Chen Yan（闫琛）

Assistant Researcher
Ubiquitous System Security Laboratory (USSLab)
Email: yanchen@zju.edu.cn Website: https://cyansec.com/

Department of Electrical Engineering
Zhejiang University
Room 303, Jiao 2 Building
38 Zheda Road, Yuquan Campus
Hangzhou, China

RESEARCH AREAS

My research area is cyber-physical system security, with a particular interest in sensing. Most of my research focus on the trustworthiness of signals that transfer from the physical world to analog and digital systems. The systems that I have analyzed and/or enhanced include sensors, personal devices such as smartphones, autonomous vehicles, IoT devices, medical devices, voice assistants, voice biometrics, etc. My research also includes biometrics, device fingerprinting, side channel, covert channel, machine learning security, and acoustics.

EDUCATION

Zhejiang University Hangzhou, China
Ph.D., Control Theory and Engineering, *Sept. 2015 – Mar. 2021*
Advisor: Prof. Wenyuan Xu
Thesis: The Security Principles, Attacks, and Defenses of Sound Sensing

Zhejiang University Hangzhou, China
B.E., Electrical and Electronics Engineering, *Sept. 2011 – Jul. 2015*
Advisor: Prof. Wenyuan Xu
Thesis: Security Analysis of In-car Sensor Systems: An Aftermarket TPMS Case Study
Minor: English Language

ACADEMIC VISITING

University of Michigan Ann Arbor, USA
Research Assistant, *Jul. – Aug. 2016*
Security and Privacy Research (SPQR) Group
Advisor: Prof. Kevin Fu

University of California, Berkeley Berkeley, USA
Summer school, *Jul. – Aug. 2013*

PUBLICATIONS

1. Yan Jiang, Xiaoyu Ji, Kai Wang, **Chen Yan**, Richard Mitev, Ahmad-Reza Sadeghi, and Wenyuan Xu. "WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens", In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2022.
2. **Chen Yan**, Xiaoyu Ji, Kai Wang, Qinhong Jiang, Zizhi Jin, Wenyuan Xu. "A Survey on Voice Assistant Security: Attacks and Countermeasures", *ACM Computing Surveys,* 2022

3. **Chen Yan**, Zhijian Xu, Zhanyuan Yin, Xiaoyu Ji, Wenyuan Xu. "Rolling Colors: Adversarial Laser Exploits against Traffic Light Recognition", In *Proceedings of the USENIX Security Symposium (USENIX Security),* 2022.
4. Kai Wang, **Chen Yan**, Richard Mitev, Xiaoyu Ji, Ahmad-Reza Sadeghi, Wenyuan Xu. "GhostTouch: Targeted Attacks on Touchscreens without Physical Touch", In *Proceedings of the USENIX Security Symposium (USENIX Security)*, 2022.
5. Wenyuan Xu, Shize Guo, Xiaoyu Ji, **Chen Yan**. "From In-band to Out-of-Band: The Vulnerability Evolution of Intelligent Systems", *Communications of the CCF*, 18, 2 (2022), 46-52.
6. Xiaoyu Ji, Yushi Cheng, Yuepeng Zhang, Kai Wang, **Chen Yan**, Kevin Fu, Wenyuan Xu. "Poltergeist: Acoustic Manipulation of Image Stabilization towards Object Mis-Labeling", In *Proceedings of the IEEE Symposium on Security and Privacy (S&P),* 2021.
7. Xiaoyu Ji, Xinyan Zhou, **Chen Yan**, Jiangyi Deng, Wenyuan Xu. "A Nonlinearity-based Secure Face-to-Face Device Authentication for Mobile Devices", *IEEE Transactions on Mobile Computing (TMC),* 2020.
8. **Chen Yan**, Hocheol Shin, Connor Bolton, Wenyuan Xu, Yongdae Kim, Kevin Fu. "SoK: A Minimalist Approach to Formalizing Analog Sensor Security", In *Proceedings of the IEEE Symposium on Security and Privacy (S&P),* 2020.
9. **Chen Yan**, Yan Long, Xiaoyu Ji, Wenyuan Xu. "The Catcher in the Field: A Fieldprint based Spoofing Detection for Text-Independent Speaker Verification", In *Proceedings of the ACM Conference on Computer and Communications Security (CCS*), 2019. (Acceptance ratio: 16%)
10. **Chen Yan**, Guoming Zhang, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, Wenyuan Xu. "The Feasibility of Injecting Inaudible Voice Commands to Voice Assistants", *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2019
11. Xinyan Zhou, Xiaoyu Ji, **Chen Yan**, Jiangyi Deng, Wenyuan Xu. "NAuth: Secure Face-to-Face Device Authentication via Nonlinearity", In *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, 2019. (**Best In-Session Presentation Award**)
12. **Chen Yan**, Kevin Fu, Wenyuan Xu. "On Cuba, Diplomats, Ultrasound, and Intermodulation Distortion." *Computers in Biology and Medicine* 104 (2019): 250-266.
13. Wenyuan Xu, **Chen Yan**, Weibin Jia, Xiaoyu Ji, Jiaohao Liu. "Analyzing and Enhancing the Security of Ultrasonic Sensors for Autonomous Vehicles." *IEEE Internet of Things Journal*, 5.6 (2018): 5015-5029.
14. **Chen Yan**, Kevin Fu, and Wenyuan Xu. "On Cuba, Diplomats, Ultrasound, and Intermodulation Distortion." *Technical report*. 2018.
15. Guoming Zhang, **Chen Yan (co-first author)**, Xiaoyu Ji, Tianchen Zhang, Taimin Zhang, and Wenyuan Xu. "DolphinAttack: Inaudible Voice Commands." In *Proceedings of the ACM Conference on Computer and Communications Security (CCS),* 2017. (Acceptance ratio: 18%, **Best Paper Award**).
16. Kevin Fu, Harold Thimbleby, Wenyuan Xu, and **Chen Yan**. "Ransomware: How we can climb out of this mess." *China Medical Devices*, 32, 7 (2017), 167-168.
17. Benjamin Ransford, Daniel B. Kramer, Denis Foo Kune, Julio Auto de Medeiros, **Chen Yan**, Wenyuan Xu, Thomas Crawford, and Kevin Fu. "Cybersecurity and medical devices: A Practical guide for cardiac electrophysiologists." *Pacing and Clinical Electrophysiology* 40.8 (2017): 913-917.
18. **Chen Yan**, Wenyuan Xu, and Jianhao Liu. "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles." *DEF CON 24,* 2016. (**Tesla Security Researcher Hall of Fame**)

