Ryan Lehmkuhl

github.com/ryanleh
ryanleh@berkeley.edu

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
Foundations of Probabilistic Proofs
Cryptography
Systems Security
Decentralized Secure Systems

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

SKILLS

PROGRAMMING
Rust • Python • C/C++
LaTeX• Golang • RISC-V
HTML • CSS

LIBRARIES
SEAL • SCALE-MAMBA
MP-SPDZ • TensorFlow
Keras • RayTune

PROGRAMS
Wireshark • GNURadio

RESEARCH

RISELAB | Undergraduate Research Assistant
September 2018 - Present | Berkeley, CA

- Working with **Raluca Popa** and **Pratyush Mishra** on techniques for **secure prediction** on **deep neural networks**.
- Working with **Alessandro Chiesa** on polynomial commitment schemes with extractability and hiding

PROJECTS

TBD | Malicious client cryptographic inference
Present | Rust, C++

- Designed and implemented a modified **SPDZ engine** in Rust
- Developed a specialized **conditional disclosure of secrets** MPC protocol

DELPHI | State-of-the-art semi-honest cryptographic inference
2019 | Rust, C++, and Python

- Developed new approaches for training **deep neural networks** 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++
- Implemented a novel **MPC** protocol and inference engine in Rust

GENETIC SCHEDULE | Genetic algorithm for complex scheduling
Winter 2019 | Python

SCRYPTO | 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

- Researched and developed **cellular network** attacks utilizing software-defined radios
- Implemented an **exploit execution management engine** capable of launching Metasploit modules and custom scripts on remote agents

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*, USENIX Security '20.