

Zelun Kong

🏠 Homepage | ✉ Email | ☎ (469) 847-2815 | 🌐 GitHub | 🎓 Zelun Kong

EDUCATION

Ph.D.	present	University of Texas at Dallas	Dallas, TX, US	Computer Engineering
Ph.D.	2021	University of Texas at Dallas	Dallas, TX, US	Computer Science
M.S.	2019	University of Texas at Dallas	Dallas, TX, US	Computer Science
B.S.	2016	Wuhan University	Wuhan, Hubei, China	Computer Science

RESEARCH INTERESTS

- **Cyber-Physical and Robotic System Security** — predictive runtime monitoring, failure detection, incident root cause analysis, and forensic analysis
- **Computer System Security** — trusted execution environments (TEE), ARM TrustZone, Intel SGX, and secure system architectures
- **AI for Security** — machine learning-based intrusion/fault detection, autonomous system protection
- **Adversarial Machine Learning** — attack and defense techniques for learning models in safety- and mission-critical applications

PUBLICATIONS

1. Minkyung Park, **Zelun Kong**, Dave (Jing) Tian, Z. Berkay Celik, Chung Hwan Kim.
DNN Latency Sequencing: Extracting DNN Architectures from Intel SGX Enclaves with Single-Stepping Attacks
In Proceedings of the 33rd Network and Distributed System Security Symposium (NDSS 2026).
2. Sudharssan Mohan, Kyeongseok Yang, **Zelun Kong**, Yonghwi Kwon, Junghwan "John" Rhee, Tyler Summers, Hongjun Choi, Heejo Lee, Chung Hwan Kim.
IMUFUZZER: Resilience-based Discovery of Signal Injection Attacks on Robotic Aerial Vehicles
In Proceedings of the 40th IEEE/ACM International Conference on Automated Software Engineering (ASE 2025).
3. **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).
4. 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).
5. **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).
6. 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).
7. 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).
8. 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).
9. 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).

HONORS AND AWARDS

- Student Conference Grants from ACM CCS 2022.
- Student Travel Grants from SecDev 2022.

EXPERIENCE

Visiting Scholar	Department of Computer Science Purdue University, West Lafayette, IN, US	<i>05/2025 – 08/2025</i>
Research Assistant	Department of Computer Science Department of Electrical & Computer Engineering University of Texas at Dallas, Richardson, TX, US	<i>01/2019 – present</i>
Research Intern	Futurewei Technologies Inc.	<i>05/2019 – 08/2019</i>

Academic Service

The University of Texas at Dallas

- Conference Reviewer
 - USENIX Security Symposium, 2025
- Journal Reviewer:
 - Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)
 - IEEE Transactions on Intelligent Vehicles (ITIV)

TEACHING

The University of Texas at Dallas

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