carolina at Wilmington*

TRACK: CAREER DEVELOPMENT

In modern enterprises, security analysts monitor threats in a security operations center by watchstanding, which is similar to a lookout on a ship watching the environs for danger. Screens typically show warnings and alerts from individual products and detectors that the enterprise has installed. Watchstanding permits a highly trained security analyst to look at all the disparate pieces of information and see if they form some pattern that might indicate an attack. Many of these products use Artificial Intelligence (AI) and data-intensive systems. The need for automation and adaptation has made AI one of the most sought-out skills in the security industry. This workshop aims to provide hands-on experience and offer an overview of tools and techniques useful for AI-assisted malware analysis. Providing attendees with the knowledge of using AI in malware analysis will be an incredibly powerful tool to bridge the cybersecurity talent gap. It will open up opportunities for not only cybersecurity-focused talent, but also for students across other concentrations like data science or ML to apply their skills to solve cybersecurity problems. Topics covered will include malware attack stages; malware data collection, feature identification and preprocessing; AI-assisted malware detection; and malware classification. Registered attendees will be provided with a handbook with the tools used during this workshop. In addition, participants will be asked to download and have the VM image ready to be used during the session.

Both Sides of a CTF: Compete and Create

Hugrun Hannesdottir, Sara Schwarz Iglesias and Dianelys Soto-Cruz, *Carnegie Mellon University*

TRACK: BEST PRACTICES

This workshop looks to fulfill one of the WiCyS conference missions – Best Practices – by educating participants with the tools and techniques needed to compete in and create their own capture the flag (CTF) challenges. This workshop is geared toward beginners and those with prior CTF experience who wish to learn more about creating their own CTF challenges. After participants learn about the basics of CTF and the aforementioned categories, they will be introduced to picoCTF by completing practice challenges that cover the CTF categories as well as different difficulty levels. Next, participants will be divided into groups of five, where each unit will have up to an hour to create their CTF challenge design. Finally, each group will showcase their design before each participant votes for their favorite. The top three designs will be invited to finish implementing their challenges and be featured on the picoCTF server under the creators' names.

Simulating Supply Chain Breaches with Arena

Elizabeth Rasnick and Chris Kadlec, *Georgia Southern University*

TRACK: CAREER DEVELOPMENT

This workshop introduces participants to the process of creating a supply chain model using Arena discrete event simulation software. This software is a tool for creating representations of complex, interdependent processes. It allows people to examine the state of a system at any point in time. People can determine how relationships between processes at one point in a system effect those in other parts of the system. For data breaches, people can determine the likely duration of the disruption and the time needed to recover to a pre-breach state. Attendees will run their multi-stage models and examine how the supply chain works under ideal circumstances. This provides a baseline performance for comparison with experimental breaches to the supply chain model. The workshop will start with a brief overview of modeling and simulation. Key terms and the mathematical underpinnings that make simulations useful will be defined. Underlying assumptions of the models will be explained so the limitations of the results are fully understood. Participants will interact with the data by varying inputs to see how the productivity of the supply chain is altered. They also will build a model with customers, retailers, wholesalers, distributors and manufacturers. This multi-echelon model gives a more accurate representation of changes to the supply chain. The discussion will incorporate the flow of data through a supply chain and how a cyberattack causes disruption, including upstream and downstream data sources. By discussing the data as it moves through the supply chain, attendees will determine potential breach points. The closing discussion will examine how these breach points can be secured or strengthened with redundancy.

2021 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

Measuring the Invisible: How Inclusion Impacts Employee Satisfaction and Company Performance (Invite Only)

Paolo Gaudiano, *Aleria*

TRACK: CAREER DEVELOPMENT

While organizations are increasingly aware of the importance of investing in Diversity & Inclusion (D&I), there is less clarity around where to start and how to create and sustain a more diverse, inclusive and equitable workplace. At Aleria, we have developed a unique framework to define and measure Inclusion, which presents an entirely new way to think about D&I, allowing allows organizations to pinpoint where exactly they need to prioritize their efforts to drive meaningful progress, and to see the impact of their initiatives in weeks, not years.

We offer an Inclusion Workshop that introduces key concepts and then guides the audience through a memorable interactive experience to demonstrate how inclusion can be measured, and how it can be used to identify opportunities to make companies more inclusive and more successful.

WORKSHOP SERIES
Thursday • 2:40 pm - 4:40 pm

Leaders, Equity and Influence: Creating a Culture of Self-Accountability

Jessica Robinson, Kelli Hudson, Sofia Martinez, Alyssa Miller, Jennifer Munoz, Noureen Njoroge, Quintana Patterson, and Mona-Lisa Pinkney, *WiCyS Racial Equity Committee*

TRACK: CAREER DEVELOPMENT

The WiCyS Racial Equity Committee (REC) will present a workshop on self-accountability and the role everyone plays in creating change in the spaces they occupy. This includes driving change, taking responsibility for learning and speaking up for what someone needs when a boundary is crossed, helping to set the example for others to follow in leading with courage. This workshop will explore the landscape of inclusive language in leadership and how this shift is occurring across industries, allowing for more equitable environments where people can thrive. Self-accountability involves unlearning behaviors and mental models rooted in racism to create new ways of thinking, use of language and allyship. The REC also will share the work they have been doing on behalf of WiCyS to support racial equity within the organization. They look forward to hearing from attendees on what is most important as a member of WiCyS regarding this topic.

How to Show Work (in Documentation) to Auditors and Regulating Bodies

Krystal Gabel, *Bank of the West*

TRACK: BEST PRACTICES

This workshop will focus on the best practices of how to address regulatory requirements in documentation. As a content strategist and cybersecurity analyst, the presenters witness the struggle keeping many security teams from producing content that speaks directly to their requirements, which in turn results in failed audits and rework. The session will look at a typical industry scenario and how work is demonstrated. The presenters will discuss drafting an implementation story with evidence, including how to perform a gap analysis, define a doc hierarchy and map requirements. They'll also write language that ties together policy, standard and procedure documents into a cohesive package. After 90 minutes, attendees will have the baseline content skills with pertinent examples to draft a core documentation set that gives an E2E picture of how to fulfill security requirements.

Personal Branding in Cybersecurity and Privacy

Barbra Mooneyhan, *BrightInsight* **and Janice Reese,** *Network PDF Cloud*

TRACK: CAREER DEVELOPMENT

In the journey of a cybersecurity or privacy professional, people can find themselves staring at a job description, preparing for an interview or negotiation, or standing in front of a career booth feeling unsure. How do they stand? Where do their hands go? What can they do or say? Ultimately, how do they represent themselves in a manner that is professional, best represents their abilities and is authentic to who they are? To be comfortable and confident in answering these questions, people must understand themselves, their abilities, opportunities, motivators and values. Join these presenters on a journey of building a personal brand in cybersecurity and privacy. They'll explore their understanding of themselves by writing their credo, mission statement and elevator pitch. Then they'll dig deeper into building their story, looking at their career visions and applying their values to determine a career path, wrapping up the session with getting insight into finding a career match.

2021 WiCyS CONFERENCE WORKSHOP DESCRIPTIONS

Build an Attack: Why Tabletop Exercises are for Everyone

Remi Cohen, *F5* **and Sayako Quinlan,** *CrowdStrike*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

This workshop starts by throwing participants into a tabletop exercise, giving them relevant background information. Participants will be grouped by their specialties, such as networking, system administrator, network defense, risk management, legal, communications and HR. This approach demonstrates that tabletop exercises are critical for identifying gaps in incident response processes and technologies, and everyone in an organization can benefit from them. Participants will be guided through the puzzle and empowered to ask the right kind of questions as they work through the scenario. After the interactive exercise, presenters will address the process for creating a tabletop simulation by identifying an attack path, developing the scenario storyline, brainstorming discussion questions and documenting takeaways. The presenters will talk about different scenarios they've developed and give tips and tricks for running a great simulation. Their experience covers both internal and customer facing tabletop development and delivery. They'll also talk about the importance of threat profiles and how that can inform scenario development.

WORKSHOP SERIES

Friday • 2:30 pm - 4:30 pm

Fellowship of the RING: Experience Cybersecurity Curriculum and Resources for K-12

Tania Williams, Jesse Hairston and Benjamin Cummins, *The University of Alabama in Huntsville*

TRACK: LOOKING AHEAD

Find out how Regions Investing in the Next Generation (RING) is impacting students nationwide and changing the way cybersecurity is taught in high schools. RING, a new and accessible K-12 curriculum crafted by Centers of Academic Excellence (CAE) colleges and universities, is ready for everyone to explore. Delve into RING, an initiative to create a free online, national high school curriculum for students without access to cybersecurity classes. It is sponsored by the National Security Agency CAE in Cybersecurity Education Innovation program. RING includes instructional slides, lesson plans, assessments (with teacher keys), hands-on labs, online games and manipulatives, CAE in Cybersecurity school career mappings and tons of graphic organizers. It is a foundational course but progresses students quickly through various concepts, including cryptography, networking and careers. This workshop provides an overview of the initiative, introduces the planning and pacing, lets participants download a lesson, and encourages people to try one of the hands-on labs.

Android Reverse Engineering

Aisha Ali-Gombe, Oluwasetemi Owoeye and Ramyapandian Vijayakanthan, *Towson University*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

This workshop introduces participants to Android applications analysis via reverse engineering and other advanced static analysis techniques. The workshop will begin by introducing the anatomy of Android apps popularly known as the APK. This first module covers Android app creation, compilation and dexing, the design of the Android manifest file, and other resources zipped into the APK. The second module explores Reverse Engineering (RE) fundamentals and the use of RE for static program analysis. Participants will gain practical skills in examining permissions, app components, SDK versions, resources and Application Programming Interface calls. The hands-on exercises will include disassembling and decompilation of sample Android applications using open-source tools like Baksmali and jadx. The last module will introduce advanced static analysis techniques such as data and control flow analysis and native code analysis for an in-depth Android behavioral analysis. Participants will gain working knowledge of examining apps for data exfiltration, espionage and privilege escalation. This workshop requires a basic understanding of Java. Attendees should bring laptops with virtualization software.

Threat Hunting Using MITRE ATT&CK for Inspiration

Lily Lee and John Stoner, *Splunk Inc.*

TRACK: BEST PRACTICES

Who wants to be a threat hunter? Perhaps the better question is who wouldn't want to be a threat hunter? So, what do people hunt for, and where do they start? This workshop will give attendees the opportunity to hunt threats using Splunk as they pursue a fictional adversary referred to as the Violent Memmes (APT-VM). During this workshop, the presenters will contextualize APT-VM using the Diamond Model and draw inspiration from the MITRE ATT&CK framework to fuel the hunts and gain insights into APT-VM's tactics, techniques and procedures. At the end of this session, not only will participants have a better idea of how to conduct their own threat hunts, but also mature their use of the ATT&CK framework. Presenters will provide additional resources including data sets that attendees can continue working with to apply these techniques against their own.

2021 WiCyS CONFERENCE PRESENTATION SESSIONS

PRESENTATION SESSIONS Thursday • 11:00 am - 11:45 am

PASTA and OCTIVE and STRIDE, Oh My! Bringing Threat Modeling Out of the Woods

Alyssa Miller, *S&P Global*

TRACK: BEST PRACTICES

Threat modeling is an extremely valuable tool in the secure software development pipeline. Some studies suggest it has a greater impact on security posture than other more widely practiced security activities. There are many different frameworks, models and methodologies that have been developed in an attempt to make threat modeling easier. Yet, despite these efforts, popular approaches to threat modeling are still often considered too cumbersome, structured or time consuming to fit into modern development cycles. In 2020, a group of 15 security professionals released the Threat Modeling Manifesto to formalize decades of combined experience into a declared vision of what threat modeling truly is and what makes it important. Learn from one of these authors about how to break with the complex models and return to the values and principles of what threat modeling should be. Discover how this often overlooked activity can actually make development pipelines more efficient while improving overall software security. Get real practical examples of how to use the manifesto as a guide to define or tailor a methodology that fits any needs and avoid common pitfalls that often derail this critical activity.

