Ye Wang

yewang758@gmail.com, yeah_wong@ku.edu | Personal Website
LinkedIn | Github | Google Scholar | ORCID

Research Interest

My research lies at the intersection of system security, sensor-driven computing, machine learning, and user-interactive systems, with a particular emphasis on safeguarding the channels through which humans interact with smart systems. I focus on adversarial attacks, side/covert channels, and the design of practical, user-friendly defenses that address real-world constraints.

- Trustworthy and privacy-preserving ML/AI: Adversarial ML; Prompt injection; AI misinformation and misuse.
- CPS/Mobile security and privacy: Covert and side channels; Sensor-driven adversarial perception; Privacy protection.
- Communication security: NFC; Optical fiber communication; UAV navigation and control-link.

Education

- **University of Kansas** — *Lawrence, Kansas, United States*
  Ph.D. in Computer Science, Department of Electrical Engineering and Computer Science — Jan. 2020 – Present
  Advisor: Prof. Fengjun Li & Prof. Bo Luo
- **Beihang University** — *Beijing, China*
  M.Eng. in Optical Engineering, School of Instrumentation Science and Optoelectronic Engineering — Sep. 2011 – Mar. 2014
  Advisor: Prof. Xiaxiao Wang
- **Beihang University** — *Beijing, China*
  B.S. in Electronic Engineering, School of Instrumentation Science and Optoelectronic Engineering — Sep. 2007 – Jul. 2011
  Advisor: Prof. Zhongyi Chu

Publications

Conference Papers

[C1] **Wang, Ye** and Luo, Bo and Li, Fengjun. Poster: A Novel Fully Sensor-driven Attack Chain. *Annual Computer Security Applications Conference (ACSAC) 2025. Accepted*.

[C2] **Wang, Ye** and Liu, Zeyan and Luo, Bo and Hui, Rongqing and Li, Fengjun. The Invisible Polyjuice Potion: an Effective Physical Adversarial Attack against Face Recognition. *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2024, 3346–3360.

[C3] Li, Kevin and Wang, Zhaohui and **Wang, Ye** and Luo, Bo and Li, Fengjun. 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.

[C4] Fan, Wei and Huang, Weiqing and Zhang, Zhujun and **Wang, Ye** and Sun, Degang. A Near Field Communication (NFC) security model based on the OSI reference model. *2015 IEEE Trustcom/BigDataSE/ISPA*, 2015, 1324–1328.

Journal Papers

[J1] Kong, Qingshan and Kang, Di and **Wang, Ye** and Zhang, Meng and Huang, Weiqing. Eavesdropping Attacks on Optical Fiber Communication and Countermeasure of Optical Fiber Sensing Technology. *Journal of Information Security Research*, 2.2 (2016): 123.

[J2] Wang, Xiaxiao and **Wang, Ye*** and Qin, Yi and Yu, Jia. Ratio error of all fiber optical current transformer caused by mean wavelength's fluctuation. *Infrared and Laser Engineering*, 2015, 44.1 (2015): 233-238.

[J3] Wang, Xiaxiao and Wang, Xichen and **Wang, Ye** and Feng, Xiujuan. A novel Faraday effect-based semi-physical simulation method for bandwidth of fiber-optic gyroscope. *Optik*, 2014, 1358–1360.

[J4] Wang, Xiaxiao and **Wang, Ye*** and Wang, Xichen and Wang, Aimin and Peng, Zhiqiang. Experimental research on the dynamic characteristics of fiber-optical current transformer. *Power System Protection and Control*, 42.3 (2014): 9-14.

[J5] Wang, Xiaxiao and Qin, Yi and **Wang, Ye***. Errors of fiber delay line polarization crosstalk for all fiber optical current sensors. *Optics and Precision Engineering*, 22.11 (2014): 2930-2936.

[J6] Wang, Xiaxiao and **Wang, Ye*** and Li, Chuansheng and others. Measurement method and experimental research of the temperature dependence of the phase delay of quarter-wave plates. *Chinese J Lasers*, 40.12 (2013): 1205004.

Research and Professional Experience

- **Institute for Information Sciences, University of Kansas** — *Lawrence, Kansas, United States*
  Graduate Research Assistant — Jan. 2020 – Present
  - Non-intrusive physical-layer masking for preventing side-channel leaks via accelerometers.
  - Combining motion-sensor side channels with covert vibration channels to form a practical attack chain.
  - Stealthy sensor-enabled logic bombs for Android that evade static analysis, dynamic analysis, and user awareness.
  - Proactive deepfakes face swap defense with identity/context protection and forensic tracing.
  - Develop an effective physical adversarial attack against face recognition CNN models.

- **Institute of Information Engineering, Chinese Academy of Sciences** *Beijing, China*
  Assistant Research Scientist Mar. 2014 – Dec. 2019
  - Designed and implemented GPS spoofing detection techniques for UAV navigation.
  - Developed a fiber-optic communication system security monitoring framework, focusing on intrusion detection.
  - Developed an unauthorized recording device detection system based on weak magnetic signal analysis.
  - Conducted research on security modeling for Near-Field Communication (NFC) devices.

