2025 CAE Community Symposium

CAE-R Community of Practice

Agnes Hui Chan
Northeastern University
Susanne Wetzel
Stevens Institute of Technology

Outline

- Mission
- Ongoing Activities of the CAE-R Community of Practice (CoP-R)
  - INSuRE
    +E/+C tracks / Summer Workshop
  - Research Symposium
  - Get-to-Know-Your-Fellow CAE-Rs
  - Special Topics Workshop
- Activities at 2025 Community Symposium
  - Birds-of-a-Feather Session
  - Panel Discussion
  - Looking to the Future

Mission

- Build a community that
  - Provides opportunities and directions to all NCAEs in cybersecurity research
  - Facilitates research collaborations between government and academia
  - Facilitates research collaborations among NCAEs
- Recognize institutions engaging in strong cybersecurity research
- Support, strengthen, and broaden workforce development
  - Cybersecurity is a fast-moving field requiring graduate to have
    - The ability to handle problems that have not been encountered before
    - The competency to acquire up to date knowledge of current developments in cybersecurity
  - Enable research education to permeate through all levels from Bachelors to PhD

INSuRE

- Goal
  - Workforce development: Connect government agencies, national labs, and FFRDCs (agencies for short) with academic institutions to improve workforce readiness by building competency in research methodology, problem solving, critical thinking, teamwork, and communication
  - Advance state-of-the-art in applied research on problems of national interest
- Benefits
  - Students and academic institutions
    - Work on real-world applied research problems in a way that otherwise may not exist at their academic institution
  - Agencies
    - Dedicated students help address applied research problems that are of interest and importance
    - Access to some of the most promising cybersecurity talents

INSuRE+E (Education Track)

- Goal: Building student competency in
  - Research methodology
  - Problem solving, teamwork, critical thinking and communication
- Logistics
  - Research projects/problems proposed by Problem Mentors (PMs) from government labs and agencies
  - PMs serve as subject area experts
  - Faculty Advisors (FAs) provide support at local NCAE institution
  - Student teams from NCAE institutions work on a project in the context of a course
- History
  - Started in 2012 with Purdue University and NSA
  - Today: 30+ institutions and 20+ agencies

INSuRE+C (Collaboration Track)

- Goal
  - Facilitate research collaboration between NCAE-R faculty and researchers at government agencies
  - Opportunity to jumpstart a research program for faculty members
- Logistics
  - Similar set-up as INSuRE+E with PMs, FAs, and student teams
  - FAs possess subject area expertise to advise research project alongside with PMs
  - Academic year commitment (plus option to span into summer with funding)
  - Research results are expected to be published in peer-reviewed public domain venue
- History
  - Started in 2021 with 2 teams from 2 CAE-Rs
  - AY24-25 there are 5 teams from 4 CAE-Rs

INSuRE Summer Workshop

- Goal
  - Provide INSuRE+E education to all NCAEs that may or may not have the capacity in offering the program in the context of a course
- Logistics
  - 2 summer sessions, each lasting 3 or 4 weeks
  - PMs serve as subject area experts, holding meetings via Zoom
  - ~24 student are selected from applicants across all NCAE institutions
  - Workshops hosted at NCAE institution - students attend in person
  - FAs from the hosting NCAE institution are in charge of local arrangements and academic advising
- History
  - Started in Summer 2024
  - Selection for 2025 ongoing

Workforce Impact of INSuRE

Cutting-edge Topic Areas	INSuRE+E	INSuRE+C	Summer	TOTAL Number of Students
	Number of Participating Students (2021-2025)			
Network Security	179	6	12	
Homomorphic Encryption/Post-Quantum/Block Chain/Privacy	100	3		
Hardware/Software Security	73			
Attack Analysis	68	2		
Cloud Security	66	3		
AI/ML Security	65	11		
Critical Infrastructure Security	56			
Malware	52	2		
Formal Methods	51	10	10	
Cybersecurity Policy	43			
TOTAL	**753**	**37**	**22**	**812**

Agencies: NSA, DoD, MITRE, MITLL, NIST, ANL, SNL, ORNL, ANL, JHUAPL, LLNL, Indiana State

Research Symposium

- Goal
  - Showcase accomplishments and capabilities of NCAE-R institutions
  - Showcase research results from the INSuRE+E/+C/Summer programs
  - Give PhD students who are ready to join the workforce a forum to showcase their PhD research accomplishments
  - Allow faculty members to learn about research interests of government agencies and labs and funding opportunities
- Logistics
  - Held annually in conjunction with NCEC
  - Program Committee of faculty from NCAE-R institutions is formed to develop the symposium program

Get-to-Know Your Fellow CAE-Rs

- Goal
  - Opportunity for NCAE-Rs to showcase their research foci and present some recent research results
  - Allow CAE institutions to learn about research expertise of NCAE-Rs
  - Provide a forum for faculty members to learn about each other's research interests and to stimulate collaborations among faculty members
- Logistics
  - All presenters are from NCAE-R institutions
  - Takes place every 4th Thursday of the month – open to all NCAE institutions
  - Features up to two CAE-R institutions each time
    - Introduction to its cybersecurity research foci
    - 2 research presentations from faculty and/or PhD students
  - Led by Professor Roberto Perdisci of University of Georgia

Special Topics Workshop

- Goal
  - Identify a current topic of national interest in cybersecurity
  - Establish state-of-the-art and to devise research directions for the community
  - Provide a forum to spur research collaborations among NCAE-R institutions, as well as with government agencies
- Logistics
  - Held annually in conjunction with NCEC
  - One-day event that facilitates open-ended discussions among a small group of academic faculty members and some government researchers
  - Topics nominated by faculty from CAE-R institutions or PMs from government agencies
  - Results of the workshop are presented to the communities at large
- Previous Workshops
  - 2022: HCI and Cybersecurity
  - 2023: Generative AI and Cybersecurity
  - 2024: Software Supply Chain Security

Activities at 2025 Community Symposium

- Birds-of-a-Feather Session
  - Smaller scale of Special Topics Workshop
  - Different topics of interest proposed and discussions led by faculty from NCAE institutions

    Ethical and Privacy Concerns of AI / LLMs in Social Engineering and Information Warfare / Cyber Conflict and State Capabilities / Behavior-based Anomaly Detection for Cyber Attacks / Sovereign AI for Cybersecurity
- Panel Discussion
  - Topic and panelists proposed by NCAE-R faculty member:

    Generic Large Language Model in Cybersecurity
- Looking to the Future
  - Strategic discussions

Sessions open to ALL symposium attendees!