Afsah Anwar

PhD Candidate
Department of Computer Science, University of Central Florida
4353 Scorpius Street, R1-368, Orlando, FL 32816-2362 USA
Email: afsahanwar@knights.ucf.edu
Phone: +1-407-451-0821

Education

Ph.D., Computer Science, University of Central Florida, Orlando, FL, USA (2017 – Current)
Advisor: Prof. Aziz Mohaisen. Topic: Software security
B.S., Electronics & Communication Engineering, Jamia Millia Islamia University, New Delhi, India (2010 – 2014)

Research Interests

My research explores the existing software vulnerability ecosystem. The resulting artifacts with the help of binary analysis, code analysis, and data science can be leveraged to have a generic vulnerability detection framework and present a consistent vulnerability database that can be used with manageable effort. I am also interested in malware analysis, particularly, in addressing obfuscation.

Professional Experience

08/2017 – Current	Research Assistant	University of Central Florida	Software systems security
05/2019 – 07/2019	Visiting Research Assistant	USC ISI	Vulnerability detection
02/2017 – 06/2017	Senior Systems Engineer	Infosys Limited	Data Analyst at *Apple*
01/2015 – 02/2017	Systems Engineer	Infosys Limited	Data Analyst at *Apple*

Technical Publications And Manuscripts

1. Afsah Anwar[§], Hisham Alasmary, Jeman Park, An Wang, Songqing Chen, David Mohaisen. "**Statically Dissecting Internet of Things Malware: Analysis, Characterization, and Detection**", International Conference on Information and Communications Security, (ICICS 2020).

2. Afsah Anwar[§], Aminollah Khormali, and Aziz Mohaisen. "**Understanding the Hidden Cost of Software Vulnerabilities: Measurements and Predictions**", *Proceeding of The 14th EAI International Conference on Security and Privacy in Communication Networks*, **SecureComm 2018**, Singapore, Singapore, August 8–10, 2018..

3. Hisham Alasmary*, Ahmed Abusnaina*, Rhongho Jang*, Mohammed Abuhamad, Afsah Anwar, DaeHun Nyang, and Aziz Mohaisen, "**Soteria: Detecting Adversarial Examples in Control Flow Graph-based Malware Classifiers**", IEEE International Conference on Distributed Computing Systems (ICDCS 2020)

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).

5. **Muhammad Saad**, Afsah Anwar, Ashar Ahmad, Hisam Alasmary, Murat Yukesl, and Aziz Mohaisen. RouteChain: Towards Blockchain-based Secure and Efficient BGP Routing. IEEE International Conference on Blockchain and Cryptocurrency (**IEEE ICBC 2019**), Seoul, South Korea, 14-17 May, 2019. (Acceptance rate: 19.6%)

6. Hisham Alasmary, Afsah Anwar[§], Jeman Park, Jinchun Choi, Daehun Nyang, and Aziz Mohaisen, "**Graph-based Comparison of IoT and Android Malware**", *The 7th International Conference on Computational Data and Social Networks* **CSoNet 2018**, Shanghai, China, 18-20 December 2018.

7. 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

8. 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)

Representative research project

1. **Vulnerability analysis**: This project aims to evaluate the vulnerability databases and measure the impact of vulnerabilities in a product on its vendor. Towards this, we work towards improving the quality of vulnerability databases and quantify the impact on a vendor in terms of the effect on its stock market price. The project is a mixture of vulnerability analysis, machine learning, manual effort, and statistics. Parts of this work have been presented at SecureComm 2018, and under review at ACM CCS 2020.

2. **IoT malware analysis**: This project aims to analyze IoT malware, and their different behavioral aspects, *e.g.*, endpoints, shell commands, graphs, etc., to detect them precisely and take cues to ensure the security of IoT devices. The project is a fusion of reverse engineering, manual effort, and machine learning algorithms. Parts of this project are accepted at ICDCS 2019 and 2020, IDSC 2019, and CSoNet 2019, and under review at DIMVA 2020.

3. **Automated vulnerability detection in binaries** This project leverages the Machine Learning algorithms and binary analysis techniques to learn rules and policies to distinguish different vulnerability types in binary applications. These rules will be then used to identify vulnerabilities in arbitrary binaries. This project is pursued in collaboration with Christophe Hauser, Jelena Mirkovic (USC ISI), and Yan Shoshitaishvili (ASU).

Public Presentations

1. Paper presentation of *Understanding the Hidden Cost of Software Vulnerabilities: Measurements and Predictions* at 14th EAI International Conference on Security and Privacy in Communication Networks, SecureComm 2018, Singapore.
2. Poster presentations at USENIX Security 2019 and NDSS 2019.

Skills

1. Python, Java, Teradata, Hive, BigQuery, Hortonworks
2. Reverse-engineering, Binary Analysis, Malware Analysis, Big Data Analytics, Vulnerability Reporting

Services

External reviewer for NDSS 2018, INFOCOM 2018, INFOCOM 2019, INFOCOM 2020, TDSC 2018, TMC 2018, TMC 2019, PETS 2019. Tutor: STEM Day (October, 2018) and STEM Summer Camp (June, 2018)

References

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