Ana McTaggart

Computer Security Researcher

about

E2-480
UCSC
Santa Cruz
California

apmctaggart@gmail.com

programming

C/C++
Python, Mathematica
bash, shell scripting
Java, LaTeX

skills

social media
social engineering
penetration testing
risk models
threat analysis
kali
Metasploit
wireshark
nmap
jack the ripper
software analysis

Interests

mathematical computation
theoretical models
practical security
programming languages
category theory
algebra
computer privacy
computer security
storage security
access patterns
oblivious computation
oblivious RAM
post quantum cryptography
distributed systems

Purpose and Goal

My goal is to gain industry experience in practical security problems. My intent with this is to have industry needs inform my research, to make effective and useful security models.

education

since 2015 **Ph.D.** student in Computer Science — University of California, Santa Cruz
Oblivious Programming Languages

2010–2015 **B.Sc.** Honors with Distinction — University of Massachusetts, Amherst
Majoring in Computer Science, Math. Minors in Physics, Sustainable Food and Farming

2008–2010 **Ashland High School** — Ashland, Massachusetts
Graduated early, focused on a strong mathematical preparation for college.

publications

2016 **Clinker, Reconstructing Sharded Data Stores Efficiently** — FAST'16, WiP Reports
Produced a theoretical method for reconstructing sharded data stores efficiently, increasing security and reliability for cloud storage, working with Sinjoni Mukhopadhyay and Professor Miller.

2015 **Computation in Cellular Automata, information theoretic characterization and classification** — Undergraduate Thesis
Classified Wolfram Cellular Automata according to information theoretic properties, identifying which ones are candidates for proof of universal computation, with Professors Barrington and Anderson

Areas of Research

2017-present **Oblivious Programming Languages and Computation** — UCSC
Focus on type checking oblivious computation models, and ensuring no information is leaked about access patterns. Raising definition of oblivious computation to include prevention of replay attacks. Secure accesses on distributed and cloud storage systems. Applied category theory for distributed systems, cryptography for access patterns

2015-present **Practical Security for Dissidents** — UCSC
Designed and taught many courses on computer security for non technical professionals and students. Foiling facial recognition using makeup patterns which reflect infrared spectrum. Detection and location of ISMI catchers/Stingrays and fake cell phone towers. Mentored undergraduate students in research.

2015-2017 **UCSC** — Deniable File Systems
Designed a steganographic and deniable file system, Artifice. Proved it is unlikely to be accessed. Wrote and obtained NSF Grant 1814347 titled, A Multi-Layered Deniable Steganographic File System. Attempted implementation of a custom device mapper, mentored masters students in implementation.