Omar Alrawi

CONTACT

alrawi@gatech.edu
alrawi.github.io
5105454778

OBJECTIVE

I am looking for a research oriented organization that values innovation and fosters a collaborative environment to enable unorthodox approach to problem solving.

EDUCATION

PhD ECE — Aug 2016

Georgia Tech

Master's Information Security — Aug 2007 — May 2009

Purdue University (CERIAS)

BS in Computer Science and Math — May 2004 — May 2007

Purdue University

WORK EXPERIENCE

Georgia Institute of Technology — August 2016

Research Assistance

Researcher for the Astrolavos Lab.

Qatar Computing Research Institute — June 2013 — July 2016

Sr. Software Engineer

At QCRI, I developed capabilities for the cyber security team to support research in the areas of malware analysis, targeted attacks, SCADA/ICS, and security analytics. I built and configured supporting hardware infrastructure, prototyped tools, and contributed to cyber security research.

Verisign Inc — Jan 2011 — Jun 2013

Malware Engineer

At iDefense I was part of the Malware Intelligence team where my main role was an incident response engineer with a 24x7 on call schedule. My team provided rapid malware analysis with a 3 hours turnaround window providing customers with actionable intelligence to help protect their networks. I proactively researched trending malware and extract indicators to track emerging threats. I also researched and built tools to automate, visualize, and streamline data gathering and analysis. As an engineer at iDefense, I also participated in writing blogs, technical papers, and intelligence briefs for customers.

Booz Allen Hamilton — Jun 2009 — Dec 2010

Consultant

At Booz Allen Hamilton I was part of new team that focused on growing malware analysis and security research capabilities. I learned and practiced in-depth reverse engineering of malware and dynamic analysis. I was in charge of setting up a new malware lab by researching and purchasing hardware and software to enable other team members to perform their tasks. I taught and mentored new team members and other cross functional teams on advanced malware analysis using dynamic and static techniques. I collaborated with team members to build malware tools that helped our client complete their missions.

PUBLICATIONS

- Omar Alrawi, Aziz Mohaisen; Chains of Distrust: Towards Understanding Certificates Used for Signing Malicious Applications, WWW 2016 Companion, April 2016
- Omar Alrawi*, Aziz Mohaisen*; Behavior-based Automated Malware Analysis and Classification, Elsevier Computers & Security, 2015
- A Mohaisen, AG West, A Mankin, O Alrawi; Chatter: Classifying Malware Families Using System Event Ordering. IEEE CNS 2014
- Omar Alrawi*, Aziz Mohaisen*; AMAL: High-Fidelity, Behavior-based Automated Malware Analysis and Classification. WISA 2014. Best Paper.
- Omar Alrawi*, Aziz Mohaisen*; AV-Meter: An Evaluation of Antivirus Scans and Labels. DIMVA 2014.
- Aziz Mohaisen, Omar Alrawi, Andrew G. West, and Allison Mankin; Babble: Identifying Malware by Its Dialects. IEEE CNS 2013.
- Aziz Mohaisen, Omar Alrawi, Matt Larson, and Danny McPherson; Towards A Methodical Evaluation of Antivirus Scans and Labels. WISA 2013.
- Omar Alrawi*, Aziz Mohaisen*; Unveiling Zeus Automated Classification of Malware Samples. WWW Workshops 2013

*contributed equally

TECHNICAL SKILLS

Specialization: Malware analysis, threat intelligence, reverse engineering
Programming: Python, C/C++, Java, etc.
Data science: numpy/scipy, scikit-learn, Theano, matplotlib
Design and architecture: software and infrastructure
System engineering and administration: Linux, Virtualization, Docker, salt
Project/people management: mentoring, team lead, SME, consulting, training

PATENTS

Systems and methods for behavior-based automated malware analysis and classification