Ahmed Abusnaina

Research Scientist (Machine Learning), Meta
1207 Westlake Ave N, Seattle, WA 98109 USA
Email: ceng.ahmed.kas@gmail.com
Phone: +1-407-929-2455

Professional Experience

03/01/2024 – Present	Senior ML Research Scientist	Meta Platforms, Inc.
06/13/2022 – 03/01/2024	ML Research Scientist	Meta Platforms, Inc.
05/26/2021 – 08/20/2021	Research Intern	Visa Research
05/27/2020 – 07/17/2020	Research Intern	Visa Research
08/23/2018 – 05/07/2022	Graduate Research Assistant	University of Central Florida
08/17/2017 – 06/30/2018	Software Engineer	ITG Software
05/26/2017 – 08/01/2017	Research Intern	University of Konstanz

Education

Ph.D.	Computer Science	University of Central Florida, Orlando, FL, USA Topic: Robust Machine Learning Applications	2018 – 2022
M.Sc.	Computer Science (GPA: 3.91)	University of Central Florida, Orlando, FL, USA	2018 – 2021
B.Sc.	Computer Engineering (GPA: 3.97)	An-Najah National University, Nablus, Palestine	2014 – 2018

Project Experience Domains

- Social Networks Modeling & Understanding
- User Behavioral Modeling & Pattern Recognition/Exploration
- Robust Machine Learning Applications
- Anomaly Detection

Machine Learning Publications And Manuscripts

1. **Ahmed Abusnaina**, Afsah Anwar, Sultan Alshamrani, Abdulrahman Alabduljabbar, Rhongho Jang, DaeHun Nyang, David Mohaisen, "**Systematically Evaluating the Robustness of ML-based IoT Malware Detection Systems**", Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID), 2022.
2. **Ahmed Abusnaina**, Yuhang Wu, Sunpreet Arora, Yizhen Wang, Fei Wang, Hao Yang, and David Mohaisen, "**Adversarial Examples Detection Using Latent Neighborhood Graph**", International Conference on Computer Vision (ICCV), 2021.
3. Afsah Anwar, **Ahmed Abusnaina**, Songqing Chen, Frank Li, and David Mohaisen, "**Cleaning the NVD: Comprehensive Quality Assessment, Improvements, and Analyses**", IEEE Transactions on Dependable and Secure Computing, 2021.
4. Abdulrahman Alabduljabbar, **Ahmed Abusnaina**, Ulku Meteriz, and David Mohaisen, "**TLDR: Deep Learning-Based Automated Privacy Policy Annotation with Key Policy Highlights**", Workshop on Privacy in the Electronic Society (WPES), 2021.
5. **Ahmed Abusnaina**, Mohammed Abuhamad, Hisham Alasmary, Afsah Anwar, Rhongho Jang,Saeed Salem, DaeHun Nyang, and David Mohaisen, "**DL-FHMC: Deep Learning-based Fine-grained Hierarchical Learning Approach for Robust Malware Classification**", IEEE Transactions on Dependable and Secure Computing, 2021.

