Ge Han

+86 13573188377
hangehg@126.com

EDUCATION

Shandong University Jinan, China
Ph.D. Candidate in Computer Science and Technology, expected June, 2024 2017.09 ~ Present
School of Computer Science and Technology

CISPA (Helmholtz Center for Information Security) Saarbrücken, Germany
Visiting Ph.D. Student supported by China Scholarship Council 2019.10 ~ 2021.09

University of Bristol Bristol, UK
MSc in Advanced Computing – Internet Technologies with Security 2014.09 ~ 2016.02
School of Computer Science, Electrical and Electronic Engineering, and Engineering Mathematics

Loughborough University Loughborough, UK
Visiting Student in Computer Science 2013.09 ~ 2014.06
School of Science

Shandong University Weihai, China
B.S. in Electronic Information Science and Technology 2010.09 ~ 2014.06
School of Mechanical, Electrical and Information Engineering

CAREER

Beijing Zhuoshi Network Security Technology co. LTD Jinan, China
An independent third-party organization focusing on information security services in the energy (power) industry.
Quality Control Engineer 2016.02 ~ 2016.07

- In charge of information security inspection, rectification and reinforcement consultation, grade protection assessment, industrial safety risk assessment, etc. for power companies
- Participating in the development of national and energy and power industry information security standards and norms

RESEARCH INTERESTS

- The evaluation of the security properties of deep learning models, including robustness, accountability, privacy, and so on.
- The application of deep learning in security-related domains, including steganography, fuzz testing, and so on.

SKILLS

English: Fluent spoken English, excellent writing and reading skills
Certificates: CET-6

Professional skills: Basic programming with C and Python
Familiar with embedded programming, MATLAB, Web technology, cryptography and etc.

PROJECTS

Trusted Robustness Study of Large-Scale Attention Networks Jinan, China
2024.01 ~ Present

Study evaluation techniques for trusted large-scale attention networks, including model reliability and accountability.

Deep Learning Model Fuzzing and Repair based on SGCC Artificial Intelligence Platform Jinan, China
2023.01 ~ 2023.12

Studied the fuzzy testing technology and repair technology for deep learning models.

Security Testing for Deep Learning Models Jinan, China

2020.07 ~ 2023.06

Studied deep learning model testing techniques, including model adversarial robustness testing techniques and model hijacking reliability testing techniques.

Intelligent Software Vulnerability Discovery Driven by Machine Learning Jinan, China
2019.12 ~ 2022.12

Studied testing methods to ensure the safety and fairness of machine learning.

Network & Information Security Supervision System for Shandong Power Enterprises Jinan, China
2014.12 ~ 2015.09

Participated in the design of Shandong Power Enterprise Network and Information Security Supervision System (preliminary draft).

PUBLICATIONS

- PRJack: Pruning-Resistant Model Hijacking Attack against Deep Learning Models.
  (Under Review) 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.
  (Under Review) 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.
  (Dissertation) University of Bristol, UK, 2015.
  Ge Han

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

AWARDS

- Excellent student (twice)
- First-prize scholarship
- Second-prize scholarship
- Third-prize scholarship (twice)
- Second-prize at the provincial level in CUMCM, 2012 (as the captain)
- First-prize in cheering team competition, 2012 (as the captain)