Omar Alrawi

Georgia Institute of Technology
School of Electrical and Computer Engineering
North Ave NW
Atlanta, GA 30332
Email: alrawi@gatech.edu, Website: alrawi.io

Research Interests

My research interest lies in empirical methods for measuring cyber attacks against networked systems by bridging the gap between network vulnerability assessment and end-host binary program analysis.

Education

Ph.D. Candidate in Electrical and Computer Engineering (Expected) May 2022
Georgia Institute of Technology Atlanta, GA
Dissertation: *Security Evaluation and Threat Analysis of Networked Systems*
Advisor: Dr. Manos Antonakakis

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, MobileBackend.vet

Create-X Launch Participant and Finalist 2019
Research Commercialization: Security evaluation of smart-home IoT deployments, YourThings.info
Award: $4,000

Cyber Security Demo Day Final 2019
First Place (Research Track): Security evaluation of smart-home IoT deployments, YourThings.info
Award: $4,000

Institute for Information Security & Privacy Demo Day 2019
Best Research Idea: Security evaluation of smart-home IoT deployments
Award: $5,000

President Fellowship 2016-2020
The President Fellowship is a supplement funding for PhD students
with exemplary levels of scholarship and innovation.
Award: $5,000/Year

Publications

Peer-Reviewed Articles

1. **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. (Acceptance rate 18.8% = 248/1319).
2. **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. (Acceptance rate 18.8% = 248/1319).
3. 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. (Acceptance rate 15.2% = 87/573).
4. 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. (Acceptance rate 14.6% = 38/261).
5. 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. (Acceptance Rate: 12.3% = 104/841).
6. **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. (Acceptance Rate: 16.2% = 113/697).
7. **Omar Alrawi**, Chaz Lever, Manos Antonakakis, Fabian Monrose. SoK: Security Evaluation of Home-Based IoT Deployments. In *IEEE Security and Privacy (Oakland)*. 2019. (Acceptance rate 12.4% = 84/679).
8. 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. (Acceptance rate 17.1% = 89/521).
9. **Omar Alrawi**, Aziz Mohaisen. Chains of Distrust: Towards Understanding Certificates Used for Signing Malicious Applications. In *Workshop on Empirical Research Methods in Information Security co-located with WWW*. 2016.
10. Aziz Mohaisen, **Omar Alrawi**. Behavior-based Automated Malware Analysis and Classification. In *Elsevier Computers & Security*. 2015.
11. A Mohaisen, AG West, A Mankin, **O Alrawi**. Chatter: Classifying Malware Families Using System Event Ordering. In *IEEE Conference on Communications and Network Security (CNS)*. 2014.
12. Aziz Mohaisen, **Omar Alrawi**. AMAL: High-Fidelity, Behavior-based Automated Malware Analysis and Classification. In *Workshop on Information Security Applications (WISA)*. 2014.
13. Aziz Mohaisen, **Omar Alrawi**. AV-Meter: An Evaluation of Antivirus Scans and Labels. In *Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)*. 2014. (Acceptance rate 23.3% = 14/60).

14. Aziz Mohaisen, **Omar Alraw**, Andrew G. West, and Allison Mankin. Babble: Identifying Malware by Its Dialects. In *IEEE Conference on Communications and Network Security (CNS)*. 2013.
15. Aziz Mohaisen, **Omar Alrawi**, Matt Larson, and Danny McPherson. Towards A Methodical Evaluation of Antivirus Scans and Labels. In *Workshop on Information Security Applications (WISA)*. 2013.
16. Aziz Mohaisen, **Omar Alrawi**. Unveiling Zeus Automated Classification of Malware Samples. In *Workshop on Simplifying Complex Networks for Practitioners co-located with WWW*. 2013.

