Xiaoyun Xu PhD Student

xiaoyun.xu@ru.nl
https://xiaoyunxxy.github.io

Education

Radboud University — Nijmegen, The Netherlands
PhD in Computer Science — 2022 - 2025
- Advisor: Dr. S. Picek
- Promotor: Prof. Dr. L. Batina
- Research area: Adversarial Machine Learning

University of Bristol — Bristol, UK
MSc in Advanced Computing — 2017 - 2018
- Thesis: Investigating the effectiveness of existing machine-learning-based compiler optimization techniques

UESTC — Chengdu, China
BEng in Software Engineering — 2013 - 2017
- Thesis: Vehicle license plate recognition based on SVM and ANN

Publications

1. **Xiaoyun Xu**, Zhuoran Liu, Stefanos Koffas, and Stjepan Picek. Towards Backdoor Stealthiness in Model Parameter Space. *ACM Conference on Computer and Communications Security (ACM CCS 2025 - Cycle A), Accepted*, 2025.
2. **Xiaoyun Xu**, Zhuoran Liu, Stefanos Koffas, Shujian Yu, and Stjepan Picek. BAN: Detecting Backdoors Activated by Adversarial Neuron Noise. *Advances in Neural Information Processing Systems (NeurIPS)* , 2024.
3. **Xiaoyun Xu**, Shujian Yu, Zhuoran Liu, and Stjepan Picek. MIMIR: Masked Image Modeling for Mutual Information-based Adversarial Robustness. *Under review at CCS Cycle B, Round 2*, 2025.
4. Zhuoran Liu, Senna van Hoek, Péter Horváth, Dirk Lauret, **Xiaoyun Xu**, and Lejla Batina. Real-world Edge Neural Network Implementations Leak Private Interactions Through Physical Side Channel. *arXiv preprint*, 2025.
5. **Xiaoyun Xu**, Oguzhan Ersoy, Behrad Tajalli, and Stjepan Picek. Universal Soldier: Using universal adversarial perturbations for detecting backdoor attacks. *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 2024.
6. **Xiaoyun Xu**, and Stjepan Picek. Poster: Boosting Adversarial Robustness by Adversarial Pre-training. *ACM Conference on Computer and Communications Security (CCS)*, 2023.
7. **Xiaoyun Xu**, Guilherme Perin, and Stjepan Picek. IB-RAR: Information Bottleneck as Regularizer for Adversarial Robustness. *IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)*, 2023.
8. **Xiaoyun Xu**, Jingzheng Wu, Mutian Yang, Tianyue Luo, Qianru Meng, Weiheng Li, and Yanjun Wu. AI-CTO: Knowledge graph for automated and dependable software stack solution. *Journal of Intelligent and Fuzzy Systems*, 2021.
9. **Xiaoyun Xu**, Jingzheng Wu, Mutian Yang, Tianyue Luo, Xu Duan, Weiheng Li, Yanjun Wu, and Bin Wu. Information leakage by model weights on federated learning. *In Proceedings of the 2020 workshop on privacy-preserving machine learning in practice, CCS workshop PPLMP*, 2020.

Experience

Leiden University 2020.10 – 2022.04

- Position: PhD student
- Exploring the combination of formal methods (model checking) and AI.

Institute of Software, Chinese Academy of Sciences 2018.10 - 2020.10

- Position: Research Assistant
- Research Topics: Knowledge Graph, security vulnerabilities, Interpretable AI.
- Developing domain knowledge graph of software vulnerabilities.

Skills

Languages: Chinese, English.

Programming: C/C++, Python, Linux, HTML, Git, CSS, Makefile, NodeJS, JavaScript, Neo4j, Cypher.

Courses: Computational Neuroscience, Cloud Computing, Computer Graphics, Data Structures and Algorithms, Database Principles and Applications, Computer Network, Image Processing, Computer Vision, etc.

Academic Services

Reviewers: BMVC, ICLR, NeurIPS

External Reviewers: S&P, NDSS, USENIX Security