You've Got a Degree, You've Got Credentials, How Do You Get a Job in Cybersecurity?

Ronda Henning, *L3Harris Technologies*

TRACK: CAREER DEVELOPMENT

How does someone get a job in cybersecurity? What happens if a person has done everything right, graduated at the top of their class, but hasn't been able to find a job? This presentation talks about searching for a job in cybersecurity, how to get hired, how to climb the career ladder for a cybersecurity career, and how to know when to walk away. The presenter is a hiring cybersecurity manager who started without a technical degree and rose to become a senior fellow in the aerospace industry.

Understanding the Phenomenon of Vulnerability Chaining Blindness

Dr. Nikki Robinson, *IBM*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

Many malicious actors use a concept called vulnerability chaining, which involves combining low- or medium-level flaws to create a more severe attack. However, there is little research being done on vulnerability chaining concepts in the academic world. There is the Mitre ATT&CK Framework, CVSS and the Cyber Kill Chain as references, but nothing to help security analysts understand the concepts of vulnerability chaining. Many defenders investigate and remediate singular vulnerabilities or security controls. But what about vulnerabilities used in combination to create more severe attacks like privilege escalation or XSS? This presentation will explore the new terminology of 'vulnerability chaining blindness' and if it can be used to describe this phenomenon. The concept is built on the criminal psychology terminology called linkage blindness and aims to describe a new spectacle in the cybersecurity field. Understanding these problems will help security analysts and engineers protect their networks more effectively.

PRESENTATION SESSIONS Thursday • 1:55 pm - 2:40 pm

A Framework for Identifying Host-Based Artifacts in Dark Web Investigations

Dr. Arica Kulm, *Dakota State University*

TRACK: LOOKING AHEAD

The dark web is part of the internet that is constantly changing, not easy to access and not indexed by search engines. The goal of the dark web is privacy and anonymity, which lends itself to criminal activity. Since these sites are not indexed, they can be more difficult to access through normal means. Software used to access the dark web is designed for privacy, so finding host-based artifacts — those left behind in file systems or the Windows registry of a device — can be difficult to find and recognize. Previous studies of dark web forensics have focused on network rather than host-based forensics. This session will discuss a framework for identifying host-based artifacts during digital forensic investigations involving suspected dark web use. This framework is reusable, comprehensive and easy to follow and will assist investigators in finding artifacts designed to be hidden or otherwise difficult to discover. Attendees will learn steps for determining if a system contains host-based artifacts for either Windows-based or macOS-based artifacts.

2021 WiCyS CONFERENCE PRESENTATION SESSIONS

Do Developers Write SUPER Secure Code?

Mary Anne Waddick, *Raytheon Technologies*

TRACK: BEST PRACTICES

Do some projects discuss secure coding through all phases of the SDLC? Are developers SUPER secure? Do they have all the tools they need to be super? This talk will go over the secure coding standards, best practices and checklists that a company's projects could use to help make the code and team more secure. The discussion will center on the use of secure coding in Agile team processes. Training and certifications available for secure coding also will be discussed. Overall, this presentation will run through design, secure code review, manual review, automated review, additional security recommendations and examples of training.

Understanding Privacy through Computational Social Science over Twitter and Reddit

Jayati Dev, *Indiana University Bloomington*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

Digital ethnography over social media provides a unique opportunity to learn about real-time opinions of the general public concerning current affairs in a natural setting. It is a method of computer-mediated data collection where traditional mixed methods research can be difficult to conduct due to time and resource constraints. In this study, they report findings and lessons learned from conducting digital ethnography using computational social science to address a key question – How can social media input be used to understand the security and privacy perceptions of users? They conducted two case studies, using Reddit and Twitter, to understand people's perception of security and privacy in various aspects of their lives. Through these two case studies, they highlight that computational social sciences provide a realistic, broader insight into the information privacy concerns of users as expressed on public platforms and how these concerns align with the general notions of information disclosure concerns expressed through news and media. They also underscore the importance of real-time insight provided on social media that could be helpful in incorporating privacy by design in products through immediate feedback that is more inclusive of different privacy perceptions of various populations and more mindful of possible threat models. They will end the presentation covering the ethical implications of doing computational social science in information security with recommendations for how to make such research more privacy preserving.

PRESENTATION SESSIONS
Friday • 10:15 am - 11:00 am

Cybersecurity for Aviation Requires a Different Perspective

Amanda Buchanan, *Raytheon Technologies*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

This presentation will review the high-level design requirements for avionics equipment, common bus protocols used for communication within aviation platforms, commercial off-the-shelf design practices, and how these can lead to vulnerabilities. The discussion will look at how providing security in this space requires not only knowledge of embedded systems but also knowledge of the specific requirements placed on aviation components and techniques and goals of the adversaries that target them. Cutting edge techniques that have been developed by applying these practices also will be discussed. Participants will learn how systems can be protected even after an adversary gains root permissions on the system and, once applied, how these techniques result in unique solutions that provide the capability for aviation platforms to perform at the highest levels, even in cyber-contested environments.

Hack the Farm Today; Own the Grid Tomorrow!

Mary Ann Hoppa, *Norfolk State University*

TRACK: CAREER DEVELOPMENT

Imagine the nation is under attack from cyberspace. Imagine electricity, clean water and natural gas are no longer available for an unspecified time in homes, public buildings, or businesses. This is not science fiction or the plot of an edgy TV show but a real possibility because critical infrastructure throughout the U.S. and abroad depends on Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) technology to maintain safe and continuous operations. ICS/SCADA hardware, software, communications, and standard operating procedures have not been modernized, becoming susceptible to cyber-attacks. This talk aims to increase awareness and understanding of ICS/SCADA cybersecurity by looking at one element of the emerging smart grid that relies upon it — wind farms. Researchers have shown how easy it is to create and inject malware to cripple them, which can open lateral paths to compromise entire utility grids. Attendees will learn what skills they can develop to become cyber warriors in safeguarding these grids, including ways to engage in relevant research and how to enter this vital segment of the cybersecurity workforce.

2021 WiCyS CONFERENCE PRESENTATION SESSIONS

Above Our Heads - How Attackers are Leveraging the Cloud

Elif Kaya and Kim Huynh, *Microsoft;* **Remi Cohen,** *F5*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

It is well established that with an increase in cloud resource availability, individuals and enterprises are empowered to create and host more content than ever. This talk will catalog how attackers who deliver malware and conduct phishing and extortion leverage pre-existing free cloud services and just how cheap it is to create their own. The presenters will examine the role of the cloud in various recent attacks, techniques to mitigate these risks while enabling productivity and try to evaluate the simplicity and cost of some of the various popular misused services. By evaluating incidents that leverage cloud software and resources, the presentation will review the types of cheap assets that help platform these attacks. This talk will attempt to narrow areas of focus that students, researchers and enterprise administrators should consider when understanding the current ecosystem of attacks. Participants will leave with outcomes of the research of the catalog of services used by attackers that correlate to popular attacks or proof of concepts in which they were used.

PRESENTATION SESSIONS

Friday • 11:15 am - 12:00 pm

How to Train Your Operator: Observations of a "Charming" Adversarial Group

Allison Wikoff, *IBM X-Force*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

Learn about three-plus years of operations and mistakes of the prolific Iranian threat group ITG18, a.k.a. Charming Kitten. This talk is an expanded and updated version of IBM X-Force's July 2020 research on ITG18, a state-sponsored Iranian threat group whose self-recorded training and hacking videos were discovered in May 2020 due to an operational security error on their part. Specifically, this presentation will cover aspects of the research NOT included in the existing public blog, as well as subsequent observations on ITG18's activities since May 2020. This talk also will provide an in-depth look at ITG18's operations over the last few years and demonstrate how the operations have (and have not) evolved, their response to public disclosures, other operational security errors they've made over the years, and how they use their capabilities for multiple, blended short- and long-term strategic objectives. This discussion also will review why this group is so challenging to defend against and examine ways to mitigate the risks tied to their modus operandi.

AI and Cybersecurity: What is Our Role?

Shafia Zubair, *Morningstar*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

The usage of Artificial Intelligence (AI) has increased exponentially, but security and privacy governance and policies have not expanded at the same rate. The pace of instituting AI and privacy regulations varies across the globe, creating a rather complex governance structure for cybersecurity personnel to operate under. This talk will delve into the risks and benefits of using AI in cybersecurity. The presentation will explore the effectiveness of using AI in security tooling and how impactful AI-based systems are in safeguarding an organization's data confidentiality, integrity and availability. Then the group will discuss the impact of these AI-based security tools on risk management, security controls and the ability to maintain reasonable due care and due diligence in current complex regulatory landscapes. Participants will work through some scenarios, for example when AI-based systems malfunction or are subjected to an adversarial attack, in order to understand the operational and legal risks of such failures. AI coupled with machine learning has a tremendous potential to strengthen defenses, but the benefits of AI in cybersecurity must be contextualized against the risks it poses.

2021 WiCyS CONFERENCE BIRDS OF A FEATHER (BoaF)

BIRDS OF A FEATHER

Thursday • 4:45 pm - 5:30 pm

Things We Wish We Knew Before Starting Our Careers in Cybersecurity

Maggie Marxen and Bailey Bercik, *Microsoft*

TRACK: CAREER DEVELOPMENT

From classrooms and whiteboard sessions to teachers and layers of management, a career in cybersecurity is vastly different than where traditional education leads people. In 2018, Maggie Marxen and Bailey Bercik transitioned from being computer science students to working in cybersecurity for Microsoft. They will share what worked for them, what didn't, and what they learned along the way. In this collaborative presentation, they want to showcase multiple paths for breaking into this industry. Audience participation is highly encouraged. Participants will walk away with several important lessons, including methods for learning about up-and-coming tech trends, productivity tips, steps for increasing a professional network and more.

The Not-So-Well-Talked-About Topic: Fostering Allyship

Han Thazin (Hannah) Tun, *OmniSOC, Indiana University;* **Amy Starzynski Coddens,** *REN-ISAC*

TRACK: CAREER DEVELOPMENT

Simply put, being a womxn in cybersecurity is hard. There's imposter syndrome, culture that is predisposed to male peacocking, inappropriate comments, pay scale differences, and the so-called glass ceiling. Some mxn have been great allies. Some refuse to acknowledge the gap. So, the question people should ask is, "How do womxn address mxn?" "How do womxn point out differences and show them a womxn's perspective without getting called 'soft,' 'emotional' or 'dumb'?" The presenters will explore being a womxn and how best to address mxn who may be coworkers, subordinates or even bosses. The presenters also aim to provide real tips and tricks that are actionable in today's workplace.

Not Everyone Starts in Technology, Where Did Your Journey Start?

Dr. Kelley Misata, *Sightline Security;* **Deborah Kariuki,** *University of Maryland Baltimore County*

TRACK: CAREER DEVELOPMENT

Inspired by recent conversations inside the WiCyS pipeline working group, this interactive discussion will discover where people got their start and how their professional origins helped frame their work in cybersecurity today. Along with the audience, the presenters want to explore this issue and understand how to encourage more underrepresented and diverse groups to join this field. Filling the cybersecurity gap with computer scientists and technologists is undoubtedly needed. They will dive into how professional starting places frame (or don't) how to approach security. They will then tie in these experiences and brainstorm strategies attendees can adopt to help keep the door open for incoming generations of middle school, high school and college students.

Fostering a Transparent Security Culture to Reduce Insider Threat

Chrysa Freeman, *Code42*

TRACK: BEST PRACTICES

This short presentation will address cultivating a transparent security culture across an organization as a necessary strategy to reduce insider risk. It will be followed by an open dialogue discussion. Today's remote workforce functions across a broad range of digital applications. These heightened touchpoints compound the number of instances where security teams flag risk. When employees operate in a toxic culture and fear being called out, they create even greater security risks. As a result, 59% of IT security leaders expect insider risk to continue increasing. To combat that, organizations can foster a more transparent and trustworthy company culture where accusations and judgements are replaced with a greater understanding of expectations and collaboration. Code42 built a unique Ninja Program encouraging employees to learn the basics of security, creating a culture where they are comfortable sharing risks instead of hiding them.

