

XIAOYUN XU

xiaoyun.xu@ru.nl \diamond <https://xiaoyunxxy.github.io/>

ACADEMIC APPOINTMENT

Radboud University, Nijmegen, The Netherlands

Nov, 2025 - Present

Postdoc, topic: Adversarial Machine Learning

EDUCATION

Radboud University, Nijmegen, The Netherlands

May, 2022 - Jan, 2026

PhD in Computer Science

Supervisor: Dr. Stjepan Picek

Thesis: No Time to Spare: Adversarial Machine Learning at Training and Inference Time

University of Bristol, Bristol, UK

2017 - 2018

MSc in Advanced Computing

Thesis: Investigating the effectiveness of existing machine-learning-based compiler optimization techniques

University of Electronic Science and Technology of China

2013 - 2017

BEng in Software Engineering

Thesis: Vehicle license plate recognition based on SVM and ANN

RESEARCH PUBLICATION

1. **Xiaoyun Xu**, Shujian Yu, Zhuoran Liu, and Stjepan Picek. MIMIR: Masked Image Modeling for Mutual Information-based Adversarial Robustness. *Accepted by The Network and Distributed System Security (NDSS)*, 2026.
2. **Xiaoyun Xu**, Zhuoran Liu, Stefanos Koffas, and Stjepan Picek. Towards Backdoor Stealthiness in Model Parameter Space. *ACM Conference on Computer and Communications Security (CCS)*, 2025.
3. **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.
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.
10. **Xiaoyun Xu**, Jingzheng Wu, Mutian Yang, Tianyue Luo, A method of shortening vulnerability attack window based on knowledge graph reasoning, CN110378126B, (Patent)

11. Vulnerability management platform based on Knowledge Graph, 2019SR0860641, (Software Copyright)

RESEARCH EXPERIENCE AND PROJECTS

- | | |
|--|-----------------------|
| Dutch national e-infrastructure (SURF Cooperative) | Jan, 2025 - Dec, 2025 |
| <ul style="list-style-type: none">• Project Title: LLM pruning against backdoor attacks• grant no. EINF-12068. | |
| Dutch national e-infrastructure (SURF Cooperative) | Sep, 2024 - Sep, 2025 |
| <ul style="list-style-type: none">• Project Title: Adversarially train the projection layer for robustness of vision and language alignment• grant no. EINF-10853. | |
| Institute of Software, Chinese Academy of Sciences | 2018 - 2020 |
| <ul style="list-style-type: none">• Research Assistant, topics: Knowledge Graph, security vulnerabilities, and Interpretable AI.• Domain knowledge graph of software vulnerabilities. | |

ACADEMIC SERVICES

- | | |
|---------------------------|---------------------------------|
| Reviewers/PC | CCS, BMVC, ICLR, NeurIPS, SaTML |
| External Reviewers | S&P, NDSS, USENIX Security |

TEACHING

- Guest Lecturer, Academic Writing and Research Methods (NWI-IBC043), 2025, Radboud University
- Teaching Assistant, Security and Privacy of Machine Learning (NWI-IMC069), 2023, Radboud University

CAMPUS EXPERIENCE

- | | |
|--|-------------------|
| Summer School, Šibenik, Croatia | 2022.06 |
| <ul style="list-style-type: none">• Topic: On real-world crypto and privacy | |
| Exchange program at Christopher Newport University, America | 2015.07 – 2015.08 |
| <ul style="list-style-type: none">• Received 10,000 (Chinese yuan) scholarship• Explored the American education model and culture | |
| Exchange program at Waseda University, Japan | 2016.01 – 2016.02 |
| <ul style="list-style-type: none">• Received a scholarship of 50,000 yen (JPY)• Learned more about Japanese culture and visited Japanese well-known enterprises | |

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 Networks, Image Processing, Computer Vision, etc. |