# MARCELA S. MELARA

Email: marcela.melara@intel.com • Web: https://masomel.info

## RESEARCH INTERESTS

Trustworthy distributed systems, software supply chain, OS security, transparency systems

## PROFESSIONAL EXPERIENCE

*Research Scientist, Security & Privacy Research* Oct 2019–present
Intel Labs

- Lead research on novel techniques for supply chain security, integrity and trust.

*Graduate Research Intern* June 2018–Feb 2019
Intel Labs

- Designed a memory isolation scheme for cloud applications using hardware-based techniques.

*OS Security Engineering Intern, CoreOS Team* Summer 2014 & 2015
Apple Inc.

- Evaluated deployment of key transparency as part of a large-scale system.
- Improved sandboxing technology in core operating system.

*Technical Intern* November 2010–April 2011
Seneca7 Race Committee

- Designed and implemented a web-based program for real-time tracking of relay race runners.

## EDUCATION

**Princeton University**, Princeton, NJ

*Ph.D.*, Computer Science September 2019
Dissertation: *Intra-Process Least Privilege and Isolation for Emerging Applications*
Advisor: Michael J. Freedman

*M.S.E.*, Computer Science June 2014
Thesis: *CONIKS: Preserving Secure Communication with Untrusted Identity Providers*

**Hobart and William Smith Colleges (HWS)**, Geneva, NY

*B.S., summa cum laude*, Computer Science May 2012
Honors Thesis: *ELARA: Environmental Liaison and Automated Recycling Assistant*
Second Major in French and Francophone Studies. Minor in Physics.

## PUBLICATIONS AND PRESENTATIONS

*Conference Papers & Journal Articles*

"A Viewpoint on Software Supply Chain Security: Are We Getting Lost in Translation?" M. S. Melara and S. Torres Arias. *IEEE Security & Privacy*, Vol. 21, Issue 6. Nov 2023.

"Hardware-Enforced Integrity and Provenance for Distributed Code Deployments." M. S. Melara and M. Bowman. *NIST Workshop on Enhancing Software Supply Chain Security*. June 2021.

"CONIKS: Bringing Key Transparency to End Users." M. S. Melara, A. Blankstein, J. Bonneau, E. Felten, M. Freedman. *USENIX Security Symposium*. August 2015.
**Caspar Bowden PET Award, 2017.**

"Shining the Floodlights on Mobile Web Tracking — A Privacy Survey." C. Eubank, M. Melara, D. Perez Botero, A. Narayanan. *W2SP*, 2013.

"Vireos: an Integrated, Bottom-Up Educational Operating Systems Project with FPGA support." M. Corliss, M. Melara. *ACM SIGCSE*, 2011.

*Invited Talks*

"Securing the Software Supply Chain: An In-Depth Exploration of SLSA." M. Lieberman, M. Melara, J. Lock, L. Capadan. *OpenSSF Tech Talk*. Oct 2023.

"Building Trust with Attestation." M. Melara, V. Scarlata. *Open at Intel Podcast*. May 2023.

"Software Supply Chains." M. Melara, B. Domingues. *Open at Intel Podcast*. Mar 2023.

"EnclaveDom: Privilege Separation for Large-TCB Applications in Trusted Execution Environments." M. Melara. *Microsoft Research Cryptography & Privacy Colloqium*. Sep 2020.

*Conference Talks*

"Auditing the CI/CD Platform: Reproducible Builds vs. Hardware-Attested Build Environments, Which is Right for You?" M. S. Melara, C. Kimes. *ACM SCORED*. Oct 2024.

"TPMs, Merkle Trees and TEEs: Enhancing SLSA with Hardware-Assisted Build Environment Verification." M. Melara, C. Kimes. *Open Source Summit NA*. Apr 2024.

"Panel Discussion: Improving Supply Chain Integrity with OpenSSF Technologies." A. Le Hors, M. Lieberman, J. White, M. Melara, I. Hepworth. *Open Source Summit NA*. Apr 2024.