2021 WiCyS CONFERENCE PANEL SESSIONS

PANEL SESSIONS Friday • 12:00 pm - 12:45 pm

Securing the Supply Chain: When Every Step is a New Weak Link

Bianca Steele and Jess Smith, *Pacific Northwest National Laboratory;* **Bob Hanson,** *Lawrence Livermore National Laboratory;* **Greg Shannon,** *Cybersecurity Manufacturing Innovation Institute;* **Cheri Caddy,** *U.S. Department of Energy*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

As the security threat landscape continues to broaden, technology becomes less secure. Supply chain security is becoming increasingly critical to all sectors of government and business as recent attacks demonstrate that pristine products straight from the manufacturer can come already compromised. The supply chain is under threat. In response, the U.S. government signed into law the Federal Acquisition Supply Chain Security Act of 2018, creating the Federal Acquisition Security Council. Now, government agencies are becoming more restrictive about what technology products can be used to ensure an agency's supply chain security. Supply chain security teams across the country are trying to verify the safety of every piece of hardware and software in their systems. Join four supply chain analysts as they discuss recent attacks as well as challenges they face investigating and ensuring the security of every type of device imaginable.

The New Threat Landscape in a Post Pandemic World

Priyam Biswas, *Intel;* **Awalin Sopan,** *Sophos;* **Abhilasha Bhargav-Spantzel and Michele Myauo,** *Microsoft;* **Reshma Shahabuddin,** *Sophos*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

The pandemic has posed a new set of challenges in the cybersecurity domain resulting in a 300% increase of cybercrime. A significant share of daily activities from professional work to household chores rely on a person's virtual presence. Attackers (threat actors) are taking advantage of this multi-fold increase of virtual footprints. The year 2020 saw a few changes, including a rise of remote office working but with low security/no vpn; more online activities; volatile market; and AI/ML used in newer attacks. Attackers are leveraging AI to take advantage of this situation. People are generally anxious during a pandemic and more vulnerable to cyberattacks. In this panel, the presenters will discuss what are some of these new challenges as well as how to prevent and overcome them. They will focus on the use of AI and other related technologies to help get there.

Acquire the Right Cybersecurity Competencies to Be More Prepared for a Job

Susanne Wetzel, *Stevens Institute of Technology;* **Dr. Sharon R. Hamilton and Zoe Fowler,** *Norwich University;* **Karen Wetzel,** *National Initiative for Cybersecurity Education (NICE)*

TRACK: CAREER DEVELOPMENT

The assessment for most academic programs is based on outcomes. Despite the fact that each student is expected to have achieved those outcomes upon graduation, there seems to be increased dissatisfaction among employers with the number of graduates lacking job readiness. This panel will explore the concept of competencies in cybersecurity as a means to bridge this gap. Specifically, the panel will discuss questions such as: What are relevant and necessary competencies in cybersecurity that students should seek to acquire? How can students determine whether or not they possess certain competencies? How can students know what competencies they can acquire as part of the degree programs? Are there ways to effectively build competencies in addition to degree programs? How can students document and display their competencies effectively?

Overcoming Imposter Syndrome in Cybersecurity

Noureen Njoroge and Dr. Mona-Lisa Pinkney, *Nike;* **Reena Madan,** *Verizon;* **Latisha Scarborough,** *Microsoft*

TRACK: CAREER DEVELOPMENT

Imposter Syndrome is defined as chronic self-doubt and a sense of intellectual fraudulence that overrides any feelings of success or external proof of competence. Cybersecurity professionals face a constantly challenging environment, in which they can easily feel out of their comfort zone. Recognizing how Impostor Syndrome can negatively impact success is critical, as is finding methods to overcome it. This group of accomplished panelists will reflect on how the current environment affected by the COVID-19 pandemic has been attributed to increased feelings of self-doubt, fraudulent beliefs, and the fear of being unmasked as an imposter. In addition, they will share how some of the most accomplished people in the world have suffered from this at some point in their lives. The panelists will give advice on how to mentally and emotionally adjust framed thinking. Just about everyone experiences Impostor Syndrome, and no one has to struggle alone. Anyone can overcome it and thrive in a cybersecurity career.

2021 WiCyS CONFERENCE LIGHTNING TALKS

LIGHTNING TALKS
Thursday • 11:00 am - 11:45 am

Community Crowd Sourcing for WiCyS Cybersecurity Resource Library

Meghan Jacquot, *WiCyS Resource Committee*

TRACK: CAREER DEVELOPMENT

At WiCyS, we are curating a Cybersecurity Resource Library for the general public. From scholarships, higher education, and research opportunities to online learning resources, resources about competitions, certifications, newsletters, podcasts, and other relevant organizations, we are searching far and wide to bring valuable information related to cybersecurity close to our community. Join us to build up and maintain these resources so that the library is fresh, useful and relevant. Find out how you can be a contributor.

A Strategic Approach to IoT Security: How an Organization Can Work Toward a Secure Future

M'Kaila Clark, *Empire State College*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

The fast growth of IoT devices and widespread adoption of this technology indicate an urgency in addressing security threats before deployment. Although IoT development is fast, it is advancing without a reliable security infrastructure to protect users. This lack of infrastructure is due to security measures being excluded from company business plans and lack of security configurations established during manufacture. Many companies do not include security in their business plan. Instead, security becomes an afterthought implemented in response to a particular threat, creating a gap between the advance in IoT and security needed to protect it. The deposit required to secure interconnected devices is massive, creating a slew of vulnerabilities for malicious individuals to exploit weaknesses. Vulnerabilities include lack of standard protection protocol, vulnerable device components, lack of update abilities, insecure data storage, insecure ecosystem interfaces, insecure network services and lack of device management. Robust security architecture is needed. How do IoT companies create a dynamic security approach to defend and combat threats while being flexible to accommodate technological advancements? This presentation will answer this question by addressing the strategic approach to developing a strong IoT security infrastructure that promotes confidentiality, integrity and availability with dynamic elements allowing for future developments.

Effectiveness of Threat Mitigation in Layers of the Open Systems Interconnection Model

Olivia A. Gallucci and Sylvia Perez-Hardy, *Rochester Institute of Technology*

TRACK: BEST PRACTICES

Security risks and mitigations are often covered by the press after large data breaches at big companies. Smaller businesses, however, also are at risk but do not have the resources to implement high-end cybersecurity protection nor the resources to survive a hack. This presentation critically examines past networking research that evaluates the effectiveness of security mitigations for each layer of the Open Systems Interconnection (OSI) model, and how cost-effective security mitigations can be implemented on a smaller business level. Research methods include an extensive reading of published research, journal articles, statistics and press articles on security threats and mitigations. The goal of the research is to provide a detailed understanding of networking and assist in hands-on applications of vulnerability mitigation. This complex study of security mitigation explores historical threats and enables future cybersecurity leaders to learn from historical failures. This presentation details the results of cost-effective security mitigations for each layer of the OSI model.

A Department of Defense Conference on Re-Entry for Women Veterans into Cybersecurity Careers

Rachelle Heller, *George Washington University;* **Costis Toregas,** *George Washington University and WiCyS Board Member*

TRACK: CAREER DEVELOPMENT

In order for the U.S. to remain a world leader in various fields of science and technology, it needs a robust and educated cyber workforce. The Center for Strategic and International Studies noted that "A recent CSIS survey of IT decision makers across eight countries found that 82% of employers report a shortage of cybersecurity skills, and 71% believe this talent gap causes direct and measurable damage to their organizations." No group is more well-positioned to fill this gap than women veterans. Compared to the general population, veterans bring extensive technical skills to the marketplace. Women, who have taken time off from their careers for family, military or personal reasons, are an under-looked yet ready population positioned to enter or re-enter a high-tech career. This presentation will address the crucial need to fill the exponentially growing cybersecurity gap. It will lead to a virtual invitation-only event, where practical strategies to overcome long-standing barriers will be shaped. This lightning talk will describe the conference agenda as well as the conference outcomes and roles that specific stakeholders will play to create structural changes to help close the gap, as well as support female veterans in finding strong career paths in cybersecurity.

2021 WiCyS CONFERENCE LIGHTNING TALKS

Demystifying Cyber Risk Metrics and Reporting

Priya Mouli, *LTI- Larsen and Toubro Infotech*

TRACK: BEST PRACTICES

This presentation will take a calculated approach to examining risk measures, metrics and reporting. First, it will define 'risk appetite' before diving into quantitative measures, risk metrics and key risk indicators (KRIs). Risk appetite is the aggregate level and type of risk a board and management are willing to assume to achieve their strategic objectives and business plan. Then it will look at the what and why of metrics. Risk metrics with thresholds and corresponding trigger actions can enable companies to stay ahead of the curve by getting visibility into risks before they occur and enabling proactive risk management. The presenter will look at the four steps in the KRI development process from key risk identification to metric definition. Along with this development process, there needs to be a metrics governance process for any changes. The next step in using KRIs, their trends and related data is to communicate them to enable risk decisions. Reporting is considered an upper management item but is important to be timely across all organizational levels from the day-to-day operational teams and middle management to leadership and the board. The presenter will talk about that and share recent experiences, success stories and case studies.

The Future of Ethical Hacking

Lauren Provost, *Norwich University*

TRACK: CAREER DEVELOPMENT

The digital world remains more vulnerable than ever with cybersecurity approaches now vital to the success of the digital economy. Approaches to cybersecurity have shifted dramatically in the past five years with new models to address the myriad of security challenges, especially with cloud computing and mobility. However, people and companies are still constantly chasing vulnerabilities. It is generally agreed upon that cybersecurity challenges must be handled as embedded in larger, complex cyber ecosystems. Comprehensive, multi-tooled approaches to cybersecurity are critical. Ethical hacking fits this need and has emerged as a more effective, multiple-strategy, comprehensive approach to cybersecurity's most pressing needs. Join the discussion on how the role of ethical hacking has become critical in cybersecurity, and learn new ways to enter a variety of pathways to becoming an ethical hacker. Several of the most challenging cases the presenter has handled over the years will be discussed.

Unmasking Cyber Command's Protections for the 2020 Election

Diana Parr, *SAIC*

TRACK: CAREER DEVELOPMENT

Few careers give people the opportunity to protect U.S. citizens from malicious cybersecurity threats. This presentation will discuss U.S. Cyber Command's role in the 2020 election and challenge the audience to appreciate the intense role of government agencies in preparing, supporting and executing capabilities to guarantee a safe and secure election free of foreign interference. This year's election included a multitude of challenges, such as mail-in voting, social media messaging, voting during a pandemic and more. This presentation will describe the preparation for the complex 2020 election with a "dress rehearsal" called Tabletop the Vote, a whole of government approach that incorporated key partners, including commercial companies involved in the voting process. The author will share some of those risks and how the teams mitigated them using familiar cybersecurity methodologies. When Election Day finally arrived on Nov. 3, many teams involved in planning were on high alert. While it took several days to count all the votes, certifications happened, and the team was confident the election was free from foreign influence and manipulation. This presentation also will discuss the various government job opportunities in the field of cybersecurity and how to apply for them.

Last Mile Education Fund: Investing in the Next Generation of Tech Talentr

Ruthe Farmer, *Last Mile Education Fund*

TRACK: CAREER DEVELOPMENT

While efforts to increase diversity within technology are working and enrollment is increasing, the structural barriers that impede success for students from low-income backgrounds remain. This prevents them from accessing opportunities required to compete with affluent peers. Leveraging insights from grant investments in 500 women and non-binary tech students, this talk will explore how corporate recruiting policies and procedures often inhibit access to these students and recommend solutions to level the playing field while reaching a significant untapped talent pool.

