Zhaohui Wang

zhwang.ku@gmail.com — zhwang@ku.edu — 785-727-3528 — zhwang-ku.github.io
LinkedIn — Github — Google Scholar — ORCID

Research Interests

My research addresses critical security and privacy challenges across the computing stack, ranging from low-level hardware vulnerabilities to high-level application interactions. I tackle these systemic challenges by designing formal models, building systematic analysis frameworks, and creating practical defensive systems that enhance trust and reliability.

- **CPS Security & Privacy:** Privacy Leakage Detection, Security Analysis, Threat Modeling and Risk Mitigation
- **System Security:** Memory Attacks, Integrity Protection, Firmware Hardening, and Vulnerability Analysis
- **Trustworthy AI/ML:** Adversarial Robustness, Secure and Interpretable LLMs, and End-to-End Auditing

Education

- **University of Kansas** — *Lawrence, KS, USA*
  Ph.D. candidate in Computer Science; *Advisors: Prof. Fengjun Li & Prof. Bo Luo* — Aug. 2019 – Present
- **Harbin Institute of Technology** — *Harbin, Heilongjiang, P.R.China*
  M.Eng. in Information and Communication Engineering; *Advisors: Prof. Yubin Xu & Prof. Lin Ma* — Aug. 2013 – Jul. 2015
- **University of Electronic Science and Technology of China** — *Chengdu, Sichuan, P.R.China*
  B.Eng. in Network Engineering — Aug. 2008 – Jul. 2012

Publications

[1] **Zhaohui Wang**, Bo Luo, and Fengjun Li. InteractionShield: Harnessing Event Relations for Interaction Threat Detection and Resolution in Smart Homes. *(Accepted to appear in the Proceedings of ACSAC 2025)*. (***ACSAC Distinguished Paper Award***) *[Acceptance rate: 20%, Artifact: Available, Functional, Reproduced]*

[2] **Zhaohui Wang**, Bo Luo, and Fengjun Li. PrivacyGuard: Exploring Hidden Cross-App Privacy Leakage Threats In IoT Apps. *Proceedings on Privacy Enhancing Technologies (PETS),* 2025, 776-791.
[Acceptance rate: 21%, Artifact: Available, Functional, Reproduced]

[3] Kevin Li, **Zhaohui Wang**, Ye Wang, Bo Luo, and Fengjun Li. Poster: Ethics of Computer Security and Privacy Research - Trends and Standards from a Data Perspective. *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS),* 2023, 3558-3560.

[4] **Zhaohui Wang**, Bo Luo, and Fengjun Li. Poster: SmartAppZoo: a Repository of SmartThings Apps for IoT Benchmarking. *Proceedings of the 8th ACM/IEEE Conference on Internet of Things Design and Implementation (IoTDI),* 2023, 448-449.

[5] Xin Hao, Qiuyu Wu, **Zhaohui Wang**, Changxing Lin. Parallel Timing Synchronization Algorithm and Its Implementation in High Speed Wireless Communication Systems. *2019 International Conference on Electronics, Information, and Communication (ICEIC),* 2019, 1-6.

[6] Xin Hao, **Zhaohui Wang**, Qiuyu Wu, Changxing Lin. A refined phase estimation based parallel carrier recovery algorithm in high speed wireless communication systems. *2018 IEEE 18th International Conference on Communication Technology (ICCT),* 2018, 732-735.

[7] **Zhaohui Wang**, Xin Hao, Changxing Lin, Qiuyu Wu. An efficient hardware LDPC encoder based on partial parallel structure for CCSDS. *2018 IEEE 18th International Conference on Communication Technology (ICCT),* 2018, 136-139.

[8] Qiuyu Wu, Changxing Lin, Bin Lu, Li Miao, Xin Hao, **Zhaohui Wang**, Yi Jiang, Wenqiang Lei, Xianjing Den, Hongbin Chen, Jun Yao, Jian Zhan. A 21 km 5 Gbps real time wireless communication system at 0.14 THz. *2017 42nd International Conference on Infrared, Millimeter, and Terahertz Waves (IRMMW-THz),* 2017, 1-2.

Teaching Experience

- **University of Kansas** — *Lawrence, KS, USA*
  Teaching Assistant
  - EECS 330: Data Structures and Algorithms — Fall 2025
  - EECS 569: Computer Forensics — Fall 2024
  - EECS 565: Introduction to Information and Computer Security — Fall 2023, Fall 2024
  - EECS 447: Introduction to Database Systems — Spring 2024

Professional Experience

- **University of Kansas** *Lawrence, KS, USA*
  Research Assistant May. 2019 – Present

  – **Hardware Fault Attacks and Defenses for AI Infrastructure**
    * Implemented a tool to reverse-engineer DRAM address mappings across diverse CPU microarchitectures
    * Exploited page-table walks to perform Rowhammer attacks, enabling controlled bit-flips for privilege escalation
    * Conducting research on kernel-level program exploitation, exploring cross-privilege boundary vulnerabilities
    * Investigating hardware-level fault injection methods to breach confidentiality and integrity of AI inference

  – **Rule Conflicts Detection and Resolution**
    * Developed a comprehensive framework leveraging logic reasoning to detect and resolve rule conflicts
    * Formalized event relationships and systematically identified event interferences to categorize rule conflicts
    * Employed model checking and SMT solving techniques to identify potential rule conflicts
    * Implemented a genetic algorithm-based method to resolve detected rule conflicts efficiently
    * Provided a GUI integrating real-world environmental factors and physical constraints

