Symposium on AI in Cybersecurity

Abstract

This symposium aims to explore the current challenges and emerging trends in the transformative role of AI and machine learning in the realm of cybersecurity, with a particular emphasis on safeguarding critical infrastructure. The objectives are as follows:

1. **Identify Current Challenges and Emerging Trends**: Explore the latest research developments and trends in AI and machine learning as they apply to cybersecurity. This includes understanding the evolving threat landscape and the innovative techniques being developed to counteract these threats.

2. **Leverage Generative AI for Defense and Counteract Malicious Use**: Examine how Generative AI (GenAI) can be employed for defensive cybersecurity measures while also understanding and mitigating the risks posed by malicious actors utilizing GenAI for cyber attacks.

3. **Establish AI-Enabled Cybersecurity Education, Operations, and Research**: Develop a comprehensive pathway for integrating AI into cybersecurity education, operations, and research. This involves leveraging best practices and strategies identified during the symposium to enhance the training and operational capabilities of cybersecurity professionals.

4. **Integrate Ethical and Trustworthy AI**: Address the importance of ethical considerations and the implementation of trustworthy AI in cybersecurity applications. Discussions will include how to integrate ethical principles into AI-driven cybersecurity tools and operations.

5. **Promote Collaboration and Innovation**: Facilitate active discussions and collaborative sessions among experts from academia, industry, and government. The aim is to promote innovation and share knowledge on best practices and strategies for advancing AI in cybersecurity.

6. **Practical Applications and Tools**: Present and discuss practical applications, tools, and resources for integrating AI into cybersecurity education and operational frameworks. This includes showcasing effective strategies for research-informed AI-enabled cybersecurity operations.

Key topics to be covered in the symposium include:

- Research trends in AI and machine learning for cybersecurity

- Role of GenAI in Cybersecurity Landscape (Both defensive and attacking)
- Benefits and risks of AI in critical infrastructure security
- Impact of AI on cybersecurity education and operations in industry and government
- Tools and resources for integrating AI into cybersecurity education and operations
- Strategies and best practices for creating research-informed AI-enabled cybersecurity education and operations
- Securing the AI/ML supply chain and addressing related challenges

By bringing together experts from various sectors, this symposium aims to foster a collaborative environment that drives forward the implementation and development of AI in cybersecurity, ensuring a secure future in an increasingly AI-integrated world.