Alejandro Cuevas

https://github.com/aledcuevas

Education

- **The Pennsylvania State University - Schreyer Honors College** — University Park, PA
  Bachelor of Science with Honors in Security and Risk Analysis - Cum Laude — *Jun. 2014 – May 2018*

Experience

- **Stevens Institute of Technology: Department of Computer Science** — Hoboken, NJ
  Visiting Scholar - Hosted by Prof. Jun Xu — *Fall 2018*
  - Worked on a selective tainting technique for high-performance kernel protection (*under submission*) and evaluating the performance of ensembling machine learning defense techniques *(to be submitted).*
- **EPFL: Laboratory for Communication and Applications** — Lausanne, Switzerland
  Software Engineer - Supervised by Prof. Jean-Pierre Hubaux — *Spring 2018 - Fall 2018*
  - Leading the implementation of "PriFi" as a VPN on mobile platforms (iOS & Android).
- **The Pennsylvania State University: LIONS Center** — University Park, PA
  Research Assistant - Advised by Profs. Peng Liu, Xinyu Xing, and Dinghao Wu — *Spring 2016 - Spring 2018*
  - Researched security metrics for moving-target defenses, challenges associated with reproduction of vulnerabilities (*published*), a deep learning approach to improve value-set analysis, and the impact of fake vulnerabilities.
- **The Pennsylvania State University: College of IST** — University Park, PA
  Learning Assistant - Advised by Prof. Anna Squicciarini — *Fall 2017*
  - Co-designed the first offering of DS300: "Privacy And Security for Data Sciences", selecting topics, designing assignments and exams, and coaching students.
- **EPFL: Decentralized and Distributed Systems Lab** — Lausanne, Switzerland
  Research Assistant - Advised by Profs. Bryan Ford & Jean-Pierre Hubaux — *Summer 2017*
  - Researched the computer security challenges in protecting humanitarian data and workers *(published).*
- **Microsoft Corporation** — Redmond, WA
  Software Engineer - Connected Devices Team — *Summer 2016*
  - Co-developed a Universal Windows Application which allows users in spatial proximity to create chat rooms and send text/files by leveraging a custom P2P protocol.
- **The Pennsylvania State University: Center for HCI** — University Park, PA
  Developer - Supervised by Prof. John M. Carroll & Prof. Ben Hanrahan — *Spring 2016*
  - Co-developed a ride-sharing app (iOS & Android).
- **The Pennsylvania State University: Schreyer Honors College** — University Park, PA
  Scholar Assistant — *Fall 2015 - Spring 2017*
  - Organized ∼15 events per semester for over 1200 students and directed a student organization of 80 members.
- **PricewaterhouseCoopers LLC** — Philadelphia, PA
  Consultant - Advisory — *Summer 2015*
  - Presented and implemented solutions to operational challenges for a company-wide human capital strategy shift.

Publications

- **On Enforcing the Digital Immunity of a Large Humanitarian Organization.** Le Blond, S., **Cuevas, A.**, Troncoso-Pastoriza, J., Jovanovic, P., Ford, B., Hubaux, J. *IEEE Symposium on Security & Privacy*, San Francisco, US, May 2018. ***Distinguished Paper Award.***
- **Understanding the Reproducibility of Crowd-reported Security Vulnerabilities.** Mu, D., **Cuevas, A.**, Yang, L., Hu, H., Xing, X., Mao, B., Wang, G. *USENIX Security Symposium*, Baltimore, US, August 2018.
- **MGUARD: Hardware-Assisted Modular Kernel Protection** Wang, Z., **Cuevas, A.**, Zhenyu, N., Chen, Y., Mu, D., Xu, J., Lin, Y., Zhang, F., Xing, X., Mao, B. *Under Submission.*

Research Projects

- **2018/19 - Evaluating the Performance of Ensembled Defenses in Machine Learning:** *In progress.*
- **2018/19 - Impact of Fake Vulnerabilities:** *In progress.*
- **2018 - MGUARD:** Hardware tracing and selective tainting for high-performance modular kernel protection.
- **2018 - DEEPVSA** : Learning the execution patterns pertaining to memory region accesses and restoring the regions that VSA fails to infer when presented an incomplete control flow.
- **2017/18 - Crowd-Sourced Vulnerabilities** : Studied challenges in the reproduction of vulnerabilities and released a dataset of 368 memory corruption vulnerabilities, `vulnreproduction.github.io`.
- **2017/18 - Security for Humanitarian Work** : First look at the unique and diverse challenges faced by humanitarian organizations when collecting, processing, and sharing data.
- **2016/17 - Moving Target Defenses** : Designed security metrics and tests for the evaluation of MTDs.

Engineering Projects

- **PriFi Client (iOS)** `Swift, Objective-C`
  Implementation of the PriFi protocol as a VPN with the `NetworkExtension` framework. *62,292 LoC*
- **PriFi Client (Android)** `Java`
  Implementation of the PriFi protocol as a per-app VPN. *96,932 LoC*
- **Proximal Sharing (UWP)** `C#`
  Text and file sharing with a custom P2P protocol based on the `RemoteSystems` API. *23,572 LoC*

Selected Awards, Honors, & Grants

- **2018** Finalist - GeekPwn Cybersecurity and Artificial Intelligence Contest @ DEFCON
- **2018** Student Scholarship - Black Hat USA
- **2018** Distinguished Paper Award - IEEE Symposium on Security and Privacy
- **2018** Student Travel Grant - IEEE Security and Privacy Symposium
- **2017** Student Enrichment Fund - College of Information Sciences and Technology
- **2017** Research Grant - Schreyer Honors College
- **2017** Research Grant - Student Engagement Network
- **2016/17** Finalist - Nittany AI Challenge
- **2016** Information Security Scholarship - $(ISC)^2$
- **2016/17/18** Undergraduate Excellence Scholarship - College of Information Sciences and Technology
- **2015/16/17/18** Dean's List (4.0/4.0)
- **2015/16/17/18** Academic Grant - Presidential Leadership Academy
- **2014/15/16/17/18** Academic Excellence Scholarship - Schreyer Honors College

Languages & Skills

- **Programming Languages**: `Python, Swift, Java, Objective-C, C#` **Technologies**: LaTeX, TensorFlow
- **Spoken Languages** : Spanish, English, French, Portuguese, Guarani