Slido: CPSP

NSF SaTC PI Meeting 2022

Breakout Session 3

Cyber-Physical Security and Privacy

Co-Leads:

WenZhan Song (University of Georgia)

Alfred Chen (University of California, Irvine)

Scribes:

Peng Liu (Pennsylvania State University)

Sauvik Das (Georgia Institute of Technology)

Slido: CPSP

Session Organizers

- **WenZhan Song** is a Chair Professor of Computer Engineering at University of Georgia, founding Director of the Center for Cyber-Physical Systems. Research Interest in IoT/CPS security, sensor networks and data analytics.
- **Alfred Chen** is an Assistant Professor Department of Computer Science, University of California, Irvine. Expertise in AI/system/network security. Current focus: AI and software security in emerging CPS, such as self-driving cars.
- **Peng Liu** is a Chair Professor of Information Sciences and Technology at Penn State University, founding Director of the Center for Cyber-Security, Information Privacy, and Trust. Research Interest in many areas of computer security (including IoT security).
- **Sauvik Das** is an Assistant Professor of Interactive Computing at Georgia Tech (joining CMU in September 2022). Research Interest at the intersection of HCI, AI and cybersecurity.

Slido: CPSP

Discussion Summary

1. What is Cyber-Physical Security and Privacy? Why is it important to society? to a secure and trustworthy cyberspace? in other ways?

- Importance: cyber, physical, human
- Aspects: security, privacy, resilience, safety, risk, trust
- Applications: transportation, health, energy, etc

2. Is there is an existing body of research and/or practice? What are some highlights or pointers to it?

- sensing, control, embedded OS, network, AI, privacy
- policy, community, education, training

Slido: CPSP

Discussion Summary

3. What are important challenges that remain? Are there new challenges that have arisen based on new models, new knowledge, new technologies, new uses, etc?

4. Are there promising directions to addressing them? What kinds of expertise and collaboration is needed (disciplines and subdisciplines)?

- Community-level CPS security testbed (and open dataset)
  - More NSF and federal grant support? Crowdsourcing?
- Threat model
  - Lack of systematic summary of attack surface / threat models pertinent to CPS/IoT
- Security and risk assessment and management
  - industry standards create incentive for improving security, resilience
- Human-in-the-loop aspects (safety, privacy, trust)
  - Highly interdisciplinary, how to systematically integrate them into security research?
- Education and training:
  - Interdisciplinary course to train students and professionals CPS domain and security knowledge

Slido: CPSP

Discussion Summary

5. Any other topic-specific questions/issues not covered by the earlier questions.

- Industry-University-Government partnership
- Policy and regulation aspects (communication with policymakers, enforcement, etc.)
- Theoretical attacks and open testbed based evaluation are not reason to reject papers/proposals