Zachary Espiritu

zacharyespiritu.com • zachary_espiritu@brown.edu

Education

Brown University

Sc.M. in Computer Science • GPA: 4.0
Sc.B. in Computer Science • GPA: 4.0
Completing both degrees in Dec 2021.

Publications

Z. Espiritu, E. A. Markatou, R. Tamassia. "Time- and Space-Efficient Aggregate Range Queries on Encrypted Databases". 2021. *Under review.*

F. Falzon, E. A. Markatou, Z. Espiritu, R. Tamassia. "Encrypted Range Search in Multiple Dimensions". 2021. *Under review.*

Awards

CrowdStrike NextGen Scholarship for Cybersecurity and AI
(6 selected nationwide)

(ISC)² Cybersecurity Scholarship
(20 selected nationwide)

1st Place at Hack@Home Security CTF
(1 out of ~100 participants)

Projects *(selected)*

Dropbox (Secure File Store)

As Head TA, authored new project for security course on using untrusted servers & PKI for secure, efficient file storage and sharing. Project scored average evals of 4.61 / 5.00 in first year.

CS Concentration Validator

Developed Racket web script using formal provers to synthesize degree completion plans for 300+ CS majors at Brown; currently being integrated into official University advising system.

Vehicle Routing Solver

Designed top-performing local search solver out of 21 teams for NP-hard vehicle routing problem in graduate-level competition. In Python and Java.

Weenix

Wrote full operating system kernel in C.

Experience

Encrypted Systems Lab Fall 2020 – Present
Researcher

- Wrote novel crypto protocol and Java / Node.js prototype for Massachusetts's *Dept. of Public Health* to securely conduct epidemic research over databases of 22 distributed MA institutions, *eliminating costly and vulnerable manual anonymization* process.

Cryptography, Anonymity, Privacy, Security (CAPS) Group Fall 2020 – Present
Researcher

- Designed 7 novel, O(1)-time, provably secure aggregate range query schemes for encrypted DBs, *lowering state-of-the-art runtime and storage overhead by up to 83%* in practice.
- Devised dynamic programming algorithm to *reduce experiment setup times by 99%*, allowing inclusion of larger Python benchmarks (3 orders of magnitude) in final publication.
- Developed 2 novel algorithmic attacks that *fully reconstruct plaintext* of multidimensional encrypted databases by exploiting geometric patterns in the database index structure.

Google Summer 2020
Software Engineering Intern, Google Cloud HSM

- Architected open-source OpenSSL engine to enable web servers to use HSM-backed keys for crypto signatures *without any source code changes*. C++ with gRPC and Bazel.

Brown PLT (Programming Languages Team) Summer 2018
Research Intern

- Created machine learning package, *used yearly in 90-student introductory CS course*, for Pyret, a functional programming language. Built using TensorFlow.js.

Negotiatus Summer 2016 and Summer 2017
Software Engineering Intern

- Led full-stack development in HTML, JavaScript, and Ruby on Rails of still-existing, core value propositions such as Scheduled Orders, *converting ~20% of non-recurring revenue into monthly recurring revenue* by 2017.
- Optimized internal-facing SQL queries via PostgreSQL materialized view caching layers and cron jobs for *up to 100x faster product searches*.

Teaching Service *(@ Brown Computer Science)*

Head Teaching Assistant (for 6 Computer Science Courses) Fall 2018 – Present

- Hired, trained, and managed 54 TAs for **Software Exploitation** (2021), **Systems Security** (2021, 2020, 2019), **Programming Languages** (2020), and **Accelerated CS Intro** (2018).
- Automated grading and project setup via Bash scripts spawning Linux Docker containers in Google Compute Engine, saving 250 staff hours in total and $4k/year in dept. budget.
- Modernized security course written assignments by writing +30 new problems covering cryptography, web security, networks, data compression, protocol vulnerability analysis.

Meta Teaching Assistant (TA Program Coordinator) Fall 2019 – Present

- Led hiring / training of 781 TAs over 56 courses by managing 112 HTAs over 14 time zones.
- Authored Bash and Python scripts and new organizational processes to reduce management workload by 300 hours, yielding department savings of $5k/year.
- Released *GrblGrader*, a modular feedback delivery and grading management system in JavaScript. Generates 1000 student impressions across 8 CS courses each year.