  – **Privacy Leakage Detection**
    * Identified a novel cross-app privacy leakage risk in IoT apps and conducted a systematic study on inference threats
    * Formalized cross-app chaining problems and defined trigger-condition-action relations to model interactions between apps
    * Inferred device profiles based on usage context, ensuring accurate modeling for devices with varying sensitivity levels
    * Quantified privacy inference probabilities to assess both direct exposure and implicit inference risks
    * Developed a GUI to provide users with visual insights into privacy risks and enable better decision-making

  – **Large-Scale Real-World IoT App Dataset**
    * Collected and cleaned a large-scale dataset of real-world open-source IoT apps from diverse sources
    * Filtered out invalid apps using regular-expression matching and symbolic execution techniques
    * Eliminated identical and near-duplicate apps by computing fuzzy hashes and applying clustering algorithms

- **Normalyze, Inc.** *Los Altos, CA, USA*
  Security Engineer Intern May. 2022 – Aug. 2022
  Software Engineer Intern May. 2021 – Aug. 2021

  – **Intelligent Document Analytics and Scalable Cloud Deployment**
    * Developed and implemented a document clustering system to automatically group similar documents
    * Designed and built a document classification pipeline for assigning documents to predefined categories
    * Devised algorithms to detect structural and semantic similarities among databases and tables
    * Deployed real-time prediction and clustering modules on AWS, enabling scalable data processing
    * Built and maintained database operations and REST APIs with comprehensive automated tests
    * Optimized Dockerfiles to containerize services and streamline CI/CD for reliable deployments

- **Microsystem & Terahertz Research Center** *Chengdu, Sichuan, P.R.China*
  Assistant Research Scientist Jul. 2015 – Jul. 2019

  – **High-Throughput LDPC Encoder and Decoder**
    * Proposed a fully parallel LDPC encoder based on the Richardson–Urbanke method for high-throughput coding
    * Designed novel partially parallel LDPC decode algorithms optimized for performance and hardware efficiency
    * Implemented LDPC encoders on Xilinx Virtex-7 FPGAs, achieving $>$10 Gbps via pipelined recursive coding
    * Developed an LDPC decoder with LUT-based layered decoding, sustaining 5 Gbps throughput

Presentations

- InteractionShield: Harnessing Event Relations for Interaction Threat Detection and Resolution in Smart Homes, 41st Annual Computer Security Applications Conference (ACSAC), Dec. 11, 2025, Honolulu, HI, USA
- InteractionShield: Harnessing Event Relations for Interaction Threat Detection and Resolution in Smart Homes, 18th Central Area Networking and Security Workshop (CANSec), Oct. 25, 2025, University of Missouri, Kansas City, MO, USA
- PrivacyGuard: Exploring Hidden Cross-App Privacy Leakage Threats In IoT Apps, 25th Privacy Enhancing Technologies Symposium (PETS), Jul. 15, 2025, George Washington University, Washington, DC, USA
- SmartAppZoo: a Repository of SmartThings Apps for IoT Benchmarking, I2S Student Organization (ISO) Meeting, Nov. 3, 2023, University of Kansas, Lawrence, KS, USA

Service and Activities

- Reviewer, Journal of Computer Security (JCS)
- Reviewer, IEEE Transactions on Dependable and Secure Computing (TDSC)
- External Reviewer, 2023 53nd Annual IEEE IFIP International Conference on Dependable Systems and Networks (DSN)
- External Reviewer, 2022 52nd Annual IEEE IFIP International Conference on Dependable Systems and Networks (DSN)
- Session Moderator, EAI SecureComm 2022, Oct. 17-19, 2022, Kansas City, MO, USA
- In-room Judge, Regional Collegiate Cyber Defense Competition, Feb. 11, 2022, Lawrence, KS, USA

Honors and Awards

- ACSAC Distinguished Paper Award — Dec. 2025
  Applied Computer Security Associates
- Top 10% in Roo CTF 2025 — Oct. 2025
  University of Missouri-Kansas City
- ACSAC Student Conferenceship Award — Oct. 2025
  Applied Computer Security Associates
- Graduate Student Travel Fund Award — Oct. 2025
  University of Kansas
- CANSec Travel Grant Award — Oct. 2025
  Central Area Networking and Security Workshop
- GEA Travel Grant — Jul. 2025
  University of Kansas
- David D. and Mildred H. Robb Award — Jun. 2025
  University of Kansas
- First-Class Academic Scholarship — Oct. 2013, Oct. 2014
  Harbin Institute of Technology
- Outstanding Undergraduate Award — Jul. 2012
  University of Electronic Science and Technology of China
- National Encouragement Scholarship — Sep. 2009, Sep. 2011
  University of Electronic Science and Technology of China
- MediaTek First-Class Scholarship — Sep. 2010
  University of Electronic Science and Technology of China
- Second Prize in Chinese Mathematics Competition — Oct. 2009
  University of Electronic Science and Technology of China

Skills

- **Programming:** Python, C, C++, Java, SQL, Go, Assembly, Shell, MATLAB, R, Lua, Nix, Groovy, Javascript, Verilog, VHDL
- **Tools:** AWS, BeautifulSoup, Docker, Git, LaTeX, Matplotlib, NumPy, NuSMV, Pandas, PyTorch, scikit-learn, SciPy, Seaborn, Selenium, spaCy, SPIN, SymPy, Ti*k*Z, Z3

References

- **Prof. Fengjun Li (Advisor)** — *University of Kansas*
  fli@ku.edu — Deane E. Ackers Professor
- **Prof. Bo Luo (Co-advisor)** — *University of Kansas*
  bluo@ku.edu — H.J. and Joan O. Wertz Professor
- **Dr. Yang Zhang** — *Cyberhaven*
  yangzhang.cs@gmail.com — Senior Director of Engineering