Zelun Kong

zelun.kong@outlook.com | (469) 847-2815 | lz3450 | Zelun Kong

EDUCATION

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

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

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

PUBLICATIONS

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

RESEARCH INTERESTS

Cyber-Physical System Security – Making CPS, such as robotics, self-driving vehicles, and drones, more usable by improving security assurance, detecting runtime errors, and investigating bug root causes.
IoT Systems Security and Privacy – Enhancing the security and privacy of IoT systems by applying TEE-based trusted computing.
Adversarial Machine Learning – Attacks and defenses against such attacks on machine learning models.

EXPERIENCE

The University of Texas at Dallas — **Dallas, TX, US**
Research Assistant — *January 2019 – present*

- Ongoing research on robotic system bug root cause investigation and runtime error detection using static analysis technology and ML-based log analysis.
- Ongoing research on MCU-based embedded system security enhancement using TEE (TrustZone) and LLVM compiler infrastructure.
- 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 two papers in ICDE and IJCNN about stream data classification and novel class detection.
- 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 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: Operating Systems Concepts

HONORS AND AWARDS

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

CURRENT RESEARCH PROJECTS

AutoTrace *(Ongoing project)*
AutoTrace is designed to be a bug root cause finding and runtime error detection framework for complex systems, like Autonomous Driving Systems (ADS) and Robotic Systems (RS), which is expected to automatically generate inputs according to the system's computational model and misbehavior for the components of the system to reproduce, locate the bugs and further find the root causes of the bugs.
- An ADS or RS consists of multiple layers intertwined in a complicated way, and safety-critical bugs may exist in any layer and even across layers.
- Reproducing the ADS bugs is challenging since any subtle changes (like physical environment changes and vehicle shifts) in the inputs may result in different behavior of ADS.
- Locating ADS bugs is also challenging because a single bug of ADS may originate from one layer or even across layers.
- AutoTrace aims to develop a framework to find the fundamental causes of ADS bugs, making the bugs reproducible and easy to locate.

Particles *(Ongoing project)*
Particles is a framework that aims to protect security-critical peripherals and data in an MCU-based embedded system from unauthorized accesses from the non-secure world while maintaining isolation between components in the secure world.
- Many MCU-based embedded systems, such as IoT, are equipped with peripherals (sensors and actuators) that are targeted by attacks to steal sensitive data or control the peripherals maliciously.
- Existing work using privileged software to isolate peripherals from such attacks may be bypassed by strong adversaries.
- Trusted Execution Environment (TEE, like ARM TrustZone) for MCUs can be used to isolate peripherals from such adversaries.
- Naively using TEE to protect all security-critical components results in a large TCB that is undesired for security and there is no isolation between untrusted components.
- Particles are designed to utilize static program analysis and LLVM passes to generate sandboxed compartments for these peripherals.
- Particles significantly reduces TCB by allowing the system to operate peripherals through the sandboxed compartments.

SKILLS

Programming Languages
C/C++, Python, Rust, Javascript, C#, Java
Machine Learning Frameworks
Pytorch