Women in CyberSecurity (WiCyS)
Global Nonprofit Organization

Ambareen Siraj
Celeste Matarazzo
Danielle Strimbu

Desiree Driver
Grace Pfohl
Maria Fanelle
Shafia Zubair
Shannon McHale

WiCyS 2027 Call For Presenters Webinar


women in CYBERSECURITY
WiCyS
WiCyS is a 501c3 nonprofit organization with global reach dedicated to bringing together women in cybersecurity from academia, research and industry to share knowledge, experience, networking and mentoring.
NSF

WiCyS Mission:

A community of women, men, allies and advocates that support the WiCyS mission to **recruit, retain and advance women in cybersecurity** as part of a ***workforce solution.***

WICYS TIMELINE

COMMUNITY BUILDING

2014 — Dr. Ambareen Siraj receives NSF funding for the first-ever Women in CyberSecurity Conference.

2015 — WiCyS reaches over 900 attendees in the first 2 years of the conference.

2016 — WiCyS reaches 1.7k women.

2017 — WiCyS organization created. Year round initiatives begin.

2018 — WiCyS becomes 5013c member based organization.

2019 — WiCyS launches Job Board++, Professional Affiliates, Student Chapters, Speaker's Bureau and Veteran's Programs.

2020 — WiCyS pilots Skills Development Training, Mentor/Mentee Program and Virtual Summit.

2021 — WiCyS continues to sustain and scale through employer collaborations and vested interest of WiCyS members.

2022 — #WiCyS 2022 reaches 16 million!

2023 — WiCyS grows to: 8100 members 224 student chapters 85 countries 67 strategic partners 62 professional affiliates.

2024 — Celebrated 10 years of WiCyS conferences

2025 — WiCyS grows to: 10800 members 331 student chapters 110 countries 69 professional affiliates.

2026 — WiCyS 2026 In-Person March 11 - 13 Washington, D.C. Virtual April 22 - 23

WORKFORCE IMPACT

WOMEN IN CYBERSECURITY
INITIATIVES

Women in Cybersecurity
WiCyS

PROGRAMS

- Early Career
- Mid Career
- Senior Career

MEDIA

- Newsletters
- Speakers Bureau
- Speaking Engagements
- Podcasts

EVENTS

- Annual Conference
- Regional Affiliate Events
- Virtual Conference
- Webinars
- Student Chapter Events

CAREER RESOURCES

- Career Fairs
- Career Growth Hub
- Conference Scholarships & Grants
- JobBoard++
- Research & Resources
- Resume Reviews

COMMUNITY

- 11K+ Members
- Affiliates
- Board of Directors
- Committees
- Mentorship
- Mission Support Team
- Online Member Platform
- Executive Leaders Network
- Student Chapters

WOMEN IN CYBERSECURITY PROGRAMS

women in CYBERSECURITY

WiCyS

EARLY CAREER

- Capture the Flag
- Cybersecurity Awareness
- Google CyberSecurity Certificate
- GRC Program
- ISC2 Fall/Spring Camp
- Security Training Scholarship
- SANS Cyber Range
- Security Training Scholarship
- Student Chapters
- Vulnerability Disclosure Program

MID CAREER

- Advisory Committee Opportunities
- AI Learning Series
- AI Security Accelorator
- Create Your Leading Edge
- GRC Program
- Professional Affiliates
- Speakers Bureau
- Stage Ready (Public Speaking Fellowship)

SR. CAREER

- Advisory Committee Opportunities
- AI Learning Series
- Speaker's Bureau
- Professional Affiliates
- SANS Executive Cyber Exercise
- Executive Leaders Network
- Stage Ready (Public Speaking Fellowship)
- Rising CISO

ALL CAREER LEVELS

- CPE Credits
- Conference Scholarships
- Skills Assessment
- Member Portal Access
- Regional Events
- Research and Resources
- Skills Assessment
- Virtual Career Fairs
- 24/7 Job Board
- Mentorship Program
- Webinars
- Women in the Middle Podcast

WiCyS Strategic Partners

TIER 1

amazon Bloomberg cisco Ford Google

LOCKHEED MARTIN Microsoft paloalto NETWORKS SentinelOne tenable

TIER 2

Adobe flare MITRE

NAVY FEDERAL Credit Union PayPal pepsico Food. Drinks. Smiles. PSEG

TIER 3

3M Science. Applied to Life. abbvie American Airlines Arete ARISTOCRAT BOEING

DELL Technologies DeVry University Edward Jones evolution EQUITY PARTNERS FORTINET HAYSTACK SOLUTIONS ISC2 JPMorganChase

Joint Hacking Training KeyBank LPL Financial nebulock salesforce SANS semperis

servicenow skillrex STATE STREET TikTok Vanguard wayfair

WiCyS 2027 Conference

March 17 - 19, 2027

Gaylord Rockies Resort and Convention Center
(Denver, CO area)

WiCyS 2027 Virtual Conference

April 28 – 29, 2027

Call For Presenters (CFP) Timeline

Submissions Open:
September 2, 2026

Submission Deadline:
September 30, 2026
5:00 PM Central Time (CT)

**Student Posters Deadline:*
November 4, 2026 at 5:00 PM CT

Notification of Status:
November 18, 2026
**Student Posters Notification: December 2, 2026*

Program Committee

Conference Co-Chair (Program)

Dr. Ambareen Siraj, Founder WiCyS

Conference Co-Chair (Program Logistics)

Celeste Matarazzo, WiCyS

Program Coordinator

Danielle Strimbu, WiCyS

Program Co-Leads

- ✔ Miranda Skar
- ✔ Jillian Sebrook
- ✔ Junia Valente
- ✔ Amani Altarawneh
- ✔ Smriti Bhatt
- ✔ Rebecca (Bex) Faerber
- ✔ Katey Reising
- ✔ Shade Adeleke
- ✔ Marcie Friedman
- ✔ Samantha Shields

Call For Presenters (CFP) Mentor Program

If you are new to submitting a Call for Presenter or just need an extra dose of encouragement, please lean in on the **WiCyS CFP mentors**.