- **Institute of Optoelectronics Technology, Beihang University** *Beijing, China*
  Graduate Research Assistant Sep. 2011 – Mar. 2014
  - Conducted research to improve the dynamic response and measurement accuracy of fiber-optic current transformers.

Honors and Awards

- Doctoral Student Research Fund Award – University of Kansas (KU) 2025
- Graduate Engineering Association Award – KU 2024
- DAVID D. and MILDRED H. ROBB AWARD – EECS, University of Kansas 2024
- ACM CCS Travel Grant Award – ACM SIGSAC, NSF 2024
- Graduate Student Travel Fund – KU Student Senate 2024, 2025
- CANSec Workshop Travel Grant Award – CANSec, NSF 2022, 2024, 2025
- The second prize of the Science and Technology Award – MIIT (PRC) 2019
- Excellent Researcher – Institute of Information Engineering, CAS 2016, 2018
- Outstanding Master's Thesis Award – Beihang University 2014
- Science and Technology Award – Ministry of Education, PRC 2013
- Graduate Guanghua Scholarship – Beihang University 2013
- Outstanding Undergraduate Thesis Award – Beihang University 2011

Teaching Experience

- **Graduate Teaching Assistant**
  University of Kansas
  - EECS 268: Programming II Spring 2025
    Instructor: *Dr. John Gibbons*
  - EECS 569: Computer Forensics Fall 2024
    Instructor: *Dr. Bo Luo*
  - EECS 565: Introduction to Information and Computer Security Fall 2025, 2024, 2023
    Instructor: *Dr. Fengjun Li*
  - EECS 447: Introduction to Database Systems Spring 2024, 2023
    Instructor: *Dr. Bo Luo*
- **Teaching Assistant**
  University of Chinese Academy of Sciences
  - Physical Space Information Security Spring, 2017
    Instructor: *Prof. Degang Sun*

Mentoring Experience

1. Yuying Li, PhD student, The University of Kansas, 01/2025-present
   Project: A novel attack chain to improve the practicality of side channel attacks
2. Weihang Hu, master student, University of Chinese Academy of Sciences, 9/2018-9/2019
   Project: CNN-based electromagnetic spectrum analysis (Master's thesis)
3. Navya Nittala and Sophia Jacob, undergraduate students, The University of Kansas, 5/2024-12/2024
   Project: Motion sensor information leakage protection

Conference Presentation

- Invited talk: A novel fully sensor-driven attack chain, I2S Student Organization (ISO) Meeting, October 23rd, 2025, Nichols Hall, The University of Kansas.
- Agile: An Effective Laser-Based Physical Adversarial Attack against Face Recognition, AI summit *Falling into AI* with Google, October 1st, 2025, Nichols Hall, The University of Kansas.
- The Invisible Polyjuice Potion: An Effective Physical Adversarial Attack against Face Recognition, ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 17th, 2024, Salt Lake City.
- The Invisible Polyjuice Potion: An Effective Physical Adversarial Attack against Face Recognition, The Central Area Networking and Security Workshop (CANSec) 2024, October 12th, 2024, University of Oklahoma, Norman, OK.
- Stealthily evading surveillance-camera face recognition, FBI and KU Cybersecurity Conference, April 4th, 2024, KU Memorial Union, the University of Kansas.
- Laser man against unauthorized facial recognition systems, The I2S Student Research Symposium (ISRS), March 3rd, 2023, Nichols Hall, The University of Kansas.

Professional Memberships

- ACM SIGSAC Membership

Professional Service

Paper Review

- Journal reviewer for Neural Networks
- Journal reviewer for IEEE Transactions on Dependable and Secure Computing (TDSC)
- External paper reviewer: ACM SIGSAC Conference on Computer and Communications Security (CCS 2025)
- External paper reviewer: the 44th IEEE International Conference on Distributed Computing Systems (ICDCS 2024)
- External paper reviewer: Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2023)
- External paper reviewer: the Annual Computer Security Applications Conference (ACSAC 2023)
- External paper reviewer: Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2022)
- External paper reviewer: IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2022)

Community Service

- GenCyber Teacher Camp, Student Volunteer and Teaching Assistant, Funded by NSA and NSF, 2023
- GEA Research Symposium, Student Judge, University of Kansas, 2023
- Session Moderator for EAI SecureComm, 2022

References

- **Dr. Fenjun Li**
  fli@ku.edu
  EECS, University of Kansas
  Deane E. Ackers Professor
- **Dr. Bo Luo**
  bluo@ku.edu
  EECS, University of Kansas
  H.J. and Joan O. Wertz Professor
- **Dr. Rongqing Hui**
  rhui@ku.edu
  EECS, University of Kansas
  Professor

Last Update: 10/2025