Marcella Hastings mhast@seas.upenn.edu marcellahastings.com

Education

University of Pennsylvania, Philadelphia, Pennsylvania USA
M.S., Ph.D., Department of Computer Science *(expected December 2020)*
Advisor: Nadia Heninger. GPA: 3.90

Tufts University, Medford, Massachusetts USA
B.S., Computer Science and Mathematics, May 2015
Summa Cum Laude

Publications

Refereed Conference Proceedings

SoK: General Purpose Compilers for Secure Multi-Party Computation. Marcella Hastings, Brett Hemenway, Daniel Noble, and Steve Zdancewic. In *40th IEEE Symposium on Security and Privacy* (Oakland '19). May 2019.

The Proof is in the Pudding: Proofs of Work for Solving Discrete Logarithms. Marcella Hastings, Nadia Heninger, Eric Wustrow. In *Financial Cryptography and Data Security* (FC '19). February 2019.

Measuring Small Subgroup Attacks on Diffie-Hellman. Luke Valenta, David Adrian, Antonio Sanso, Shaanan Cohney, Joshua Fried, Marcella Hastings, J. Alex Halderman, Nadia Heninger. In *Network and Distributed System Security Symposium* (NDSS '17). February 2017.

Weak Keys Remain Widespread in Network Devices. Marcella Hastings, Joshua Fried, and Nadia Heninger. In *Proceedings of the 2016 ACM on Internet Measurement Conference* (IMC '16). November 2016.

Work Experience

Software Applications and Innovations Lab, Boston, MA USA, May 2019 - August 2019
Research Intern. Implementing feature libraries and a cryptographically secure protocol for generating preprocessing data in the JIFF framework for secure multi-party computation.

MIT Lincoln Laboratory, Lexington, MA USA, May - August 2014
Research Intern. Developed an end-to-end prototype for a cryptographically secure mechanism for authentication from a single fortified device.

Google, New York, NY USA, June - August 2013
Engineering Practicum Intern. Designed and implemented a client-facing interface and implementation for a saving filters feature with the DoubleClick for Publishers team.

Invited Talks

General purpose compilers for secure multi-party computation
DC Area Crypto Day, December 2018
Theory and Practice of Multi-Party Computation Workshops, June 2019
Real World Cryptography, January 2020

Teaching

Designed course materials, taught hands-on programming labs, developed grading software, managed teaching assistants, and held regular office hours for undergraduate and graduate-level courses.

University of Pennsylvania: CIS 331: Introduction to Networks and System Security, Spring 2017. CIS 556: Cryptography, Fall 2016. GEMS Computer Science Workshop, Summer 2017.

Tufts University: COMP 170: Theory of Computation, Spring 2015. COMP 50: Problem-Solving by Computer, Fall 2013. COMP 11: Introduction to Computer Science, Fall 2012 - Spring 2015.