Omar Alrawi

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

Research Interests

My research interest lies in studying and improving software security through a principled and informed approach. Specifically, I design research methods informed by system and network data measurements to assess the security of open-source software and binary programs. My holistic approach combines vulnerability analysis and malware analysis to improve the security of deployed systems at scale.

Education

Ph.D. Electrical and Computer Engineering May 2023
Georgia Institute of Technology Atlanta, GA
Dissertation: *A Systematic Approach to Prioritize Vulnerabilities in IoT Deployments*
Advisors: Dr. Manos Antonakakis and Dr. Fabian Monrose

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. Runze Zhang, Mingxuan Yao, Haichuan Xu, **Omar Alrawi**, Jeman Park, Brendan Saltaformaggio; Hitchhiking Vaccine: Enhancing Botnet Remediation With Remote Code Deployment Reuse. In *The Network and Distributed System Security Symposium (NDSS)*, 2025. (Acceptance rate: 16%).
2. Eman Maali, **Omar Alrawi**, Julie McCann; Evaluating Machine Learning-Based IoT Device Identification Models for Security Applications. In *The Network and Distributed System Security Symposium (NDSS)*, 2025. (Acceptance rate: 16%).
3. Yufei Du, **Omar Alrawi**, Kevin Snow, Manos Antonakakis, Fabian Monrose; Improving Security Tasks Using Compiler Provenance Information Recovered At the Binary-Level. In *The ACM Conference on Computer and Communications Security (ACM CCS)*, 2023. (Acceptance rate: 19%).
4. **Omar Alrawi***, Athanasios Avgetidis*, Kevin Valakuzhy, Charles Lever, Paul Burbage, Angelos Keromytis, Fabian Monrose, Manos Antonakakis; Beyond The Gates: An Empirical Analysis of HTTP-Managed Password Stealers and Operators. *In USENIX Security (SEC)*, 2023. (Acceptance rate: 28%).
5. Aaron Faulkenberry, Athanasios Avgetidis, Zane Ma, **Omar Alrawi**, Charles Lever, Panagiotis Kintis, Fabian Monrose, Angelos Keromytis, Manos Antonakakis; View from Above: Exploring the Malware Ecosystem from Upper DNS Hierarchy. In *The Annual Computer Security Applications Conference (ACSAC)*, 2022. (Acceptance rate: 24.1%).
6. Priyanka Dodia, Mashael Al Sabah, **Omar Alrawi**, Tao Wang; Exposing the Rat in the Tunnel: Using Traffic Analysis for Tor-based Malware Detection. In *The ACM Conference on Computer and Communications Security (ACM CCS)*, 2022. (Acceptance rate: 18%).
7. **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).
8. **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).
9. 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).
10. 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).
11. 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).

12. **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).
13. **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).
14. 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).
15. **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.
16. Aziz Mohaisen, **Omar Alrawi**. Behavior-based Automated Malware Analysis and Classification. In *Elsevier Computers & Security*. 2015.
17. 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.
18. Aziz Mohaisen, **Omar Alrawi**. AMAL: High-Fidelity, Behavior-based Automated Malware Analysis and Classification. In *Workshop on Information Security Applications (WISA)*. 2014.
19. 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).
20. 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.
21. 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.
22. Aziz Mohaisen, **Omar Alrawi**. Unveiling Zeus Automated Classification of Malware Samples. In *Workshop on Simplifying Complex Networks for Practitioners co-located with WWW*. 2013.

Grants & Proposals

GTRI IRAD (Phase 2) - PI amount: $40,000

Grant to support Cyber Analytic Network for Attribution & Reconnaissance Yield (CANARY) project. CANARY revolutionizes traditional malware sandboxes by combining enhanced tracking capabilities to identify malware operator relationships.

GTRI IRAD (Phase 1) - PI amount: $25,000

Grant to support Cyber Analytic Network for Attribution & Reconnaissance Yield (CANARY) project. CANARY revolutionizes traditional malware sandboxes by combining enhanced tracking capabilities to identify malware operator relationships.

Aspiring PI Workshop amount: Travel Grant
Grant to support two day workshop at the University of Chicago focusing on NSF proposal writing. The workshop guides participant through NSF funding tracks and educates junior faculty on correctly framing their research initiative.

Signature Management using Operational
Knowledge and Environments - Co-PI amount: $22,600,000
Grant to support the development of data-driven tools to automate the planning and execution of threat-emulated cyber infrastructure needed for network security assessments like red team exercises.

Research & Professional Experience

Senior Research Scientist August 2022
Research Faculty - Georgia Tech Atlanta, GA
I am the research director of the Center for Cyber Operations Enquiry and Unconventional Sensing (COEUS). My role involves managing an $18 million DARPA project for the center. I am responsible for integrating with external performers, designing and overseeing the implementation of a large-scale cybersecurity testbed, and advising students on their research. I am also involved in writing proposals for additional grants and conducting community service for security conferences, workshops, and journals. I plan to teach computer science and security courses in the upcoming term.

Research Assistant August 2016 to July 2022
Georgia Tech Atlanta, GA
My Ph.D. research under my advisors Professor Manos Antonakakis and Fabian Monrose 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 January 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 December 2010
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.