To request a mentoring session, email **program@wicys.org**.

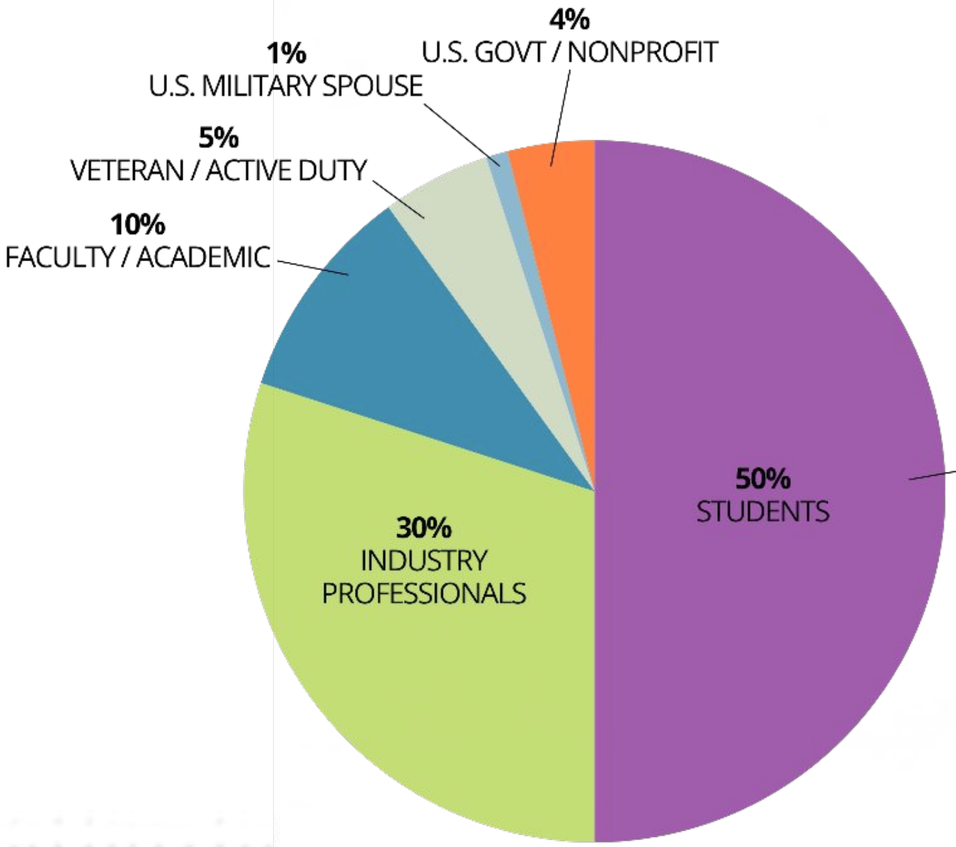
The deadline to request a mentor is **September 15, 2026**.

#WICYS2026

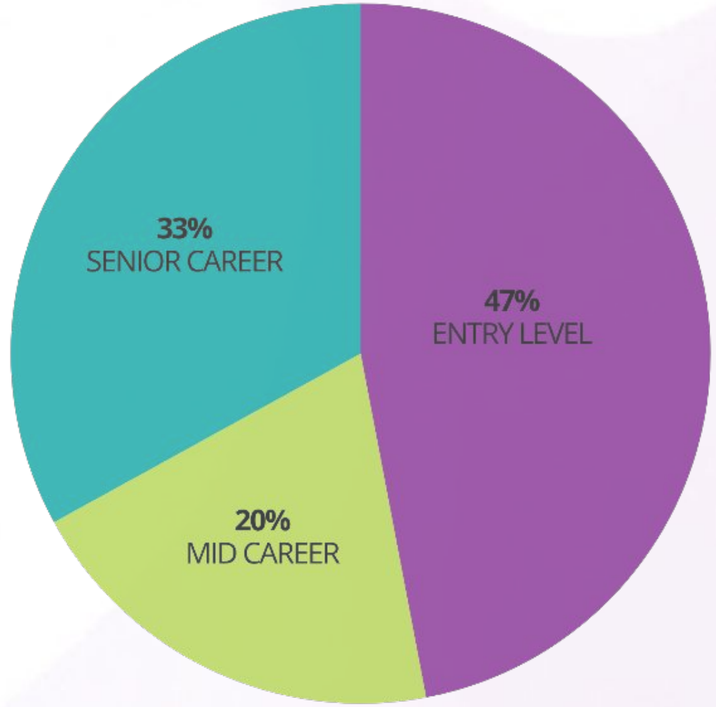
By The Numbers

2,027 Attendees	**865** Scholarships	**500+** Volunteers	**1,115** First Timers
23 Countries Represented	**122** Student Chapters Represented	**60** Affiliates Represented	**649** Senior Level

