

# XIAOYUN XU

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

## ACADEMIC APPOINTMENT

**Radboud University, Nijmegen, The Netherlands**  
Postdoc, topic: Adversarial Machine Learning

Nov, 2025 - Present

## EDUCATION

<b>Radboud University, Nijmegen, The Netherlands</b>	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	
<b>University of Bristol, Bristol, UK</b>	2017 - 2018
MSc in Advanced Computing	
Thesis: Investigating the effectiveness of existing machine-learning-based compiler optimization techniques	
<b>University of Electronic Science and Technology of China</b>	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. AICTO: 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)

## RESEARCH EXPERIENCE AND PROJECTS

---

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

## ACADEMIC SERVICES

---

<b>Reviewers/PC</b>	CCS, BMVC, ICLR, NeurIPS, SaTML
<b>External Reviewers</b>	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

---

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

## SKILLS

---

<b>Languages</b>	Chinese, English.
<b>Programming</b>	C/C++, Python, Linux, HTML, Git, CSS, Makefile, NodeJS, JavaScript, Neo4j, Cypher.
<b>Courses</b>	Computational Neuroscience, Cloud Computing, Computer Graphics, Data Structures and Algorithms, Database Principles and Applications, Computer Networks, Image Processing, Computer Vision, etc.