

# Kaiming Huang

📍 State College, PA, USA    ✉ kzh529@psu.edu    ☎ +1-814-699-2033    🔗 lightninghkm.github.io

## Research Interest

---

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 developing robust, effective, and efficient defenses against memory-related vulnerabilities while ensuring cost-effectiveness. I am dedicated to addressing the evolving challenges in software security arising from emerging features and continuous software development, with the ultimate objective of strengthening systems against persistent cyber threats. Recently, I have also been exploring the AR/VR Security spaces.

## Education

---

|                                                                                                                                                                                                      |                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <b>The Pennsylvania State University</b><br>Ph.D. in Computer Science and Engineering<br>Advisor: Dr. Trent Jaeger<br>Co-Advisor: Dr. Jack Sampson                                                   | <i>Aug 2020 – May 2025</i> |
| <b>The Pennsylvania State University</b><br>M.S. in Computer Science and Engineering<br>Advisor: Dr. Trent Jaeger<br>Thesis: <i>DataGuard: Guarded Pages for Augmenting Stack Object Protections</i> | <i>Aug 2018 – Jul 2020</i> |
| <b>Northeastern University</b><br>B.Eng. in Information Security                                                                                                                                     | <i>Oct 2014 – Jun 2018</i> |

## Publications

---

1. **SoK: Challenges and Paths Toward Memory Safety for eBPF**  
*Kaiming Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, Trent Jaeger*  
*IEEE S&P (Oakland) 2025*
2. **Top of the Heap: Efficient Memory Error Protection for Safe Heap Objects**  
*Kaiming Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, Trent Jaeger*  
*ACM CCS 2024*
3. **SoK: Understanding the Attack Surface in Device Driver Isolation Frameworks**  
*Yongzhe Huang, Kaiming Huang, Matthew Ennis, Vikram Narayanan, Anton Burtsev, Trent Jaeger, Gang Tan*  
*Arxiv. In submission*
4. **OPTISAN: Using Multiple Spatial Error Defenses to Optimize Stack Memory Protection within a Budget**  
*Rahul George, Mingming Chen, Kaiming Huang, Zhiyun Qian, Thomas La Porta, Trent Jaeger*  
*USENIX Security 2024*
5. **Comprehensive Memory Safety Validation: An Alternative Approach to Memory Safety**  
*Kaiming Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, Trent Jaeger*  
*IEEE Security and Privacy Magazine Special Issue on Memory Safety 2023*
6. **Assessing the Impact of Efficiently Protecting Ten Million Stack Objects from Memory Errors Comprehensively**  
*Kaiming Huang, Jack Sampson, Trent Jaeger*  
*IEEE SecDev 2023*
7. **Evolving Operating System Kernels Towards Secure Kernel-Driver Interfaces**  
*Anton Burtsev, Vikram Narayanan, Yongzhe Huang, Kaiming Huang, Gang Tan, Trent Jaeger*

8. **KSplit: Automating Device Driver Isolation**

*Yongzhe Huang, Vikram Narayanan, David Detweiler, **Kaiming Huang**, Gang Tan, Trent Jaeger, Anton Burtsev*  
*OSDI 2022*

9. **The Taming of the Stack: Isolating Stack Data from Memory Errors**

***Kaiming Huang**, Yongzhe Huang, Mathias Payer, Zhiyun Qian, Jack Sampson, Gang Tan, Trent Jaeger*  
*NDSS 2022*

10. **Employing Attack Graphs for Intrusion Detection**

*Frank Capobianco, Rahul George, **Kaiming Huang**, Trent Jaeger, Srikanth Krishnamurthy, Zhiyun Qian, Mathias Payer, Paul Yu*  
*NSPW 2019*

## Experience

---

**Samsung Research America**

Security Research Intern

*May 2022 – Aug 2022,  
State College, PA*

- Deployed Intel CETs to Samsung BIOS packages.
- Analyzed a TOCTTOU issue in Samsung BIOS SMM handler.
- Emulated Samsung BIOS SMM in QEMU to launch fuzz testing.

**Research Assistant**

Various Projects in Memory Safety and Software Security

*Feb 2019 – Fall 2024,  
State College, PA*

- Investigated advanced memory-safety defenses and exploit generation techniques (e.g., data-flow integrity violations in BOPC) to identify and mitigate security vulnerabilities related to memory errors.
- Employed static analysis and symbolic execution techniques to detect and prevent memory error exploits.
- Explored memory safety validation assisted information flow analysis.
- Explored dedicated defense placement by classifying unsafe objects/operations through static validation.
- Formalized exploit generation by designing intermediate representations and identifying reusable primitives.
- Mentored undergraduates in creating IDE plug-ins that integrate source-level security checks.

## 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 on thesis projects in software security.

## Awards & Services

---

- Student Travel Grant, ACM CCS 2024.
- 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 for IEEE Transactions (Computers, Industrial Informatics), IET Electronic Letters.
- External Reviewer for USENIX, IEEE S&P, NDSS, CCS (2019–2024).

## Skills

---

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

**Tools:** LLVM, angr, KLEE, IDA, Ghidra, GDB, Burp Suite, Metasploit, Wireshark, Microsoft Office, LaTeX.

## References

---

- **Trent Jaeger** — Advisor, Professor, University of California, Riverside. Email: [trentj@ucr.edu](mailto:trentj@ucr.edu)
- **Jack Sampson** — Co-Advisor, Associate Professor, The Pennsylvania State University. Email: [jms1257@psu.edu](mailto:jms1257@psu.edu)
- **Gang Tan** — Collaborator, Professor, The Pennsylvania State University. Email: [gtan@psu.edu](mailto:gtan@psu.edu)
- **Mathias Payer** — Collaborator, Associate Professor, EPFL. Email: [mathias.payer@nebelwelt.net](mailto:mathias.payer@nebelwelt.net)
- **Hayawardh Vijayakumar** — Mentor, Samsung Research America. Email: [h.vijayakuma@samsung.com](mailto:h.vijayakuma@samsung.com)