David Hacker

+1 (805) 368-5071 • dmhacker.2019@gmail.com • https://dmhacker.github.io

Education

University of California San Diego — **La Jolla**
Major: Computer Science, Minor: Mathematics, 3.94, Provost Honors — *2017–2021*

Relevant Courses: Basic Data Structures, Advanced Data Structures, Discrete Mathematics, UNIX Tools & Techniques Computer Architecture & Systems Programming, Database Applications, Computer Graphics, Digital Design Techniques Computational Theory, Linear Algebra, Calculus & Analytic Geometry, Differential Equations, Software Engineering

Work Experience

Positions Held

Bloomberg L.P. — **New York City**
Software Engineering Intern — *June 2019–August 2019*

- Member of Bloomberg's real-time market data infrastructure team
- Designed a distributed cache to offload requests for snapshots of security data, lessening the load on the main infrastructure
- Created utilities for converting between legacy and modern intraday trading ticks that have been requested by many engineers
- Integrated a UI component for testing the cache into a widely-used internal diagnostic tool
- Presented and demoed an interactive version of the application to the CTO's office
- Cache is scheduled for deployment in the future and is expected to handle several billion queries & events per day

University of California San Diego — **La Jolla**
CSE Department Tutor — *April 2018–Present*

- CSE 20, Discrete Mathematics: Spring 2018
- CSE 21, Mathematics for Algorithms & Systems Analysis: Fall 2018, Spring 2019
- Held office hours on a weekly basis and provided tutoring to students who required additional help
- Graded students' homework assignments, midterms and final exams

Medspace — **La Jolla**
Software Engineering Intern — *February 2018–September 2018*

- Wrote a command line tool in C# to import 166 million rows of CSV data into a Neo4j graph database
- Created an ASP.NET Core backend & RESTful API to interface with the database
- Implemented a k-dimensional tree in the backend to speed up geospatial queries by a factor of several hundred
- Managed nearly $20,000 worth of server resources, used to store data and host the backend
- Designed another backend using the Java Spring framework to supply customers with medical analytics
- Integrated an Auth0 authentication system into the Spring backend to protect user data

Notable Projects

RLWE Cryptography: *C++, Number Theoretic Library, Libsodium*

- Implemented several prominent post-quantum cryptosystems related to the ring learning with errors (RLWE) problem
- Designed a fast version of the Fan-Vercauterean cryptosystem, allowing for computations on encrypted data
- Additionally integrated NewHope key exchange & Ring-TESLA digital signature algorithms

Dual_EC_DRBG Backdoor: *Rust, GNU Multiple Precision Arthimetic*

- Demonstrated how a Shumlow-Ferguson attack could be used to break a dual elliptic curve random number generator
- Heavily optimized the attack by writing custom implementations for NIST P-256, P-385, and P-521 elliptic curves
- Can determine a generator's internal state in less than 30 seconds using an 8-core i7-8650U processor

Alexa YouTube Skill: *NodeJS, FFmpeg, AWS Lambda, Heroku*

- Created a skill that lets Amazon Alexa devices play audio from YouTube videos as a hobbyist project
- Supports four languages: English, German, French, Italian
- Downloaded over 5000 times and has over 120 stars on GitHub
- Reviewed by the German tech channel Venix, which has over 25,000 subscribers

Technical Skills

Languages: C, C++, C#, Rust, Java, Python, JavaScript, ARM Assembly

Web & UI Frameworks: MEAN, Spring, ASP.NET Core, Flask, React Native, wxWidgets