Ye Wang

785-727-8235 | yewang758@gmail.com
LinkedIn | Github | Google Scholar | ORCID

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

Research Interest

With a strong academic background in both Electrical Engineering and Computer Science, I bring a unique perspective to security research at the intersection of the physical and digital worlds. Specifically, advanced sensor spoofing attacks and defenses in modern machine-learning back-end systems and user-centric scenarios, with emphasis on:

- Human-imperceptible and out-of-band signal spoofing, where subtle sensor manipulations can bypass robust machine-learning models.
- Legitimate user-interaction–driven spoofing, exploiting natural signals generated through ordinary user behavior to evade detection.
- Integrated side-channel and covert-channel strategies, enabling non-intrusive defenses as well as stealthier, end-to-end attack chains.

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, controlled via a non-intrusive protocol that minimizes detection and resource footprint.
  - 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 Fellow Mar. 2014 – Dec. 2019
  - Conducted research on GPS spoofing of UAV (drone) navigation systems and developed practical detection and mitigation techniques to harden navigation reliability.
  - Developed a fiber-optic communication system security monitoring framework, focusing on intrusion detection.
  - Developed a recording device detection system based on weak magnetic signal analysis, enabling reliable identification of hidden or unauthorized audio recorders.
  - Conducted research on security modeling for Near-Field Communication (NFC) devices, focusing on threat analysis and framework design to enhance secure interactions.

- **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

Publications

[1] **Wang, Ye**, 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.

[2] 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.

[3] Qingshan, Kong, Kang Di, **Wang Ye**, 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.

[4] 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.

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

[6] 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.

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

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

[9] Xiaxiao, Wang, **Ye, Wang***, Chuansheng, Li, 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.

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
2. Weihang Hu, Master Student, University of Chinese Academy of Sciences, 9/2018-9/2019

Conference Presentation and Invited Talks

- 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.
- The Invisible Polyjuice Potion: An Effective Physical Adversarial Attack against Face Recognition, FBI and KU Cybersecurity Conference, April 4, 2024, KU Memorial Union, the University of Kansas.
- The Invisible Polyjuice Potion: An Effective Physical Adversarial Attack against Face Recognition, The I2S Student Research Symposium (ISRS), March 3rd, 2023, Nichols Hall. The University of Kansas.

Professional Memberships

- **ACM SIGSAC Membership**

Honors and Awards

- **Graduate Engineering Association Award** *2024*
  GEA, University of Kansas $500
- **DAVID D. and MILDRED H. ROBB AWARD** *2024*
  EECS, University of Kansas $1,000
- **ACM CCS Travel Grant Award** *2024*
  NSF $1,000
- **Graduate Student Travel Fund** *2024*
  KU Student Senate $750
- **CANSec Travel Grant Award** *2024*
  CANSec committee $500
- **CANSec Travel Grant Award** *2022*
  CANSec committee $500
- **The second prize of the Science and Technology Award** *2019*
  Ministry of Industry and Information Technology of the People's Republic of China. 2nd
- **Excellent Researcher** *2018*
  Institute of Information Engineering, Chinese Academy of Sciences. $3000
- **Excellent Researcher** *2016*
  Institute of Information Engineering, Chinese Academy of Sciences. $3000
- **Science and Technology Award** *2013*
  Ministry of Education of the People's Republic of China.
- **Graduate Guanghua Scholarship** *2013*
  Beihang University. $300

Professional Service

Paper Review

- **Journal reviewer for IEEE Transactions on Dependable and Secure Computing (TDSC).**
- **External paper reviewer for ACM SIGSAC Conference on Computer and Communications Security (CCS '25)**
- **External paper reviewer for the 44th IEEE ICDCS 2024**
- **External paper reviewer for the 52nd Annual IEEE/IFIP (2023 DSN) conference**
- **External paper reviewer for the Annual Computer Security Applications Conference (ACSAC) 2023.**
- **External paper reviewer for the 52nd Annual IEEE/IFIP (2022 DSN) conference**
- **External paper reviewer for the 2022 IEEE TrustCom**

Community Service

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

Organizing committee

- **National Conference on Information Security** 2018
- **National Conference on Information Security** 2016

References

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