Miguel A. **Arroyo**

miguel@arroyo.me | miguel.arroyo.me | mayanez | maarroyo12

Education

Columbia University *New York, NY*
Ph.D in Computer Science *2016-2020*
Dissertation: Bespoke Security for Resource Constrained Cyber-Physical Systems
Advisor: Prof. Simha Sethumadhavan

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 *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

Pre-Print Publications

SPAM: Stateless Permutation of Application Memory
arXiv 2007.13808 *2020*
M. Tarek Ibn Ziad & *Miguel A. Arroyo*, Simha Sethumadhavan

Using Name Confusion to Enhance Security
arXiv 1911.02038 *2020*
M. Tarek Ibn Ziad, *Miguel A. Arroyo*, Evgeny Manzhosov, Vasileios P. Kemerlis, Simha Sethumadhavan

Experience

Rockstar Games *Carlsbad, CA*
Game Security Engineer *Dec. 2020 - PRESENT*

- Support all Rockstar titles including Grand Theft Auto V and Red Dead Redemption from malicious actors and insider threats.
- Research and implement various forms of anti-tamper technologies and/or DRM.
- Proactively research unknown vulnerabilities in our products and implement appropriate mitigations.
- Reverse engineer software intended to compromise online gaming environments.

Columbia Computer Architecture and Security Technology Lab (CASTL) *New York, NY*
Research Assistant *Aug. 2015 - Dec. 2020*

- 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).

Intel *Santa Clara, CA*
Graduate Intern *May 2019 - Aug. 2019*

- 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.

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 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.

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.
- 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.
- 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.

Teaching Experience

Instructor *New York, NY*

Oxbridge Academic Programs *Jun. 2016 - Aug. 2016*

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

Teaching Assistant *New York, NY*

Security I (COMS W4181) *Sep. 2018 - Dec. 2018*
Computer Architecture (CSEE 4824) *Jan. 2018 - May 2018*
Intro to Python (ENGI E1006) *Jan. 2015 - May 2015*
Intro to CS in Java (COMS W1004) *Aug. 2012 - May 2013*

Academic Service

Reviewer, IEEE Symposium on Security and Privacy *2018, 2021*
Reviewer, Communications of the ACM *2020*
Reviewer, IEEE Design & Test *2019*

Talks & Outreach

SPAM: Stateless Permutation of Application Memory with LLVM *Virtual, AoE*

LLVM Developers' Conference *Oct 2020*

A Look at Memory Safety *Virtual, AoE*

Silicon Valley Cyber Security Meetup *May 2020*

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

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

Go Go Gadget! An Introduction to Return Oriented Programming *Santa Clara, CA*

Silicon Valley Cyber Security Meetup *Apr. 2019*

WACI: How to Make Driving Awesome *Williamsburg, VA*

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

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)

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)

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