WENHAO WANG

(+86)15210983075 ◇ wangwenhao@iie.ac.cn ◇ https://heartever.github.io

EDUCATION

University of Chinese Academy of Sciences *Sept. 2009 - Jan. 2015*
Ph.D. in Information Security
Supervisor: Prof. Dongdai Lin

Ocean University of China *Sept. 2005 - July 2009*
B.E. in Computer Science and Technology

WORK EXPERIENCE

Institute of Information Engineering, CAS *Since Nov. 2018*
Associate Professor

- State Key Laboratory of Information Security
- Courses: Security Chips (40 hours)

Indiana University Bloomington *Apr. 2016 - Aug. 2018*
Visiting Researcher

- Participate in the organization of the iDash privacy & security workshop

Institute of Information Engineering, CAS *Feb. 2015 - Oct. 2018*
Assistant Professor

- State Key Laboratory of Information Security

SELECTED PUBLICATIONS

✉ Corresponding author(s), ___ Advised by me, [ ] Equal Contributions

- *The Road to Trust: Building Enclaves within Confidential VMs*
  Wenhao Wang, Linke Song, Benshan Mei, Shuang Liu, Shijun Zhao, Shoumeng Yan✉, XiaoFeng Wang, Dan Meng, Rui Hou✉
  Network and Distributed System Security Symposium (NDSS) 2025 (CCF-A)
- *Screening Least Square Technique assisted Multivariate Template Attack against the Random Polynomial Generation of Dilithium*
  Haopeng Fan, Hailong Zhang✉, Yongjuan Wang✉, **Wenhao Wang**, Yanbei Zhu, Haojin Zhang, Qingjun Yuan
  IEEE Transactions on Information Forensics and Security (TIFS) (CCF-A)
- *ThermalScope: A Practical Interrupt Side Channel Attack Based On Thermal Event Interrupts*
  Xin Zhang, Zhi Zhang, Qingni Shen, **Wenhao Wang**, Yansong Gao, Zhuoxi Yang, Zhonghai Wu
  The 61st Design Automation Conference (DAC 2024) (CCF-A)

- *Cache attacks on subkey calculation of Blowfish*
  Haopeng Fan,**Wenhao Wang**✉, Yongjuan Wang, Xiangbin Wang, Yang Gao
  Journal of Computer Security (JCS) (CCF-B)
- *PP-Stream: A Privacy-Preserving Neural Network Inference Service with Stream Processing*
  Qingxiu Liu, Qun Huang, Xiang Chen, Sa Wang, **Wenhao Wang**, Shujie Han, Patrick P. C. Lee
  40th IEEE International Conference on Data Engineering (ICDE 2024) (CCF-A)
- *Verifying Rust Implementation of Page Tables in a Software Enclave Hypervisor*
  Zhenyang Dai, Shoumeng Yan, Vilhelm Sjoberg, Yu Chen, **Wenhao Wang**, Hongbo Chen, XiaoFeng Wang, Shubham Sondhi, Laila Elbeheiry, Sean Noble Anderson, Xinyuan Sun, Zhaozhong Ni, Kinnary Dave, Xupeng Li, Yuekai Jia, Yu Zhang, Shuang Liu, Zhengyu He
  International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS 2024) (CCF-A)
- *SegScope: Probing Fine-grained Interrupts via Architectural Footprints*
  Xin Zhang, Zhi Zhang, Qingni Shen, **Wenhao Wang**, Yansong Gao, Zhuoxi Yang, Jiliang Zhang
  30th IEEE International Symposium on High-Performance Computer Architecture (HPCA 2024) (CCF-A)
- *The Danger of Minimum Exposures: Understanding Cross-App Information Leaks on iOS through Multi-Side-Channel Learning*
  [Zihao Wang, Jiale Guan], XiaoFeng Wang, **Wenhao Wang**, Luyi Xing, Fares Alharbi
  ACM Conference on Computer and Communications Security (ACM CCS 2023) (CCF-A)
- *Tossing in the Dark: Practical Bit-Flipping on Gray-box Deep Neural Networks for Runtime Trojan Injection*
  Zihao Wang, Di Tang✉, XiaoFeng Wang, Wei He, Zhaoyang Geng, **Wenhao Wang**✉
  USENIX Security 2024 (CCF-A)
- *WhistleBlower: A System-level Empirical Study on RowHammer*
  [Wei He, Zhi Zhang], Yueqiang Cheng, **Wenhao Wang**✉, Wei Song, Yansong Gao, Qifei Zhang, Kang Li, Dongxi Liu, Surya Nepal
  IEEE Transactions on Computers (TC) (CCF-A)
- *Implicit Hammer: Cross-Privilege-Boundary Rowhammer through Implicit Accesses*
  [Zhi Zhang, Wei He], Yueqiang Cheng, **Wenhao Wang**, Yansong Gao✉, Dongxi Liu, Kang Li, Surya Nepal, Anmin Fu, Yi Zou
  IEEE Transactions on Dependable and Secure Computing (TDSC) (CCF-A)
- *HyperEnclave: An Open and Cross-platform Trusted Execution Environment*
  Yuekai Jia, Shuang Liu, **Wenhao Wang**✉, Yu Chen, Zhengde Zhai, Shoumeng Yan, Zhengyu He
  2022 USENIX Annual Technical Conference (USENIX ATC) (CCF-A)
- *SoftTRR: Protect Page Tables Against RowHammer Attacks using Software-only Target Row Refresh*
  [Zhi Zhang, Yueqiang Cheng], Minghua Wang, Wei He, **Wenhao Wang**✉, Nepal Surya, Yansong Gao, Kang Li, Zhe Wang, Chenggang Wu
  2022 USENIX Annual Technical Conference (USENIX ATC) (CCF-A)
- *Trust Beyond Border: Lightweight, Verifiable User Isolation for Protecting In-Enclave Services*