2021 WiCyS CONFERENCE LIGHTNING TALKS

LIGHTNING TALKS
Thursday • 1:55 pm - 2:40 pm

Improving Cybersecurity Field Preparedness by Gamification and Scenario-Based Activities

Molly Cooper, *Ferris State University*

TRACK: BEST PRACTICES

Cyberattacks are becoming more prevalent, and data, information and other assets can be lost. Increased sophistication and complexity can add difficulty in defending, recognizing and responding against such attacks. A critical line of defense against cyberattacks are well-trained cybersecurity professionals. Researchers highlight the criticality of training in cyber incidents for cybersecurity decision makers. Development and validation of cybersecurity skills, as well as testing cybersecurity preparedness at all levels of an organization, is needed before an actual event occurs. Rehearsing cybersecurity situations before they occur could prove beneficial for the decision-making process. Current and future cybersecurity students and professionals need to be prepared for cyber defense and response. This research investigates the effects of improving the cybersecurity preparedness gap by using realistic scenario-based role-playing games and capture the flag events as a way to train cybersecurity students on cyber incidents, readiness and response in order to recall scenario actions in the event of an actual crisis such as phishing, malware, DDoS attacks, resource constraints, compliance audits and ransomware. By rehearsing realistic cybersecurity attacks and situations, students were more involved with cybersecurity class activities; felt more prepared for cybersecurity situations; improved cybersecurity exam scores; and had a better grasp on cybersecurity concepts.

Highlights of Mainframe Security

Elizabeth Schweinsberg, *US Digital Service*

TRACK: BEST PRACTICES

Mainframe security is often relegated to compliance and auditing or full-disk encryption. Modern infosec topics of vulnerabilities, pen testing and threat detection are not well represented. In fact, there are only two CVEs for the most popular operating system – IBM's zO/S. There are plugins for testing parts of mainframes for popular pen testing tools, but there is limited information on digital forensics and threat detection. However, people must do it, right? This lightning talk will give an overview of mainframes, the current state of offensive security for them and how to learn more!

Crowd-Sourced Vulnerability Disclosure Program Working to Keep the DOD "Left of Boom"

Melissa S. Vice, *DoD Cyber Crime Center (DC3), VDP*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

Learn how the Department of Defense (DOD) became the first federal agency to establish a Vulnerability Disclosure Program (VDP) that now runs the largest ethical hacking program in the world. It also provides a legal means for security researchers around the world to discover and report weaknesses in DoD systems. Established in 2016, this program allows private, uncompensated security researchers to report vulnerabilities without fear of federal prosecution or civil liability if they comply with policy conditions. Every day over the past four years, these researchers have probed DoD websites for avenues of exploitation, discovering over 27,000 new vulnerabilities previously unknown to system owners and their automated scanning tools. DoD information systems and networks have been compromised through unpatched or unknown vulnerabilities in websites, systems, networks and applications. VDP's objective is to reduce the time between when a vulnerability is discovered and the issue is fixed by providing an open avenue to share directly with the DoD for remediation. This talk will demystify common misconceptions between the VDP and Bug Bounties, as well as introduce a new innovative pilot program designed to bring the VDP's lessons to the Defense Industrial Base. A number of cybersecurity career opportunities through VDP initiatives will be discussed.

Communities Within WiCyS Community: Special Interest Groups

Rian Sondag, *WiCyS*

TRACK: CAREER DEVELOPMENT

As a WiCyS community member, anyone has the ability to form special interest groups within the community portal. WiCyS has communities of cybersecurity apprentices, veterans and military spouses, nonprofits, high school students, LGBTQs, Asian Americans and Pacific Islanders, neurodiverse individuals and more! Join this session to learn about all the special communities within WiCyS. If there is not one that serves an interest, find out how to start one!

2021 WiCyS CONFERENCE LIGHTNING TALKS

2021 Executive Orders and What They Mean for the Software Supply Chain

Megan Moloney, *Guidehouse, National Security Segment*

TRACK: CURRENT TECHNOLOGY AND CHALLENGES

This Lightning Talk will concentrate on the executive order issued by the Biden Administration regarding supply chain risk management. This order specifically calls out cyberattacks and their ability "to reduce critical manufacturing capacity and the availability and integrity of critical goods, products and services." In the time allotted, the presentation will cover a condensed overview of the order itself, describing its focus on batteries, critical minerals/strategic materials and pharmaceuticals as well as the 100-day review requirements posed on the Secretaries of Energy, Defense, and Health and Human Services. There also will be a clear connection drawn as to how that order will impact the cybersecurity community. While seemingly narrow, it will have a broad reach and implications. Because of the presenter's professional role, she will be able to talk to these developments and bring timely supply chain risk management information to the audience, particularly those in the public sector.

Identity Governance: How to Prevent Reputational Damage

Vidya Ganesh, *Farmers Insurance*

TRACK: BEST PRACTICES

As recently as Feb 12, 2021, leaked credentials were used to gain access to the Oldsmar water treatment facility in Florida through remote access software known as TeamViewer. With the upending of business as usual norms as a result of the COVID-19 pandemic and more work happening virtually, cyberattacks are growing increasingly sophisticated and turning their focus to any public or private government, B2C, B2B, financial services, healthcare, pharmaceutical, insurance and utilities infrastructure. Compromise at any of these critical risk areas can bring down consumer confidence and negative impact to the economy, so the potential for damage cannot be ignored or misunderstood. Most often, these malicious attackers gain access through hacking the user accounts of an organization's employees and contractors. Tight access management and control of access to applications and data is critical to ensuring a secure, operating company. If recent internet security breaches were examined, it would be clear that nearly all of them could have been foiled with three simple security solutions as the first line of defense – multifactor authentication, secure reverse proxy and privileged access management. Join the discussion as these areas are covered.

Experience Leading a Deployed USMC Cyber Team

Svetla Walsh, *United States Marine Corps*

TRACK: BEST PRACTICES

This presenter led a U.S. Marine Corps (USMC) cyber team during her first deployment from 2020 to 2021. In 2018, she graduated from the U.S. Naval Academy, where she studied information technology and attended a number of tech conferences including WiCyS and Grace Hopper. While at the Academy, she experienced having only one woman technology professor, whom she witnessed hold her own among the computer science department faculty. The presenter was always interested in technology but did not own a computer until freshman year in college. Even after earning a Bachelor of Science in information technology, she still wanted to understand more about the tech field. After attending the Army Cyber School in Fort Gordon, Georgia, she was introduced to the certification process. It was an experience that taught her that being in the technology field meant being a life-long learner. Her background in computers plus professional experience as a USMC Cyberspace Officer has been challenging yet rewarding. By sharing her story, she wants other women to see themselves in places of opportunity within national security.

NICE Workforce Framework for Cybersecurity WiCyS Video Album

Dr. Ambareen Siraj, *CEROC, WiCyS;* **Mimi Vertrees,** *Tennessee Technological University;* **Rian Sondag,** *WiCyS*

TRACK: CAREER DEVELOPMENT

The National Initiative for Cybersecurity Education (NICE) Workforce Framework for Cybersecurity is a resource that describes the work and roles in the cybersecurity profession. WiCyS Video Album of the work roles is an initiative to feature WiCyS members, who are professionals in cybersecurity currently serving in these positions. Join this session to learn about the progress, see examples, and find out how to be part of this outreach initiative to generate awareness about cybersecurity jobs to the general public including students, parents and educators.

2021 WiCyS CONFERENCE STUDENT POSTERS

STUDENT POSTERS
Thursday • 9:45 am - 11:00 am

1. Anomaly Detection Model for Remote Patient Monitoring Based on End User Behavior

Deepti Gupta and Ali Saman Tosun, *University of Texas at San Antonio,* **Maanak Gupta,** *Tennessee Technological University,* **Smriti Bhatt,** *Texas A&M University- San Antonio*

Internet of Things (IoT) has grown rapidly in the last decade and continues to develop in terms of dimension and complexity, offering a wide range of devices to support diverse set of applications. With ubiquitous internet, connected sensors and actuators, networking and communication technology along with artificial intelligence, smart cyber-physical systems provide services rendering assistance and convenience to humans in their daily lives. Internet of Medical Things (IoMT) is a subset of the IoT and represents a connected infrastructure of medical devices, software applications, health systems and services. Remote Patient Monitoring (RPM) is a prominent IoMT application and secure RPM has become an active research domain. However, proliferation of IoMT devices increase the potential for malicious activities that can lead to catastrophic results including theft of personal information, data breach and compromised medical devices putting human lives at risk. IoMT generate tremendous amounts of data that depict user behavior patterns including both personal and professional day-to-day activities and daily routine health monitoring. In this context, there could be anomalies generated due to various reasons, such as unexpected user behavior, faulty sensor or abnormal values from malicious/compromised devices. To address this problem, there is an imminent need to develop a framework for securing the smart healthcare infrastructure while identifying and mitigating such anomalies. In this research, we focus on anomaly detection model to secure the healthcare infrastructure for IoMT applications. We propose an anomaly detection model that analyzes typical behavior of monitored users in the context of RPM, which comprises smart home and smart health devices, and identifies anomalous activities using the Hidden Markov Model (HMM). We setup a testbed with multiple IoMT devices and sensors to collect data and use the HMM model to train both network and user behavioral data. Based on the experimental results, our proposed model achieved over 98% accuracy in identifying the anomalies.

2. ComPriSec

Lisa McKee, *Dakota State University*

Data privacy laws have been around for years, but recent laws including GDPR and CCPA have increased the need and awareness of privacy assessments. Organizations are working to understand what these laws mean to them and how to conduct privacy assessments. There is a significant difference between Privacy Impact Assessments (PIA) and Data Protection Impact Assessments (DPIA), but knowing when to perform each is challenging. Additionally, PIA and DPIA do not account for all activities in a comprehensive privacy assessment program. Conducting privacy assessments requires coordination with teams in compliance, privacy and security (ComPriSec). There are often barriers when working cross-functionally. Some organizations may have one individual wearing many hats in a ComPriSec role, presenting challenges in defining the separation of duties between compliance, privacy and security. Teams may collectively decide to use zero trust as a method of addressing the risks identified throughout the privacy assessment process. This session will present a new privacy assessment methodology, solutions for ComPriSec conflicts and how to utilize privacy in a zero-trust world.

3. A Taxonomy of Cyberattacks in Smart Manufacturing Systems Through the Perspective of the NIST Cybersecurity Framework Manufacturing Profile

Bethanie Williams and Marena Soulet Vargas, *Tennessee Tech University*

A revolution in manufacturing systems is underway with smart manufacturing becoming an integral component of the broader push towards Industry 4.0. As the modern manufacturing industry continues to bridge digital and physical environments through the use of Internet of Things (IoT), cloud systems, data analytics and machine learning, this integration has led to an increase in cyber-physical attacks with ongoing discovery of new security challenges. In this poster, we present a comprehensive study of the common security challenges and attacks faced by smart manufacturing systems today and use the NIST Cybersecurity Framework Manufacturing Profile as a guideline to address cyber incidents that have occurred within the manufacturing sector. The attack taxonomy we present identifies, defines and classifies cyberattacks in the smart manufacturing sector and will aid both researchers and manufacturers to determine which business function(s) is/are at risk as a result of such attacks and take protective measures accordingly.

2021 WiCyS CONFERENCE STUDENT POSTERS

4. Analyzing How Priority Transformations Affect the Shape and Operation Speed of Self-Balancing Binary Search Trees

Alexis Vanderwilt, *Dakota State University*

Storage and fast retrieval of data is a fundamental problem in computer science. As more and more data is created, it becomes harder to search through quickly. This creates the need for a data structure that can efficiently store the data, allowing for quick information retrieval. Self-balancing binary search trees, also known as treaps, have become a popular option for data storage because of their search efficiency. Treaps use a random 'priority' value sorted with a heap to keep the binary search tree balanced, which optimizes the searching speed. The purpose of this work is to determine if data locations in a treap could be modified in a way that allows commonly searched items to be retrieved quickly. This would create a new type of data structure that speeds up search time for common objects, giving most users a faster response time. This is especially important in large databases that are often searched through. This creates a data structure that shows what elements are most important to users because the most searched for items will be near the top. This is an important aspect to analyze as this may impact the security of the data structure. Showing which items are most important to users may create a target on those items for hackers to exploit. Additionally, cybersecurity professionals may be able to use this data structure to recognize patterns they could not see before in a target's search history or in their files if used while developing penetration testing tools. This work aims to weigh the pros and cons of new data structure against existing solutions.

