Tao Ni (Tony)

MMW-1403, 83 Tat Chee Avenue, Kowloon Tong, Kowloon, Hong Kong SAR
+852 62632360 taoni2-c@my.cityu.edu.hk https://tony520.github.io/

RESEARCH

My research primarily revolves around **cyber-physical systems security** with a specific emphasis on identifying side-channel vulnerabilities and protecting sensing-involved computation in diverse embedded and mobile platforms via the integration of hardware-software co-design and cutting-edge AI models. I'm dedicated to exploring **contactless side channels** in various IoT platforms (e.g., VR/AR, satellite, cloud, and LLMs), as well as developing **software-defined defense mechanisms**.

EDUCATION

City University of Hong Kong, Hong Kong SAR 2021 – 2024

- Doctor of Philosophy (Ph.D.) in Computer Science
- Thesis: Contactless Side Channels in Mobile Charging Systems: Attacks and Defenses
- Dissertation Committee: Weitao Xu, Qingchuan Zhao, Cong Wang (Chair), Zhenjiang Li

Australian National University, Canberra, Australia 2019 – 2020

- Master of Computing in Computer Science

Shanghai Jiao Tong University, Shanghai, China 2014 – 2018

- Bachelor of Engineering in Electrical Engineering

PUBLICATIONS

Refereed Conference Publications

[C1] **Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel**

Tao Ni, Xiaokuan Zhang, Qingchuan Zhao

*30th ACM Conference on Computer and Communications Security (**CCS**), 2023.*

[Acceptance Rate = 235/1222 = 19.2%, 15 Pages]

[C2] **Exploiting Contactless Side Channels in Wireless Charging Power Banks for User Privacy Inference via Few-shot Learning**

Tao Ni, Jianfeng Li, Xiaokuan Zhang, Chaoshun Zuo, Wubing Wang, Weitao Xu, Xiapu Luo, Qingchuan Zhao

*29th Annual International Conference on Mobile Computing and Networking (**MobiCom**), 2023.*

[Acceptance Rate = 92/377 = 24.4%, 15 Pages]

[C3] **XPorter: A Study of the Multi-Port Charger Security on Privacy Leakage and Voice Injection**

Tao Ni, Yongliang Chen, Weitao Xu, Lei Xue, Qingchuan Zhao

*29th Annual International Conference on Mobile Computing and Networking (**MobiCom**), 2023.*

[Acceptance Rate = 92/377 = 24.4%, 15 Pages]

[C4] **Uncovering User Interactions on Smartphones via Contactless Wireless Charging Side Channels**

Tao Ni, Xiaokuan Zhang, Chaoshun Zuo, Jianfeng Li, Zhenyu Yan, Wubing Wang, Weitao Xu, Xiapu Luo, Qingchuan Zhao

*44th IEEE Symposium on Security and Privacy (**S&P, Oakland**), 2023.*

[Acceptance Rate = 195/1147 = 17.0%, 17 Pages]

[C5] **Eavesdropping Mobile App Activity via Radio-Frequency Energy Harvesting**

Tao Ni, Guohao Lan, Jia Wang, Qingchuan Zhao, Weitao Xu

*32nd USENIX Security Symposium (**USENIX Security**), 2023.*

[Acceptance Rate = 422/1444 = 29.2%, 18 Pages]

[C6] **A Simple and Fast Human Activity Recognition System Using Radio Frequency Energy Harvesting**

Tao Ni, Yongliang Chen, Keqi Song, Weitao Xu

*4th Workshop on Combining Physical and Data-Driven Knowledge in Ubiquitous Computing, ACM International Joint Conference on Pervasive and Ubiquitous Computing (**UbiComp CPD Workshop**), 2021.*

[**Best Paper Award**, 6 Pages]

[C7] **RF-Egg: An RF Solution for Fine-Grained Multi-Target and Multi-Task Egg Incubation Sensing**

Zehua Sun, Tao Ni, Yongliang Chen, Di Duan, Kai Liu, Weitao Xu

*30th Annual International Conference on Mobile Computing and Networking (**MobiCom**), 2024.*

