

Miguel A. Arroyo

✉ miguel@arroyo.me | 🏠 miguel.arroyo.me | 📷 mayanez | 🌐 maarroyo12



Education

Columbia University

PH.D IN COMPUTER SCIENCE

Dissertation: Bespoke Security for Resource Constrained Cyber-Physical Systems

Advisor: Prof. Simha Sethumadhavan

New York, NY

2016-PRESENT

M.PHIL IN COMPUTER SCIENCE

2016-2018

M.S. IN COMPUTER ENGINEERING

2014-2015

B.S. IN COMPUTER ENGINEERING

2009-2013

Publications

Practical Byte-Granular Memory Blacklisting using Califorms

IEEE/ACM INTERNATIONAL SYMPOSIUM ON MICROARCHITECTURE (MICRO) - IEEE MICRO TOP PICKS HONORABLE MENTION

Hiroshi Sasaki, Miguel A. Arroyo, M. Tarek Ibn Ziad, Koustubha Bhat, Kanad Sinha, Simha Sethumadhavan

Columbus, OH

2019

YOLO: Frequently Resetting Cyber-Physical Systems for Security

SPIE DEFENSE AND COMMERCIAL SENSING

Miguel A. Arroyo, M. Tarek Ibn Ziad, Hidenori Kobayashi, Junfeng Yang, Simha Sethumadhavan

Baltimore, MD

2019

Pre-Print Publications

SPAM: Stateless Permutation of Application Memory

ARXIV 2007.13808

M. Tarek Ibn Ziad & Miguel A. Arroyo, Simha Sethumadhavan

2020

Using Name Confusion to Enhance Security

ARXIV 1911.02038

M. Tarek Ibn Ziad, Miguel A. Arroyo, Evgeny Manzhosov, Vasileios P. Kemerlis, Simha Sethumadhavan

2020

Experience

Columbia Computer Architecture and Security Technology Lab (CASTL)

RESEARCH ASSISTANT

- Designed & implemented a comprehensive memory corruption defense as a LLVM/Clang compiler pass and run-time library that permutes application memory by instrumenting loads and stores which protects against software and hardware threats.
- Proposed a new architectural primitive, called Name Confusion, implemented in gem5 and supported by a custom LLVM toolchain, which provides N-variant execution for control-flow protection at near zero cost.
- Explored program behavior using the LLVM compiler framework and binary instrumentation tools (eg. PIN, DynamoRIO) to guide the design of a cache formatting scheme called *Califorms* to provide memory safety.
- Designed & implemented *YOLO*, a novel security defense leveraging inertia, using a combination of C/C++ and assembly at the real-time operating system (RTOS) level to provide resilient operation for CPS microcontrollers (eg. ARM Cortex-M series).

New York, NY

Aug. 2015 - PRESENT

Intel

GRADUATE INTERN

- Performed headroom studies to aid the design of experimental hardware optimizations targeting multiple JIT engines (eg. Javascript V8, Java HotSpot) by instrumenting JIT engine source code to collect dynamic profile data using Intel PIN.
- Investigated performance tradeoffs of various GPGPU programming languages (eg. OpenCL, SYCL, CUDA, CM) on Intel iGPUs to compare benefits of explicit vs implicit SIMD programming paradigms.

Santa Clara, CA

May 2019 - Aug. 2019

Ardupilot (Google Summer of Code)

DEVELOPER

- Worked with Ardupilot, an autonomous vehicle autopilot firmware, on designing & implementing an efficient low-latency (in the order of a few μs) protocol to manage transport of sensor data for various vehicle types.
- Extended low-level drivers and OS internals (in C++) for an ARM Cortex-M series microcontroller to integrate and process sensor data for load-balancing tasks in coordination with the main flight controller (ARM Cortex-A) improving battery usage and overall compute performance.

New York, NY

May 2017 - Aug. 2017

Amazon

SOFTWARE DEVELOPER ENGINEER

- Developed market specific features for the *checkout* and *detail* pages for India (amazon.in) marketplace.
- Architected and implemented Amazon Business Wholesale India (amazonbusiness.in) business management backend systems using Java & Spring involving the design of appropriate DB schemas (in Amazon RDS) & infrastructure organization (in AWS) to accommodate for large traffic volume.
- Designed infrastructure routing framework and migration for Quidsi platform using Java, Spring, & AWS.

