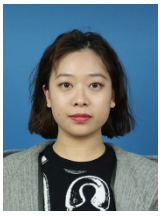
韩歌



+86 13573188377
hangehg@126.com

教育经历

山东大学 济南，中国
计算机科学与技术博士生（预计毕业时间 2024.06） 2017.09 ~ Present
计算机科学与技术学院

CISPA (Helmholtz Center for Information Security) 萨尔布吕克，德国
联合培养博士生 2019.10 ~ 2021.09

University of Bristol 布里斯托，英国
理学硕士，高级计算——网络安全技术 2014.09 ~ 2016.02
计算机科学、电气与电子工程与工程数学学院

Loughborough University 拉夫堡，英国
访学生，计算机科学 2013.09 ~ 2014.06
理学院

山东大学 威海，中国
理学学士，电子信息科学与技术 2010.09 ~ 2014.06
机电与信息工程学院

工作经历

北京卓识网安技术股份有限公司 济南，中国
质检工程师 2016.02 ~ 2016.07

- 负责电力企业信息系统的安全检查、整改加固咨询、等级防护评估、行业安全风险评估等工作。
- 参与国家及能源电力行业信息安全标准规范的制定。

研究方向

- 深度学习模型的安全研究，包括鲁棒性、隐私性、可问责性等安全属性。
- 深度学习在安全相关领域的应用，包括隐写、模糊测试等。

掌握技能

语言技能：熟练掌握英语的听说读写。
专业技能：熟练掌握 C++和 Python 编程，熟悉嵌入式编程，MATLAB, Web 技术，密码学等。

项目经历

基于人工智能平台的深度学习系统的模糊测试和修复技术研究 济南，中国
2023.01 ~ 2023.12

- 国家电网公司科学技术项目。
- 研究面向深度学习模型的模糊测试技术以及深度学习系统的漏洞自动化修复技术。

机器学习驱动的智能软件漏洞挖掘 济南，中国
2019.12 ~ 2022.12

- 国防科技创新特区项目。
- 研究机器学习模型的测试技术，以确保模型的安全性和公平性。
- 完成论文《FuzzGAN: A Generation-Based Fuzzing Framework For Testing Deep Neural Networks》。

山东省电力企业网络与信息安全监管体系研究 济南，中国
2014.12 ~ 2015.09

- 参与设计《山东省电力企业网络与信息安全监管系统(初稿)》

研究成果

- PRJack: Pruning-Resistant Model Hijacking Attack against Deep Learning Models.
  （投稿中）International Joint Conference on Neural Networks (IJCNN), 2024.
  Ge Han, Zheng Li, Shanqing Guo

- Detection and Attribution of Models Trained on Generated Data.
  IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2024.
  Ge Han, Ahmed Salem, Zheng Li, Shanqing Guo, Michael Backes, Yang Zhang

- FuzzGAN: A Generation-Based Fuzzing Framework For Testing Deep Neural Networks.
  The 24th IEEE International Conference on High Performance Computing and Communications (HPCC), 2022.
  Ge Han, Zheng Li, Peng Tang, Chengyu Hu, Shanqing Guo

- DeepKeyStego: Protecting Communication by Key-dependent Steganography with Deep Networks.
  The 21st IEEE International Conferences on High Performance Computing and Communications (HPCC), 2019.
  Zheng Li, **Ge Han**, Shanqing Guo

- FragDroid: Automated User Interface Interaction with Activity and Fragment Analysis in Android Applications.
  The 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018.
  Jia Chen, **Ge Han**, Shanqing Guo, Wenrui Diao

- Evaluation and Integration of Bit-Sliced Block Ciphers.
  （学位论文）University of Bristol, UK, 2015.
  Ge Han

- Microcontroller Based Light Control System.
  （学位论文）Loughborough University, UK, 2014.
  Ge Han