Know Your Audience



OUR STUDENTS	
5.83%	Community College Student
1.66%	Cybersecurity Boot Camp
33.43%	Graduate Student (MS)
7.21%	Graduate Student (PhD)
1.11%	High School Student
0.97%	Post Baccalaureate
1.66%	Undergraduate Student - Freshman
16.92%	Undergraduate Student - Junior
23.16%	Undergraduate Student - Senior
8.04%	Undergraduate Student - Sophomore



This information was collected from the WiCyS 2026 attendees

Meet our Panelists

Shannon McHale
Staff Security Engineer

Desiree Driver
Technical Program Manager

Grace Pfohl
Senior Consultant, ethOS Compliance

Shafia Zubair
Cybersecurity & GRC Leader

Maria Fanelle
Cloud Engineer

Women in Cybersecurity WiCyS SM

WiCyS 2027 Program Tracks

Technical Skill Building - technical skill development in all areas of cybersecurity and/or privacy
- *Example: A workshop on secure coding practices for AI-integrated applications.*

Research and Innovation with Emerging Techniques - scientific research addressing real-world cybersecurity challenges or emerging tools, algorithms and techniques used in cybersecurity
- *Example: A study evaluating the effectiveness of biometric authentication against AI attacks.*

Tools, Trends, Perspectives, and Sector-specific applications - Cybersecurity tools with specialized use cases across domains, applications within critical infrastructure and industry sectors, or perspectives and analysis on cybersecurity trends, challenges, or current events
- *Example: A threat modeling application tailored for healthcare providers.*

Education, Workforce Development and Community - cybersecurity education (formal and informal) at all levels from K to Grey, workforce development initiatives to align with current and future cybersecurity job demands, or community outreach and partnerships that promote access to cybersecurity knowledge and resources
- *Example: A hands-on K-12 cybersecurity curriculum designed for after-school programs.*

Career Development, Advancement & Management - internships, apprenticeships and job search, leadership, career development/growth, and personal wellness
- *Example: A hands-on session exploring job searching strategies using AI tools.*

Lightning Talks

Lightning talks highlight fresh ideas, unique perspectives, valuable experiences and emerging trends in cybersecurity and/or privacy. Lightning Talks are five-minute talks (with or without formal presentations) with a maximum of one listed presenter.

Hired – and Hacked: The Hidden Dangers in Job Applications

Speaker(s): Ida Musheyev-Polishchuk

What if a dream job application turned into a cyberattack? Job hunting is a stressful and often obscure process in which applicants are frequently put in the vulnerable state of being rushed through the application process with unfamiliar counterparties. Applicants often are too emotionally charged to catch typical red flags they would have otherwise avoided, and attackers know this. This talk details a real-world case study of a social engineering attack, where a user was compromised while applying for a role from a fake job posting. In this attack, the user, believing they were engaging in legitimate pre-screening, was successfully convinced to run a simple, yet highly malicious, curl command in their system shell, downloading and executing a persistent keylogger designed to steal credentials and exfiltrate data off their machine. This talk demonstrates how a combination of social engineering and technical deception can target even security-aware individuals, emphasizing the human element in cybersecurity. This session will dissect the attack chain, from the initial social engineering lure to execution of the keylogger, and provide a rapid-fire review of the immediate incident response steps and remediation steps. Attendees will leave with practical, immediate takeaways on how to recognize red flags in applications and prioritize vigilance even when under pressure. This case study underscores the importance of the human element in system security and provides a powerful cautionary tale for security professionals and students alike.

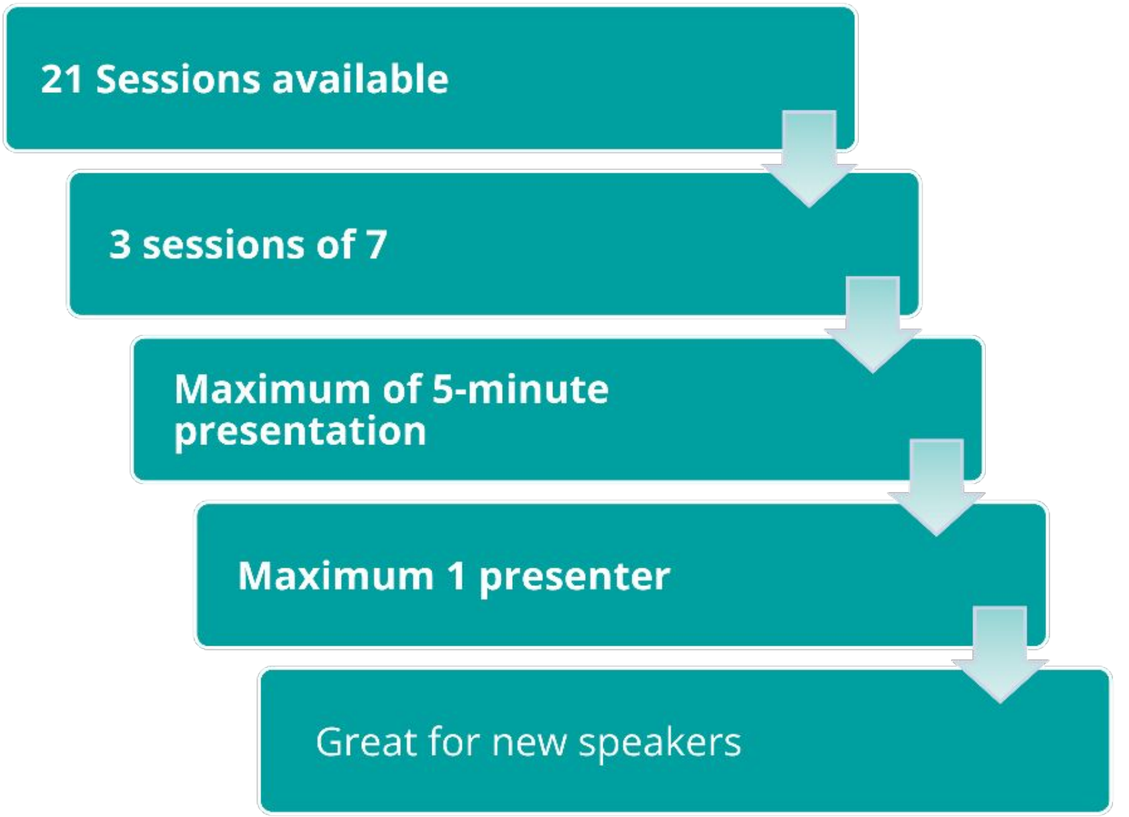
The PhD Dilemma: Prestige, Cost and Payoff in Today's Age

