Breakout Session: AI for Security

Potomac I; Wednesday, 6/1 - 1:30-3 PM EDT; Thursday, 6/2 - 10:30-11:30 AM EDT

- Sagar Samtani, Indiana University (ssamtani@iu.edu)
- Anita Nikolich, University of Illinois at Urbana Champaign (anitan@illinois.edu)
- Gang Wang, University of Illinois at Urbana Champaign (gangw@illinois.edu)
- Saptarshi Debroy, City University of New York (CUNY) (sd1998@hunter.cuny.edu)

AI for Security: Overview

- Common cybersecurity tasks: asset identification, control allocation, vulnerability management, threat detection and response
  - Challenges: data overload, limited human resources, etc.
- Role of AI for cybersecurity:
  - Automate common cybersecurity tasks, e.g., sifting through data more efficiently and effectively than a human
  - Identify patterns in large datasets missed by manual analysis
- Breakout Session Discussion:
  - **Topic 1:** Data/Model Sharing Needs
  - **Topic 2:** Needs of AI Working with Humans
  - **Topic 3:** Needs of AI-Cyber Workforce Development

Discussion - Data/Model Sharing Needs

Why cannot we share data? Are they real excuses?

Discoverability; centralization; quality; unclear metadata/needs; encryption; NDAs; company restrictions

How to standardize the data sharing process and format?

Increase centralization; need for APT, automotive, SDN datasets; NSF OAC, supplements, dedicated programs (?) → stick to a definition!

Is it possible to share large "pre-trained" models for general downstream security applications?

Yes, but need to develop/share, e.g., HuggingFace; the role of transfer learning/knowledge; validation

How to run large-scale AI models to secure resource constrained systems?

Critical for 5G/6G; IoT devices are constrained; emphasis on IoT testbeds e.g., AERPAW

Discussion - Needs of AI Working with Humans

How to make AI-based security tools truly usable?

Understand security workflows; need concepts/end-goals when developing AI; new set of usability metrics?; consolidate toolsets

Why do human analysts trust/distrust AI systems?

Operational environment different than theoretical; lack of ways to confirm or explain AI model decisions; what types of AI for what types of problems?

How can human analysts work/learn with AIs?

Beyond labels; increase human in the loop; very context dependent!; role of ethics?

Discussion - Needs of AI-Cyber Workforce Development

What are some of the challenges your institution faces when teaching AI for cyber?

Institutional roadblocks discoverability, accessibility, benchmarks; competitions are useful!

How are AI-cyber lab resources different than cybersecurity-only resources?

Larger data/compute requirements; more background knowledge; lack of faculty expertise
→ co-instructors with synergistic knowledge

How would knowing employer needs for AI for cybersecurity help with curricular development?

Helps specify real/operational problems; balancing fundamentals with trends

How to promote dataset and resource sharing in CyberCorps community to help develop AI for cybersecurity curriculums?

Converge AI and cyber communities; competitions; need for textbooks and playbooks!