Miguel A. Arroyo

(929) 340 - 8117 | miguel@arroyo.me | miguel.arroyo.me | mayanez | mayanez

Education

Columbia University — *New York, NY*

PH.D IN COMPUTER SCIENCE — *PRESENT*

M.PHIL IN COMPUTER SCIENCE — *2016-2018*

M.S. IN COMPUTER ENGINEERING — *2014-2015*

B.S. IN COMPUTER ENGINEERING — *2009-2013*

Skills

SOFTWARE DEVELOPMENT

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

FOREIGN LANGUAGES

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

Publications

Using Name Confusion to Enhance Security

ARXIV PRE-PRINT — *2020*

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

Practical Byte-Granular Memory Blacklisting using Califorms — *Columbus, OH*

IEEE/ACM INTERNATIONAL SYMPOSIUM ON MICROARCHITECTURE (MICRO) - **IEEE MICRO TOP PICKS HONORABLE MENTION** — *2019*

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

YOLO: Frequently Resetting Cyber-Physical Systems for Security — *Baltimore, MD*

SPIE DEFENSE AND COMMERCIAL SENSING — *2019*

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

Experience

Columbia Computer Architecture and Security Technology Lab (CASTL) — *New York, NY*

RESEARCH ASSISTANT — *Aug. 2015 - PRESENT*

- Designed & implemented a comprehensive memory safety defense as a LLVM/Clang compiler pass and runtime library that permutes program data by instrumenting loads and stores.
- Proposed a new architectural primitive, named the Phantom Address Space, implemented in gem5 and supported by a custom LLVM toolchain, which provides N-variant execution at near zero cost.
- Explored program behavior using the LLVM compiler framework and binary instrumentation tools to guide the design of a cache formatting scheme called Califorms to enhance security.
- 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).

Intel — *Santa Clara, CA*

GRADUATE INTERN — *May 2019 - Aug. 2019*

- Performed headroom studies for experimental hardware optimizations targeting multiple JIT engines (eg. Javascript V8, Java HotSpot). Instrumented 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.

Ardupilot (Google Summer of Code) — *New York, NY*

DEVELOPER — *May 2017 - Aug. 2017*

- Worked with Ardupilot, an autonomous vehicle autopilot firmware, on designing & implementing an efficient low-latency (in the order of a few microseconds) protocol to manage transport of sensor data for various vehicle types. [`https://goo.gl/ecHqSk`]
- 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.

Amazon
Seattle, WA

Software Developer Engineer — *Jul. 2013 - Jan. 2015*

- 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 accomodate for large traffic volume.
- Designed infrastructure routing framework and migration for Quidsi platform using Java, Spring, & AWS.

Software Developer Engineer Intern — *Jun. 2012 - Aug. 2012*

- 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.

Columbia Intrusion Detection Systems Lab
New York, NY

Research Assistant — *Aug. 2012 - May 2013*

- Found vulnerabilities in embedded system firmware from devices such as Cisco routers, VoIP phones, and firewalls using reverse engineering tools such as IDA Pro. [`http://youtu.be/f3zUOZcewtA`]
- Built database for processing and vetting firmware images for vulnerabilities using Python & MongoDB.

International Physics Olympiad (IPhO)
Hanoi, Vietnam

Team Leader — *Jul. 2008*

- Selected after a series of examinations to represent Puerto Rico at the International Physics Olympiad 2008, a competition that tests general physics knowledge.
- Attended one month training at Recinto Universitario de Mayaguez to prepare for competition.
- Competed at IPhO 2008 in Vietnam.

U.S. Department of Energy National Science Bowl
Washington, D.C.

Co-Captain — *Apr. 2008 - May 2008*

- 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.

Awards

2017 **Scholar,** RSAC Security Scholar — *San Francisco, CA*

A nomination-based program for cybersecurity students to present their research to leading-experts at the RSA Conference.

2017 **Fellow,** Columbia SEAS Translational Fellowship — *New York, NY*

A competitive program that provides funding and mentorship to pursue commercialization of a technology originating from research.

Talks

YOLO: Frequently Reseting Cyber-Physical Systems for Security
New York, NY

Workshop on the Design and Analysis of Robust Systems (DARS) — *Jul. 2019*

WACI: How To Make Driving Awesome
Williamsburg, VA

ACM Architectural Support for Programming Languages and Operating Systems (ASPLOS) — *Mar. 2018*

Writing

A Computer Architecture Solution to Fake News and Autonomous Car Accidents

ACM SIGGARCH — *Jun. 2018*

`https://goo.gl/jp8zGQ`

Patents

Cache Line Formats for Fine-Grained Memory Safety

Pending — *2019*

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

Secured Cyber-Physical Systems

US10417425 — *2016*

Miguel A. Arroyo, Simha Sethumadhavan, Jonathan Weisz