Speaker(s): Prajna Bhandary

The decision to pursue a PhD in cybersecurity or computer science is often framed as the pinnacle of academic achievement, but the realities of doctoral study are rarely openly discussed. While a PhD can lead to opportunities in research, academia and thought leadership, it also requires navigating challenges that are not always obvious at the start. This session will take a candid look at the PhD experience and highlight what aspiring doctoral students should be prepared for before committing. Drawing from personal experience of the presenter, it will touch on the dependence on research funding and how it shapes the direction of work, the intense focus required to stay motivated through years of study and the growing role of artificial intelligence in research, raising questions about how doctoral training might evolve. The talk also will contrast the relative benefits of a master's degree, which often provides faster and more flexible returns. Attendees considering doctoral study will leave with an honest perspective on what to expect, what challenges to prepare for and how to decide if this path aligns with their long-term goals.

Lightning Talks Notes

- Listed presenter receives complimentary registration. There is no complimentary lodging or lodging stipend provided. There is no travel support.
- Alternatively, all WiCyS members are eligible to apply for a scholarship that includes shared lodging.



Panels

Panels provide opportunities to spotlight discussion on a current, relevant topic in cybersecurity and/or privacy. Panel submitters are responsible for selecting appropriate panelists to participate. Each panel is 45 minutes in length. In addition to the moderator, there can be three or four panelists; a panel has a minimum of three and a maximum of four panelists and one moderator listed. At the time of submission, panelist names should be confirmed. Submit all confirmed names and their affiliation info along with the abstract.

Governance and Guardrails by Design: Redefining Cybersecurity, Privacy and AI Across Industries

Speaker(s): Sara Lazarus, Laura Sawka and Prabhmeet Kohli

Room: Maryland C **Track(s):** **Career Level:** All

As artificial intelligence (AI) transforms industries, the intersection of cybersecurity, data governance and privacy is emerging as the defining challenge of our time. Traditional compliance models can't keep pace with autonomous systems, data-driven decisioning and sector-specific threats from ransomware in healthcare to algorithmic bias in financial services. This fireside chat will spotlight how governance and guardrails by design enables organizations to embed cybersecurity, privacy and governance principles into their operations, tools and AI systems from inception. Women leaders driving transformation across critical sectors will share how they operationalize governance strategies that protect and empower, turning compliance into capability and innovation. The discussion will provide perspectives on evolving trends: unpacking why traditional compliance and privacy approaches don't keep pace with the evolving threat landscape: how governance models can secure data pipelines across sectors: and how organizations can build privacy-driven trust ecosystems that fuel responsible AI adoption and support business innovation. Participants will leave with actionable strategies for aligning technology advancement with cybersecurity, privacy and governance to support innovation and enable growth.

Decrypting Tomorrow: How We Build Trust in a Post-Quantum World

Speaker(s): Alana Scott, Taylor Hartley, Emily Fane and Richu Channakeshava

Room: Maryland 4-6 **Track(s):** **Career Level:** Mid/Senior

Quantum computing is reshaping the future of cryptography and with it, the foundations of cybersecurity. As quantum capabilities advance, traditional public, key algorithms face obsolescence, forcing organizations to confront the urgent need for quantum-resilient systems. This panel brings together quantum security leaders at the intersection of applied cryptography and real-world security strategy. Together, they will explore the technical, operational and policy dimensions of transitioning to post-quantum cryptography (PQC). Discussion topics include the practical challenges of PQC migration, organizational readiness, NIST standardization progress and the broader implications of quantum vulnerabilities. The panel also will highlight pathways for security practitioners, especially women in cybersecurity, to shape the next era of resilient cryptographic infrastructure. Participants will leave with a clear understanding of what quantum readiness means in practice and how to take actionable steps toward securing systems for the post-quantum age.