Research & Professional Experience

Research Assistant (Current Position) August 2016
Georgia Tech Atlanta, GA

My Ph.D. research under my advisor Professor Manos Antonakakis focused on developing systematic methodologies that integrate network vulnerability assessments and binary program analysis to discover latent security flaws in networked systems, such as smart-home IoT devices, mobile applications, cloud endpoints, and network services.

Data Scientist January 2017 to December 2017
Sophos Abingdon, United Kingdom

My work at Sophos focused on developing machine learning models to detect and label emerging malware threats. I worked with Dr. Konstantin Berlin to migrate malware feature extraction code to Amazon Web Services, which allowed production systems to scale. Also, I prototyped a multi-label deep learning model to assign malware family labels to detected threats.

Sr. Research Engineer June 2013 to August 2016
Qatar Computing Research Institute (QCRI) Doha, Qatar

My work at QCRI focused on building the cyber security research group by developing malware analysis tools, training new hires, and contributing to the group's research agenda. I worked with local stakeholders like Aljazeera News and Qatar's Ministry of Interior to align, prioritize, shape the research topics for the cyber security group.

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

My work focused on offering incident response service to fortune 50 companies spanning banks, the defense industry, consumer retail, chip manufacturers, and government agencies. I manually investigated cyber attacks, built custom tools to support automated remediation of attacks, researched new malware tactics, and documented and shared my findings with customers.

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

My work focused on malware analysis and incident response for the Department of Defense. I researched and developed offensive security tools to support our client's mission. The tools centered around covert and counterintelligence cyber tactics.

Teaching& Invited Talks

Teaching Experience

Guest Lecturer 2022
Computer Science 8803: Internet Data Science
Georgia Institute of Technology, Atlanta, Georgia

Guest Lecturer 2021
Electric and Computer Engineering 6747: Advanced Topics in Malware Analysis
Georgia Institute of Technology, Atlanta, Georgia

Guest Lecturer 2019
Electric and Computer Engineering 6612: Computer Network Security
Georgia Institute of Technology, Atlanta, Georgia

Invited Talks

A Systematic Approach for Studying Security Flaws and Threats
in Smart-Home IoT Deployments Mar, 2022
Computer Science Department
University of Maryland, College Park, Maryland

A Systematic Approach to Studying The Vulnerabilities and Threats
of Smart-Home IoT Devices Mar, 2022
Technology, Policy and Management (TPM) Labs
TU Delft, Virtual

A Systematic Approach to Studying The Vulnerabilities and Threats
of Smart-Home IoT Devices Mar, 2022
Security and Analytics Lab (SEAL)
University of Central Florida, Virtual

Security Evaluation of Home-Based IoT Deployments Feb, 2019
Messaging Mobile Malware Anti-Abuse Working Group (M3AAWG), San Francisco, CA

Security Evaluation of Home-Based IoT Deployments Nov, 2019
Institute for Information Security & Privacy (IISP) Cybersecurity Lecture Series
Georgia Institute of Technology, Atlanta, Georgia

Mentoring

Students

Morgan Mango (B.E. Georgia Tech, 2019) contributed to the automated malware analysis system, which is used by many researchers in the lab for experiments. After graduating, she joined Johns Hopkins University's Applied Physics Laboratory, in Laurel, MD, as a Cyber Security Engineer.

Sahana C (M.S. Georgia Tech, 2019) contributed to the IoT malware exploit analysis pipeline, which culminated in one publication in Usenix Security. After graduating, she joined Facebook, in Seattle, WA, as an Application Security Engineer.

Ryan Elder (M.S. Georgia Tech, 2019) contributed to a large-scale analysis of python and ruby package managers to assess the security of the software supply chain. His work culminated in a publication in NDSS. After graduating, he joined the Southwest Research Institute in San Antonio, TX, as a Research Engineer.

Nicholas Joaquin (B.E. Georgia Tech, 2020) contributed to the IoT malware analysis pipeline, which culminated in one publication in Usenix Security. After graduating, he joined Apple, in Cupertino, CA, as a CPU Top Level Verification Engineer.

