Yi Cai

(878) 600-1933 *yicai@andrew.cmu.edu* *Homepage* *GitHub*

RESEARCH INTERESTS

I am committed to advancing trustworthy foundational software, encompassing a broad spectrum from programming languages and compilers to secure computing systems, leveraging formal methods, logics, and types.

EDUCATION

Carnegie Mellon University Pittsburgh, PA
M.S. in Electrical and Computer Engineering Jan. 2021 – Dec. 2023

University of Waterloo Waterloo, Canada
M.E. in Electrical and Computer Engineering Sept. 2020 – Aug. 2021

University of Electronic Science and Technology of China Chengdu, China
B.E. (First Class Honors) in Electronics and Electrical Engineering Aug. 2016 – June 2020

PUBLICATIONS

Hedwig: Automatically Compiling Security Protocols to Verified, High Assurance, Performant Implementations
Pratap Singh, Joshua Gancher, Yi Cai, and Bryan Parno.
In preparation

RESEARCH EXPERIENCE

Secure Foundations Lab, Carnegie Mellon University
Advised by Prof. Bryan Parno May 2023 – Present

- Designed and implemented a verified, performant, and secure library for parser and serializer combinators in Rust that supports cryptographic constant-time parsing.
- Constructed a compiler that translates data format specifications to formally verified, performant parsers and serializers.

CyLab, Carnegie Mellon University
Advised by Prof. Limin Jia Sept. 2023 – Dec. 2023

- Implemented a type-driven, hybrid approach for secure information-flow control in WebAssembly, with a controlled declassification mechanism.

Institute of Image Processing, UESTC
Advised by Prof. Shuaicheng Liu Dec. 2019 – June 2020

- Implemented an encoder-decoder-based deep learning tool for video deburring.

Vision and Learning Lab, UAlberta
Advised by Prof. Li Cheng July 2019 – Spet. 2019

- Conducted experiments on state-of-the-art human action detection algorithms.

TEACHING EXPERIENCE

Teaching assistant – Introduction to Computer Security Fall 2023
Prof. Bryan Parno, CMU

- Revised assignments for software, cryptography, and web exploits, held weekly office hours, and upgraded course auto-grader infrastructure.

Teaching assistant – Introduction to Computer Systems Spring & Summer 2023
Prof. Swarun Kumar & Prof. Greg Kesden, CMU

- Held weekly recitations and office hours on topics including x86 assembly, caching, virtual memory, signals and exceptions, network and concurrent programming.

PROFESSIONAL EXPERIENCE

Oregon Programming Languages Summer School Eugene, OR
Participant Summer 2023

- Studied topics from proof theory, logical relations, dependent type theory to program synthesis, program analysis, and verified compilation.

Cyphercor Inc. Ottawa, Canada
Software Engineer Spet. 2021 – Spet. 2022

- Led the development of secure multi-factor authentication services for Windows Remote Desktop, Local Windows Logon, and iframe-based web integration.

HONORS

OPLSS Fellowship (Oregon Programming Languages Summer School) June 2023
James Watt Scholarship for Research Overseas Apr. 2019
Outstanding Undergraduate Students Award (UESTC, top 5%) Aug. 2018
Excellent Student Award (UESTC, top 10%) 2017-2019

SKILLS

Programming Languages
Multilingual, ranked with personal preference: Rust, Standard ML, Haskell, OCaml, λ-calculus, Typed Racket, Typescript, C0, Zig, C, C#, Go, python, Java, C++, JavaScript, MATLAB

Proof Assistants & Verification Languages
Dafny, Verus, Coq, Isabelle/HOL

Architectures
x86-64, WebAssembly, MSP430

Miscellaneous
Tree-sitter, Language Server Protocol (LSP), Yacc, Pest, Nvim, Bash, Git, LaTeX, Markdown, React, Node.js, MySQL, MongoDB, SQLite