Panel Notes

- The moderator receives complimentary registration There is no complimentary lodging or lodging stipend provided. There is no travel support.
- Up to four (4) panelists receive reduced rate conference registration ($300 discount). There is no complimentary lodging or lodging stipend provided. There is no travel support.
- Alternatively, all WiCyS members are eligible to apply for a scholarship that includes shared lodging.

7 Sessions available

45 minutes duration

Minimum 3 panelists and 1 moderator, maximum 4 panelists and 1 moderator

Panelists with different backgrounds and viewpoints on the topic

Clear takeaways from the panel discussion

At the time of submission, panelist names must be confirmed.

Presentations

Technical presentations highlight innovations, research & development projects, technical skills development, internships/co-ops experiences, service-learning and outreach projects, or other interesting experiences related to cybersecurity and/or privacy. Technical presentations are 45 minutes long, including time for Q&A, with a maximum of two listed presenters.

AI in the Exam Room: Powering Healthcare While Protecting Privacy

Speaker(s): Harshini Chellasamy and Julia Kip

Room: Maryland C **Track(s):** **Career Level:** All **CPE Credits:** 1

Picture a routine checkup where AI listens as closely as a clinician. From screening and triage to surgical visualization and post-visit planning, AI tools are transforming every stage of patient care. The upside is real: faster workflows, smarter decisions and more meaningful human connection during visits. Yet, as AI listens, learns and predicts, a critical question emerges – what happens to privacy when the most sensitive health data fuels the algorithm? This session examines how clinician-facing AI is reshaping workflows and redefining patient trust. Presenters will examine the expanding role of AI in healthcare today, from decision support to documentation, and confront the real-world risks that affect patients and providers – data leakage, model bias, overreliance on AI, hallucinations and weak oversight. Additionally, participants will explore the other side of the equation, highlighting how responsible adoption can unlock tangible benefits in access, accuracy and equity of care. Grounded in real-world experience implementing digital transformations across the healthcare industry, this session also will highlight how providers can embed privacy-by-design, apply Responsible AI principles and use privacy-preserving technologies to enable innovation safely. Attendees will leave with a clear understanding of how healthcare providers are adopting AI and how they can mitigate privacy/security risks. Presenters will focus on the data-protection technologies that can safeguard patients while empowering clinicians. With personal health data people need to ask, what guardrails are being considered?

Spilling the Beans: Graph Neural Networks That Actually Get Java Security

Speaker(s): Rhette Wallach

Room: Maryland 4-6 **Track(s):** **Career Level:** Mid **CPE Credits:** 1

Traditional static analysis tools rely on pattern matching and rule-based heuristics, resulting in high false positive rates and missed vulnerabilities in complex code flows. This session introduces a novel approach using graph neural networks (GNN) to detect security vulnerabilities by learning from code property graphs that capture program semantics. The presenter has a production-ready framework that models Java codebases as heterogeneous graphs containing control flow, data flow and program dependencies. By applying graph attention networks with Bayesian uncertainty quantification, the system achieves 100% detection accuracy on 22+ common weakness enumeration classes while providing confidence scores rather than binary alerts.The framework implements research-grade taint tracking with context-sensitive analysis, field-sensitive pointer analysis and interprocedural data flow tracking. Unlike traditional tools that flag every user input as critical, this approach understands program semantics to distinguish between sanitized and exploitable data flows. Advanced features include implicit flow detection through control dependencies and counterfactual explanations that suggest minimal code changes to eliminate vulnerabilities. Attendees will learn how machine learning can enhance security analysis, understand the technical architecture of GNN-based vulnerability detection and gain practical knowledge for integrating automated analysis into CI/CD pipelines. The session covers real-world case studies, benchmark comparisons with commercial tools and discusses the intersection of program analysis research and practical security engineering. This work bridges academic research (ACM, PLDI, FSE) with industry needs, demonstrating how deep learning can augment human security expertise rather than replace it.

Presentation Notes

44 Sessions available	**45 minutes duration**
Maximum 2 presenters	Audience interaction is limited to 10 min Q&A

- If accepted for **In-person Conference**, listed presenters (maximum of 2) receive complimentary registration. There is no complimentary lodging or lodging stipend provided. There is no travel support. Alternatively, all WiCyS members are eligible to apply for a scholarship that includes shared lodging.
- If accepted for **Virtual Conference**, listed presenters receive complimentary virtual conference registration.

Workshops

Workshops are hands-on sessions (technical/professional development) on any topic related to cybersecurity and/or privacy. The audience should be engaged and participate in activities throughout the session. Workshops are 1 hour and 45 minutes in length with a maximum of four listed presenters. Workshops should be suitable for a large audience (>150 attendees).

NeuroCode 2.0: The Mind as the New Attack Surface

Speaker(s): Mariami Kentchadze

Room: Maryland D **Track(s):** **Career Level:** All **CPE Credits:** 2 **Laptop Recommended**

NeuroCode 2.0 dives into the frontier where neuroscience and cybersecurity collide — when the human brain becomes both credential and target. As brain-computer interfaces and neuro-wearables capture thought patterns and emotional data, new vulnerabilities emerge: neural spoofing, cognitive leakage and "dream-phishing." This workshop blends emerging research with interactive ethical simulations. Participants will explore how brainwave-based authentication could be exploited, debate neural-data ownership and design safeguards to protect cognitive privacy. Through short scenario labs and guided discussion, attendees will learn how to map traditional security frameworks onto this uncharted, human-centered terrain. By the end, participants will grasp why protecting the mind's data layer may define the next decade of cybersecurity and how interdisciplinary collaboration between technologists, ethicists and neuroscientists will be vital to secure it.

