Jonathan Fuller

Georgia Institute of Technology
Atlanta, GA 30332
✉ fullerj@gatech.edu
fullerj.github.io

Research Interests

Cyber forensics and systems security with a focus on malware analysis, large-scale security measurement, binary program instrumentation, and mobile/IoT security.

Education

Ph.D. in Electrical and Computer Engineering — Fall 2019 - Present
Georgia Institute of Technology — Atlanta, GA
Cyber Forensics Innovation Laboratory
Advisor: Dr. Brendan Saltaformaggio

Master of Science in Computer Science — 2016
Air Force Institute of Technology — Dayton, OH
Thesis: *A Misuse-Based Intrusion Detection System for ITU-T G.9959 Wireless Networks*
Advisor: Dr. Benjamin Ramsey

Bachelors of Science in Computer Science — 2007
University of Alabama at Birmingham — Birmingham, AL

Honors & Awards

Advanced Civil Schooling Fellowship — 2014-2016, 2019-2022
The Advanced Civil Schooling Fellowship is a highly competitive and funds select Army Officers who have demonstrated exceptional performance as well as scholastic achievement to pursue graduate education on a full-time basis.

Publications

Peer-Reviewed Articles

J. Fuller, B. Ramsey, M. Rice, and J. Pecarina, "Misuse-based Detection of Z-Wave Network Attacks," *Computers & Security*, 64, pp. 44-58, 2017.

B. Ramsey, **J. Fuller**, and C. Badenhop, "Efficacy of Physical Layer Preamble Manipulation for IEEE 802.11 a/ac," *IEEE Electronic Letters*, 52(8), pp 669-671, 2016.

C. Badenhop, **J. Fuller**, J. Hall, B. Ramsey, and M. Rice, "Evaluating ITU-T G.9959 based Wireless Systems used in Critical Infrastructure," in *Critical Infrastructure Protection IX*, S. Shenoi and M. Rice, Eds, Heidelberg, Germany: Springer, 466, pp. 209-227, 2015.

J. Fuller and B. Ramsey, "Rogue Z-Wave Controllers: A Persistent Attack Channel," *10^{th} IEEE International Workshop on Practical Issues in Building Sensor Network Applications (SenseAPP)*, pp 734-741, 2015.

J. Fuller, B. Ramsey, J. Pecarina, and M. Rice, "Wireless Intrusion Detection of Covert Channel Attacks in ITU-T G.9959-based Networks," *11^{th} International Conference on Cyber Warfare and Security (ICCWS)*, pp 137-145, 2015.

Presentations

J. Fuller and B. Ramsey, "Stealthy and Persistent Access to Z-Wave Gateways," *DerbyCon 5.0 "Unity"*, Louisville, KY, 2015.

Thesis

J. Fuller. A Misuse-Based Intrusion Detection System for ITU-T G.9959 Wireless Networks. In *The Air Force Intitute of Technology Theses and Dissertations*, 2016.

Relevant Coursework

Advanced Malware Analysis, Reverse Engineering, Secure Computer Systems, Network Security, Advanced Programming Techniques, Advanced Algorithm Design, Mobile Device and SCADA Security, Advanced Topics in Computer Networks.

Professional Certifications

Certified Information System Security Professional Active

The CISSP designation is a globally recognized standard attesting to an IT security professional's technical skills and hands-on experience implementing and managing a security program.

Research Experience

Graduate Research Assistant Fall 2019 - Present

Georgia Institute of Technology Atlanta, GA

Under the guidance of Dr. Brendan Saltaformaggio, my research focuses on preventing malware from accurately performing reconnaissance by using program analysis techniques and reverse engineering. This approach aims to dissect malicious software toward automated detection and identification of their operational capabilities while subverting data gathering to enable active response deception.

Professional Experience

United States Army Officer Dec 2007 - Present

I have served in various leadership positions in the United States Army spanning three career field designations. I began as an Armor Officer where I led a reconnaissance platoon during combat operations. I next served as a Communications Officer managing tactical communications for special operations forces. Most recently, I specialized as a Network Systems Engineer where I am responsible for planning, designing, engineering, implementing, operating, and securing Army and DoD information networks and services.

Service

External Reviewer (Total = 12)

USENIX Security Symposium	2021
IEEE Symposium on Security and Privacy (S&P)	2021
Network and Distributed System Security Symposium (NDSS)	2020-2021
ACM Conference on Computer and Communications Security (CCS)	2020
IEEE European Symposium on Security and Privacy (Euro S&P)	2020-2021
ACM ASIA CCS (AsiaCCS)	2021
Annual Computer Security Applications Conference (ACSAC)	2020
Research in Attacks, Intrusions and Defense (RAID)	2020
The Web Conference (formerly WWW)	2020
Computers & Security Journal (COSE)	2019