Dennis Li (B.S. Georgia Tech, 2020) contributed to a systematic evaluation of public malware analysis services where the results are part of an ongoing research paper. After graduating, he joined Google, in Sunnyvale, CA, as a Software Engineer.

Kevin Valakuzhy (Ph.D. Georgia Tech, enrolled) contributed a binary emulation platform to analyze IoT malware, an in-depth binary analysis of commodity malware, and a longitudinal analysis of smart-home IoT devices. His work culminated in two publication (in Usenix Security and S&P-Oakland) and one ongoing research that is in preparation for a top tier security conference submission.

Aaron Faulkenberry (Ph.D. Georgia Tech, enrolled) contributed to longitudinal security analysis of smart-home IoT devices where the results are part of ongoing research that is in preparation for a top tier security conference submission.

Runze Zhang (Ph.D. Georgia Tech, enrolled) contributed to an analysis pipeline that aids law enforcement to rapidly identify vulnerabilities in malware communication to take down Android botnets. His work has culminated in one paper under submission.

Srimanta Barua (M.S. Georgia Tech, enrolled) contributed to malware reverse engineering and ground truth collection to evaluate malware forensic system, which has culminated in one publication in Usenix Security.

Taleb Hirani (B.E. Georgia Tech, enrolled) contributed to malware reverse engineering and ground truth collection to evaluate malware forensic system, which has culminated in one publication in Usenix Security.

Service

Conference Reviewer

Annual Computer Security Applications Conference (ACSAC)	2022
Symposium on Research in Attacks, Intrusions and Defenses (RAID)	2022

Journal Reviewer

IEEE Transactions on Dependable and Secure Computing (TDSC)	2019
IEEE Transactions on Mobile Computing (TMC)	2018, 2019, 2021
IEEE Internet of Things (IoT)	2019
ACM Transactions on Privacy and Security (TOPS)	2018, 2019
ACM Computing Surveys (CSUR)	2019, 2020, 2021
ACM Digital Threats: Research and Practice (DTRAP)	2020
Elsevier Computer Networks (COMNET)	2019

External Conference Reviewer (Total: 25 conferences, 93 papers)

ACM Conference on Computer and Communications Security (CCS)	2016, 2020
IEEE Symposium on Security and Privacy (S&P)	2018 to 2020
USENIX Security Symposium (SEC)	2017, 2021
Network and Distributed System Security Symposium (NDSS)	2017 to 2020, 2022
IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)	2019
Annual Computer Security Applications Conference (ACSAC)	2016 to 2021
International Symposium on Research in Attacks (RAID)	2018 to 2020

Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)	2019
Symposium on Electronic Crime Research (eCrime)	2018
European Workshop on Systems Security (EuroSec)	2019
European Symposium on Research in Computer Security (ESORICS)	2016

Community Outreach

High-School Physics Teacher (associated with Ilm Academy) 2019-2020

Volunteered to teach physics to home-schooled high-school students through Georgia's Connections Academy program. I adapted the class curriculum for in-person and online teaching to accommodate for the onset of the COVID19 pandemic.

Select Media Coverage

Full list available on my website

We're Surrounded by Billions of Internet-connected Devices. Can We Trust Them?
Newsweek, 10/24/19

Amazon Sidewalk Will Share Your Internet With Strangers. It's Not As Scary As It Sounds.
New York Times - The Wirecutter, 06/7/21

The Best Smart LED Light Bulbs
New York Times - The Wirecutter, 08/10/21

Learn how (in)secure your IoT devices are with YourThings scorecards
TechRepublic, 09/4/19

Cloud-based app backends - a rat's nest of mobile phone security vulnerabilities
diginomica, 08/19/19

New Tool Reveals Big Vulnerabilities In Mobile Apps That Use Multiple Clouds
Defense One, 08/13/19

Patents

Systems and Methods for Behavior-based Automated Malware Analysis and Classification 2017
US Patent 9,769,189