Cheng Shen

CECA, Peking University (Lab)
100871 (Postal code)

15010038536 (Tel)
chengshen@pku.edu.cn (Email)
chengshen.space (Home page)

Education

- **Peking University** *EECS·Computer System Structure* 2018.09 – Now Ph.D. candidate
- **Peking University** *EECS·Machine Intelligence* 2014.09 – 2018.06 Bachelor's degree

Internship

- **Huawei** *CSPL, 2012 Lab* 2021.08 – 2022.08 Full-time
  - Hardware authentication and covert communication based on electromagnetic side channel.
- **HiSilicon** *ALPHA LAB, Kirin Solution* 2021.08 – 2022.08 Full-time
  - Chip security implementation test and wireless side-channel attack.
- **MSRA** *System Research Group* 2020.12 – 2021.08 Full-time
  - Study the threat of computer's electromagnetic leakage to users' privacy.

Research

- My main research interest lies in information security related to electromagnetic radiation (EMR) side channels in computing systems. In particular, I am committed to provide a off-load security monitoring system for smart devices through sensing EM leakage of computing behavior.
- **Computers are whispering all the time through the EM leakage.** By sensing and understanding such language of the computer, we can learn the running state of devices, which helps enhance user's privacy security. My current work can be divided into three parts:

  1) Learning: By analyzing the circuit structure and the data transmission process in the computing system, construct the generation model of EM leakage to realize the in-depth understanding of the EM signal's characteristics.

  2) Hearing: Customize the wireless sensing algorithms based on the characteristics of EM signals, which is aimed to distinguish and track EM signals from different targets at a longer distance and finer granularity in the crowded wireless communication environment.

  3) Translating: Extract sensitive computing behaviors from collected EM signals to enhance privacy security in real security scenarios such as computing device authentication and software legality check.

Publications

- **EarFisher: Detecting Wireless Eavesdroppers by Stimulating Memory EMR**
  - USENIX NSDI 2021 First Author (First from PKU)
  - Description: EarFisher is the first system that can detect wireless eavesdroppers and differentiate them from legitimate receivers. Prior to this work, there has been a lack of effective methods to detect eavesdroppers although eavesdropping is a fundamental threat to the wireless communication. EarFisher stimulates eavesdroppers to show up on EM side channels by actively releasing bait traffic. And in the actual deployment case, EarFisher achieves accurate detection and location of eavesdroppers in an indoor environment of 1600 ft^2 at cost of $150.
- **When LoRa Meets EMR: Electromagnetic Covert Channels Can Be Super Resilient**
  - IEEE S&P 2021 First Author

  - Description: EMLoRa is the first EM covert channel attack that is super resilient to attenuation. EMLoRa challenges the high attenuation shielding by converting the memory bus into a LoRa transmitter. The experiment results show that EMLoRa can achieve 100m-level transmission in the outdoor environment, which also poses a serious threat to the TEMPEST standard developed by NATO.

- **Electromagnetic Fingerprinting of Memory Heartbeats: System and Applications**
  - ACM UbiComp 2022 First Author
  - Description: In this paper, we propose MemScope, an EM sensing system that senses and fingerprints memory heartbeats. MemScope uses the rich spectral characteristics of the EM signals from the memory bus to build stable and robust device fingerprints. The experiment results show that combined with the customized signal sensing algorithms, MemScope can detect illegitimate devices, such as rogue APs and hidden cameras, over a distance of 30m in the actual office environment.

Projects

- **AI-based Security Test of On-chip Encryption Implementation** *HiSilicon* 2022.01-2022.03
  - Description: This project attempts to evaluate the side channel information leakage during the running of on-chip encryption through AI technology. In the preliminary work, I am mainly responsible for **migrating** the existing side channel analysis models to the mainstream Pytorch platform and **optimizing** the model structure. Furthermore, for the RSA implementation on the Hi-XXXX chip, I am responsible for designing the neural network for **pseudo-wheel recognition** and **random number recognition**, and proposed revisions to the related implementations on subsequent chips.
- **Wireless Side Channel Platform Construction** *HiSilicon* 2021.08-2022.01
  - Description: By introducing **wireless signal processing**, this project extends the applicable scope of intrusive side-channel analysis to wireless scenarios, greatly expanding the applicable scenarios of side-channel technology and reducing equipment costs. This project starts from the **substrate coupling** of the RF chip, and extends the distance of AES key cracking to 3m in the office environment. I am also trying to build the **MIMO platform** to further improve the analysis distance.
- **Security Monitoring Based on Side-channel** *Huawei* 2021.12-2022.03
  - Description: Using physical side-channel information to build the identity and behavior authentication system for smart devices. I am mainly involved in the design of three works including: **Bluetooth car key authentication** based on carrier frequency offset, **optical fiber eavesdropping detection** based on optical phase offset, and the design and implementation of **SRAM PUF algorithms**.
- **EMRadar: EM Side-channel Threats Evaluation System** *MSRA* 2021.03-2021.08
  - Description: EMRadar can automatically evaluate the risk of leakage of information that users care about in the EM signals from target devices. Drawing on the speech recognition system, EmRadar uses a **point classifier** to extract the privacy-related signals in the long-term EM traces. The extracted EM signals are fed into candidate ML algorithms to assess the granularity of information leakage. During the above process, the signals are converted into timestamp-level representation and instance-level representation with **TS2Vec** to resist possible signal distortion. The system ultimately informs the user at what distance and at what time granularity the attacker is likely to obtain their privacy.

Awards

- **Huawei Genius Youth** 2022.04
- **Academic Innovation Award of Peking University (Top 1% in PKU)** 2021.12
- **Nomination Award of the MSRA Fellowship (28 people in Asian)** 2021.10
- **Peking University President Scholarship (Top 1% in PKU)** 2021.06
- **Peking University Merit Student Award (Top 5% in PKU)** 2020.11