

# Ryan Lehmkuhl

github.com/ryanleh

ryanleh@berkeley.edu | (619) 890-9031

## EDUCATION

### UC BERKELEY

B.S. ELECTRICAL  
ENGINEERING AND  
COMPUTER SCIENCE  
Class of 2021  
Dean's List  
Regents' Scholar  
GPA: 3.9 / 4.0

## COURSEWORK

### GRADUATE

Systems Security  
Decentralized  
Secure Systems  
Lattices and Post-  
Quantum Cryptography  
(Audit)

### UNDERGRADUATE

Computer Security  
(Student Instructor)  
Cryptography  
Abstract Algebra I & II  
Artificial Intelligence  
Operating Systems  
Optimization Models  
Probability and Random  
Processes  
Efficient Algorithms &  
Intractable Problems  
Machine Structures  
Discrete Mathematics &  
Probability Theory  
Data Structures  
Linear Algebra  
Information Devices &  
Systems I & II  
(Lab Assistant)

## SKILLS

### PROGRAMMING

Python • Rust • C/C++  
Java • ~~TeX~~ • Assembly  
HTML • CSS • XML

### FRAMEWORKS

TensorFlow • Keras  
RayTune

### PROGRAMS

Wireshark • GNURadio

## RESEARCH

### RISELAB | UNDERGRADUATE RESEARCH ASSISTANT

September 2018 - Present | Berkeley, CA

- Working under Raluca Popa and Pratyush Mishra on techniques for **secure prediction** on **deep neural networks**.

## PROJECTS

### DELPHI | EFFICIENT DEEP NEURAL NETWORK CRYPTOGRAPHIC INFERENCE

2019 | Rust, C++, and Python

- Developed new approaches for training DNN architectures that are performant with cryptographic techniques using **Keras** and **RayTune** in Python
- Built a secure two-party protocol for convolution and matrix multiplication using **fully homomorphic encryption** with Microsoft's SEAL library in C++
- Integrated Python and C++ backends into a complete inference protocol utilizing **state-of-the-art MPC techniques** written in Rust

### GENETIC SCHEDULE | SCHEDULE OPTIMIZER W/ COMPLEX CONSTRAINTS

Winter 2019 | Python

### PINTOS (CS162) | OPERATING SYSTEM KERNEL

Spring 2019 | C

- Designed and implemented **file system**, **user space programs + syscalls**, **scheduling algorithms**, **user space allocator**, and **synchronization primitives** in a team of four

### SCRIPTO | SECURE FILE ENCRYPTOR/DECRYPTOR

Summer 2018 | Python & Rust

- Password-protected authenticated file encryption using **AES-GCM** and **PBKDF2**

### SECURE FILE STORE (CS161) | SHARED FILE STORE IN A MALICIOUS SETTING

Spring 2018 | Python

- Provides secure upload/download functionality, **hierarchical sharing/revocation**, and efficient updates to large files using a **Merkle Tree**

### SCADA NETWORK TCP SESSION HIJACKER | MITM EXPLOIT

Summer 2016 | Python

- Concurrently executes **ARP cache poisoning**, **TCP session hijacking**, and **packet sniffing/injection** to hijack a SCADA controller used by the Navy

## EXPERIENCE

### CIRCADENCE | RESEARCH AND DEVELOPMENT INTERN

Summers 2017, 2018 | San Diego, CA

- Built a **software-defined radio** TCP/IP modem using **QPSK modulation** in GNURadio
- Researched **cellular network** attacks utilizing software-defined radios
- Implemented an **exploit execution management engine** capable of launching Metasploit modules and custom scripts on remote agents
- Configured an **ELK stack** for data throughput to a machine learning algorithm

### SPAWAR | RESEARCH AND DEVELOPMENT INTERN

Summers 2015, 2016 | San Diego, CA

- Performed **vulnerability analysis** that helped earn over **\$200,000** in lab funding

## PUBLICATIONS

- [1] P. Mishra, R. Lehmkuhl, A. Srinivasan, W. Zheng, and R. Ada Popa, *Delphi: A cryptographic inference service for neural networks*, Accepted USENIX Security '20.