ZIHAO ZHAN

Texas Tech University, Department of Computer Science, Box 43104, Lubbock, TX, 79409
(+1) 6154231315 ⋄ zihao.zhan@ttu.edu

EDUCATION

Vanderbilt University *Aug 2018 - Oct 2021*
Ph.D. in Electrical Engineering

Vanderbilt University *Aug 2016 - Aug 2018*
M.S. in Electrical Engineering

University of Science and Technology of China *Aug 2012 - May 2016*
B.S. in Physics

RESEARCH INTERESTS

System Security, Computer Architecture, Hardware Security

WORK EXPERIENCES

Texas Tech University *Jul 2024 - Present*
Assistant Professor

University of Florida *Oct 2021 - Jul 2024*
Postdoctoral Associate

HORNORS AND AWARDS

Distinguished paper award at the 2022 IEEE Symposium on Security and Privacy (**Oakland'22**)

Runner-up for the 2021 C.F. Chen Best Graduate Student Paper Award

Best paper nomination at the 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST '20)

PUBLICATIONS

[**CCS'24**] Hanqiu Wang, **Zihao Zhan**, Haoqi Shan, Siqi Dai, Max Panoff, and Shuo Wang. Gazeploit: Remote keystroke inference attack by gaze estimation from avatar views in vr/mr devices. pages 1731–1745, 2024

[**Security'24**] **Zihao Zhan**, Yirui Yang, Haoqi Shan, Hanqiu Wang, Yier Jin, and Shuo Wang. Voltschemer: Use voltage noise to manipulate your wireless charger. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 3979–3995, 2024

[DATE'24] Hanqiu Wang, Max Panoff, Zihao Zhan, Shuo Wang, Christophe Bobda, and Domenic Forte. Programmable em sensor array for golden-model free run-time trojan detection and localization. In *2024 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pages 1–6. IEEE, 2024

[**Oakland'22**] **Zihao Zhan***, Zhenkai Zhang*, Sisheng Liang, Fan Yao, and Xenofon Koutsoukos. Graphics peeping unit: Exploiting em side-channel information of gpus to eavesdrop on your neighbors. In *2022 IEEE Symposium on Security and Privacy*, pages 1440–1457. IEEE, 2022. (* Co-first author)

[**Oakland'22**] Haoqi Shan, Boyi Zhang, **Zihao Zhan**, Dean Sullivan, Shuo Wang, and Yier Jin. Invisible finger: Practical electromagnetic interference attack on touchscreen-based electronic devices. In *2022 IEEE Symposium on Security and Privacy*, pages 1246–1262. IEEE, 2022. **(Distinguished paper award)**

[WOOT'22] Sisheng Liang, **Zihao Zhan**, Fan Yao, Long Cheng, and Zhenkai Zhang. Clairvoyance: Exploiting far-field em emanations of gpu to" see" your dnn models through obstacles at a distance. In *2022 Workshop on Offensive Technologies*. IEEE, 2022

[HaSS] **Zihao Zhan**, Zhenkai Zhang, and Xenofon Koutsoukos. A high-speed, long-distance and wall-penetrating covert channel based on em emanations from dram clock. *Journal of Hardware and Systems Security*, 6(1-2):47–65, 2022

[HOST'20] **Zihao Zhan**, Zhenkai Zhang, and Xenofon Koutsoukos. Bitjabber: The worlds fastest electromagnetic covert channel. In *2020 IEEE International Symposium on Hardware Oriented Security and Trust*, pages 35–45. IEEE, 2020. **(Best paper nomination)**

[**Oakland'20**] Zhenkai Zhang*, **Zihao Zhan***, Daniel Balasubramanian, Bo Li, Peter Volgyesi, and Xenofon Koutsoukos. Leveraging em side-channel information to detect rowhammer attacks. In *2020 IEEE Symposium on Security and Privacy*, pages 862–879. IEEE, 2020. (* Co-first author)

[ASHES'18] Zhenkai Zhang, **Zihao Zhan**, Daniel Balasubramanian, Xenofon Koutsoukos, and Gabor Karsai. Triggering rowhammer hardware faults on arm: A revisit. In *Proceedings of the 2018 Workshop on Attacks and Solutions in Hardware Security*, pages 24–33, 2018

PRESENTATIONS

Invited Talks

· Defenses and Attacks Leveraging Far-field Electromagnetic Side-channel Information.@ the University of Delaware, 2022.

Conferecne Presentations

· VoltSchemer: Use Voltage Noise to Manipulate Your Wireless Charger. @ the 2024 USENIX Security Symposium
· Graphics peeping unit: Exploiting EM Side-channel Information of GPUs to Eavesdrop on Your Neighbors. @ the 2022 IEEE Symposium on Security and Privacy.
· Clairvoyance: Exploiting Far-field EM Emanations of GPU to "SEE" Your DNN Models Through Obstacles at A Distance. @ the 2022 IEEE Workshop on Offensive Technologies
· BitJabber: The World's Fastest Electromagnetic Covert Channel. @ the 2020 IEEE International Symposium on Hardware Oriented Security and Trust
· Triggering Rowhammer Hardware Faults on ARM: A Revisit. @ the 2018 Workshop on Attacks and Solutions in Hardware Security.

PROFESSIONAL SERVICES

Program Committee 34th Great Lake Symposium on VLSI, 2024
Publicity Chair 2nd EAI SmartSP, 2024