Zachary Espiritu

Website: zacharyespiritu.com • **Email**: zachary_espiritu@brown.edu
GitHub: ZacharyEspiritu • **LinkedIn**: zacharyespiritu

Education

Brown University **Concurrent Sc.B and Sc.M in Computer Science** • GPA: 4.0 / 4.0 Jan 2021 – Present

- **Relevant courses:** Algorithms, Cryptography, Distributed Systems, Formal Methods, Graphics, Human-Computer Interaction, Operations Research, Operating Systems, Probability, Software Security and Exploitation, Systems Security.

Experience

Encrypted Systems Lab **Researcher** Aug 2020 – Present

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

Crypto & Privacy Group **Researcher** Sep 2020 – Present

- Designed 7 novel, constant-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 (by 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 **Software Engineering Intern, Google Cloud HSM and KMS** May 2020 – Aug 2020

- Architected and developed open-source OpenSSL engine allowing web servers (such as Apache and Nginx) to use Google Cloud HSM keys for cryptographic signatures *without source code changes*. C++ with gRPC and Bazel components.

Brown PLT **Research Intern, Programming Languages** May 2020 – Aug 2020

- Wrote machine learning package, *used yearly in 90-student functional programming course*, for Pyret language.

Negotiatus **Software Engineering Intern** May 2020 – Aug 2020

- 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 SQL queries via PostgreSQL materialized view caching layer for *up to 100x faster product searches*.

Department Service

Head Teaching Assistant (for Computer Systems Security and Software / Binary Exploitation) Sep 2018 – Present

- Hired, trained, and directly managed 54 TAs as HTA for multiple courses, including **Software / Binary Exploitation** (2021), a course on discovering security vulnerabilities in software, and **Computer Systems Security** (2021, 2020, 2019), a generalist course covering defenses and pen-testing in Linux systems security, web application security, and cloud storage security.
- Designed new project for 92 students in security course on applied cryptography fundamentals, security design review, and using untrusted servers for secure, efficient file storage and sharing. Project scored average student evaluations of 4.51 / 5.00.
- Automated 3 courses' grading and project setup via Bash scripts integrated with Linux VMs and Docker containers in Google Compute Engine, saving 250 staff hours over 3 courses and $4k/year in dept. budget.

Meta Teaching Assistant (TA Program Coordinator) May 2020 – Aug 2020

- 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 grading management system. JavaScript; 1000 student impressions/year across 8 CS courses.

Awards

CrowdStrike NextGen Cybersecurity Scholarship	*(6 selected nationwide)*	Aug 2021
(ISC)2 Undergraduate Security Scholarship	*(20 selected nationwide)*	May 2021
1st Place at Hack@Home Cybersecurity CTF	*(out of 100 participants at CTF)*	Nov 2020

Publications

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

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