On the Curation of Artifacts in the Era of AI/ML for Cybersecurity

- ACSAC'22 Panel

- **S. Jay Yang (moderator)**, Professor & Director of Global Outreach @ ESL GCI, Rochester Institute of Technology
  - Researcher and teacher on AI/ML for better cyber defense operations; proponent of quality research artifacts.
- **David Balenson**, Senior Supervising Computer Scientist, Networking and Cybersecurity Division, USC Information Science Institute
  - Longtime proponent of cybersecurity experimentation (PIVOT, SEARCCH, CEF, LASER)
- **Rob Beverly**, Program Director, NSF Office of Advanced Cyberinfrastructure
  - Security researcher performed some of the first ML applications for transport layer traffic in 2000s.
  - NSF: AI Institutes, CICI RSSD, OSTP Holdren memo.
- **Emma Tosch**, Researcher, Northeastern University
  - System building, programming language support for experimentation, data collection processes.
- **Sagar Samtani**, Assistant Professor and Grant Thornton Scholar, Kelley School of Business, Indiana University
  - Researcher on deep learning-based cyber threat intelligence, testbed and infrastructure development.
- **Sebastián García**, Security Researcher and Teacher, Stratosphere Laboratory, Czech Technical University
  - Leader behind CTU-13 and many other datasets that have been used and cited by >1K papers.

On the Curation of Artifacts in the Era of AI/ML for Cybersecurity

- ACSAC'22 Panel

Topics for Discussion:

- Artifacts: what is special about them for cybersecurity AI/ML R&D?
- Are there high quality code/data to conduct cybersecurity AI/ML research and experiments? What makes them good?
- What might be the main reasons that it is challenging to produce/curate quality artifacts for cybersecurity AI/ML R&D?
- How do we measure the quality of these artifacts now as a community? What works and what does not?
- Who are the consumer/users of these artifacts? Other researchers, industry, practitioners? Do they/we care?

YOUR thoughts and questions?

How to go forward?

On the Curation of Artifacts in the Era of AI/ML for Cybersecurity

- ACSAC’22 Panel

How to go forward?

- What roles can conferences and journals play in curating quality artifacts for cybersecurity AI/ML research?
- What can we do to help researchers (e.g., PhD students) to produce higher quality artifacts for cybersecurity AI/ML?
- What can funding agencies do to help the community elevates the development and sharing of quality artifacts?
- What are needed to sustain the improvement and uses of artifacts after they are first released?
- How to broaden the usage of quality artifacts for cybersecurity AI/ML R&D?