6. Hisham Alasmary, Afsah Anwar, **Ahmed Abusnaina**, Abdulrahman Alabduljabbar, Mohammad Abuhamad, An Wang, DaeHun Nyang, Amro Awad, and David Mohaisen, "**ShellCore: Automating Malicious IoT Software Detection by Using Shell Commands Representation**", IEEE Internet of Things Journal, 2021.
7. Sultan Alshamrani, **Ahmed Abusnaina**, Mohammed Abuhamad, Daehun Nyang, and David Mohaisen, "**Hate, Obscenity, and Insults: Measuring the Exposure of Children to Inappropriate Comments in YouTube**", The International Workshop on Natural Language Processing for Social Media (SocialNLP 2021).
8. Sultan Alshamrani, **Ahmed Abusnaina**, Mohammed Abuhamad, Anho Lee, DaeHun Nyang, and David Mohaisen, "**An Analysis of Users Engagement on Twitter During the COVID-19 Pandemic: Topical Trends and Sentiments**", International Conference on Computational Data and Social Networks (2021).
9. Hisham Alasmary*, **Ahmed Abusnaina***, Rhongho Jang*, Mohammed Abuhamad, Afsah Anwar, DaeHun Nyang, and David Mohaisen, "**Soteria: Detecting Adversarial Examples in Control Flow Graph-based Malware Classifiers**", IEEE International Conference on Distributed Computing Systems (ICDCS 2020).
10. Sultan Alshamrani, **Ahmed Abusnaina**, Mohammed Abuhamad, Anho Lee, DaeHun Nyang, and David Mohaisen, "**An Analysis of Users Engagement on Twitter During the COVID-19 Pandemic: Topical Trends and Sentiments**", International Conference on Computational Data and Social Networks (CSoNet 2020).
11. Aminollah Khormali, **Ahmed Abusnaina**, Songqing Chen, DaeHun Nyang, and David Mohaisen, "**From Blue-Sky to Practical Adversarial Learning**", IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA 2020).
12. **Ahmed Abusnaina***, Rhongho Jang*, Amin Kharmali, DaeHun Nyang, and David Mohaisen, "**Deep Fingerprinting Defender: Adversarial Learning-based Approach to Defend Against Website Fingerprinting**", IEEE International Conference on Computer Communications (INFOCOM 2020)
13. Sultan Alshamrani, Mohammed Abuhamad, Ahmed Abusnaina, and David Mohaisen, "**Investigating Online Toxicity in Users Interactions with the Mainstream Media Channels on YouTube**", International Workshop on Mining Actionable Insights from Social Networks (MAISoN 2020) – with CIKM 2020.
14. Sultan Alshamrani, **Ahmed Abusnaina**, and David Mohaisen, "**Hiding in Plain Sight: A Measurement and Analysis of Kids' Exposure to Malicious URLs on YouTube**", The ACM/IEEE Workshop on Hot Topics on Web of Things (HotWoT 2020) – with ACM/IEEE SEC 2020.
15. **Ahmed Abusnaina**, Mohammed Abuhamad, DaeHun Nyang, Songqing Chen, An Wang, and David Mohaisen, "**Insights into Attacks' Progression: Prediction of Spatio-Temporal Behavior of DDoS Attacks**", The World Conference on Information Security Applications (WISA 2020).
16. Mohammed Abuhamad, **Ahmed Abusnaina**, DaeHun Nyang, and David Mohaisen, "**Sensor-based Continuous Authentication of Smartphones' Users Using Behavioral Biometrics: A Contemporary Survey**", IEEE Internet of Things Journal, 2020
17. Jinchun Choi, Mohammed Abuhamad, Ahmed Abusnaina, Afsah Anwar, Sultan Alshamrani, Jeman Park, Daehun Nyang, and David Mohaisen, "**Understanding the Proxy Ecosystem: A Comparative Analysis of Residential and Open Proxies on the Internet**", IEEE Access, 2020.
18. **Ahmed Abusnaina**, Hisham Alasmary, Mohammed Abuhamad, Saeed Salem, DaeHun Nyang, and Aziz Mohaisen, "**Subgraph-based Adversarial Examples Against Graph-based IoT Malware Detection Systems**", International Conference on Computational Data and Social Networks (CSoNet 2019).
19. **Ahmed Abusnaina***, Amin Kharmali*, Murat Yuksel and Aziz Mohaisen, "**Examining the Robustness of Learning-Based DDoS Detection in Software Defined Networks**", IEEE Conference on Dependable and Secure Computing (IDSC 2019).
20. Jinchun Choi, **Ahmed Abusnaina**, Afsah Anwar, An Wang, Songqing Chen, Daehun Nyang and Aziz Mohaisen, "**Honor Among Thieves: Towards Understanding the Dynamics and Interdependencies in IoT Botnets**", IEEE Conference on Dependable and Secure Computing (IDSC 2019).
21. Hisham Alasmary, Aminollah Khormali, Afsah Anwar, Jeman Park, Jinchun Choi, **Ahmed Abusnaina**, Amro Awad, DaeHun Nyang, and Aziz Mohaisen, "**Analyzing and Detecting Emerging Internet of Things Malware: A Graph-based Approach**", IEEE Internet of Things Journal, 2019.
22. **Ahmed Abusnaina**, Amin Khormali, Hisham Alasmary, Jeman Park, Afsah Anwar, and Aziz Mohaisen. "**Adversarial Learning Attacks on Graph-based IoT Malware Detection Systems**". IEEE International Conference on Distributed Computing Systems (ICDCS 2019), Texas, US, 7-10 July 2019 (acceptance rate 19.6%).

