Guangke Chen

Phone: (+86) 191-2170-2230 Email: chengk@shanghaitech.edu.cn
Website: `guangkechen.site`

Education Experiences

ShanghaiTech University, Shanghai, China Sept. 2019 - Present
Computer Science Ph.D student Supervisor: Fu Song

- GPA: major 3.91 / 4.0 total 3.8 / 4.0
- Selected Courses: Convex Optimization (A+) Deep Learning (A) Cryptography (A) Algorithm Design and Analysis (A) Theory of Computation (A+)

South China University of Technology (SCUT), Guangzhou, China Sept. 2015 - June 2019
Information Engineering Bachelor

- GPA: 3.77 / 4.0
- Thesis: Adversarial Attack against Speaker Recognition System

Honors and Awards

- 2022 | Merit Student | ShanghaiTech University
- 2020 | National Scholarship for Graduate | ShanghaiTech University
- 2020 | Merit Student | ShanghaiTech University
- 2018 | Nomination of the top ten merit students (20 students in total) | SCUT
- 2018 | National Scholarship | SCUT
- 2018 | Outstanding conclusion of national College Students' Innovation and Entrepreneurship Training Program (project leader) | SCUT
- 2017 | National Encouragement scholarship | SCUT
- 2016 | Enterprise Scholarship | SCUT
- 2016, 2017, 2018 | Merit Student | SCUT

Research Interests

Security and privacy of machine learning (e.g., voiceprint recognition and speech recognition)

Security and privacy of multimedia (e.g., speech)

Publications

1. Who is Real Bob? Adversarial Attacks on Speaker Recognition Systems
   Guangke Chen, Sen Chen, Lingling Fan, Xiaoning Du, Fu Song, Yang Liu
   In Proc. of the 42nd IEEE Symposium on Security and Privacy (Oakland, S& P), 55-72, 2021 (CCF-A, Accept rate: 115/952=12%, **citation>120**)
2. QFA2SR: Query-Free Adversarial Transfer to Speaker Recognition Systems
   Guanke Chen, Yedi Zhang, Zhe Zhao, Fu Song
   USENIX Security Symposium 2023 (CCF-A)

3. AS2T: Arbitrary source-to-target adversarial attack on speaker recognition systems
   Guangke Chen, Zhe Zhao, Fu Song, Sen Chen, Lingling Fan, Yang Liu
   IEEE Transactions on Dependable and Secure Computing (TDSC)
   (CCF-A, IF=6.791)

4. Towards Understanding and Mitigating Audio Adversarial Examples for Speaker Recognition
   Guangke Chen, Zhe Zhao, Fu Song, Sen Chen, Lingling Fan, Feng Wang, Jiashui Wang
   IEEE Transactions on Dependable and Secure Computing (TDSC)
   (CCF-A, IF=6.791)

5. Attack as Defense: Characterizing Adversarial Examples using Robustness
   Zhe Zhao, **Guangke Chen**, Jingyi Wang, Yiwei Yang, Fu Song, Jun Sun
   In Proc. of the 30th International Symposium on Software Testing and Analysis (ISSTA), 42-55, 2021
   (CCF-A, Accept rate: 51/219=23%)

6. Attack as Detection: Using Adversarial Attack Methods to Detect Abnormal Examples
   Zhe Zhao, **Guangke Chen**, Tong Liu, Taishan Li, Fu Song, Jingyi Wang, Jun Sun
   Under review

7. BDD4BNN: A BDD-based Quantitative Analysis Framework for Binarized Neural Networks
   Yedi Zhang, Zhe Zhao, **Guangke Chen**, Fu Song, Taolue Chen
   In Proc. of the 33rd International Conference on Computer-Aided Verification (CAV), 175-200, 2021
   (CCF-A, Accept rate: 79/290=27%)

8. QVIP: An ILP-based Formal Verification Approach for Quantized Neural Networks
   Yedi Zhang, Zhe Zhao, **Guangke Chen**, Fu Song, Min Zhang, Taulue Chen, Jun Sun
   To appear in the 37th IEEE/ACM International Conference on Automated Software Engineering (ASE) 2022. (CCF-A)

9. ACROBAT: Accelerating CEGAR-based Neural Network Verification via Adversarial Attacks
   Zhe Zhao, Yedi Zhang, **Guangke Chen**, Fu Song, Taolue Chen and Jiaxiang Liu
   To appear in the Proc. of the 29th Static Analysis Symposium (SAS) 2022 (CCF-B)

10. Precise Quantitative Analysis of Binarized Neural Networks: A BDD-based Approach
    Yedi Zhang, Zhe Zhao, **Guangke Chen**, Fu Song, Taolue Chen
    ACM Transactions on Software Engineering and Methodology (TOSEM, CCF-A)

Patents

1. A deep learning-based approach for distinguishing abnormal speech
   Xiaohui Feng, **Guangke Chen**, Qianhua He, Xiaolan Wu, Yanxiong Li | CN108766419B
   Granted

2. Method and apparatus for monitoring psychological stress with integration of pulse rate variability and sleep quality
   Xiaofen Xing, **Guangke Chen**, Shiyao Jiang, Litao Lin, Donghua Chen | CN107874750B
   Granted

3. Audio adversarial example defense based on speech acoustic feature compression
   Fu Song, **Guangke Chen**, Zhe Zhao | CN114242083A
   Pending

4. Adversarial example detection method based on robustness differences
   Fu Song, Zhe Zhao, **Guangke Chen** | CN112381150A
   Pending

5. Adversarial example detection method based on attack cost
   Fu Song, Zhe Zhao, **Guangke Chen** | CN112381152A

Pending

Services

- Program Committee Member:
  - the 23rd International Conference on Information and Communications Security (ICICS 2021)
  - the 24th International Conference on Information and Communications Security (ICICS 2022)
- Artifact Evaluation Committee Member:
  - Usenix Security 2023
- Session Chair:
  - Session 8 (Attack and Vulnerability Analysis II) of ICICS 2022
- Reviewer:
  - the 24th ISCA INTERSPEECH Conference (InterSpeech 2023)
  - IEEE Transactions on Dependable and Secure Computing (TDSC) (x2)
  - Springer Cybersecurity 2023
  - ACM Transactions on Privacy and Security
- Sub-reviewer:
  - The 33rd IEEE International Symposium on Software Reliability Engineering (ISSRE 2022)
  - IEEE Transactions on Reliability (TR) 2022
- Teaching Assistant:
  - CS240 Algorithm Design and Analysis, ShanghaiTech University, 2020-2021, Spring Semester

Skills and Qualifications

- Languages: native in Chinese, proficient in English (CET-6: 520)
- Programming: Python, Matlab, Java, C/C++, LaTeX
- Techniques:
  Machine learning (NumPy, Scipy, Scikit-learn)
  Deep learning (PyTorch, TensorFlow)
  Speech processing (Kaldi, torchaudio, SpeechBrain)