C3E Challenge Problem Overview

Dan Wolf and Don Goff, Co-PIs

- Since 2016, the National Science Foundation has provided support to perform follow-up research on the Challenge Problem topics
- Researchers receive a modest honorarium
- Results are presented at the following Workshop
- Posters, papers, and video presentations are all submitted

History of C3E Cybersecurity Challenge Problem Topics:
- Identity Discovery Challenge (2012)
- APT Infection Discovery Using DNS Data (2013)
- Metadata-based Malicious Cyber Discovery (2014)
- Novel Approaches to Avoid Misattribution (2015)
- Modeling Consequences of Ransomware (2016-17)
- Adversarial Machine Learning (ML), connections with Explainable Artificial Intelligence (XAI), and Decision Support Vulnerabilities (2018)
- Cognitive Securing and Human-Machine Teaming (2019)
- Economics of Security and Continuous Assurance (2020-2021)
- Supply Chain Software Static Analysis Coverage, AI, and Victimology (2021-2022)
- Cyberpsychology Aspects of Foreign Malign Influence and Generative AI and Large Language Models (2023-2024)

About October 15, 2024:
- We'll notify ~150 potential researchers of funding and solicit proposals on the two topics below
- Form a review panel to evaluate proposals
- Offer honorariums based on reviews of those proposals

Researchers will:
- Provide posters and video presentation at C3E 2025
- Final paper due at end of CY25

Sociotechnical Aspects of Human-AI Systems

This Challenge Problem will ask technologists and social/behavioral researchers to identify areas of future research.

Generative Technologies and Specification

This Challenge Problem will focus on the use of generative technologies to assist with development of specifications.

Computational Cybersecurity in Compromised Environments
2023 Fall Workshop | September 12-14 | Florida Institute of Technology in Melbourne, Florida