Wenhao Wang, Weijie Liu, Hongbo Chen, XiaoFeng Wang, Hongliang Tian, Dongdai Lin
IEEE Transactions on Dependable and Secure Computing (TDSC) (CCF-A)

- *BitMine: An End-to-End Tool for Detecting Rowhammer Vulnerability*
  [Zhi Zhang, Wei He], Yueqiang Cheng, **Wenhao Wang**, Yansong Gao✉, Minghua Wang, Kang Li, Surya Nepal, Yang Xiang
  IEEE Transactions on Information Forensics & Security (TIFS) (CCF-A)
- *Practical and Efficient in-Enclave Verification of Privacy Compliance*
  Weijie Liu, **Wenhao Wang**✉, Hongbo Chen, XiaoFeng Wang✉, Xiaozhu Meng, Yaosong Lu, Hongbo Chen, Xinyu Wang, Qingtao Shen, Kai Chen, Haixu Tang, Yi Chen, Luyi Xing
  51st IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2021) (CCF-B)
- *Randomized Last-Level Caches Are Still Vulnerable to Cache Side-Channel Attacks! But We Can Fix It*
  Wei Song, Boya Li, Zihan Xue, Zhenzhen Li, **Wenhao Wang**, Peng Liu
  2021 IEEE Symposium on Security and Privacy (S&P 2021) (CCF-A)
- *Enabling Rack-scale Confidential Computing using Heterogeneous Trusted Execution Environment*
  Jianping Zhu, Rui Hou✉, XiaoFeng Wang✉, **Wenhao Wang**, Jiangfeng Cao, Boyan Zhao, Zhongpu Wang, Yuhui Zhang, Jiameng Ying, Lixin Zhang, Dan Meng
  2020 IEEE Symposium on Security and Privacy (S&P 2020) (CCF-A)
- *Bluethunder: A 2-level Directional Predictor Based Side-Channel Attack against SGX*
  Tianlin Huo, Xiaoni Meng, **Wenhao Wang**✉, Chunliang Hao, Pei Zhao, Jian Zhai, Mingshu Li✉
  IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES 2020) (CCF-B)
- *Beware of Your Screen: Anonymous Fingerprinting of Device Screens for Off-line Payment Protection*
  Zhe Zhou, Di Tang, **Wenhao Wang**, XiaoFeng Wang, Zhou Li, Kehuan Zhang Annual Computer Security Applications Conference (ACSAC 2018) (CCF-B)
- *Correlation Cube Attacks: From Weak-Key Distinguisher to Key Recovery*
  Meicheng Liu, Jingchun Yang, **Wenhao Wang**, Dongdai Lin
  37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt 2018) (CCF-A)
- Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races
  [Guoxing Chen, **Wenhao Wang**✉], Tianyu Chen, Sanchuan Chen, Yinqian Zhang, XiaoFeng Wang, Ten-Hwang Lai, Dongdai Lin
  2018 IEEE Symposium on Security and Privacy (S&P 2018) (CCF-A)
- *A community effort to protect genomic data sharing, collaboration and outsourcing*
  Shuang Wang, Xiaoqian Jiang, Haixu Tang, Xiaofeng Wang, Diyue Bu, Knox Carey, Stephanie OM Dyke, Dov Fox, Chao Jiang, Kristin Lauter, Bradley Malin, Heidi Sofia, Amalio Telenti, Lei Wang, **Wenhao Wang**, Lucila Ohno-Machado
  NPJ genomic medicine
- *iDASH secure genome analysis competition 2017*