Build, Break, Defend: Securing the Model Context Protocol in Action

Speaker(s): Shruti Datta Gupta and Spandana Gorantla

Room: Maryland D **Track(s):** **Career Level:** All **CPE Credits:** 2 **Laptop Required**

The Model Context Protocol (MCP), open-sourced by Anthropic in late 2024, has quickly become foundational to modern agentic workflows, enabling AI systems to dynamically interact with tools, data sources and APIs. With this flexibility comes a new class of vulnerabilities that traditional security models fail to capture. In this hands-on, challenge-driven workshop, participants will be introduced to the fundamentals of MCP — its architecture, components and role in enabling agentic interoperability. Through guided exercises, they'll build a toy MCP server, gaining an understanding of how an MCP setup works as well as tool registration, resource endpoints and request–response flows. Teams will move into a CTF-style break phase, exploiting intentionally vulnerable MCP instances to capture flags tied to issues such as context poisoning, naming impersonation and over-permissive tool integrations. This interactive format encourages participants to think like attackers, share discoveries and connect exploits to underlying design weaknesses. Finally, the session will transition to defense, where participants will apply structured threat-modeling frameworks - STRIDE and MITRE ATLAS - to collaboratively design practical mitigations for MCP-based systems. No prior MCP experience is needed, just a laptop, GitHub account, code editor and, most importantly, curiosity. Code scaffolds and lab guides will be provided. Key takeaways will be learning how to design, deploy and reason about MCP servers and agent integrations; the unique vulnerabilities introduced by MCPs and how they differ from traditional APIs; practical CTF-style experience in exploiting and defending MCPs; and framework for threat modeling and securing next-generation agentic architectures.

Workshop Notes

- First two (2) listed presenters receive complimentary registration. There is no complimentary lodging or lodging stipend provided. There is no travel support.
- Up to two (2) additional presenters receive reduced rate conference registration ($300 discount). There is no complimentary lodging or lodging stipend provided. There is no travel support.
- Alternatively, all WiCyS members are eligible to apply for a scholarship that includes shared lodging.

18 Sessions available

1 hour 45 minutes duration

Maximum 4 listed presenters

Suitable for large audience >150

Submission should state what technology (laptops or mobile devices) is required for the workshop

Workshop design should assume no prior setup from attendees.

Any required software installation or configuration must be factored into the 1 hour 45 minutes workshop timeline. Keep it simple!

Student Posters

Posters provide opportunities for students to present their work to the audience at WiCyS in poster format. The Poster judging process will select winners in both the undergraduate and graduate categories. The Winners of the poster competition in both undergraduate and graduate categories receive travel support for future security conference(s) of their choice. Runners-up receive prizes as well.

Securing the Vehicle Firmware Supply Chain

Iwinosa Aideyan, Clemson University

Modern vehicles rely on continuous software updates; however, today's update mechanisms primarily verify metadata rather than ensuring the integrity of the software itself. This creates a critical gap in the automotive supply chain: a binary can be modified and rebuilt under inconsistent environments or injected with malicious code while still appearing trustworthy to update systems downstream. This research addresses that gap by developing a decentralized, tamper-evident build-verification pipeline that ensures a vehicle's firmware truly corresponds to its source code. The system integrates three core capabilities: real-time capture of code changes; deterministic, reproducible builds executed across multiple independent nodes; and cryptographic binding of each binary to its software bill of materials. If every node produces byte-identical outputs, the artifact is accepted for deployment. If any deviation occurs, caused by tampering, environmental drift or toolchain inconsistencies, the system immediately detects the divergence and halts the update process. The framework was deployed on a multi-node virtual testbed and evaluated across more than 90 build executions. Results show 100% reproducibility in controlled settings, consistent resource usage across nodes and automatic detection of all injected faults, including modified dependencies and altered toolchains. The approach provides an auditable, traceable and verifiable chain of custody for firmware from commit to deployment. This research demonstrates how deterministic builds combined with distributed trust can significantly enhance the resilience of automotive software pipelines, offering a practical security layer for future secure over-the-air updates.

FED-STGODE: Federated Spatial-Temporal Graph ODE Networks for Traffic Flow Prediction

Naome Etori, University of Minnesota

Traffic flow prediction (TFP) is essential in intelligent transportation systems as it helps reduce congestion, improve road safety and lower air pollution. Accurate and timely TFP supports better traffic management through optimized signal control and infrastructure planning. However, traditional TFP models rely on large amounts of heterogeneous data from sensors, cameras and GPS devices, raising privacy, ownership and integration challenges. To address these issues, this study explores privacy-preserving machine learning approaches using federated learning (FL) for TFP. Four FL-based models were developed and evaluated: Spatial-Temporal Graph ODE Networks (STGODE) as the primary model, and gated recurrent unit, recurrent neural network and long short-term memory as benchmarks. The key objective is to integrate FL with predictive models to safeguard user data while maintaining high forecasting accuracy. The approach employs the FedAvg algorithm to aggregate model updates from multiple decentralized clients without sharing raw data, enhancing privacy during training. The proposed models were assessed on multiple real-world TFP datasets and their performance was compared against centralized and non-federated counterparts. Experimental results demonstrate that FL-based STGODE achieves competitive accuracy while preserving data privacy, confirming the feasibility of federated approaches for intelligent traffic management. The study contributes to developing privacy-aware, data-efficient TFP systems and provides an open-source code base for Fed-STGODE to encourage reproducibility and further research.

