Leiqi Wang

Mobile: (+86)13070123818
E-mail: wangleiqi@iie.ac.cn
University of Chinese Academy of Sciences, Beijing

EDUCATION

- **University of Chinese Academy of Sciences, DE** **Beijing, 2018-present**
  - Major: Cyberspace Security, score: 3.59/4
- **University of Science and Technology Beijing, BE** **Beijing, 2014-2018**
  - Major: Internet of Things Engineering, score: 87.532/100
    Thesis: Anomaly Behaviour Detection of Internal User Based on User Role
  - Double degree: Financial Engineering, score: 80/100
    Thesis: Risk Analysis of Small Business Based on Naive Bayes

Honor: Outstanding Graduate of the University, Merit Student, Excellent Student Cadre, People's Second-class Scholarship

PROJECTS

- **Construction of network attack and defense shooting range** **2022-present**
  - Imitate a whole adversary between red and blue teams using CALDERA and ATT&CK and record the entire audit logs.
- **Research on abnormal behaviour monitoring technology** **2019-2021**
  - Propose a new dynamic detection method, which is based on device running snapshot combined with Bi-LSTM. The detection method can effectively and quickly identify malicious software and is 10% higher than DNN, LSTM in Precision and Recall. It gets rid of the dependence on expert knowledge.
- **Network product ecology website construction** **2019-2020**
  - Collect all products' details that need releasing on the website and design a script to process the information automatically into the required format. This website is already up and running.

ACADEMIC RESEARCH

Research on Key Technologies of Network Attack Traffic Detection and Identification Based on Deep Learning

- **Attack Detection on Imbalanced Network Traffic (Paper Accepted)**
  - Problems: Existing machine learning-based approaches typically train the model on a balanced dataset and get a superior detection result. However, the actual network traffic data is imbalanced due to the less frequent network attacks than the normal, which decreases the models' performance.
  - Solution: AOPL, consisting of Attention Mechanism Enhanced Oversampling (AMEO) and Parallel Deep Learning (PDL), is proposed to reduce the impact of imbalanced data.
  - Conclusion: Significantly, AMEO can help models perform better attack detection on the imbalanced data. Extensive comparison experiments on four real network traffic datasets show that AOPL has better Accuracy, Precision, and F1-score performances.
- **Attack Classification on Encrypted Network Traffic**
  - Problems: 80% of network traffic is encrypted. TLS, while protecting user privacy, also gives attackers advantages because plaintext based detection is not effective and attacks can't be discovered.
  - Solution: It is planned to propose an attack fingerprint method based on the graph for comparison during attack classification. This method can recognize the unseen attack. The experiment is in progress.
- **Defense against Deep Learning Attacks (Future Plan)**

- Motivations: Deep learning models are no longer safe, and there are a lot of research on how to make them broken down. Mistakes in attack detection and classification caused by DL security will make a huge loss.

PUBLICATIONS

- Zijun Cheng, Degang Sun, **Leiqi Wang,** Qiujian Lv, Yan Wang, MMSP: A LSTM Based Framework for Multi-Step Attack Prediction in Mixed Scenarios. ISCC 2022 (Accepted)
- **Leiqi Wang,** Weiqing Huang, Qiujian Lv, Yan Wang, Haiyan Chen, AOPL: Attention Enhanced Oversampling and Parallel Deep Learning Model for Attack Detection in Imbalanced Network Traffic. WASA (2) 2021: 84-95, doi: 10.1109/ISCC53001.2021.9631465
  Link: https://link.springer.com/chapter/10.1007/978-3-030-86130-8_7
- Jianguo Jiang, Xu Wang, Yan Wang, Qiujian Lv, MeiChen Liu, Tingting Wang, **Leiqi Wang**, GSketch: A Comprehensive Graph Analytic Approach for Masquerader Detection Based on File Access Graph, 2021 IEEE Symposium on Computers and Communications (ISCC), 2021, pp. 1-6, doi: 10.1109/ISCC53001.2021.9631465.
  Link: https://ieeexplore.ieee.org/document/9631465
- **Leiqi Wang**, Ce Li, Qiujian Lv, Yan Wang, Ning Li, Weiqing Huang. Fast detection method of malware based on device running snapshot, the 30th National Conference on Information Security (IS), 2020

SELECTED GRANTS AND HONORS

- Excellent Student Cadre — April 2021
- Merit Student — April 2020
- Beijing University Students Instrumental Music Category performance silver award — September 2018
- National Computer Design Contest, National first prize — August 2017
- National College Students Innovation and Entrepreneurship Competition, Municipal third prize — April 2017
- University of Science and Technology Beijing Intelligent Car Competition, University-level second prize — December 2015

SKILLS

- Programming: Python(scikit-learn, keras, pytorch), C, Linux shell command
- Office: Microsoft Word, Excel, PowerPoint, Mindmanager
- Hobby: violin, reading

LEADERSHIP EXPERIENCE

- **Chairman of the Student Union of Research Office** — 2021-present
  - Coordinate the needs and work of students and teachers in the research office. Responsible for WeChat public account operation.
- **Chairman of Sichuang Technology Center** — 2016-2017
  - Led 40 members to complete the teaching of robot programming in primary and middle schools. Writing the Arduino robot class materials.