ZIHAO ZHAN

327 Benton Hall, University of Florida, Gainesville, FL, 32611
(+1) 6154231315 ⋄ zhan.zihao@ufl.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

University of Florida *Oct 2021 - Present*
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

[**Security'24**] **Zihao Zhan**, Yirui Yang, Haoqi Shan, Hanqiu Wang, Yier Jin, and Shuo Wang. Use voltage noise to manipulate your wireless charger. *Accepted in 2024 USENIX Security Symposium*

[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. *Accepted in 2024 Design, Automation and Test in Europe Conference*

[**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

· 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.