Student Posters

Two categories: Undergraduate and Graduate

First listed researcher and presenter must be a **female student**

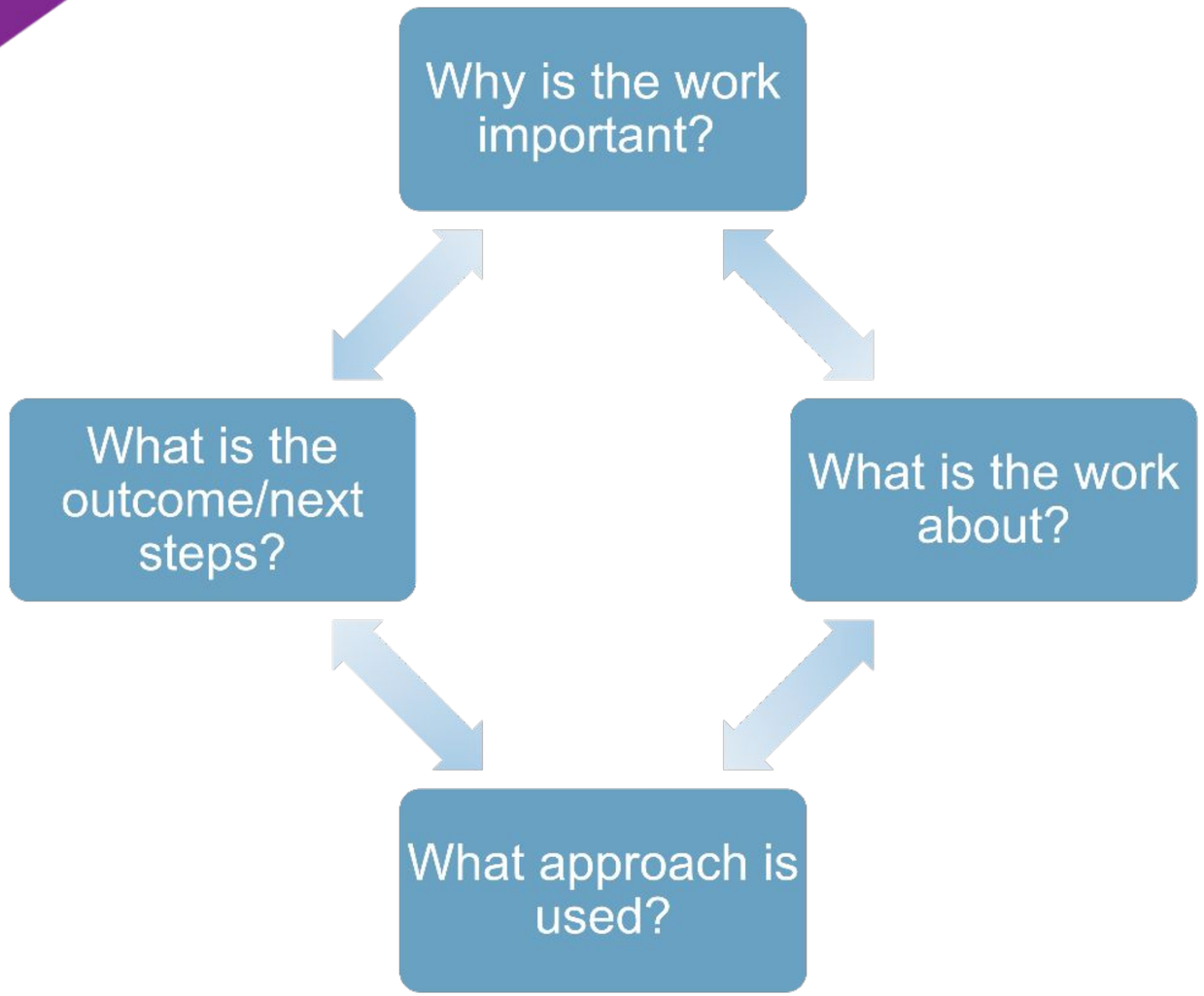
Can be about work-in-progress

- Submissions must be presented in person, and the first listed presenter must be the lead presenter. Maximum of 4 presenters.
- The **first listed student** of an accepted poster receives an automatic scholarship to register for and attend WiCyS 2027. A $75 registration processing fee is required. The scholarship includes shared lodging. If shared lodging is declined, the student is responsible for paying for their own lodging.
- **Additional students** listed on a poster may apply for a scholarship for attendance; these are not granted automatically nor guaranteed.
- Presenting a poster at the conference is a student member benefit. Accepted poster presenters must become a student member ($30 annual membership) if they are not already a student member before they can register for the conference.

Some Past Poster Presenters

Poster Session Notes

Highlight major points of research/work



Submission Selection Process

Presenters can submit multiple proposals in different categories and tracks.

Reviewers selected from WiCyS members who volunteer.

