

EDUCATION	<b>Radboud University</b> <i>PhD in Computer Science</i> • Advisor: Dr. S. Picek • Promotor: Prof. Dr. L. Batina • Research area: Adversarial Machine Learning	Nijmegen, The Netherlands 2022 - 2025
	<b>University of Bristol</b> <i>MSc in Advanced Computing</i> • Thesis: Investigating the effectiveness of existing machine-learning-based compiler optimization techniques	Bristol, UK 2017 - 2018
	<b>UESTC</b> <i>BEng in Software Engineering</i> • Thesis: Vehicle license plate recognition based on SVM and ANN	Chengdu, China 2013 - 2017
PUBLICATIONS	1. <b>Xiaoyun Xu</b> , Zhuoran Liu, Stefanos Koffas, and Stjepan Picek. Towards Backdoor Stealthiness in Model Parameter Space. <i>ACM Conference on Computer and Communications Security (ACM CCS 2025 - Cycle A)</i> , Accepted, 2025.	
	2. <b>Xiaoyun Xu</b> , Zhuoran Liu, Stefanos Koffas, Shujian Yu, and Stjepan Picek. BAN: Detecting Backdoors Activated by Adversarial Neuron Noise. <i>Advances in Neural Information Processing Systems (NeurIPS)</i> , 2024.	
	3. <b>Xiaoyun Xu</b> , Shujian Yu, Zhuoran Liu, and Stjepan Picek. MIMIR: Masked Image Modeling for Mutual Information-based Adversarial Robustness. <i>Under review</i> , 2025.	
	4. Zhuoran Liu, Senna van Hoek, Péter Horváth, Dirk Lauret, <b>Xiaoyun Xu</b> , and Lejla Batina. Real-world Edge Neural Network Implementations Leak Private Interactions Through Physical Side Channel. <i>arXiv preprint</i> , 2025.	
	5. <b>Xiaoyun Xu</b> , Oguzhan Ersoy, Behrad Tajalli, and Stjepan Picek. Universal Soldier: Using universal adversarial perturbations for detecting backdoor attacks. <i>IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)</i> , 2024.	
	6. <b>Xiaoyun Xu</b> , and Stjepan Picek. Poster: Boosting Adversarial Robustness by Adversarial Pre-training. <i>ACM Conference on Computer and Communications Security (CCS)</i> , 2023.	
	7. <b>Xiaoyun Xu</b> , Guilherme Perin, and Stjepan Picek. IB-RAR: Information Bottleneck as Regularizer for Adversarial Robustness. <i>IEEE/IFIP International Conference on Dependable Systems and Networks Workshops (DSN-W)</i> , 2023.	
	8. <b>Xiaoyun Xu</b> , Jingzheng Wu, Mutian Yang, Tianyue Luo, Qianru Meng, Weiheng Li, and Yanjun Wu. AI-CTO: Knowledge graph for automated and dependable software stack solution. <i>Journal of Intelligent and Fuzzy Systems</i> , 2021.	
	9. <b>Xiaoyun Xu</b> , Jingzheng Wu, Mutian Yang, Tianyue Luo, Xu Duan, Weiheng Li, Yanjun Wu, and Bin Wu. Information leakage by model weights on federated learning. <i>In Proceedings of the 2020 workshop on privacy-preserving machine learning in practice, CCS workshop PPLMP</i> , 2020.	
EXPERIENCE	<b>Leiden University</b> • Position: PhD student • Exploring the combination of formal methods (model checking) and AI.	2020.10 – 2022.04
	<b>Institute of Software, Chinese Academy of Sciences</b> • Position: Research Assistant • Research Topics: Knowledge Graph, security vulnerabilities, Interpretable AI. • Developing domain knowledge graph of software vulnerabilities.	2018.10 - 2020.10

## 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