5. Cryptanalysis of WPA3

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

In 2016, Key Reinstallation Attack (KRACK) was discovered, which made billions of devices vulnerable to data theft and manipulation. It showcased a serious flaw in the way WPA2 was engineered. After the discovery of this attack, Wi-Fi Alliance started the shift toward the successor of WPA2, which would be more secure than its predecessor. WPA3 was launched in 2018 as the next generation of Wi-Fi security. It is built upon WPA2, providing security and countermeasures against attacks that affected WPA2 while also retaining backward compatibility with WPA2. WPA3 introduces three new protocols and suites, namely Opportunistic Wireless Encryption (OWE), Simultaneous Authentication of Equals (SAE) and WPA3-SAE Enterprise that contain new cipher suites and encryption methods to make it difficult for attackers to read the client's data transmission streams. WPA3-SAE, based on dragonfly key exchange, is a Password Authenticated Key Exchange (PAKE), i.e. it turns the password into a high entropy key decreasing the chances of the key being discovered. It replaces WPA2-PSK, which was vulnerable to offline dictionary attacks and prevents the KRACK against a four-way handshake. Dragonfly Handshake also provides security when connected with an access point that only supports open Wi-Fi mode. OWE addresses problems in open networks by encrypting all the traffic hence blocking passive attacks. In transition mode, OWE supports 802.11 "open" authentication. An AP in OWE transition mode will have two virtual access points (VAP) – one to connect with "open" and another to connect with OWE. Since SAE uses Dragonfly Handshake, a crucial part of WPA3, and affects the enterprise security part of WPA3, a lot of research has been done to discover the attacks on it and mitigation tactics. Not much attention has been given to OWE suites as its main function is to provide backward compatibility with open mode Wi-Fi. Our research is divided into two parts. First, we discovered two new attack vectors against WPA3-OWE suite. Because WPA3 is not an authentication protocol and uses Diffie Hellman Key Exchange which is susceptible to Man-in-the-Middle attack, we researched and found that theoretically OWE also is susceptible to this same attack. For another attack, we exploited code 77 that an Access Point (AP) sends in one of the management frames if the client requests a cryptographic suite not supported by the AP. Second, we tried to come up with new mitigation schemes for two of the attacks discovered on WPA3-SAE suite, attack on SAE in downgrade mode and attack on multiplicative groups that the client and AP agree on to be used for encryption during the authentication frame exchange.

2021 WiCyS CONFERENCE STUDENT POSTERS

6. Cybersecurity Policy Constructs: Lessons from Congress' Approach to Cybersecurity

Jennifer Lake, *The University of Texas at Austin*

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

This poster proposal is a part of a larger research project that will explore how the U.S. Congress has treated the issue of cybersecurity from the 1970s through 2018 (the 93rd through 116th Congresses). This poster will showcase the analysis of Congress' work during the 99th Congress when it passed the Computer Fraud and Abuse Act (CFAA). The work will examine the text of cybersecurity-related bills introduced and identify not only a dictionary of cybersecurity-related terms but, more importantly, will identify latent cybersecurity constructs in the bills. These policy constructs will tell us a great deal about how Congress has interacted with cybersecurity as a policy issue, what concepts have been enacted, and what constructs have not been enacted (which policy options Congress discarded or has difficulty enacting). The illumination of these constructs will provide a comprehensive understanding of the cybersecurity legislative landscape and the policy environment that confronts policymakers today. The unique contribution of the work proposed here is to analyze the full scope of the congressional cybersecurity policy debates. Much has been written concerning existing (enacted) cybersecurity policy, but nothing has yet comprehensively addressed the full scope of the work of Congress on the issue. So, the first contribution is to compile this complete legislative history. The second major contribution will be to develop the latent cybersecurity policy constructs embedded in the legislation. The research will use topic modeling techniques paired with selected manual reviews to conduct the analysis. The third contribution will be to analyze the cybersecurity policy constructs to understand why certain ones were enacted while others were not. This analysis will potentially assist future policymakers in legislating cybersecurity policy. The fourth contribution will be an analysis of the current (2020) state of the cybersecurity policy environment and look to the future at those constructs or issues that still need to be addressed.

7. An Algorithm for Fingerprint Authentication

Catherine Berrouet, *Florida Atlantic University*

An authentication algorithm using Delaunay Triangulation is introduced for detection of a matched pair of fingerprints. For this algorithm implementation, we sample a set of minutiae points for a pair of fingerprints and find the largest maximal clique for each fingerprint's triangulation to obtain the largest set of mutually consistent point pairs by using defined rotation-invariant feature vectors in the matching process. The first implementation of this algorithm is presented. The accuracy of this implementation is proved under the construction of a Delaunay Triangulation.

8. Exploring Feasibility Problem in Access Control Policy Mining Domain

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

Access control means only legitimate users get access to resources inside the system. To elaborate, access control generally regulates access to system resources based on many possible criteria, e.g., verifying the user credential, environmental condition, resource characteristics, etc. With the growing complexity and advancement of technology, new robust and resilient models are being added in the access control domain to keep pace with the rapidly changing requirements. As a result, access control research emerges from the earliest access control matrix to new paradigms, such as Attribute-Based Access Control (ABAC) and Relationship-Based Access Control (ReBAC). Instead of starting from scratch with a new model, another aspect of coping with real-world challenges is migration, which saves time, money and efforts. When a system is protected by an established access control model, the process of automated migration to another model is called the policy mining problem. In general, policy mining works require the existing model and various supplemental information to migrate from one system to another. According to the current literature study, policy mining tasks are most often guided through sets of certain assumptions. For example, the generated access control system must be semantically equivalent to the existing one along with an identical set of users and resources. Our work begins here: We question the feasibility of access control policy mining under certain assumptions. A formal name has been given to this quest, feasibility problem of access control policy mining, which is essentially an insightful

2021 WiCyS CONFERENCE STUDENT POSTERS

study of various forms of policy mining problems. In this study, the concept of feasibility analysis in access control policy mining domain will be showcased with respect to two renowned access control paradigms – Attribute-Based Access Control and Relationship-Based Access Control. A brief overview of feasibility detection algorithms, the workflow and associated complexity will be presented as well. Finally, the pros and cons of the presented approaches will be discussed with future directions.

9. Memory Analysis of macOS Userland Runtime using Objective-C and Swift Data Structures

Modhuparna Manna, *Louisiana State University*

In recent times, there has been a huge surge in the number of macOS malware samples. There have been many instances where nation states, criminal groups, intelligence agencies and individual hackers have targeted macOS users, resulting in huge financial losses and compromised highly sensitive data. Compared to the earlier days, when kernel malware attacks were more common, today there is an increased emphasis on userland malware. macOS malware samples such as Crisis, Ventir, Realtime-Spy, etc., contain userland components, which can perform malicious activities such as keystroke logging, taking screenshots and so on. Unfortunately, there has not been an equal amount of growth in the field of cybersecurity to combat the novel techniques utilized by the macOS userland malware. Currently, there exists a huge gap in the research and development on the defense side, and there is an urgent need to develop and implement new methods to detect and analyze sophisticated userland malware.

Historically, during a cyber-crime investigation, the general trend was to pull the plug and send only the hard disk for investigation. This led to the loss of forensic artifacts present in the physical memory (RAM) of the compromised digital device. Today, with the growth of Memory Forensics, we can take a live capture of the compromised system and analyze information related to network connections, processes, clipboard data, private browsing data and so on. Memory Forensics is especially helpful if we do not have the application source code to reverse engineer or the application executable to be able perform binary analysis. To perform a memory analysis, we only need a memory snapshot of the compromised system, which we can gather using the existing memory acquisition tools. Furthermore, there are memory analysis frameworks such as Volatility and Rekall, which provide plugins to analyze the memory snapshots. However, there are hardly any existing plugins to analyze macOS application data.

In this research effort, we contribute to cybersecurity research by writing plugins for one of the most popular memory analysis frameworks, Volatility. Our plugins help detect and analyze macOS malware as well as find information in macOS benign applications. Forensic investigators of all skill levels can leverage these plugins to perform memory analysis on macOS applications in an automated, scalable and flexible manner.

In this research, we look into the Objective-C and Swift source code (open-sourced by Apple) and study the memory layout of the relevant data structures. We then analyze macOS memory snapshots to locate these data structures and find information about the macOS application. We can find information about the list of classes, instance and class methods, instance and class variables, and the values stored in the variables. We identify data types including characters, strings, URLs, integers, floating-point numbers, boolean values, class pointers, type pointers, etc. We have written three volatility plugins: mac_analyze_classes provides information on the list of classes, mac_analyze_variables is used to analyze the variables, and mac_analyze_code helps identify the instance and class methods. Our work is an important contribution to Memory Forensics as it helps in the forensic analysis of both malicious and benign macOS applications. Forensic investigators can now find suspicious classes, persistent methods and interesting information such as URL and string data contained in instance variables of macOS applications. We also can find forensic artifacts, including chat messages, notes, timestamps, etc., from non-malicious macOS applications such as messages, calendar and clock. To test our plugins, we have created a malware testbed containing macOS malware samples and used our plugins to analyze these malware samples. Presently, we are able to gather interesting information with respect to classes, methods and instance variables used by real macOS malware samples such as Ventir, Realtime-Spy and Mac Loader.

2021 WiCyS CONFERENCE STUDENT POSTERS

10. On Reliability of Userland Memory Forensics

Sneha Sudhakaran and Golden G. Richard III, *Louisiana State University***, Aisha Ali-Gombe,** *Towson University*

This research examines the impact of critical runtime activities in memory acquisition and evidence recovery for userland memory forensics on Android devices. Specifically, we focus on the effect of Garbage Collection (GC) and process states as metrics for memory analysis' reliability. On Android, a process runs in its distinct environment called the Android Runtime (ART) and allocates objects in RegionSpace and LargeObjectSpace memory maps. Unused objects are deallocated and removed from the memory maps using the Concurrent Copying GC algorithm. When executing, a process can occupy five distinct states – foreground, background, visible, service and empty. In this research, we perform an in-depth analysis of 120 memory images acquired with the following GC and process state combinations – foreground and no GC triggered; foreground and GC triggered; background and no GC triggered; and background and GC triggered. Using DroidScraper and AmpleDroid, we recover the remnant of in-memory objects from all the images. The evaluation results demonstrated that more objects are recovered when the process is in the background, and no GC is triggered. We also examined some significant changes when GC is triggered, and the object is in the foreground. We concluded that external factors such as GC and process states can have some significant effect on forensics recovery, and our new metric can help analysts determine the reliability of evidence recovery based on the state of a target process.

11. The Psychology Behind Cybercrime

Anastasia Kolovani, *Rider University*

Cybercrime is increasing at a high-speed rate. Cybercriminals are getting smart in their attacks, and more individuals across the globe are becoming victims. Types of cybercrimes include cyberstalking, where an individual is relentlessly harassed in the cyber realm, identity theft and Denial of Service attacks, to name a few. The internet, while it has opened so many opportunities and brought people together, also has a dark side that provides a lot of ease for criminals because of its anonymity and lure to different crimes. Cybercrime, unlike crime in the physical realm, is invisible. You don't see the perpetrator or even know you have become a victim until your identity has been stolen, you have lost access to all your devices or this invisible criminal is now watching your every move in the physical and cyber realm. Understanding the psychology behind cybercrimes can eventually lead to a discovery of ways to put an end to these crimes. This includes understanding the why behind these kind of attacks. It's important to know what triggers cybercriminals and how they plan their attacks. Are victims chosen at random or is there more of a methodology behind each attack? What is the cybercriminal really looking for? Looking at the psychology of the victims is important as well because we need to see what victims of a certain cybercrime (like identity theft) all have in common. Are certain personalities more likely to become victims of cybercrime? Are certain age groups more sustainable as well? It is important to understand how this can be stopped. We can address this by looking at different methodologies used and working on new and improved ways to use psychology in detecting crime while making individuals more aware of the dangers of the internet and how they can better protect without overwhelming themselves.