Submissions will be peer reviewed with presenter name, email and affiliation anonymized.

Submission reviewed by at least two reviewers.

Reviewers submit reviews with scores using our CFP system.

Sub-committees meet to discuss submissions with respective co-leads, program committee and select recommendations.

Program committee leadership meets to discuss all TOP recommendations and finalize selections.

Presenters are notified and asked to register by deadline.

Selection Goals

Balance program portfolio across tracks and categories

No repeat of the same content from recent WiCyS conferences

Provide opportunities to presenters across different backgrounds and organizations

Quality is the topmost priority!!!

WiCyS 2027 Rubric

01 Relevant Subject Matter
Content is relevant to cybersecurity, privacy or career-development in the area of cybersecurity/privacy.

02 Matched to Track
Technical Skill Building; Research & Innovation with Emerging Techniques; Tools, Trends, Perspectives, & Sector-specific applications; Education, Workforce Development & Community; Career Development, Advancement & Management.

03 Technical or Thought-Provoking
Content is technical (for technical topics) or thought provoking (for non-technical topics).

04 Timely Topic
Content is timely, addressing current trends and contemporary cybersecurity challenges.

05 Creative & Innovative
Content is creative and innovative in its approach and presentation.

06 Clear Takeaways
Content has clear takeaways or research outcomes for the audience.

07 Engaging Session
Content is engaging and/or interactive for the session attendees.

08 Broad Appeal
Content applies to a broad and diverse group of WiCyS attendees.

09 Well-Articulated Abstract
Abstract description is well-articulated and provides a clear overview of the content.

10 Comprehensive Outline
Outline provides a good view of the submission's session content, activities, and outcomes.

What Reviewers Look For in Proposals

General Submission Guidelines

Key recommendations & rules for presentation proposals

Relevant & Specific

- Cybersecurity Focus: Clearly describe topics in cybersecurity and data privacy matched to specific tracks.
- Career Impact: Include actionable concepts that facilitate professional growth for cyber professionals.
- Inclusive Content: Open to all—topics do not need to apply exclusively to females in cybersecurity.
- Non-Commercial: Absolutely no vendor sales pitches in the proposal.

Concise & Anonymized

- To the Point: State specifically what problem or topic your session will address.
- 250-Word Abstract: Summary for the conference program (max 250 words).
- Detailed Outline: Unpublished structural breakdown for reviewer evaluation.
- Strict Anonymity: Absolutely **NO** submitter names, companies, or affiliations in the abstract or outline.
- **Experience:** The abstract may speak to experience and qualifications

Third-Person Perspective

- Objective Voice: Write all abstracts and outlines strictly in third-person phrasing.

DON'T SAY: "I will talk about my experience with incident response..."

DO SAY: "This session will present key incident response strategies..."

Submission Modifications

- Submission Edits: You may update/edit your submission until September 30th 5pm CT (November 4th 5pm CT for poster submissions).
- Hard Cutoff: Changes or late submissions after the deadline are strictly prohibited.

Meet our Panelists

Shannon McHale
Staff Security Engineer

Desiree Driver
Technical Program Manager

Grace Pfohl
Senior Consultant, ethOS Compliance

Shafia Zubair
Cybersecurity & GRC Leader

Maria Fanelle
Cloud Engineer

Women in CyberSecurity WiCyS SM

Top 10 Reasons to Submit to WiCyS CFP

01 Largest Global Stage
Be seen and heard at the largest world stage that spotlights women in cybersecurity.

02 Showcase Your Work
Showcase your talent and work at a conference bringing industry, government, & academia together.

03 Share Knowledge & Experiences
Share your valuable knowledge, research, and experiences with your community.

04 Sharpen Presentation Skills
Grow professionally and sharpen your public speaking and presentation skills.

05 Welcoming For Everyone
A supportive, high-energy venue built for 1st timers and old timers alike!

06 Feel Right at Home
Connect and feel completely at home with your own cybersecurity community.

07 Inspire Others Like You
Become a role model and inspire others who share your passion.

08 Recruit, Retain & Advance
Help to recruit, retain, and advance more women in cybersecurity.

09 Help Your Community Advance
Drive the cybersecurity field forward by helping your community advance.

10 YOUR Voice Matters!
Because YOUR unique voice, experience, and perspective matter!

Submission through WiCyS CFP portal

Deadline September 30, 2026 5PM Central Time (Posters November 4, 2026 5PM Central Time)

WiCyS 2027 Call For Presenters: https://www.wicys.org/events/wicys-2026/call-for-presenters

Reminders

- Anyone can submit
- Mentoring request is available until September 15, 2026
- Presenters must submit by deadline
- Accepted presenters must register by deadline

“If your actions create a legacy that inspires others to dream more, learn more, do more and become more, then, you are an excellent leader.”

— Dolly Parton

For more information, contact:

program@wicys.org

Stay Connected!

Find us on Instagram
@WiCySorg

Find us on FaceBook
@Women in CyberSecurity - WiCyS

Find us on LinkedIn
@Women in CyberSecurity (WiCyS)

Find us on X
@WiCySorg

Find us on YouTube
@WomeninCyberSecurityWiCySorg

Find us on Flickr
@WiCyS

women in CYBERSECURITY WiCyS

RECRUIT, RETAIN and **ADVANCE**
Women in Cybersecurity