"Panel Discussion: DEI for the OpenSSF Community." M. McElaney, J. Kjell, J. White, C. Voong, M. Melara. *SOSS Community Day NA*. Apr 2024.

"All things in-toto! Supply chain attestations, policies, and adoption stories, oh my!" M. Melara, S. Torres Arias. *KubeCon & CloudNativeCon NA*. Nov 2023.

"Using FPGAs to Create a Complete Computer System for the Classroom." M. Melara. *NYCWiC 2011*.

*Patents*

"Concept for Performing Operations on an Asset." C. M. Bowman, P. Narayana Moorthy, B. Vavala, M. S. Melara. *US Patent Application 18/343,797*. 2024.

"Method and apparatus for multi-dimensional attestation for a software application." M. S. Melara, B. Vavala, M. Steiner, V. Scarlata, A. L. Vahldiek-Oberwagner. *US Patent Application 18/311,253*. 2023.

"Attestation of operations by tool chains." V. Scarlata, A. Trivedi, R. Lal, M. S. Melara, M. Steiner, A. L. Vahldiek-Oberwagner. *US Patent 11650800*. 2023.

"Optimizing deployment and security of microservices." P. Saxena, A. L. Vahldiek-Oberwagner, M. Vij, K. A Doshi, C. H. Morales, C. M. Bowman, M. S. Melara, M. Steiner. *US Patent Application 17/561,676*. 2022.

*Blog Posts*

"Building Trust in AI: An End-to-End Approach for the Machine Learning Model Lifecycle." M. Spoczynksi, M. Melara, S. Szyller. *Intel Community Tech Innovation Blog*. December 2024.

"The Opportunity for DEI Participation in the Security Industry (And OpenSSF)." C. Voong, J. White, J. Kjell, M. Melara, M. McElaney. *OpenSSF Blog*. May 2024.

"Why Making Johnny's Key Management Transparent is So Challenging." M. Melara. *Freedom to Tinker*. March 2016.

"There's Something Wrong With This Picture..." M. Melara. Guest blogger, *Grand Central Blog*. November 2010.

"Busy Moms Need Energy." M. Melara. Guest blogger, *Grand Central Blog*. October 2010.

*Posters*

"Protecting the IoT Against Data Leaks through Intra-Process Access Control." M. Melara. *Stony Brook University, National Security Institute Security & Privacy Day 2017*.

"Building an Automatic and Scalable Tool for Improving Environmental Recycling: ELARA." M. Melara. *HWS Summer Research Symposium 2011*.

"Using FPGAs to Create a Complete Computer System for the Classroom." M. Melara. *HWS Summer Research Symposium 2010*.

*Manuscripts*

"SoK: A Defense-Oriented Evaluation of Software Supply Chain Security." E. Ishgair, M. S. Melara and S. Torres Arias. *ArXiv Preprint*. May 2024.

"Enabling Security-Oriented Orchestration of Microservices." M. S. Melara and M. Bowman. *ArXiv Preprint*. May 2021.

"EnclaveDom: Privilege Separation for Large-TCB Applications in Trusted Execution Environments." M. S. Melara, M. J. Freedman, and M. Bowman. *ArXiv Preprint*. July 2019.

"Pyronia: Redesigning Least Privilege and Isolation for the Age of IoT." M. S. Melara, D. Liu, and M. J. Freedman. *ArXiv Preprint*. March 2019.

## MENTORING

*PhD Advising*

Eman Abu Ishgair (*Purdue University*). Co-advised with Santiago Torres Arias

*Interns Mentored, Intel Labs*

Eman Abu Ishgair (*Purdue University*), Summer 2024
Project: "Private SBOM Exchange"

*Undergraduate Students Mentored*

Jessica May. CRA-W Collaborative Research Experiences for Undergraduates, Summer 2017
Project: "Stormship: Smart Tool for Revealing Malicious Scripts Hidden in Plain Sites". Co-advised with Nick Feamster

Huy Quoc Vu. Google Summer of Code, Summer 2016
Project: "CONIKS for Tor Messenger". Co-mentored with Arlo Breault (*The Tor Project*)