12. Finding a Topology Obfuscation Method for IEEE 802.15.4 Protocol

Sara Schwarz, *Carnegie Mellon University, Information Networking Institute*

The Internet of Things, an area of work where common daily devices are being connected to the internet, is growing quickly, which in itself is creating new risks. Security in this area now concerns the physical wellbeing of the users in addition to their digital data. This fact should enforce the persistency in the field's security research. Researchers looking into vulnerabilities in the Zigebee Network (Dimitrios-Georgios Akestoridis, Madhumitha Harishankar, Michael Weber and Patrick Tague. 2020. "Zigator: Analyzing the Security of Zigbee-Enabled Smart Homes." Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks, WiSec '20, Association for Computing Machinery, New York, NY, USA, 77–88. DOI: https://doi.org/10.1145/3395351.3399363) found an information leak at the MAC Layer, which states that by analyzing the MAC headers, the topology for a Zigbee Network can be inferred by simply pairing and keeping record of the source and destination addresses from the MAC headers between packets. The IEEE 802.15.4 protocol is the standard for the MAC and PHY layers being used by Zigbee and many other IoT Networks. This protocol does not enforce encryption for the packets' MAC headers when being sent through the network, providing this leverage for reconnaissance attacks.

There are a couple of attack scenarios that can break a Zigbee Network and create a digital and physical threat to users. These attacks, because of their complex nature, need to be strategized and thought out. The vulnerability

2021 WiCyS CONFERENCE STUDENT POSTERS

in inferring topologies can provide an attacker with a motivation based on the possible reward they could acquire and the effort and resources they would need to put into the attack, which is information they could infer by the topology. For example, by knowing the size of the network, an attacker can infer how many resources they would need, or by knowing whether there are various networks connected through one device could mean an attacker can create a small attack through that one device and create a bigger aftermath by affecting both networks. Being able to know the network's topology also will provide the attacker with an outline from which they can create an attack plan based on strategies formed by having an idea of how the network is set up.

The contribution of this project is specific to helping fix a leak in the IEEE 802.15.4 protocol. The risk and harm of this leak is specific to threat models where sophisticated attacks are being used and the attack model has passive listeners. This project will show the efficiency in running a Topology Obfuscation method for the IEEE 802.15.4 protocol, which will ensure information regarding the network's topology cannot be inferred by passive listeners while maintaining the use of low energy consumption. Since research concerning ad hoc networks is a novel area, this project also will help provide resources or insight for others in the community. The project has already begun the contribution process for the NS3 Open Source Simulator project in providing the missing association primitives for the 802.15.4 standard.

13. Cyber Attack Exploitation of a Smart Farm Architecture

Sina Sontowski and Maanak Gupta, *Tennessee Technological University*

Smart farming is taking on a bigger role in the agricultural sector due to its ability to tackle global food shortages by increasing supply. A smart farm might have internet-connected devices such as sensors that allow for real-time monitoring of crops and livestock or even drones to assist with pesticide deployment. However, the use of internet-connected devices opens the smart farm up to vulnerabilities that attackers can exploit. A potential attacker can remotely control the devices, which can cause devastating consequences, especially during harvesting where it's of uttermost importance to monitor crops in real-time. During my research, I performed a Denial of Service attack on a smart farm architecture. I was able to proof with a deauthentication attack that it is possible for an attacker to hinder normal farming operations. I am currently expanding my work by including more protocols. A Zigbee sensor has been incorporated for more attack scenarios. I am planning to execute a man-in-the-middle attack involving data injection.

14. Recruiting From Marginalized Girls with Workshops on Cryptography, Coding & Cybersecurity

Vanessa Primer, *Pierce College District*

How do we get youth into the pipeline, specifically those from marginalized communities? I was privileged to volunteer with Expanding Your Horizons, and I created and presented workshops on Cryptography, Coding & Cybersecurity: A look at fun historical facts like hairstyles being used to hide maps, inspirational women in STEM, and an interactive "Hour of Coding" Caesar Cipher activity. I examined how ciphers work and what else a cipher can do, to how things can go wrong. How did we get from the Caesar Cipher to post-quantum cryptography and algorithms? This is a history and a look into the future with our future women in cybersecurity. I also have signed on to the planning committee for the Highline Youth STEM Conference, at Young Educated Ladies Leading, the Black and Brown Male Summit, and for Geek Girl Con in the DIY Science Zone. My poster shows the workshop and activity I created to be used to promote STEM. To make this a fully interactive session, each girl received her own cipher wheel. We coded, encoded and discussed how cryptography is part of our daily lives. With the girls leading the direction, we nested and reversed codes and found ways to make them more secure.

2021 WiCyS CONFERENCE STUDENT POSTERS

15. Application Labeling Using Time-Based Network Flow Features as an Alternative to Packet Payload-Based Methods

Anusha Sinha, Konstantina Dimaki, and Joshua Fallon, *The Software Engineering Institute at Carnegie Mellon University*

Network flow data has been used by network administrators and security professionals to analyze, optimize and defend for decades. The shift in recent years toward new network protocols that encrypt packet payloads by default or misuse older protocols has led to increased difficulties in labeling applications or protocols in flow data. In this work, we propose application and protocol identification methods using machine learning models trained on time-based features extracted from network flow data. We show these methods are agnostic to encryption or the misuse of older protocols. Network flow maintains its relevance in the cyber intelligence community because it is still the most efficient way to collect information on traffic in large networks. We therefore focus our efforts on classes of models that provide fast inference times, specifically shallow decision trees, shallow neural networks and ensembles thereof. We use statistical models of payload entropy between protocols to augment the machine learning models and classify protocols based on whether time-based flow features or more standard payload-based logic is more effective for identifying the protocol. Finally, we present a large-scale, labeled dataset for the advancement of application and protocol inference using features derived from network flow data.

16. Using The OneUp Gamification Platform For Making A Difference To Overall Student Experiences In Online Undergrad Cybersecurity Courses: A Preliminary Research Study

Momoka Kinder, Meghyn Winslow, and Ankur Chattopadhyay, *Northern Kentucky University*

With the emergence of the COVID-19 pandemic, a lot of the in-person cybersecurity courses had to transform into online, asynchronous classes. Achieving student motivation, engagement and active participation in such courses can prove to be a challenge for instructors amidst this ongoing pandemic. Existing literature shows there have been prior studies that use gamification tools for increasing student motivation and engagement in cybersecurity classes, in particular online courses. The OneUp platform is one such unique gamification tool for learning that utilizes proven game design principles through warmup exercises and serious challenges. This motivates students by helping them earn digital badges and virtual currencies, resulting in increased student engagement and enhanced learning in online courses across multiple computing disciplines. However, even though there have been previous instances of research studies on student motivation and engagement using OneUp in computing courses, there has been limited research on the benefits of using it in cybersecurity classes, particularly the online, asynchronous courses at the undergraduate level. In this poster, we present our unique preliminary research experiment to study the impact of using OneUp as a supplementary aid in a couple of online cybersecurity courses based on introductory cybersecurity topics for undergraduates.

We describe how we used OneUp to add different gamification elements in a variety of gamified practice exercises with different difficulty levels, i.e., warmup questions and serious challenges, which offer digital badge earning opportunities for students. We discuss how we created this additional OneUp layer of gamified instructional scaffolding to support the student learning process, supplement the online learning environment of two cybersecurity classes, and motivate students to gain further skills and more knowledge in beginners' cybersecurity topics. We show how our supplemental gamified components helped enhance the learning experience for participating students by boosting their motivation and engagement, thus contributing to further development of cybersecurity knowledge and skills through routine practice and self-testing. We then share our initial results from this experiment that includes a comparative study of the learning assessment-based outcomes of the online students who chose to use OneUp as a supplementary learning aid with the performance outcomes of those online students who opted out of it. Additionally, we share the quantitative and qualitative data we obtained through student survey responses based on their OneUp usage experiences. We also analyze the preliminary learner data that we collected during this research experiment, in an initial effort to determine OneUp's potential for improving overall student experiences, in terms of motivation, engagement and performances. We finally list our reflections and takeaways from this strategic study of using OneUp as a gamified learning tool in online undergraduate cybersecurity courses.

2021 WiCyS CONFERENCE STUDENT POSTERS

17. Forensic Analysis of popular alternative apps to TikTok: Byte, Dubsmash and Triller

Yansi Kim, Shinelle Hutchinson, Maanasa Govindarajan, Apoorva Shrivastava, and Umit Karabiyik *Purdue University*

As of 2021, TikTok has unprecedently become one of the most used social video platforms. Due to its Chinese origins and alleged data privacy violations, many TikTok enthusiasts considered moving to alternative social video platforms. To that end, numerous substitute related apps have appeared on the Google Play store and Apple's app store. In this poster, the authors identified the three most downloaded alternative apps to TikTok and forensically analyzed each of them on Samsung Galaxy S7 (Android 8) and iPhone 7 A1660 (iOS 13.3.1) smartphones. These alternates are Dubsmash, Byte and Triller. The forensic investigation was conducted from the data and user privacy lens, identifying and reporting relevant artifacts to further aid investigators during a digital criminal investigation.

This study follows the forensic investigation model suggested by the National Institute of Standards and Technology (NIST) for populating mobile test devices. The forensic software tools used to acquire these devices included Cellebrite UFED 4PC and Magnet AXIOM Process. Cellebrite and Magnet are extensively used and accepted by digital forensic investigators and courts of law. The methodology included populating both devices using a series of steps. The authors downloaded and signed into three apps using dedicated email accounts. Following NIST guidelines, they set up interaction between Android and iPhone user accounts, including (1) creating video content; (2) posting this content on the feed; (3) saving content into the phone's gallery; (4) testing the auto-destruction feature present in these apps; (5) following and unfollowing hashtags and other people's accounts; (6) blocking people's accounts; (7) exchanging text and multimedia messages; (8) testing draft messaging features for possible cloud storage; (9) searching keywords; (11) liking, commenting and resharing other's content; and (12) downloading other people's content into the phone's storage.

The examination and analysis of the resultant forensic images were done using Magnet AXIOM Examine. For Samsung's forensic image, the file size was 29.7 GB, and for the iPhone was 8.68 GB. The investigation of these apps exposed a multitude of data and privacy leakage areas in both phones. For example, Byte stored the database file byte.db on Android, which stores all the account and social media activity-related information in plain text. This information included the user's entered bio information and URL links to their profile pictures. The authors identified the number of followers, a binary value for if followed, unfollowed or blocked, along with associated usernames, exchanged messages, geolocations of the videos, whether these videos were deleted or not, hashtags followed and unfollowed, and comments made on other users' posts. The analysis of the Dubsmash app on iOS indicates the logs of user interaction with the app as the authors were able to recover the timestamps for the user's last like, post and join date. Additionally, they recovered the user's birthday, username, email address, URL links to the videos posted, and URL links to videos other users posted. They also could get the join date for other users whose videos showed up in the app user's "For You" section. Overall, these apps pose significant user privacy data leaks, which are uncovered in this investigation.

18. Automating Binary Analysis of PLCs

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

Binary analysis is used to discover and exploit vulnerabilities in the binary code and prove or disprove properties of the code actually executed. In the past, several efforts have been made in automating binary analysis of software. One example is the Angr framework. However, this framework supports only a limited number of architectures that do not include those for programmable logic controllers (PLCs). These PLCs are a critical component of Industrial Control Systems that directly monitor and control a physical process such as a nuclear plant, water treatment and gas pipelines. Given their importance, they often are a target of attackers who intend to disrupt an industrial process. PLCs come with firmware installed in order for them to function the way they should. Like all software, the firmware installed can have bugs, and it is imperative to identify these before the product is released into the wild. Our work extends the Angr framework to support the architecture of PLCs such as Schneider Electric's Modicon M221 PLC. We then use the framework to identify certain vulnerabilities and launch attacks on the PLC. We also extend this framework and add a model of authentication bypass flaws based on the attacker's ability to determine the required inputs to perform privileged operations.