[Acceptance Rate = 48/207 = 23.2%, 15 Pages]

[C8] **FLoRa: Energy-Efficient, Reliable, and Beamforming-Assisted Over-The-Air Firmware Update in LoRa Networks**

Zehua Sun, Tao Ni, Huanqi Yang, Kai Liu, Yu Zhang, Tao Gu, Weitao Xu

*22nd International Conference on Information Processing in Sensor Networks (**IPSN**), 2023.*

[Acceptance Rate = 22/83 = 26.2%, 13 Pages]

[C9] **F^{2}Key: Dynamically Converting Your Face into a Private Key Based on COTS Headphones for Reliable Voice Interaction**

Di Duan, Zehua Sun, Tao Ni, Shuaicheng Li, Xiaohua Jia, Weitao Xu, Tianxing Li

*22nd ACM International Conference on Mobile Systems, Applications, and Services (**MobiSys**), 2024.*

[Acceptance Rate = 43/263 = 16.3%, 15 Pages]

[C10] **MobileKey: A Fast and Robust Key Generation System for Mobile Devices**

Keqi Song, Zimeng Zhu, Huanqi Yang, Tao Ni, Weitao Xu

*5th Workshop on Combining Physical and Data-Driven Knowledge in Ubiquitous Computing, ACM International Joint Conference on Pervasive and Ubiquitous Computing (**UbiComp CPD Workshop**), 2022.*

[6 Pages]

Refereed Journal Publications

[J1] **FLoRa+: Energy-Efficient, Reliable, Beamforming-Assisted, and Secure Over-The-Air Firmware Update in LoRa Networks**

Zehua Sun, Tao Ni, Huanqi Yang, Kai Liu, Yu Zhang, Tao Gu, Weitao Xu

*ACM Transactions on Sensor Networks (**TOSN**), 2024.*

[J2] **SwipePass: Acoustic-based Second-factor User Authentication for Smartphones**

Yongliang Chen, Tao Ni, Weitao Xu, Tao Gu

*ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (**UbiComp/IMWUT**), 2022.*

[J3] **mmSign: mmWave-based Few-Shot Online Handwritten Signature Verification**

Mingda Han, Huanqi Yang, Tao Ni, Di Duan, Mengzhe Ruan, Yongliang Chen, Jia Zhang, Weitao Xu

*ACM Transactions on Sensor Networks (**TOSN**), 2023.*

HONORS/AWARDS

Research Tuition Scholarship (RTS), City University of Hong Kong, 2023–2024

Outstanding Academic Performance Award (OAPA), City University of Hong Kong, 2023–2024

UbiComp/ISWC CPD Workshop, Best Paper Award, 2021

City University of Hong Kong Studentship, 2021–2025

Zhiyuan Honor Scholarship, Shanghai Jiao Tong University (10%), 2014–2015, 2015–2016

Academic Excellence Scholarship, Shanghai Jiao Tong University (30%, 30%, 15%), 2015, 2016, 2017

PROFESSIONAL SERVICE

Technical Program Committee (TPC)

- ICML 2024
- IEEE MASS 2024

Artifact Evaluation Committee (AEC)

- ACM MobiSys 2024
- ACM MobiCom 2024
- ACM CCS 2023

Journal Reviewer & Conference Subreviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Mobile Computing (TMC)
- IEEE Transactions on Network and Service Management (TNSM)
- Ad Hoc Networks
- IET Information Security
- IEEE ICDCS 2024, Subreviewer
- ICICS 2024, Subreviewer
- ICCCN 2024, Subreviewer

TEACHING EXPERIENCE

CS 1302 Introduction to Computer Programming, Semester A, 2023-2024

CS 1302 Introduction to Computer Programming, Semester B, 2022-2023

GE 2324 The Art and Science of Data, Summer Term, 2022-2023

CS 1302 Introduction to Computer Programming, Semester A, 2022-2023

CS 1302 Introduction to Computer Programming, Semester B, 2021-2022

GE 2324 The Art and Science of Data, Summer Term, 2021-2022

CS 3347 Software Engineering Principles and Practice, Semester A, 2021-2022