Ahmed Abusnaina

Department of Computer Science, University of Central Florida
1014 McDaniel Creek Ct, Oviedo, FL 32765 USA
Email: ahmed.abusnaina@knights.ucf.edu
Phone: +1-407-929-2455

Education

PH.D., Computer Science, University of Central Florida, Orlando, FL, USA (2018 – Current)
Advisor: Prof. Aziz Mohaisen. Topic: Machine Learning
B.S., Computer Engineering, An-Najah National University, Nablus, Palestine (2014 – 2018)

Research Interests

Machine Learning Application, Natural Language Processing, Adversarial Machine Learning, Internet of Things Security, Malware Analysis, and User Privacy

Professional Experience

08/2018 – Current	Research Assistant	University of Central Florida	Machine Learning
08/2017 – 06/2018	Software Engineer	ITG Software	Web Development

Technical Publications And Manuscripts

1. Amin Kharmali, Ahmed Abusnaina, 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)
2. 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)
3. 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
4. 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%).
5. Ahmed Abusnaina, Amin Khormali, Hisham Alasmary, Jeman Park, Afsah Anwar, Ulku Meteriz, and Aziz Mohaisen. "**Breaking Graph-based IoT Malware Detection Systems Using Adversarial Examples**", The 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), Miami, FL, US, May 15-17, 2019. (Poster)
6. Ahmed Abusnaina, Amin Khormali, Hisham Alasmary, Jeman Park, Afsah Anwar, Ulku Meteriz, and Aziz Mohaisen. "**Examining Adversarial Learning against Graph-based IoT Malware Detection Systems**", The Network and Distributed System Security Symposium (NDSS 2019), San Diego, CA, US, Feb 23-27, 2019. (Poster)
7. Ahmed Abusnaina, Mohammed Abuhamad, DaeHun Nyang, Songqing Chen, An Wang, and Aziz Mohaisen, "**Ensemble Prediction of Spatio-Temporal Behavior of DDoS Attacks**", AAAI Conference on Artificial Intelligence (AAAI 2020) (in submission)
8. Ahmed Abusnaina, Hisham Alasmary, Mohammed Abuhamad, 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) (in submission)

9. Sultan Alshamrani, Mohammed Abuhamad, Ahmed Abusnaina, DaeHun Nyang, and Aziz Mohaisen, "**Politics, Religion, and Insults: Measuring the Exposure of Children and Adolescents to Inappropriate Comments in YouTube**", International AAAI Conference on Web and Social Media (ICWSM 2020) (in submission)
10. Hisham Alasmary, Ahmed Abusnaina, Rhongho Jang, DaeHun Nyang, and Aziz Mohaisen, "**Soteria: Detecting Adversarial Examples in Control Flow Graph-based Malware Classifiers**", IEEE International Conference on Computer Communications (INFOCOM 2020) (in submission)
11. Amin Kharmali, Ahmed Abusnaina, Rhongho Jang, and Aziz Mohaisen, "**Deep Fingerprinting Defender: Adversarial Learning-based Approach to Defend Against Website Fingerprinting**", IEEE International Conference on Computer Communications (INFOCOM 2020) (in submission)
12. Amin Kharmali, Ahmed Abusnaina[§], Songqing Chen, DaeHun Nyangm and Aziz Mohaisen, "**COPYCAT: Practical Adversarial Deep Learning Attacks on Visualization-Based Malware Detection**", ACM Conference on Data and Application Security and Privacy (CODASPY 2020) (in submission)

Representative research project

1. **Machine Learning applications in security**: This project aims to investigate machine and deep learning approaches in detecting, analyzing, modeling, and defending against adversaries.
2. **Adversarial Learning**: This project aims to investigate the robustness of several machine/deep learning models by generating practical adversarial examples.

Skills

1. Python, C/C++, Java, PHP, JS, Latex
2. Machine Learning, Natural Language Processing, Malware Analysis, Data Analysis

Services and Activities

- External reviewer for IEEE CNS 2019.
- Reviewer for Transactions on Mobile Computing 2019.

References

Aziz Mohaisen, Associate Professor
Department of Computer Science
University of Central Florida
E-mail: mohaisen@cs.ucf.edu
Phone: (407) 823-1294