Omar Alrawi

Georgia Institute of Technology
School of Electrical and Computer Engineering
Atlanta, GA 30332
Phone: (510) 545-4778 Email: alrawi@gatech.edu Website: https://alrawi.io

Research Interests

I am studying the security of home-based IoT devices and their mobile apps, cloud backends, and network protocols using active and passive measurement techniques. I am also investigating malware threats affecting IoT, mobile, and cloud platforms to understand their impact on critical internet services.

Education

Ph.D. Candidate in Electrical and Computer Engineering — Enrolled
Georgia Institute of Technology — Atlanta, GA

Master of Arts in Linguistics (CERIAS) — May 2009
Purdue University — West Lafayette, IN
Thesis: *Ontological Semantics Spam Filters*
Advisor: Dr. Victor Raskin

Bachelor of Science in Computer Science and Math — May 2007
Purdue University — West Lafayette, IN

Honors & Awards

CSAW Applied Research Competition Finalist — 2019
Impactful Applied Research - The Betrayal At Cloud City - https://mobilebackend.vet/

Create-X Launch Participant and Finalist — 2019
Research Commercialization: https://YourThings.info

Cyber Security Demo Day Final — 2019
First Place (Research Track) Security evaluation of smart-home IoT deployments.

Institute for Information Security & Privacy Demo Day — 2019
Best Research Idea - https://YourThings.info

President Fellowship — 2016-2020
The President Fellowship is a supplement funding for PhD students with exemplary levels of scholarship and innovation.

Patents

Systems and methods for behavior-based automated malware analysis and classification
Patent Number: US9769189B2
Granted: 2017-09-19

Industry Experience

Data Scientist (part-time) — January 2017 to December 2017
Sophos — Abingdon, United Kingdom

Sr. Engineer — June 2013 to August 2016
Qatar Computing Research Institute — Doha, Qatar

Security Engineer — October 2011 to June 2013
Security Intelligence - iDefense - Verisign Inc. — Reston, VA

Consultant — June 2009 to October 2011
Booz Allen Hamilton — Annapolis Junction, Maryland

Selected Publications

Omar Alrawi, Charles Lever, Kevin Valakuzhy, Ryan Court, Kevin Snow, Fabian Monrose, Manos Antonakakis. The Circle Of Life: A Large-Scale Study of The IoT Malware Lifecycle. In *USENIX Security Symposium (SEC)*, 2021.

Omar Alrawi*, Moses Ike*, Matthew Pruett, Ranjita Pai Kasturi, Srimanta Barua, Taleb Hirani, Brennan Hill, Brendan Saltaformaggio; Forecasting Malware Capabilities From Cyber Attack Memory Images. In *USENIX Security Symposium (SEC)*, 2021.

Ruian Duan, **Omar Alrawi**, Ranjita Pai Kasturi, Ryan Elder, Brendan Saltaformaggio, Wenke Lee. Measuring and Preventing Supply Chain Attacks on Package Managers. In *The Network and Distributed System Security Symposium (NDSS)* 2021.

Roberto Perdisci, Thomas Papastergiu, **Omar Alrawi**, Manos Antonakakis. IoTFinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis. In *IEEE European Symposium of Security and Privacy (EuroS&P)*. 2020.

Ranjita Pai Kasturi, Yiting Sun, Ruian Duan, **Omar Alrawi**, Ehsan Asdar, Victor Zhu, Yonghwi Kwon, Brendan Saltaformaggio. TARDIS: Rolling Back The Clock On CMS-Targeting Cyber Attacks. In *IEEE Security and Privacy (Oakland)*. 2020.

Omar Alrawi, Chaoshun Zuo, Ruian Duan, Ranjita Kasturi, Zhiqiang Lin, Brendan Saltaformaggio. The Betrayal At Cloud City: An Empirical Analysis Of Cloud-Based Mobile Backends. In *USENIX Security Symposium (SEC)*. 2019.

Omar Alrawi, Chaz Lever, Manos Antonakakis, Fabian Monrose. SoK: Security Evaluation of Home-Based IoT Deployments. In *IEEE Security and Privacy (Oakland)*. 2019.

Ruian Duan, Ashish Bijlani, Yang Ji, **Omar Alrawi**, Yiyuan Xiong, Moses Ike, Brendan Saltaformaggio, Wenke Lee. Automating Patching of Vulnerable Open-Source Software Versions in Application Binaries. In *The Network and Distributed System Security Symposium (NDSS)*. 2019.

Aziz Mohaisen, **Omar Alrawi**. Behavior-based Automated Malware Analysis and Classification. In *Elsevier Computers & Security*. 2015.

Aziz Mohaisen, **Omar Alrawi**. AV-Meter: An Evaluation of Antivirus Scans and Labels. In *Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*. 2014.