C3E Challenge Problems

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)

On October 1, 2023:

- 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 2024
- Final paper due at end of CY24

Cyberpsychology Aspects of Foreign Malign Influence

- What gaps are there in this approach?
- What are the long-term implications of this approach?
- What tools might be developed to actively scan social media to identify and assess false information?
- How can AI be used counter such information campaigns?
- How can attribution be determined for the source of such campaigns?

Generative AI and Large Language Models

- Trustworthiness
- Validation related to meeting user intentions
- Concerns related to automation bias, the ELIZA effect, and fluency
- Prompt engineering in eliciting high-utility output from large language models
- Identifying and characterizing the bounds of coherent generation
- Human-Computer Interaction (HCM) approaches that address what the appropriate interface is to help a user make sense of LLM generations