赵 哲

上海市浦东新区中科路 1 号上海科技大学

zhaozhe1@shanghaitech.edu.cn

教育经历

上海科技大学 **上海**

博士研究生（硕博连读）：计算机软件与理论 2018 年 9 月至今

- 研究领域为 AI 安全: 导师：宋富教授
  - 对抗样本生成与防御，
  - 神经网络测试与验证。
- GPA: 3.96/4.0
- 就读期间获**国家奖学金**，校级三好学生

上海科技大学 **上海**

访问学生 2018 年 3 月至 2018 年 9 月

中国海洋大学 (985，211) **山东，青岛**

工学学士，国家保密学院：计算机科学与技术 2012 年 8 月至 2016 年 6 月

- 曾获**国家励志奖学金**，市级优秀志愿者，校级社会实践奖学金、优秀学生、优秀学生干部、优秀毕业生等

工作经历

Hewlett-Packard（HP，惠普） 2016 年 7 月至 2017 年 11 月

测试开发工程师，负责自动化测试、性能测试脚本编写，自动化测试培训等 上海

论文发表

博士期间已发表四篇高质量学术论文，其中两篇为第一作者（含共同一作），另有两篇一作论文在投。

4. [**CCF-A**] **Zhe Zhao**, Guangke Chen, Jingyi Wang, Yiwei Yang, Fu Song, Jun Sun. *Attack as Defense: Characterizing Adversarial Examples using Robustness.* ISSTA 2021

3. [**CCF-A**] Yedi Zhang, **Zhe Zhao**, Guangke Chen, Fu Song, Taolue Chen. *BDD4BNN: A BDD-based Quantitative Analysis Framework for Binarized Neural Networks.* CAV 2021

2. [**CCF-A**] Guangke Chen, Sen Chen, Lingling Fan, Xiaoning Du, **Zhe Zhao**, Fu Song, Yang Liu. *Who is Real Bob? Adversarial Attacks on Speaker Recognition Systems.* S&P Oakland 2021

1. [**CCF-A**] Lei Bu†, **Zhe Zhao**†, Yuchao Duan, Fu Song. *Taking Care of The Discretization Problem: A Comprehensive Study of the Discretization Problem and A Black-Box Adversarial Attack in Discrete Integer Domain.* TDSC, early access, †co-first author

科研竞赛

- 百度 AI 安全对抗赛 **第一名** 2019 年 12 月
- 阿里安全-CVPR 2021：防御模型的白盒对抗攻击竞赛 **第三名** 2021 年 3 月
- 阿里安全-ACM MM 2021：针对电商标识检测的鲁棒性防御比赛 **第三名** 2021 年 7 月
- OPPO 安全 AI 挑战赛 **优胜奖** 2021 年 12 月

志愿服务

论文审稿人 ISSRE 2021, ICICS 2021, CAV 2020, ICECCS 2022 2020 2019

学生志愿者 ISSTA 2019

助教 曾任 CS132（软件工程）课程助教，获评信息学院卓越助教奖