Santiago Torres-Arias

PhD Candidate in Computer Science

Email: santiago@nyu.edu
GitHub: github.com/SantiagoTorres
Website: https://badhomb.re/orhttps://sangy.xyz

Research interests: Computer Security, Cryptography, Operating Systems, Privacy, Binary and Malware Analysis

- **I'm an Open Source-oriented developer.** I have made contributions to large scale open source projects such as the Linux Kernel, Git, Briar, and Mutt/NeoMutt. I'm also a member of the Arch Linux CVE Monitoring Team.
- **Good team work and leadership skills**. I currently lead two projects within New York University's Center for Cyber Security. I'm the team lead for PolyPasswordHasher and Toto. I'm also a main contributor to The Update Framework (TUF) project.
- **Dev-ops/Sw engineering research**. My current research focuses on elucidating and developing novel ideas to create reliable robust software.

Education

Ph.D *2015–current*
Doctor Of Philosophy in Computer Science
New York University: Tandon School of Engineering, U.S., **GPA: 3.800**

M.S. *2013–2015*
Master of Science in Cyber Security
New York University: Polytechnic School of Engineering, U.S., **GPA: 4.0**

B.S. *2007–2012*
Bachelor of Science in Electrical and Telecommunications Engineering,
Universidad Iberoamericana, Mexico, **GPA:** 8.5/10

Awards

NYU-TSOE *Research Assistanship*
A research assistanship that covers my full tuition expenses during the doctoral program, as well as other living expenses.

CONACyT *Scholarship*
Mexican Council of Science and Technology Scholarship for outstanding Mexican scholars studying abroad. This covers part of my living expenses and the total of my tuition.

NYU-TSOE *Scholarship*
A 8,000 USD per year Merit-Based Scholarship offered by New York University: Polytechnic School of Engineering to cover my Master-degree's expenses.

CENEVAL *Diploma*
Diploma of outstanding performance in the Computer Science accreditation exam, awarded by the Mexican Evaluation Center.

Experience

Ln(Phi) *July 2014–Current.*

- Ln(Phi) is a Mexican startup that focuses on research, innovation and implementation of software-related projects (see more at lnphi.com).
- I'm the lead security expert. I periodically audit 4 products through code reviews, unit and penetration testing.
- I'm also the lead of DevOps. With all the team, we elaborate new ways to provide continuous integration and continuous assurance of the software we develop.

Mexico City Justice Court *Apr 2012 – Aug 2012*

- Security Audit of the internal networks.
- Developer of automatic digitalization systems. I developed an automated system for OCR scanning and text embedding for old documents.
- Via a Liaison, I provided the same service for more than 40 courts across the city, as well as Mexico's National Forensic Service.
- I maintained and documented manuals for computer users of different levels of expertise.

Universidad Iberoamericana *Jan 2012 – May 2012*

- High School lecturer: Programming fundamentals.
- Taught a classroom of 10 students on how to hack the Pokemon red GameBoy game. Through this, they learned programming fundamentals such as data structures, constants, integrity checks and to never trust your input.

Research

in-toto: Protecting the Software Supply Chain
July 2015–Current.

- Version Control System auditing. Analyzed the way multiple version control systems store their metadata and how a malicious attacker can exploit vulnerabilities in it. This work culminated in collaborations with the Git development team.
- Design of in-toto. in-toto is a tool to secure the way multiple process within the software development lifecycle communicate with each other. Our intention is to provide integrity and auditability guarantees from the moment a developer commits a line of code to the moment the end user installs a package.

PolyPasswordHasher: A secure Password Storage Mechanism
Feb 2014–Current.

- PolyPasswordHasher (PPH) uses a Cryptographic Secret Sharing Algorithm and Salted Hashing protects password databases so that, even if they are stolen, it would take one billion years for attackers to crack a single password.
- I implemented PPH for multiple languages (C, Python) and frameworks (Django) so that organizations – such as Target and Sony – can seamlessly use PPH to protect millions of users.
- Leading a research project to measure how the choice of user passwords would affect the security provided by PPH in real-life scenarios
- Lead a team of 5 people with different backgrounds in developing new implementations of PPH for new and widespread platforms.

