Kaiming Huang

814.699.2033 | kzh529@psu.edu | State College, PA

RESEARCH STATEMENT

My primary area of expertise lies in advancing the field of software security, program hardening, static/dynamic program analysis, automatic vulnerability detection, exploit generation, and reverse engineering. My research is driven by the goal of contributing to the development of robust, effective, and efficient defenses against memory-related vulnerabilities. To be more specific, my research aims to ensure the security of systems and software while maintaining cost-effectiveness. I'm dedicated to addressing the evolving challenges in software security that arise from emerging features and the continuous development of programs. My ultimate objective is to strengthen systems against the ever-present cyber threats.

EDUCATION

The Pennsylvania State University — Aug. 2020 - Dec. 2024
Doctor of Philosophy, Computer Science and Engineering — State College, PA, USA

- **Advisor**: Dr. Trent Jaeger

The Pennsylvania State University — Aug. 2018 – Jul. 2020
Master of Science in Computer Science and Engineering — State College, PA, USA

- **Advisor**: Dr. Trent Jaeger

Northeastern University — Oct. 2014 – Jun. 2018
Bachelor of Engineering in Information Security — Shenyang, China

PUBLICATION

Top of the Heap: Efficient Memory Error Protection for Safe Heap Objects — **ACM CCS 2024**
Kaiming Huang*, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, Trent Jaeger.*

OPTISAN: Using Multiple Spatial Error Defenses to Optimize Stack Memory Protection within a Budget — **USENIX Security 2024**
Rahul George, Mingming Chen, ***Kaiming Huang****, Zhiyun Qian, Thomas La Porta, Trent Jaeger.*

Comprehensive Memory Safety Validation: An Alternative Approach to Memory Safety — **IEEE S&P**
Kaiming Huang*, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, Trent Jaeger.*

Assessing the Impact of Efficiently Protecting Ten Million Stack Objects from Memory Errors Comprehensively — **SecDev 2023**
Kaiming Huang*, Jack Sampson, Trent Jaeger.*

Evolving Operating System Kernels Towards Secure Kernel-Driver Interfaces — **HotOS 2023**
Anton Burtsev, Vikram Narayanan, Yongzhe Huang, ***Kaiming Huang****, Gang Tan, Trent Jaeger.*

KSplit: Automating Device Driver Isolation — **OSDI 2022**
Yongzhe Huang, Vikram Narayanan, David Detweiler, ***Kaiming Huang****, Gang Tan, Trent Jaeger, Anton Burtsev.*

The Taming of the Stack: Isolating Stack Data from Memory Errors — **NDSS 2022**
Kaiming Huang*, Yongzhe Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, Trent Jaeger.*

DataGuard: Guarded Pages for Augmenting Stack Object Protections **Master Thesis**
Kaiming Huang.

Employing attack graphs for intrusion detection **NSPW 2019**
*Frank Capobianco, Rahul George, **Kaiming Huang**, Trent Jaeger, Srikanth Krishnamurthy, Zhiyun Qian, Mathias Payer, Paul Yu.*

TALK

The Taming of the Stack: Isolating Stack Data from Memory Errors
GLSD 2021 and CRA Seminar in July 2021, NDSS 2022 in April 2022

EXPERIENCES & PROJECTS

Samsung Research America Security Research Internship, May. 2022 – Aug. 2022

- Deploying Intel CETS to Samsung BIOS packages.
- Analyzing TOCTTOU issue in Samsung BIOS SMM handler.
- Emulating Samsung BIOS SMM for booting in QEMU to launch fuzz testing.

Comprehensive and Practical Memory Safety Defense Research Assistant, Jan. 2020 – Present

- Examined shortcomings of existing protection schemes on stack and heap data
- Leveraged static analysis and guided symbolic execution for verifying the safety of stack and heap memory objects against spatial, type, and temporal memory errors.
- Applied runtime isolation for safe stack and heap objects and remove unnecessary runtime checks.

Memory Safety Validation Assisted Information Flow Analysis Research Assistant, Jan. 2024 – Present

- Identified the shortcoming of existing information flow analyses are unaware of memory errors.
- Leveraged static analysis to automatically identify malicious information flow.

Formalizing Automatic Exploit Generation Research Assistant, Feb. 2021 – Present

- Designed the intermediate representation for synthesizing exploits in compiler backend.
- Investigated and designed the methods for extracting primitives in given vulnerabilities.

Adding Security Plug-ins into IDEs Research Assistant, Feb. 2021 – May. 2022

- Mentored 2 undergraduate students on adding security checks at source code level through plug-ins of CLion.
- Plug-ins designed mainly focused on spatial memory errors.

Detecting and Preventing DFI violations in BOPC Attack Research Assistant, Feb. 2019 – Jun. 2019

- Identified possible Data-Flow Integrity violations in Block-Oriented Programming attack (angr, IDA).
- Designed a lightweight DFI checking for preventing BOPC exploits.
- Augmented BOPC to generate exploits with DFI deployed.

Identifying Potential Step-stone Gadgets in Memory Attack Research Assistant, Jul. 2019 – Dec. 2019

- Used fuzzing and symbolic execution to identify reachable/exploitable objects through memory errors.
- Designed an approach for chaining potentially exploitable memory objects (gadgets) for synthesizing more powerful attacks through initial memory error.

Teaching

Teaching Assistant Software Security (Spring 2022), Python (Spring 2024), System Programming (Fall 2024).
Recitation Instructor Python (Spring 2024).
Student Mentor Mentored 3 Undergraduate Students for thesis related to software security.

Awards & Services

First Prize Scholarship Software College, Northeastern University

Second Prize Chinese Mathematics Modeling Contest for College Students

First Prize Mathematical Modeling Contest of Northeastern University

Reviewer IEEE Transaction of Computers, IEEE Transaction on Industrial Informatics, IET Electronic Letters

External Reviewer USENIX 2019, IEEE S&P 2020, NDSS 2020, USENIX 2020, CCS 2020, NDSS 2021, NDSS 2022, CCS 2023, USENIX 2023, USENIX 2024

SKILLS

Languages : C, C++, Python, Scala, Java, JavaScript, HTML/CSS, SQL, Go, Rust

Tools : LLVM, angr, KLEE, IDA, AFL, Sanitizers, GDB, Burp Suite, Metasploit, Wireshark, Microsoft Office, Latex