Seattle, WA

Jul. 2013 - Jan. 2015

SOFTWARE DEVELOPER ENGINEER INTERN

- Implemented a performance metric monitoring system on FireOS (Kindle Android variant) using Java & Hadoop that allowed for development of key performance enhancements for Kindle FreeTime within FireOS.

Jun. 2012 - Aug. 2012

Columbia Intrusion Detection Systems Lab

RESEARCH ASSISTANT

- Found vulnerabilities in embedded system firmware from devices such as Cisco routers, VoIP phones, and firewalls using reverse engineering tools such as IDA Pro.
- Built database for processing and vetting firmware images for vulnerabilities using Python & MongoDB.

New York, NY
Aug. 2012 - May 2013

International Physics Olympiad (IPhO)

TEAM LEADER

- Selected after a series of examinations to represent Puerto Rico at the International Physics Olympiad 2008, a competition that tests general physics knowledge.
- Competed at IPhO 2008 in Vietnam.

Hanoi, Vietnam
Jul. 2008

U.S. Department of Energy National Science Bowl

CO-CAPTAIN

- Represented Saint John's School in Condado, PR at regional and statewide rounds.
- Acted as the team's spokesperson and solved issues in the event of disputes over questions during the competition.
- Trained in solving Physics and Chemistry questions of the competition.
- Won regional & statewide rounds and competed in National rounds in Washington D.C.

Washington, D.C.
Apr. 2008 - May 2008

Teaching Experience

Instructor

OXBRIDGE ACADEMIC PROGRAMS

- Designed a curriculum for Oxbridge's New York College Experience program Computer Science course of 15 high-school students.

New York, NY
Jun. 2016 - Aug. 2016

Teaching Assistant

SECURITY I (COMS W4181)
COMPUTER ARCHITECTURE (CSEE 4824)
INTRO TO PYTHON (ENGI E1006)
INTRO TO CS IN JAVA (COMS W1004)

New York, NY
Sep. 2018 - Dec. 2018
Jan. 2018 - May 2018
Jan. 2015 - May 2015
Aug. 2012 - May 2013

Talks & Outreach

SPAM: Stateless Permutation of Application Memory with LLVM

LLVM DEVELOPERS' CONFERENCE

Virtual, AoE
Oct 2020

A Look at Memory Safety

SILICON VALLEY CYBER SECURITY MEETUP

Virtual, AoE
May 2020

YOLO: Frequently Resetting Cyber-Physical Systems for Security

WORKSHOP ON THE DESIGN AND ANALYSIS OF ROBUST SYSTEMS (DARS)

New York, NY
Jul. 2019

Go Go Gadget! An Introduction to Return Oriented Programming

SILICON VALLEY CYBER SECURITY MEETUP

Santa Clara, CA
Apr. 2019

WACI: How to Make Driving Awesome

ACM ARCHITECTURAL SUPPORT FOR PROGRAMMING LANGUAGES AND OPERATING SYSTEMS (ASPLOS)

Williamsburg, VA
Mar. 2018

Skills

SOFTWARE DEVELOPMENT

C/C++ · Python · Assembly (x86,ARM) · Java · Go · Lua · Lisp · LaTeX | Clang+LLVM · Docker · Git · CMake/Make · GDB

FOREIGN LANGUAGES

Spanish (Native) · French (Advanced) · Japanese (Intermediate)

Honors & Awards

- IEEE Micro Top Picks from 2019 Computer Architecture Conferences honorable mention
- RSAC Security Scholar 2017
- Columbia SEAS Translational Fellowship 2017 (one of three)

Academic Service

Reviewer, IEEE Symposium on Security and Privacy

2018, 2021

Reviewer, Communications of the ACM

2020

Reviewer, IEEE Design & Test

2019

Patents

Methods & Systems for Fine Granularity Memory Blacklisting to Detect Memory Access Violations

US16744922

2019

Hiroshi Sasaki, Miguel A. Arroyo, M. Tarek Ibn Ziad, Simha Sethumadhavan

Control Flow Protection Based on Phantom Addressing

US62904887

2019

M. Tarek Ibn Ziad, Miguel A. Arroyo, Evgeny Manzhosov, Simha Sethumadhavan

Secured Cyber-Physical Systems

US10417425

2016

Miguel A. Arroyo, Simha Sethumadhavan, Jonathan Weisz