Zelun Kong

Email | (469) 847-2815 | GitHub | Zelun Kong

EDUCATION

The University of Texas at Dallas — **Dallas, TX, US**
Computer Engineering — *Ph.D. Student, August 2019 – Present*

The University of Texas at Dallas — **Dallas, TX, US**
Computer Science — *M.S., August 2017 – May 2018*

Wuhan University — **Wuhan, Hubei, China**
Computer Science — *B.S., September 2012 – June 2016*

RESEARCH INTERESTS

Cyber-Physical System Security – Enhancing security of existing or build security-aware CPS.
IoT Systems Security and Privacy – Enhancing the security and privacy of IoT systems.
Adversarial Machine Learning – Attacks and defenses against attacks on ML models.

PUBLICATIONS

1. **Zelun Kong**, Minkyung Park, Le Guan, Ning Zhang, Chung Hwan Kim.
   TZ-DATASHIELD: Automated Data Protection for Embedded Systems via Data-Flow-Based Compartmentalization
   Proceedings of the 2025 Network and Distributed System Security Symposium (NDSS 2025).
2. Bangjie Yin, Wenxuan Wang, Taiping Yao, Junfeng Guo, **Zelun Kong**, Shouhong Ding, Jilin Li, Cong Liu.
   Adv-makeup: A new imperceptible and transferable attack on face recognition
   Proceedings of the 2021 International Joint Conferences on Artificial Intelligence (IJCAI 2021).
3. **Zelun Kong**, Junfeng Guo, Ang Li, Cong Liu.
   PhysGAN: Generating Physical-World-Resilient Adversarial Examples for Autonomous Driving
   Proceedings of the 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2020).
4. Husheng Zhou, Wei Li, **Zelun Kong**, Junfeng Guo, Yuqun Zhang, Bei Yu, Lingming Zhang, Cong Liu.
   DeepBillboard: systematic physical-world testing of autonomous driving systems
   Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering (ICSE 2020).
5. Zhuoyi Wang, **Zelun Kong**, Swarup Changra, Hemeng Tao, Latifur Khan.
   Robust High Dimensional Stream Classification with Novel Class Detection
   Proceedings of the IEEE 35th International Conference on Data Engineering (ICDE 2019).
6. Zhuoyi Wang, Hemeng Tao, **Zelun Kong**, Swarup Chandra, Latifur Khan.
   Metric Learning based Framework for Streaming Classification with Concept Evolution
   Proceedings of the 2019 International Joint Conference on Neural Networks (IJCNN 2019).
7. Zheng Dong, Cong Liu, Soroush Bateni, **Zelun Kong**, Liang He, Lingming Zhang, Ravi Prakash, Yuqun Zhang
   A General Analysis Framework for Soft Real-Time Tasks
   IEEE Transactions on Parallel and Distributed Systems (TPDS 2019).

EXPERIENCE

The University of Texas at Dallas **Dallas, TX, US**

Research Assistant *January 2019 – present*

- Ongoing research on robotic root cause investigation using static analysis technology and ML-based log analysis.
- Published TZ-DATASHIELD in NDSS 2025, used TEE (TrustZone) and LLVM compiler infrastructure to enhance security of MCU-based embedded system security.
- Published *PhysGAN* and *Deepbillboard* in CVPR (first author) and ICSE, utilized CV technologies to find the vulnerabilities of the steering model of autonomous driving systems through physical-world adversarial examples.
- Published two papers in ICDE and IJCNN about stream data classification and novel class detection.
- Published *Adv-Makeup*, collaborated with Tencent YouTu Research and designed a unified adversarial face generation method to help find vulnerabilities of face recognition models.
- Published a soft real-time tasks analysis framework in TPDS.

Futurewei Technologies Inc. **Plano, TX, US**

Research Intern of Baseband SoC Team *June 2019 – August 2019*

- Developed a reinforcement learning-based scheduling algorithm for resource-limited embedded systems.

TEACHING

The University of Texas at Dallas

- CS/SE 4348 (Guest Lecture): Operating Systems Concepts