Md. Ahsan Ayub

Atlanta, GA 30318, USA | mayub42@tntech.edu | linkedin.com/in/mdahsanayub | ahsanayub.github.io

Education

Tennessee Technological University — Cookeville, TN
Ph.D. in Computer Science. CGPA 3.93/4.00. — *Aug 2018 – May 2023*

Experience

Security Data Scientist — June 2023 – August 2023
Dropzone AI (Contractual) — *Seattle, WA*
- Integrated 4 security monitoring tools in the Company's alert investigation platform to perform analytical work in SOCs autonomously by leveraging the large language model (LLM)-based autonomous AI agents.
- Developed and refined prompts to specialize GPT language models in security operations without causing hallucination.

Graduate Research Assistant — Aug 2018 – May 2023
Cybersecurity Education, Research & Outreach Center (CEROC) — *Cookeville, TN*
- Examined the structural dissimilarities (PE metadata) between 2,436 ransomware and 3,014 benign application with built machine learning models and reported accuracy, precision, recall, and F_1 scores in low 90s using Random Forest classifier.
- Proposed a novel static-informed dynamic analysis approach for early detection of cryptographic windows ransomware and reported 97.67%, 92.38%, and 86.42% accuracy within 120, 60, and 30 seconds of their behavioral logs, respectively.
- Published 10 peer-reviewed scholarly articles in ransomware, cryptography, adversarial ML, DGA, and covert communication.

Security Engineer (Intern) — Jan 2022 – Dec 2022
AllianceBernstein — *Nashville, TN*
- Processed a large number of geographical security events on SIEM to document security incidents and to present actionable insights on the anomalous IP ranges for the incident response and risk mitigation tasks.
- Utilized open-source tools to discover trends and emerging threats and identify known/unknown web applications security vulnerabilities including cross-site scripting, cross-site request forgery, SQL injection, DoS attacks, and API attacks.
- Developed custom methodologies, payloads, and exploits to detect and remedy security issues, such as OWASP Top 10.

Software Project Manager — Feb 2017 – July 2018
Appinion BD Limited — *Dhaka, Bangladesh*
- Led Dev and UI/UX teams to build a scalable and reliable sales learning app for 1,500+ users of a pharmaceutical company.

Skills

Programming Languages: Proficient in Python, C/C++, and SQL. Familiar with JAVA, C#, R, Shell Scripting, JS, and PHP.
Frameworks and Tools: Metasploit, Splunk, Nmap, Nessus, Burp Suite, Matplotlib, Scikit-learn, Docker, Git, CI/CD, MySQL, RESTful API, Static Application Security Testing (SAST), and Dynamic Application Security Testing (DAST).
Cybersecurity Practices: Intrusion Analysis, Threat Modeling, API Security, Secure System Design and Architecture, Identity and Access Management (IAM), Disaster Recovery and Business Continuity, Secure Deployment Practices, and Cloud Security.

Certifications

- **AWS Certified Cloud Practitioner**, issued on Aug 2023 by Amazon Web Services (AWS).
- **eLearnSecurity Junior Penetration Tester (eJPT)**, issued on Aug 2022 by eLearnSecurity - an INE Company.
- **CompTIA Security+**, issued on Feb 2022 by CompTIA.
- **Sequences, Time Series, and Prediction** & **Neural Networks and Deep Learning** by DeepLearning.AI in 2020.

Leadership

Competitive Programming Coach at Tennessee Tech University — Oct 2021 – May 2023
- Taught mathematics, data structure, and algorithms-related problem-solving topics through lectures and practice contests.

President of the Computer Science Graduate Student Club at Tennessee Tech University — Sep 2019 – Aug 2021
- Organized bi-weekly seminars to promote the research environment and enable the club members to network and collaborate.

Honors and Awards

- Best poster in the 2021 Student Research and Creative Inquiry Day (CS Graduate Track) at Tennessee Tech University.
- 2^{nd} prize for the 2015 Web Application Development/Showcasing intra-college competition at my undergraduate university.

Selected Publications

- **M. A. Ayub**, A. Siraj, B. Filar, and M. Gupta, "RWArmor: a static-informed dynamic analysis approach for early detection of cryptographic windows ransomware," International Journal of Information Security (2023), pp. 1-24. (Manuscript)
- **M. A. Ayub** and A. Siraj, "Similarity Analysis of Ransomware based on Portable Executable (PE) File Metadata," 2021 IEEE Symposium Series on Computational Intelligence (SSCI), Orlando, FL, USA, 2021, pp. 1-6. (GitHub)
- **M. A. Ayub**, A. Continella, and A. Siraj, "An I/O Request Packet (IRP) Driven Effective Ransomware Detection Scheme using Artificial Neural Network," 2020 IEEE International Conference on Information Reuse and Integration (IRI). (GitHub)
- **M. A. Ayub**, W. A. Johnson, D. A. Talbert, and A. Siraj, "Model Evasion Attack on Intrusion Detection Systems using Adversarial Machine Learning," 2020 54th Annual Conference on Information Sciences and Systems (CISS). (GitHub)