Minitrack Introduction: Cybersecurity in the Age of Artificial Intelligence, AI for Cybersecurity, and Cybersecurity for AI

Mark Patton
University of Arizona
mpatton@email.arizon.edu

Sagar Samtani
Indiana University
ssamtani@iu.edu

Hsinchun Chen
University of Arizona
hsinchun@email.arizona.edu

Hongyi Zhu
University of Texas at San Antonio
hongyi.zhu@utsa.edu

Abstract

Cybersecurity and Artificial Intelligence (AI) are key domains whose intersection gives great promises and poses significant threats. Indeed, the National Academy of Science (NAS), the National Science Foundation (NSF), and othßer respected entities have noted the significant role that AI can play in cybersecurity, and the importance of ensuring the security of AI-enabled algorithms and systems. This minitrack focuses on AI and Cybersecurity that works in broader domains, collaborative inter-organizational realms, shared collaborative domains, or with collaborative technologies. The papers in this minitrack have the potential to offer interesting and impactful solutions to emerging areas, including unmanned aerial vehicles and open source software security.

Keywords: Cybersecurity, Artificial Intelligence, Machine Learning, Deep Learning, Collaboration, Data Analytics, Cybersecurity for Artificial Intelligence

1. Introduction

Cybersecurity and Artificial Intelligence (AI) are emerging as two interrelated domains whose intersection provides new unique situations, both threats and opportunities. The nature of AI and cybersecurity encompasses many domains. While some perspectives are narrowly focused (e.g., point solutions inside an organization identifying threats in a network stream), many are very sweeping and are either collaborative or tackle collaborative domains (e.g., identifying intentional or unintentional cybersecurity threats propagating across collaboration platforms). Indeed, enhancing our capabilities in AI for cybersecurity has been noted as a key national priority by significant entities such as the National Science Foundation (NSF), the National Science Technology Council (NSTC), and the National Academy of Science (NAS).

Implementing AI and Cybersecurity can also be internal to an organization or broadly collaborative (e.g., organizations working and competing together in adversarial AI research). Conversely, cybersecurity for AI has point solutions internal to organizations and broadly collaborative domains (e.g., collaboratively protecting from adversarial examples in shared data sets or shared models with multi-organizational transfer learning). However, the range and scope of how AI could be used for cybersecurity and how to improve the cybersecurity of AI still need to be studied more critically important areas. Similarly, more work must be examined to examine the security of AI models in mission-critical or operational environments.

2. Minitrack Goals and Focus

In this minitrack, we sought to help cultivate the community of scholars who are working in the intersection of cybersecurity and AI. Broadly, the topics and research areas included, but were not limited to:

- Novel applications of Artificial Intelligence, Machine Learning, and Deep Learning in Cybersecurity as it pertains to multi-user/multi-organizational collaborative domains and/or systems.

URI: https://hdl.handle.net/10125/106439
978-0-9981331-7-1

- Adversarial AI/Machine Learning Applications in Cybersecurity that collaboratively span organizations or apply to collaborative systems (i.e., malware, phishing, or any applicable threat/identification domain).
- Protecting AI that is used collaboratively (i.e., shared data sets, shared models, shared applications) or spans collaborative domains from cybersecurity threats (i.e., adversarial examples, trojans, model inversion).
- Using AI to protect AI in any appropriate wide-reaching setting.

The authors for each submitted paper were encouraged to provide sufficient details about their implementation (e.g., code, datasets, computational setups, etc.) to help facilitate reproducibility.

3. Papers

Each paper went through a rigorous peer review process. Conflicts of interest were carefully managed throughout the review process. Ultimately, two papers were selected for acceptance for this minitrack. We provide the title, abstract, and keywords for each paper that was accepted to the minitrack below. Interested readers are encouraged to access the full copy of the paper in the proceedings.

Paper 1 Title: Detecting Spoofing and GPS Jamming in UAVs: Multiclass Approach to Attack Diagnosis.

Abstract: As Unmanned Aerial Vehicles (UAVs) become increasingly popular and affordable, it is essential to ensure their safe operation, especially around critical devices such as the aircraft's Global Positioning System (GPS). GPS plays an indispensable role in aviation systems. This study presents an efficient multiclass detection method to identify GPS attacks on UAVs, focusing on differentiating between spoofing and jamming attacks. The proposed approach outperforms existing methods. The results obtained in this study contribute to increasing the security of UAVs and provide valuable information for developing robust detection systems to combat evolving threats in the UAV domain.

Keywords: Smart Detection, Unmanned Aerial Vehicles, Detection Attacks, GPS Attacks, Security Failure.

Paper 2 Title: Suggesting Alternatives for Potentially Insecure Artificial Intelligence Repositories: An Unsupervised Graph Embedding Approach

Emerging Artificial Intelligence (AI) applications are bringing with them both the potential for significant societal benefit and harm. Additionally, vulnerabilities within AI source code can make them susceptible to attacks ranging from stealing private data to stealing trained model parameters. Recently, with the adoption of open-source software (OSS) practices, the AI development community has introduced the potential to worsen the number of vulnerabilities present in emerging AI applications, building new applications on top of previous applications, naturally inheriting any vulnerabilities. With the AI OSS community growing rapidly to a scale that requires automated means of analysis for vulnerability management, we compare three categories of unsupervised graph embedding methods capable of generating repository embeddings that can be used to rank existing applications based on their functional similarity for AI developers. The resulting embeddings can be used to suggest alternatives to AI developers for potentially insecure AI repositories.

Keywords: Artificial Intelligence, Open-source Software, Cybersecurity, Unsupervised Graph Embedding.

4. Acknowledgements

We thank all of the authors for their contributions to this workshop. We wish to acknowledge all of the reviewers who worked hard to review the papers that were submitted to this minitrack. This minitrack is based upon work funded by DGE-2038483 (SaTC-EDU), DGE-1946537 (SFS), and OAC-1917117 (CICI).