Brown R. Farinholt

CONTACT INFORMATION

Department of Computer Science and Engineering
University of California, San Diego
9500 Gilman Drive, Mail Code 0404
La Jolla, CA 92093-0404 USA

Voice: (804) 814-9556
Email: bfarinho@cs.ucsd.edu
Web: https://cseweb.ucsd.edu/~bfarinho/

EDUCATION

University of California, San Diego, La Jolla, California USA

Ph.D., Computer Science, expected 2019
M.S., Computer Science, 2015

Clemson University, Clemson, South Carolina USA

B.S., Computer Engineering, 2013

ACADEMIC EXPERIENCE

University of California, San Diego, La Jolla, California USA

Malware Research **June, 2014 - present**
Advisor: Kirill Levchenko. Analyze remote access trojan (RAT) malware and associated operator behavior and criminal activity. Reverse engineer RAT C&C protocols, conduct distributed Internet-wide scans for controllers, and sinkhole infections. Operate a system that perpetually downloads and dynamically analyzes manually-operated malware, constructing behavioral profiles of malicious actors from API logs and network traces.

Avionics & IoT Security Research **August, 2013 - present**
Advisors: Stefan Savage, Kirill Levchenko. Work on security topics related to consumer and commercial avionics. Monitor and analyze ACARS and ADS-B traffic. Conducted security analysis of consumer-grade IoT ADS-B receivers, forced malicious firmware updates and developed traffic-spoofing iOS and Android applications. (Aerosec research site: http://aerosec.org)

Industrial Control Systems Security Research **August, 2014 - December, 2015**
Advisor: Kirill Levchenko. Monitored and processed DNP3 microwave traffic from power grid SCADA devices to develop a method of passive grid device identification. Presented an analysis of state-of-the-art computer-based attacks on components of the U.S. power grid for Master's thesis.

Clemson University, Clemson, South Carolina USA

Undergraduate Researcher, Internet Democracy Project **August, 2012 - June, 2013**
Advisor: Richard Brooks. Developed a system for reporters in oppressive countries to anonymously and securely access the Internet. Mimicked botnet behavior, DNS tunneling, fast flux.

Developer, Cloud-based Smartphone Application Project **August, 2011 - January, 2012**
Advisor: Helen Shen. Developed a smartphone application using Microsoft Azure cloud-computing for Project Hawaii: http://research.microsoft.com/en-us/projects/hawaii/fall2011.aspx

PUBLICATIONS

Brown Farinholt, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharmdasani, Haikuo Yin, Stevens LeBlond, Damon McCoy, Kirill Levchenko. *To Catch a Ratter: Monitoring the Behavior of DarkComet RAT Operators in the Wild.* In *Proceedings of the 38th IEEE Symposium on Security and Privacy (Oakland 2017)*, San Jose, California, May 2017.

Devin Lundberg, Brown Farinholt, Edward Sullivan, Ryan Mast, Stephen Checkoway, Stefan Savage, Alex C. Snoeren, Kirill Levchenko. *On The Security of Mobile Cockpit Information Systems.* In *Proceedings of the ACM Conference on Computer and Communications Security (CCS 2014)*, Scottsdale, Arizona, November 2014.

Relevant Classes

CSE 227: *Computer Security*
Project: Reverse engineered the firmware update process of a popular, consumer-grade ADS-B receiver. Built Android application to push malicious updates to legitimate devices.

CSE 222A: *Computer & Communication Networks*
Project: Built and deployed Internet-wide scanner for IPSec services. Evaluated chosen key lengths/cipher suites, found several device populations not adherent to NIST security recommendations.

CSE 221: *Operating Systems*

Professional Experience

QTS Data Centers, Dulles, VA USA

Security Engineering Intern **June, 2016 - October, 2016**
Evaluated and oversaw the test deployment of Bromium Endpoint Protection to select company devices. Presented findings and recommendations to company staff and leadership. Began implementing visualization platform for IDS logs to be made available to customers.

Shockoe Mobile App Development, Richmond, VA USA

Developer **June, 2013 - September, 2013**
Developed mobile applications for Android and iOS devices using Appcelerator's Titanium Mobile Development Environment. Worked on a small team of developers, met demanding deadlines, and gained experience in graphical design and user interfacing.

Federal Reserve Information Technology, Richmond, VA USA

Information Technology Intern **May, 2012 - August, 2012**
Developed tools using Excel and VBA that expedited compilation, reformatting, and analysis of large amounts of data pertaining to application development. Produced metrics simplifying the application design lifecycle for improvement. Redesigned and implemented department website.

Federal Reserve Bank of Richmond, Richmond, VA USA

Currency Technology Office Engineering Intern **May, 2011 - August, 2011**
Researched and produced a whitepaper on design structure matrices, and applied my findings successfully to two major, long-term Fed projects. Worked with design engineers to improve the efficiency of certain supply chain distribution networks, focusing on complex feedback loops.

Honors and Awards

National Scholars Program (Full Scholarship), Clemson University	2009 - 2013
Graduated Magna Cum Laude with General & Departmental Honors, Clemson	2013
President's List, Clemson	2009 - 2013
Rhodes Most Outstanding Junior in Computer Engineering Award, Clemson	2012
National Merit Scholarship, National A.P. Scholarship	2009

Affiliations and Leadership

Rady School of Business Micro-MBA Program, UCSD	2014
Athletic Department Tutoring & Mentoring Program, Clemson	2010 - 2013
College Reading & Learning Association Tutor Certification Levels I-II	2013
Captain, CCDC Security Team, Clemson	2013
Order of Omega Greek Honor Society, Clemson	2012 - 2013
Secretary, Tau Beta Pi Engineering Honor Society, Clemson	2010 - 2013
Student Government Research & Development Committee, Clemson	2011 - 2012
WSBF Radio Station Website Redesign Committee, Clemson	2012