The Update Framework: A Secure Update System
Sept 2013–current

- Provide support, feedback and update TUF's designs. Currently, we are working in adapting TUF to car update systems.
- Designed and built tools for developers to protect software packages hosted on the Python Package Index (PyPI). TUF is currently being deployed in bleeding edge technologies such as Docker hub and CoreOS.
- Designed and conducted experiments to show that Diplomat, a novel security system for protecting community repositories (such as PyPI), protects 99% of users even if attackers control the repository for a month.

Publications

Conference Paper – USENIX '16 "On Omitting Commits and Committing Omissions: Preventing Git metadata tampering that (re)introduces vulnerabilities". **S. Torres-Arias**, A. Kumar Ammula, R. Curtmola, J. Cappos.

Conference Paper – NSDI '16 "Diplomat: Using Delegations to Protect Community Repositories". T. K. Kuppusamy, V. Diaz, **S. Torres-Arias**, J. Cappos.

Conference Paper – Under peer review "{PASS}: Gaining the Higher Ground Against Password Crackers" J. Cappos, **S. Torres-Arias**. (ACSAC 2016)

Article "PolyPasswordHasher: Improving Password Storage Security", Login; Magazine, Security issue. `December 2014`.

Talks & Posters

Talk "PolyPasswordHasher: no password left behind", Army Cyber Institute, "Cyber Talks", `September 2016`.

Poster "PolyPasswordHasher: no password left behind", New England Networking and Systems Day, `October 2014`.

Volunteering

The Briar Project
Nov 2015- current

- The Briar project is a distributed messaging application for first responders and activists. I'm an occasional commiter to the project.
- I revamped the "introduction client" which is used to add contacts in the network by using a trusted middleman.
- Refactored of Tor-related UI elements. I updated modules for connectivity via tor.
- I Refactored user interfaces in general. Translated current programmatic user interfaces to XML, so the project's designers could easily edit them.

NeoMutt
May 2016 - current

- Mutt is a command line Mail User Agent (much like Thunderbird or outlook). I'm an official developer of it's successor, NeoMutt.
- I maintain the new-mail feature. Which is the notification handler for when a new mail arrives.

Arch Linux
July 2015 - current

- Arch Linux is one of the most popular and robust Linux Distributions. I'm member of the Arch Linux CVE Monitoring Team.
- I constantly notify developers of new vulnerabilities, as well as interact with vendors for appropriate disclosure and patching of vulnerabilities. I'm also part of the team that writes and elaborates the Arch Security Advisories (ASA), to notify the community and IT experts of security updates for Arch Linux's packages. You can follow us on `https://twitter.com/arch_security`
- I'm also part of the testing team. I verify that packages are correct before they are released to the general public.

Universidad Iberoamericana
Feb 2009 - May 2014

- Co-founded the Software-development group. We Focus on teaching introductory programming and computer science to undergraduate students.
- Creator of MATSOL, an iOS and Android toolkit for engineering students. On its good days, MATSOL used to be the top-25 most downloaded educational application on spanish-speaking countries.

Technical Skills

Languages

- Spanish (Native proficiency), English (107 TOEFL IBT), French (B1 DELFT).

Programming Languages

- C, Python, Java, shellscript (bash/zsh variants), ASM (x86, PIC, MSP430), MATLAB/Octave, Objective-C, PHP, SQL and C++.
- **Frameworks/API's/etc:** Django, OpenGL, Repy, pydasm, iOS, Android, Travis (CI).
- Systemd Unit writing, system tracing, automated debugging, and application profiling.
- **Operating Systems:** Linux (Debian, RedHat, Arch, LFS variants), Windows, MacOS, Minix.
- **Favorite tools**: Vim, Git, tmux, neomutt, gdb, automake, radare2.