PHILIP WANG

(+1)-301-758-0191 | philip2000@outlook.com | linkedin.com/pwang00 | github.com/pwang00

Education

University of Maryland, College Park — Aug. 2018 – May 2022
Double Degree in Computer Science, Mathematics
Gemstone Honors Program (Presidential Scholarship) — Overall GPA: 3.548/4.00

Technical Strengths

Languages: Python (most familiar), Rust, Java, C, Go, Haskell, LLVM IR, x86 and MIPS assembly
Technologies: Git, Docker, GDB, Ghidra, IDA, Visual Studio, PyTorch, SageMath, Standard Linux utilities
Interests: Software Engineering, Software Security, Cryptography, Compilers, Performance Optimizations

Experience

Amazon Web Services — Aug. 2022 – Feb. 2023
Software Development Engineer — *Crystal City, VA*

- Led an effort to migrate Italy electronic invoicing logic to a newer set of Java-based invoicing microservices.
- Set up cross-region connectivity and implemented AWS CDK stacks for our services to provision their AWS account resources and ensure consistency across all CI/CD pipeline stages.
- Developed an Apache Velocity converter to replace our Italy Java Lambda converter, greatly improving extensibility by enabling our team to customize invoicing payloads before submitting to our government-facing invoice processor.
- Added API calls to fetch and decrypt encrypted tokens to retrieve personally identifiable information.

Raytheon CODEX — Jun. 2021 – Aug. 2021
Vulnerability Research Intern — *Austin, TX*

- Conducted in-depth reverse engineering, and exploitation of services running on MIPS embedded systems with ASLR, W⊕X, and other protections, using Ghidra and gdb/gdbserver to analyze and remotely debug the service binaries.
- Successfully discovered two buffer overflow vulnerabilities via protocol fuzzing and exploited them via **ROP**, and also found a denial-of-service vector caused by an unaligned memory access.

Trail of Bits — Dec. 2020 – Jun. 2021
Security Engineer Intern (Remote) — Dec. 2019 – Jan. 2020

- *2020-2021*: Implemented a **proof of concept** for a black-box model inversion attack on deep-learning classifiers from **arXiv:1902.08552**, along with Docker and Google Colaboratory support, for **PrivacyRaven**, a Python machine-learning assurance and research tool, and published work to Trail of Bits **blog**.
- *2019-2020*: Shipped a DigitalOcean droplet provisioner for **Manticore**, a symbolic execution engine, which involved designing a protobuf protocol for serializing and sending internal execution states across SSH, a terminal UI for visualizing state information, and Ansible playbooks for setting up droplets and running Manticore analysis jobs. Published work to Trail of Bits **blog** and **Github**.

Projects and Contributions

Piet LLVM Compiler | Rust, LLVM IR — Apr. 2023 – Present

- Wrote **PietCC**, a fully functional interpreter and ahead-of-time compiler for the **Piet** esoteric language, in Rust and LLVM IR using **inkwell** as an IR generator, llc for lowering to native assembly, and clang for linking.
- Added support for program codel-size inference, white block tracing and elimination, warning about nontermination for certain classes of programs, and emitting optimized IR through running LLVM optimization passes.

Cosmos-SDK / Osmosis | Golang — Mar. 2023 – Present

- **Fixed** an issue where 65-byte Ethereum ECDSA signatures generated by **Geth** would fail to verify under Cosmos due to an unsound optimization that compared the parities of the signature ecrecover byte and user ECDSA public key y-coordinate instead of using Geth's ecrecover method to recover a public key from the signature and validate it.

Cryptographic Attacks | Python, SageMath — Apr. 2017 – Present

- Maintaining and updating a **repository** for my implementations of algebraic attacks on cryptographic primitives based on cryptanalysis literature. Notably contains Coppersmith's attack for factorizing RSA moduli given 1/4 higher order bits of a prime factor, and Cheng's $4p-1$ elliptic curve CM-based factorization for backdoored RSA moduli.

Achievements

Capture the Flags | Teams: **Sice Squad**, **DiceGang**

- 1st place out of 387 teams in University of Illinois's SIGPWNY UIUCTF 2020.
- 1st place out of 1494 teams in RedpwnCTF 2020.
- 8th place out of 1301 teams in the qualification round for New York University's CSAW CTF 2019.
- 11th place out of 1278 teams in Hackasat Satellite Security CTF 2020.