2021 WiCyS CONFERENCE STUDENT POSTERS

19. Empirical Analysis of PLC Authentication Protocols in Industrial Control Systems

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

Programmable logic controllers (PLCs) are embedded devices widely used in Industrial Control Systems for the automation and control of physical processes such as nuclear plants, power grid stations and gas pipelines. They are equipped with a special program called control logic that defines how to control these individual processes. Attackers target control logic of a PLC to sabotage a physical process. For instance, Stuxnet has infected the control logic of a Siemens S7-300 PLC to manipulate centrifuges' motor speed periodically from 1,410 Hz to 2 Hz to 1,064 Hz. Most PLCs employ password-based authentication mechanisms to prevent unauthorized acquisition of or modification to the control logic they run. This poster helps attendees gain an understanding of proprietary authentication mechanisms and serious authentication protocol design issues in five industry-scale PLCs by four different vendors — Allen-Bradley, Schneider Electric, AutomationDirect and Siemens. We present a study that first determines the proprietary protocol used by each PLC followed by identifying vulnerabilities in the authentication mechanisms, including lack of nonces, weak password hash encoding, small-sized encryption key, weak encryption algorithm and client side authentication. Finally, we confirm the vulnerability discoveries by creating and testing their proof-of-concept exploits derived from MITRE ATT&CK base of advisory tactics and techniques. For a brief illustration, consider Modicon M221 PLC. After studying its authentication protocol, it is discovered that while reading the PLC memory requires password authentication, the PLC does not restrict an unauthorized user to overwrite a password hash in the PLC memory remotely, making it vulnerable to password reset attack. We have disclosed the vulnerabilities to respective vendors who have already released firmware patches and respective CVEs.

20. Enriching Honeypot Data using Cyberthreat Intelligence

Caitlin Allen and Adam Cunningham, *Champlain College*

Cybersecurity is a rapidly growing field that becomes more complex as time goes on. There are numerous aspects of security that branch out into their own equally complex fields. Many companies and organizations struggle to properly prepare for attacks against them and fail to utilize threat intelligence or offensive security measures to mitigate these attacks. Many experts struggle to properly digest the information that can be provided by threat intelligence. This project aims to take data gathered by honeypots to enrich reports that can be provided to cybersecurity experts to improve their security posture. While honeypots and threat intelligence are properly established in the field and have copious research behind their workings and capabilities, the knowledge around applying them to a readable format is limited. This research aims to bridge that gap between threat intelligence and security hardening. The project will be accomplished by creating a virtual network that emulates an enterprise network. Offensive security mechanisms will be installed on these machines in the appropriate sections to produce the results needed for enriching reports.

WiCyS COMMUNITIES

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

Professional Affiliate Community
Together. We Grow.

Student Chapter Community
Together. We Achieve.

2021 WiCyS CONFERENCE STUDENT POSTERS

21. Teachers Perception and Understanding of Zoom Security within the Digital Transformation of the Classroom Caused by COVID-19

Taryn DeRubertis and Lila Rajabion, *SUNY Empire State College*

At the beginning of 2020, the world changed forever because of COVID-19. With lockdowns implemented across countries, a digital transformation occurred in most classrooms. With everyone forced online, traditional classroom security ideas were forced to change overnight. Teachers have been prepared on what to do during a lockdown within a school system or how to handle children in traditional classrooms. As COVID-19 hit so quickly, teachers may have been underprepared on what security protocols needed to be implemented while meeting online. With unprepared teachers and unclear security guidelines, which may not have been implemented properly, this led to something called "Zoom bombings." These occur when a nefarious user or users gain access to a Zoom meeting and proceed to cause havoc within it. Through research and surveys, we look to answer how Zoom has improved security since the beginning of the pandemic and how it is training teachers to become familiar with setting up these virtual classrooms to prevent Zoom bombings. This paper will answer these questions by examining Zoom's security history and teacher surveys on how they have become trained on its security. This paper will explore and ask teachers what tools they suggest could be improved or implemented within the Zoom security framework to help teachers better secure their digital classrooms.

22. The Automated Attribution Problem: Qualitative Attribution Analysis in a Data-Driven World

Katherine Schroeder, *Marymount University*

There is a need in the cybersecurity field, particularly in the area of threat analysis, to develop automated reasoning tools that can tackle difficult, expensive and time-consuming tasks of cyberattack attribution. While several tools and methods have been developed and studied, at this time none of them appear to have reached an acceptable level of reliability and still require manual threat analysis as input. Using scoring tables and metrics, the author examines repeatability, reproducibility, scalability, input quality dependence, and the rate of success of automated reasoning tools against themselves as well as with each other. This study shows that while leading threat analysis tools are a promising concept, they fail to provide a reasonable level of reliability at this time.

AFFILIATE MEETUP

TOGETHER. WE GROW.

Friday, 10:15am - 11:00am - Summit 2-3

Come meet affiliate leadership from small, medium, and large affiliates as they form a freestyle panel to support all your efforts in the local affiliates. We will talk strategies. best practices, social media and much more!

Bring your questions and let's grow stronger and soar together in 2021!

WiCyS STUDENT CHAPTER MEETUP

TOGETHER. WE ACHIEVE.

Friday, 11:15am - 12:00pm - Summit 2-3

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

Adobe

Let's create trusted experiences that matter

Making great experiences requires trust. At Adobe, we're committed to protecting the security, privacy, and availability of our products, systems, and data — so our customers can deliver trusted experiences to users every day. Learn more and consider joining our team today.

adobe.com/careers
trust.adobe.com

Google

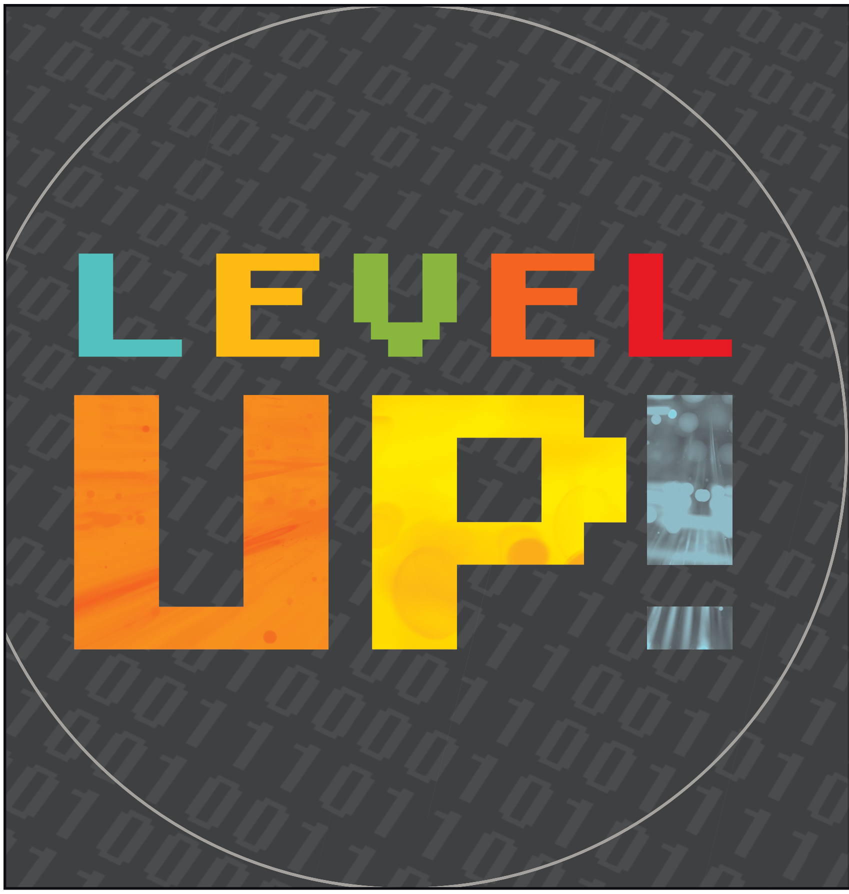
Every day you're safer with Google

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



Investigate. Analyze. Develop. Operate. Protect.

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

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

mastercard.com

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

Women in STEM at the National Security Agency

CYBERSECURITY GLOBETROTTER

Passionate About Mentoring the Next Generation – Especially Girls

Sturhonda James
NSA Cybersecurity Liaison

Sturhonda James is making the most of her career at NSA. She's been working in cybersecurity in Hawaii for four years, and now overseas. James likes the fact that at NSA, she has the ability to give back to the community. She volunteers for a youth cyber program and the NSA K-12 Speakers Bureau, which sends employees into schools to give talks on STEM.

"I am super passionate about mentoring the next generation of cybersecurity professionals and giving young girls who aspire to work in cybersecurity reflections of themselves."

Learn more at IntelligenceCareers.gov/NSA

NSA offers technical professionals:

- **Tuition Assistance**
- **Professional Training & Development**
- **Leadership Opportunities**
- **A Friendly Environment that Fosters Innovation**
- **The Time to Enjoy Family & Friends**
- **An Opportunity to Contribute to the Good of the Nation**

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

Secure the Future of Cybersecurity

Meet our staff at **Booth 111** and learn more about career opportunities at the Software Engineering Institute.

Apply today! Visit our website for more information. **sei.cmu.edu/careers**

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.

Program Highlights:

- NSA Center of Academic Excellence – CDE
- First CyberCorp NSF SFS program in the State of TN
- Only DoD Cyber Scholarship (CySP) Program in TN
- CyberEagles student cybersecurity club
- NSF Women in CyberSecurity- Founding Institution
- WiCyS Student Chapter (CyberEagles-W)
- NSF-NSA GenCyber Camp Program
- CTF, defense and offense competition teams
- **The place to be for cyber in Tennessee!**

1020 Stadium Drive • POB 5134 • PRSC 414 • Cookeville, TN 38505 • (931) 372-3519
ceroc@tntech.edu • http://www.tntech.edu/ceroc • @TNTechCEROC

Authenticity defines me.

ShuDon
Raleigh, USA
ibm.com/careers

IBM

IBM and the IBM logo are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available at ibm.com/trademark. ©International Business Machines Corp. 2021.

praetorian

We help today's leading organizations gain confidence that their place in the next wave of innovation is secured.

Praetorian is a cybersecurity solutions company whose mission is to make the digital world safer and more secure. Through expertise and engineering, Praetorian helps today's leading organizations solve complex cybersecurity problems across critical enterprise assets and product portfolios. From the Cloud to IoT, we are bringing together the world's security expertise to solve the cybersecurity problem and secure the next-wave innovation.

Our Approach

First we find, then we fix, then we stop, then we solve.

Our Vision

To solve the cybersecurity problem.

Our Mission

To make the world a safer and more secure place.

RICE

MASTER OF COMPUTER SCIENCE | MASTER OF DATA SCIENCE

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

Visit **online.rice.edu** to access Rice's world-class, convenient masters degrees.

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

Sfdc.co/WiCyS2021

salesforce

Get ahead of the threats of tomorrow.

Advance your career on our cyber team.

Here, you'll secure, protect and provide solutions to ever-evolving threats. As we continue to connect people to the networks of the future, we're looking for the best talent to join us.

Explore a range of opportunities at verizon.com/cybersecurity

verizon✓

Verizon is an equal opportunity/disability/vet employer

At Visa, securing the world's payments is priority one!

We work every day to protect the integrity of the payments ecosystem. We reduce risk, fight fraud and cybercrime, and empower users with the tools, technologies and intelligence they need for better digital payment experiences.

Security Architecture & Product Engineering	Cyber Defense
Identity & Access Management	Cyber Engineering

Visit **www.visa.com/careers**

CONNECT WITH THE WICYS COMMUNITY ON SOCIAL MEDIA!