23. **Ahmed Abusnaina**, Afsah Anwar, Sultan Alshamrani, Abdulrahman Alabduljabbar, RhongHo Jang, Daehun Nyang, David Mohaisen. "**ML-based IoT Malware Detection Under Adversarial Settings: A Systematic Evaluation**". International Symposium on Research in Attacks, Intrusions and Defenses (RAID) (Accepted, available at arXiv).
24. **Ahmed Abusnaina**, Afsah Anwar, Sultan Alshamrani, Muhammad Saad, RhongHo Jang, Daehun Nyang, David Mohaisen. "**One Step Forward, Two Steps Back: Exposing the Limitations of Model Retraining in Machine Learning-based Malware Detection**". Under submission.
25. **Ahmed Abusnaina**, Yizhen Wang, Sunpreet Arora, Ke Wang, Mihai Christodorescu, David Mohaisen. "**Burning the Adversarial Bridges: Robust Malware Detection Against Binary-level Mutations**". Under submission.
26. **Ahmed Abusnaina**, Yizhen Wang, Sunpreet Arora, Ke Wang, Mihai Christodorescu, David Mohaisen. "**Burning the Adversarial Bridges: Robust Malware Detection Against Binary-level Mutations**". Under submission.

Patent Disclosures

1. **Ahmed Abusnaina**, Yuhang Wu, Sunpreet Arora, and Yizhen Wang, *Adversarial Examples Detection Using Latent Neighborhood Graph*.
2. **Ahmed Abusnaina**, Yizhen Wang, Sunpreet Arora, Ke Wang, and Mihai Christodorescu, *Burning the Adversarial Bridges: Robust Malware Detection Against Binary-level Mutations*.

Public Presentations

- Fast Abstract presentation of *Systemically Evaluating the Robustness of ML-based IoT Malware Detectors* at The IEEE/IFIP International Conference on Dependable Systems and Networks (DSN-S 2021), Virtual, June 21-24, 2021.
- Paper presentation of *Soteria: Detecting Adversarial Examples in Control Flow Graph-based Malware Classifiers* at IEEE International Conference on Distributed Computing Systems (ICDCS 2019), Virtual, 29 November - 1 December 2020.
- Paper presentation of *Insights into Attacks' Progression: Prediction of Spatio-Temporal Behavior of DDoS Attacks* at The World Conference on Information Security Applications (WISA 2020), Virtual, 26-28 August 2020.
- Paper presentation of *Deep Fingerprinting Defender: Adversarial Learning-based Approach to Defend Against Website Fingerprinting* at the IEEE International Conference on Computer Communications (INFOCOM 2020), Virtual, 9-10 July 2020.
- Paper presentation of *Adversarial Learning Attacks on Graph-based IoT Malware Detection Systems* at IEEE International Conference on Distributed Computing Systems (ICDCS 2019), Texas, US, 7-10 July 2019.
- Poster presentation of *Examining Adversarial Learning against Graph-based IoT Malware Detection Systems* at The Network and Distributed System Security Symposium (NDSS 2019), San Diego, CA, US, Feb 23-27, 2019.
- Poster presentation of *Breaking Graph-based IoT Malware Detection Systems Using Adversarial Examples* at The 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), Miami, FL, US, May 15-17, 2019.

References

Muhammad Saad, Research Scientist (Collaborator)
Paypal
E-mail: muhsaad@paypal.com

Mohammed Abuhamad, Assistant Professor (Collaborator)
Department of Computer Science

Loyola University Chicago
E-mail: mabuhamad@luc.edu