Yongming Fan

Address: 3390 Marlton Ct, West Lafayette, IN 47906
Email: fanym0919@gmail.com | Cell: (812) 327-8479

EDUCATION BACKGROUND

Purdue University, West Lafayette, IN May 2025
- **Doctor of Philosophy: Computer Science** *at College of Science*
  Research Areas: Applied Cryptography, Software Security, and Privacy

Indiana University Bloomington, Bloomington, IN May 2020
- **Master of Science: Computer Science** *at School of Informatics, Computing, and Engineering*
  $37,000 UITS Graduate Student Fellowship (2018); Can$7,500 Vision: Science to Applications Awards (2019)
- **Bachelor of Arts: Mathematics** *at College of Arts and Sciences*
- **Bachelor of Science: Computer Science** *at School of Informatics, Computing, and Engineering*
  $2,000 Anurag & Aruna Mendhekar Scholarship (2017)

RESEARCH PROJECTS

Automated Security Trust Evaluation for zk-SNARK Proof with Greybox Differential Fuzzing
- Create an innovative greybox fuzzing tool based on AFL that enhances efficiency of input generation and code coverage monitor to detects software crashes, cryptographic errors, and possible forgery in zk-SNARKs proofs to gain higher trust.

SNARKProbe: An Automated Security Analysis Framework for zk-SNARKs Implementations
- Design an automated security analysis framework for zk-SNARKs libraries (e.g. libsnark, bellman, arkworks, circom) to detect various issues, such as edge case crashing, cryptographic operation errors, and/or inconsistencies with protocol.

A Systematic Study of Cryptographic Function Identification Approaches in Binaries
- A survey of identifying cryptographic primitive techniques (e.g. IDA, magic constant, I/O mapping) in binary application by evaluating the state-of-the-art tools to taxonomize their performance, strengths, weaknesses, and future developments.

WORKING EXPERIENCE

School of Optometry, Indiana University Bloomington, Bloomington, IN
Software Developer August 2019 – August 2020
- Developed software programs in MATLAB, specializing in various applications, including contrast sensitivity perimetry, retinal image segmentation, and realistic neural processing simulations to provide accurate and reliable ophthalmic diagnostics for patients.
- Enhanced existing ophthalmic instruments software programs by implementing effective and high-quality methods for data display and image processing.

Department of Electrical Engineering and Computer Science, York University, Toronto, ON
Visiting Scholar June 2019 – August 2019
- Designed an integrated intelligent system to detect and identify vehicle traffic from intersection cameras in the Greater Toronto Area, enabling sensing, analysis, simulation, and 3D visualization of urban mobility.
- Tested and fine-tuned application parameters in real-world scenarios to strengthen the technology sector, improve efficiency, reduce greenhouse gas emissions, and enhance the livability of urban regions in Ontario.

Research Technologies, Pervasive Technology Institute, Bloomington, IN
Application Developer April 2018 – June 2020
- Designed and developed multiple online course systems and course websites about High-Performance Computing Systems from scratch, utilizing HTML, JavaScript, and PHP for both front-end and back-end development.
- Created application programming interfaces (APIs) for course systems to ensure compliance with federal and state student record privacy regulations and facilitate seamless content integration for future system upgrades.
- Collaborated with university students, faculty, and researchers to create engaging and interactive learning platforms.

SKILLS & INTERESTS

Programming: Python, Rust, Java, C/C++, Go, JavaScript, MySQL **Tools:** IDA Pro, VSCode, GDB, Wireshark
Interests: Hiking, Emergency Medical Service, Fire and Rescue, Kayak, Volunteer Income Tax Assistance