Michael Rochlin. Princeton University Junior Independent Work, Spring 2015
Project: "Coniks 2.0: Publicly Verifiable Keystore with Key Changing and Verifying Capabilities". Co-advised with Ed Felten

*Intel-Princeton REU*

Lois Omotara, Summer 2023
Priya Naphade, Summer 2022

*Científico Latino Graduate School Mentoring Initiative*

Jessica Williams, Fall 2023
Brittany Gomez, Fall 2020

## TEACHING

*Graduate Teaching Fellow* Summer 2017–Winter 2018
Princeton University, McGraw Center for Teaching and Learning

- Provided instructional consultation for TAs via classroom observations.
- Led the annual Assistant in Instruction Orientation for new Computer Science TAs.

*Assistant in Instruction*
Princeton University

- COS 461: Computer Networks Spring 2014
  Instructor: Prof. Michael Freedman
- COS 318: Operating Systems Fall 2013
  Instructors: Prof. Kai Li, Dr. Andrew Bavier

*Physics Teaching Fellow* Fall 2011–Spring 2012
Hobart and William Smith Colleges, Center for Teaching and Learning

- Held walk-in evening office hours for students taking Physics courses of any level.

*Evening Teaching Assistant* Fall 2010–Spring 2011
Hobart and William Smith Colleges, Dept. of Mathematics and Computer Science

- Held walk-in evening office hours for students taking introductory Computer Science courses.

*Teaching Assistant*
Hobart and William Smith Colleges, Dept. of Mathematics and Computer Science

- CPSC 124: Introduction to Programming Fall 2011, Spring 2012
  Instructors: Prof. Davd Eck, Prof. Carol Critchlow, respectively
- MATH 131: Calculus II Fall 2009
  Instructor: Prof. Kevin Mitchell

## HONORS AND AWARDS

| | |
|---|---|
| USENIX Security Noteworthy Reviewer Award | August 2023 |
| Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies | July 2017 |
| Siebel Scholars Class of 2014 | July 2013 |
| Princeton University President's Fellowship | Fall 2012–Spring 2013 |
| Phi Beta Kappa | May 2012 |
| Honors in Computer Science | April 2012 |
| HWS Dept. of Mathematics and Computer Science John S. Klein Prize | April 2012 |
| Roderic '52 and Patricia '53 Ross Endowed Centennial Scholarship | Fall 2011–Spring 2012 |
| Hai Timiai Women's Senior Honors Society | April 2011 |
| HWS Dept. of Mathematics and Computer Science William Ross Proctor Prize | April 2010 |
| Phi Beta Kappa Book Award | April 2010 |
| First Year Academic Achievement Award | April 2009 |
| William Smith College Dean's List | Fall 2008–Spring 2012 |

## SERVICE ACTIVITIES

| | |
|---|---|
| **Technical Advisory Council**, Open Source Security Foundation (OpenSSF) | 2024–present |
| **Co-Chair**, OpenSSF Diversity, Equity and Inclusion Working Group (DEI WG) | 2024–present |
| **Workshop Organizer**, ACM Workshop on Software Supply Chain Offensive Research and Ecosystem Defenses (SCORED) | 2022–present |
| **Specification Maintainer**, CNCF in-toto Attestation Framework | 2023–present |
| **Specification Maintainer**, OpenSSF Security Levels for Software Artifacts (SLSA) | 2024–present |
| **Program Committee**, Linux Foundation SigstoreCon: Supply Chain Day | 2024 |
| **Program Committee**, Linux Foundation SOSS Community Day EU | 2024 |
| **Program Committee**, ACM EuroSec | 2024 |
| **External Reviewer**, Proceedings on Privacy Enhancing Technologies (PoPETS) | 2018 |
| **External Reviewer**, International World Wide Web Conference (WWW) | 2015 |
| **Regional Lead, NJ**, Siebel Scholars | Fall 2014–Spring 2016 |
| **Hiring Committee**, HWS Dept. of Physics Faculty | Spring 2012 |
| **Hiring Committee**, HWS Dept. of French and Francophone Studies Faculty | Spring 2012 |