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

FLOWCODE PRIVACY.FLOWCODE.COM

FLOWCODE PRIVACY.FLOWCODE.COM

FLOWCODE PRIVACY.FLOWCODE.COM

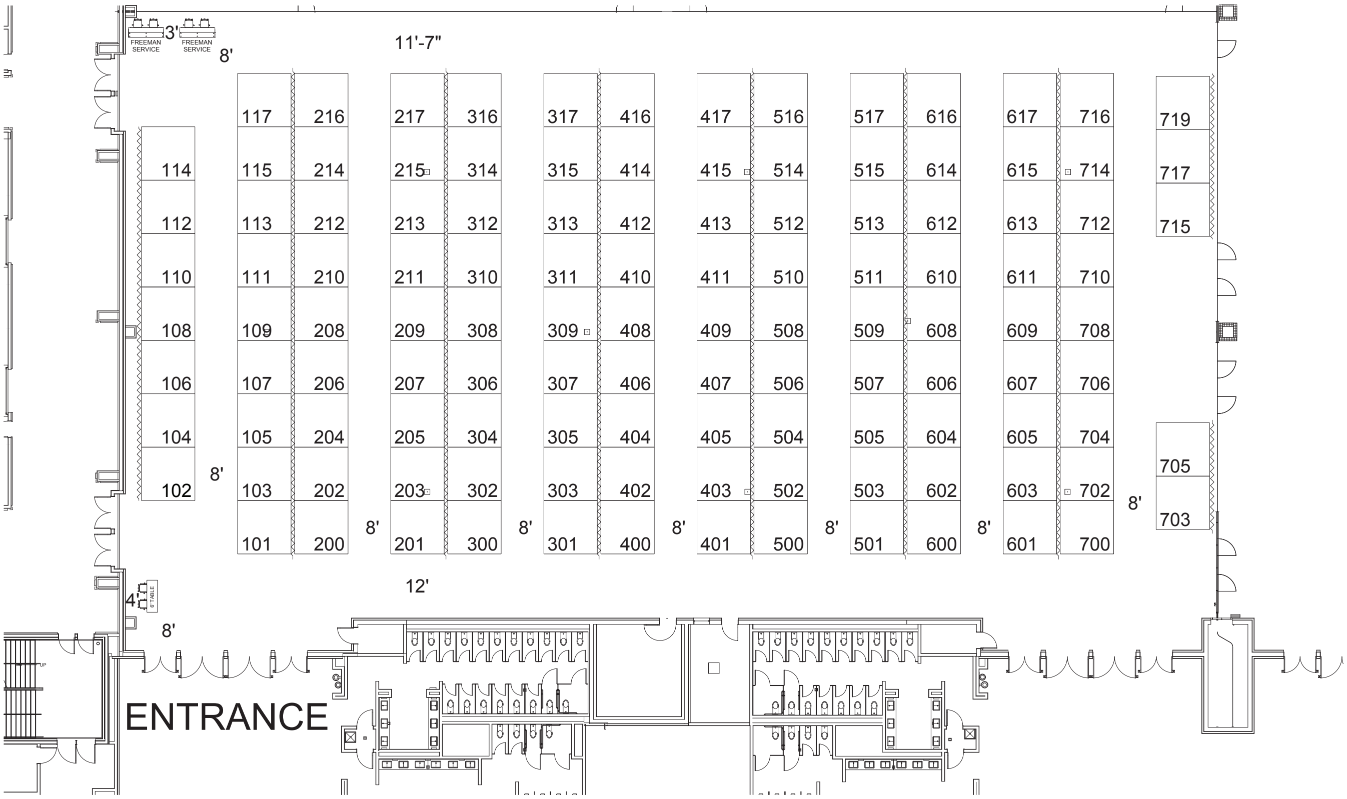
FLOWCODE PRIVACY.FLOWCODE.COM

EVENTS, PRIZES, TRAVEL AWARDS & SPECIAL ITEMS

SPONSORS - WiCyS THANKS YOU

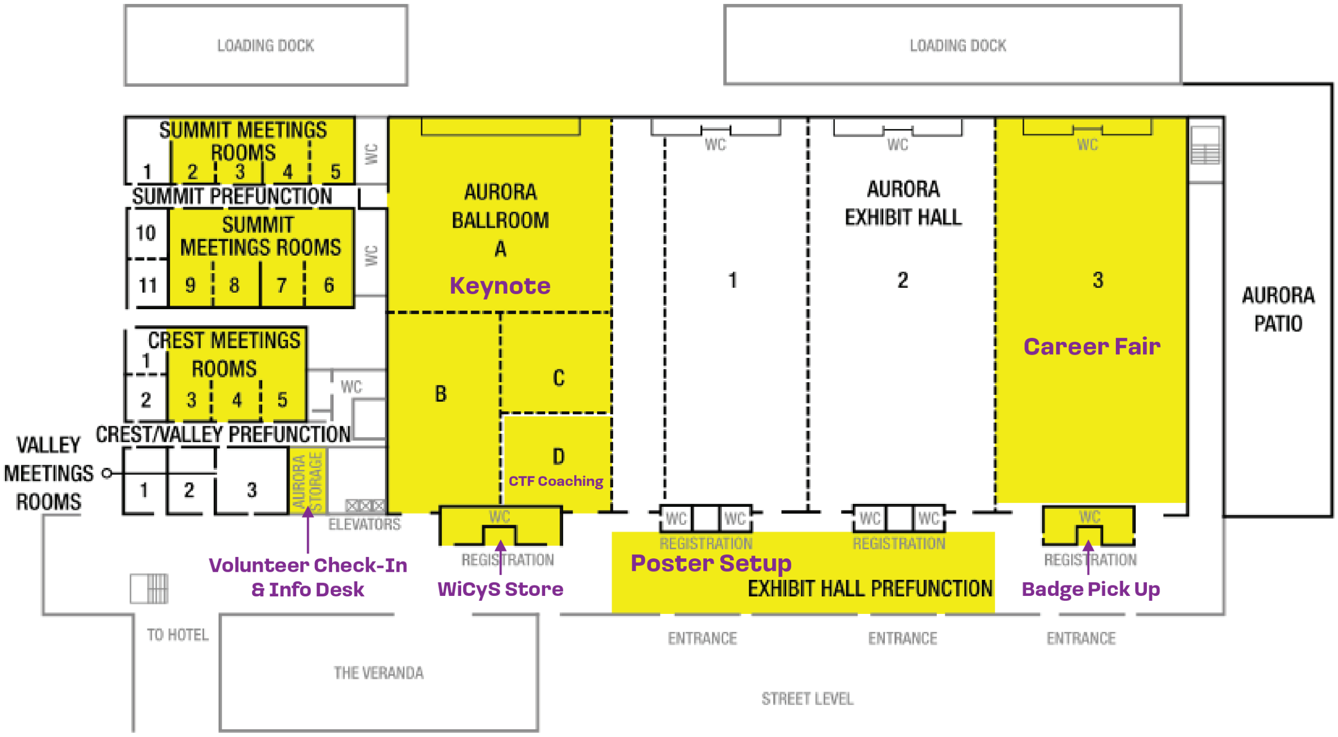
Adobe	Travel Awards
Air Force Civilian Service	Travel Awards
Amazon	Selfie Station
Anonymous	Travel Awards
Bank of America	Travel Awards
Carnegie Mellon University - SEI	Selfie Station
Cisco	Conference Bags, Travel Awards
Department of State	Breaks, Charging Station
Elastic	Travel Awards
Goldman Sachs	Travel Awards
Google	Travel Awards
Google Training Program	Travel Awards
MasterCard	Travel Awards
Metropolitan State University of Denver	Headshots
Optum	Conference Shirts, Travel Awards
Praetorian	Travel Awards
Raytheon Technologies	Travel Awards
Salesforce	Career Village Funding, Travel Awards
SentinelOne	Travel Awards
Palo Alto Networks	Travel Awards
Target	Travel Awards
Target Training Program	Travel Awards
Visa	Travel Awards
Walmart	Travel Awards
Workday	Lanyards, Travel Awards

VISIT THE CAREER FAIR



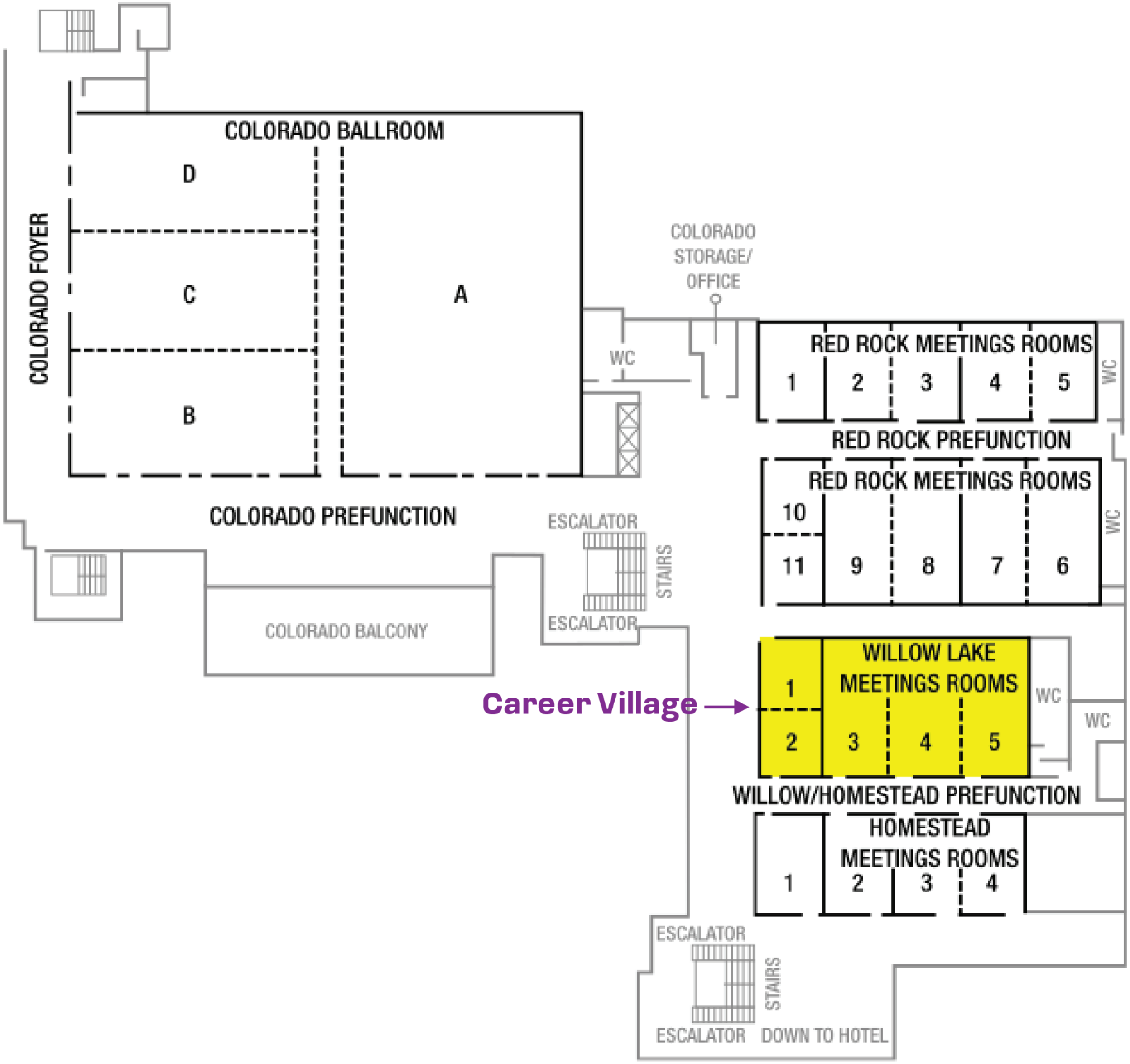
2021 WiCyS CONFERENCE VENUE MAPS

AURORA BALLROOM / EXHIBIT HALL AND MEETING ROOMS LEVEL 2



2021 WiCyS CONFERENCE VENUE MAPS

CONVENTION CENTER LEVEL 3



women in
CYBERSECURITY
WiCyS

WiCyS.ORG

JOIN WiCyS IN SUPPORTING WOMEN IN CYBERSECURITY

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

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