XiaoFeng Wang, Haixu Tang, Shuang Wang, Xiaoqian Jiang, **Wenhao Wang**, Diyue Bu, Lei Wang, Yicheng Jiang, Chenghong Wang
BMC Medical Genomics 2018

- *Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX*
  Wenhao Wang, Guoxing Chen, Xiaorui Pan, Yinqian Zhang, XiaoFeng Wang, Vincent Bindschaedler, Haixu Tang, Carl A. Gunter
  2017 ACM Conference on Computer and Communications Security (CCS 2017) (CCF-A)

MANUSCRIPTS

✉ Corresponding author(s), ___ Advised by me, [ ] Equal Contributions

- *CryptPEFT: Parameter-Efficient Fine-Tuning for Privacy-Preserving Neural Network Inference*
  Saisai Xia, **Wenhao Wang**✉, Zihao Wang, Yuhui Zhang, Yier Jin, Dan Meng, Rui Hou
  In submission
- *Learning from Proof-of-Concepts: Hybrid Fuzzing of Deep Learning Compilers and Libraries*
  Zizhuang Deng, Sanchuan Chen, Guozhu Meng, **Wenhao Wang**, Tong Liu, Xueqing Zhang, Yidi Kao, Kai Chen
  In submission
- *The Early Bird Catches the Leak: Unveiling Timing Side Channels in LLM Serving Systems*
  [Linke Song, Zixuan Pang], **Wenhao Wang**✉, Zihao Wang, XiaoFeng Wang, Hongbo Chen, Wei Song, Yier Jin, Dan Meng, Rui Hou
  In submission
- *virtCCA: Virtualized Arm Confidential Compute Architecture with TrustZone*
  Xiangyi Xu, **Wenhao Wang**✉, Yongzheng Wu, Zhennan Min, Zixuan Pang, Yier Jin✉
  In submission
- *Understanding TEE Containers, Easy to Use? Hard to Trust*
  [Weijie Liu, Hongbo Chen], XiaoFeng Wang, Zhi Li, Danfeng Zhang, **Wenhao Wang**, Haixu Tang
  In submission
- *Toward Scalable Fully Homomorphic Encryption Through Light Trusted Computing Assistance*
  Wenhao Wang, Yichen Jiang, Qintao Shen, Weihao Huang, Hao Chen, Shuang Wang, XiaoFeng Wang, Haixu Tang, Kai Chen, Kristin Lauter, Dongdai Lin

PATENTS

- *System for decentralized ownership and secure sharing of personalized health data*
  Shuang Wang, XiaoFeng Wang, Haixu Tang, **Wenhao Wang**, Ali Farahanchi, Hao Zheng
  US Patent 11,003,791

PROFESSIONAL SERVICES

- Reviewer for journals *IEEE TDSC*, *IEEE Security & Privacy*, *IEEE TC*, *ACM Transactions on Privacy and Security*, *CyberSecurity*, *SCN*, *JNCA*.

- Sub-reviewer for *CCS* (2018, 2020), *NDSS* (2017, 2018, 2021), *S&P* (2017, 2020, 2021), *Usenix Security* (2017, 2018, 2021), *HPCA* (2019), *ESORICS* (2018, 2020), Asiacrypt (2020), *AsiaCCS* (2017, 2018, 2019) and *RECOMB* (2019) etc.
- TPC member for *ACM CCS 2019*, *GenoPri (2020, 2021)*, *ACNS (2023)*.
- General Chair for *Inscrypt 2022*.

AWARDS

- 2018 ACM SIGSAC China Rising Star Award, and ACM China Rising Star Nomination Award
- 2017 Young Star Award of Institute of Information Engineering, CAS

TALKS

- *Confidential Computing, in Chinese*. China Conference on Data Security and Privacy (ChinaPrivacy2019), Oct. 2019, Guilin
- *Confidential Computing, in Chinese*. Nankai University, July 2019, Tianjin
- *Side Channel Risks in Hardware Trusted Execution Environments (TEEs)*, Institute of Software, July 2019, Beijing
- *Side Channel Risks in Hardware Trusted Execution Environments (TEEs)*. ACM TURC 2019 (SIGSAC), May 2019, Chengdu
- *Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX*. ACM CCS 2017, Nov. 2017, Dallas