Service

Organizing Committees

Co-Chair of IoT Security and Cyber Threat Intelligence (IoT SCTI)	2023
Co-Chair of Workshop on AI and Threat Intelligence (WAITI)	2024
Co-Chair of Annual Computer Security Applications Conference (ACSAC) Workshop	2024
Co-Chair of IEEE Conference on Communications and Network Security (CNS) Poster	2023

Conference Reviewer

Annual Computer Security Applications Conference (ACSAC)	2022, 2023, 2024
Symposium on Research in Attacks, Intrusions and Defenses (RAID)	2022, 2023, 2024
The Web Conference (WWW)	2024, 2025
ACM Workshop on Secure and Trustworthy Superapps (SaTS)	2023, 2024
NDSS Workshop on Security and Privacy in Standardized IoT (SDIoTSec)	2024

Journal Reviewer

IEEE Transactions on Information Forensics and Security (TIFS)	2023
IEEE Transactions on Dependable and Secure Computing (TDSC)	2019, 2023, 2024
IEEE Transactions on Mobile Computing (TMC)	2018, 2019, 2021, 2022
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

Board of Governance for ILM Academy (Primary and Secondary Private School)	2023 to present
Georgia Tech K-12 InVenture Prize Judge	2023

Volunteer as a judge for students from schools across Georgia to present their ideas for early feedback.

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
Anker's Eufy lied to us about the security of its security cameras
The Verge, 11/30/22

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

Teaching& Invited Talks

Teaching Experience
Instructional Assistant 2023
Electrical and Computer Engineering 8803: Advanced Computer Security
Georgia Institute of Technology, Atlanta, Georgia

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

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

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

Invited Talks
Security Evaluation of IoT Deployments May, 2024
Computer Science Department
DePaul University, Chicago, Illinois

Security Evaluation of IoT Deployments Feb, 2024

Computer Science Department
Spelman College, Atlanta, Georgia

Security Evaluation of IoT Deployments Feb, 2024
Computer Science Department
University of Georgia, Athens, Georgia

Security Evaluation of IoT Deployments Feb, 2024
Computer Science Department
Georgia State University, Atlanta, Georgia

Security Evaluations of Smart-Home IoT Deployments Sep, 2023
Computer Science Department
Emory University, Atlanta, Georgia

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

Advising & Mentoring

Advised Students

Allen Chang (BS Georgia Tech, enrolled) contributed a novel measurement approach to map out threat intelligence sharing between security vendors, threat intelligence platforms, and security analysis portals. His ongoing research is in preparation for a top-tier security conference submission.

Brian Teachout (MS Georgia Tech, enrolled) contributed a comprehensive measurement study to characterize internet outages' impact on IoT infrastructure. His ongoing research is in preparation for a top-tier security conference submission.

Vinny Adjibi (Ph.D. Georgia Tech, enrolled) contributed a novel approach that quantifies domain registration quality of brand protection services for Fortune 500 companies where the results are part of ongoing research that is in preparation for a top-tier security conference submission.

Yufei Du (Ph.D. Georgia Tech, enrolled) contributed a novel compiler provenance framework to identify which compiler optimizations induce security bugs. His work culminated in one publication (in ACM CCS) and one ongoing research in preparation for a top-tier security conference submission.

Eman Maali (Ph.D. Imperial College London, enrolled) contributed a systematic framework to assess and compare IoT device identification techniques for practical use in large networks. Her ongoing research is in preparation for a top-tier security conference submission.

Xinye Zhao (Ph.D. Georgia Tech, enrolled) contributed a systematic network behavior profiling framework to understand and predict IoT network traffic pattern evolution. His ongoing research is in preparation for a top-tier security conference submission.

Kevin Valakuzhy (Ph.D. Georgia Tech, enrolled) contributed a binary emulation platform to analyze IoT malware and an in-depth binary analysis of commodity malware. His work culminated in two publications (in Usenix Security) and one ongoing research in preparation for a top-tier security conference submission.

Aaron Faulkenberry (Ph.D. Georgia Tech, enrolled) contributed methods and experiments to study internet surveillance where the results are part of ongoing research that is in preparation for a top-tier security conference submission.

Thanos Avgetidis (Ph.D. Georgia Tech, enrolled) contributed a comprehensive study of malware operators and their business affiliations to understand the tactics and techniques of malicious actors. His work culminated in one publication (in Usenix Security) and one ongoing research in preparation for a top-tier security conference submission.

Mentored Students

Srimanta Barua (M.S. Georgia Tech, 2022) 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, 2022) contributed to malware reverse engineering and ground truth collection to evaluate malware forensic system, which has culminated in one publication in Usenix Security.

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.

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.

Patents

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

Forecasting Malware Capabilities From Cyber Attack Memory Images 2022
Filed Patent

References

Professor Manos Antonakakis
Georgia Institute of Technology
School of Electrical and Computer Engineering
North Ave NW
Atlanta, GA 30332
404-385-2534
manos@gatech.edu

Professor Angelos Keromytis
Georgia Institute of Technology
School of Electrical and Computer Engineering
North Ave NW
Atlanta, GA 30332
404-894-5177
angelos@gatech.edu

Professor Roberto Perdisci
University of Georgia
School of Computing
Athens, GA 30602
(706) 542-3482
perdisci@uga.edu

Professor Fabian Monrose
Georgia Institute of Technology
School of Electrical and Computer Engineering
North Ave NW
Atlanta, GA 30332
fabian@ece.gatech.edu

Professor Mustaque Ahamad
Georgia Institute of Technology
College of Computing
North Ave NW
Atlanta, GA 30332
404-894-2593
mustaq@cc.gatech.edu