Schuyler Rosefield
schuyler@rosefield.org

Education

Northeastern University — Boston, MA
PhD in Computer Science — 2018-Present
Advisor: abhi shelat

Northeastern University — Boston, MA
Bachelor of Science in Mathematics — Graduated Fall 2017
GPA: 3.49/4.0 — Honors: Dean's List

Research

Goal: My primary research interests are in creating efficient specialized multiparty computation protocols. I am also interested in the areas of searchable encryption and fully homomorphic encryption.

- **Multiparty Generation of an RSA Modulus**
  Megan Chen, Ran Cohen, Jack Doerner, Yashvanth Kondi, Eysa Lee, Schuyler Rosefield, and abhi shelat
  Manuscript

Work Experience

MIT Lincoln Lab — **Lexington, MA**
Research Intern — *Summer 2019*

- Implemented new primitives and asyncronous execution mode in internal MPC framework
- Performance optimization resulting in order of magnitude improvement for large computations
- Created submission for the IDASH Privacy and Security competition for secure multiparty neural network training. Devised a model that provides high accuracy for the challenge data set and allows for efficient MPC evaluation

NGPVAN — **Somerville, MA**
Software Security Engineer — *May 2015 - August 2018*

- Owner of fixing identified vulnerabilities and handling security report list
- Guided and prioritized the engineering security roadmap
- Extended API to allow authentication with ephemeral bearer tokens following the OAuth2 spec
- Created a library to handle encryption key management and automatic key cycling with a simple interface to AES-GCM
- Manual web application penetration testing to identify xss, rce, csrf, and other vulnerabilities
- Implemented framework-level mitigations for the above vulnerability types

Personal Projects

- Designed a high performance big number library in C++11 to perform calculations on arbitrary-precision integers (github.com/Rosefield/BigNum)
- Created a distributed file store application using distributed hash tables (DHTs) in asyncio Python (github.com/Rosefield/DHTFileStore)
- Made a program to identify samples of (distorted) audio from a known source (github.com/Rosefield/SongFingerprint)

Computer Skills

- C, C++, C#, rust, x86 asm, Python, SQL
- Usage of git, agile development, and secure software development
- Up-to-date understanding of modern security best practices with particular interest in crypto protocols

Other Interests

- Completion of wargames (such as those on `https://overthewire.org`) and CTFs (third place at CSAW 2015 finals)
- Fire juggling with torches and group juggling