19. **Chen Yan**, and Wenyuan Xu. "Security and Privacy Challenges of Modern Automobiles." *Communications of the CCF*, 12, 1 (2016), 20-27.

INVITED TALKS

- **Bench Council Conference on Big Data & AI**, Online, *Mar. 2020*
  The Security of Intelligent Voice Systems
- **University of Oxford**, Oxford, United Kingdom, *Feb. 2019*
  Analog Security of Cyber-Physical Systems: A Trust Crisis in Sensors
- **China Internet Security Conference (ISC) - HackPwn 2017**, Beijing, China, *Sept. 2017*
  Deceiving Eyes: Analog and Sensing Security
- **XCon 2017**, Beijing China, *Aug. 2017*
  A Trust Crisis with Sensors in Automobiles
- **China Automotive Cyber Security Summit 2017**, Shanghai, China, *Feb. 2017*
  Sensing Security of Autonomous Vehicles
- **POC 2016**, Seoul, Korea, *Nov. 2016*
  Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles
- **PacSec 2016**, (presented by Prof. Wenyuan Xu) Tokyo, Japan, *Oct. 2016*
  Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles
- **DEF CON 24**, Las Vegas, United States, *Aug. 2016*
  Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles
- **IEEE TrustCol 2015**, Hangzhou, China, *Oct. 2015*
  Security and Privacy Challenges of Smart Vehicles
- **GeekPwn 2015 Open Course**, Shanghai, China, *Jun. 2015*
  Reverse Engineering an Aftermarket TPMS
- **Shanxi Government Security Workshop**, Taiyuan, China, *Jun. 2015*
  Automotive System Security

SELECTED HONORS

- Doctoral Dissertation Award, **ACM China**, *2021*
- First Prize of Beijing Municipal Science and Technology Progress Award, **Government of Beijing**, *2020*
- Award of Honor for Graduate, **Zhejiang University**, *2019*
- LuoCi-LinWenzhen Scholarship, **Zhejiang University**, *2019*
- ZJU Scholarship for Outstanding Doctoral Candidates, **Zhejiang University**, *2019*
- Student Travel Grant, **ACM CCS**, 2019
- Top 10 Academic Advances of Zhejiang University in 2017, **Zhejiang University**, *2018*
- Best Paper Award, **ACM CCS**, 2017
- Tesla Motors Information Security Recognition (No. 094/6831), **Tesla Motors**, *2016*
- 1st Prize winner of Winter HackPwn Car Hacking Contest, **Syscan360**, *2016*
- Student Stipends, **CHES**, *2016*
- Student Travel Award, **AsiaCCS**, *2016*
- 1st Prize winner of HackPwn, **Qihoo 360**, *2015*

- 1st Prize Scholarship on Academic Performance, **Zhejiang University**, *2014*
- Outstanding Student Awards, **Zhejiang University**, *2014*
- Texas Instrument Scholarship, **Texas Instrument**, *2014*

Professional Activities

Technical Program Committee (TPC)

- ACM CCS 2021

Reviewer

- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Information Forensics and Security (TIFS)
- IEEE Transactions on Cognitive and Developmental Systems (TCDS)
- IEEE Vehicular Technology Magazine (VTM)
- IEEE Intelligent Transportation Systems Magazine (ITSM)
- ACM IMWUT 2021
- IEEE Sensors 2019

Other Service

- Chair Assistant: NDSS 2022, NDSS 2023
- Volunteer: DEF CON 24 Car Hacking Village, Las Vegas, United States, *Aug. 2016*
- Chair Assistant: 2015 China Internet Security Conference (ISC) IoT Forum, Beijing, China, *Sept. 2015*

SELECTED NEWS COVERAGE

- On Cuba, Diplomats, Ultrasound, and Intermodulation Distortion (2018):
  - IEEE Spectrum: https://spectrum.ieee.org/semiconductors/devices/finally-a-likely-explanation-for-the-sonic-weapon-used-at-the-us-embassy-in-cuba
  - The Conversation: https://theconversation.com/can-sound-be-used-as-a-weapon-4-questions-answered-83627
  - FREEBUF: https://www.freebuf.com/articles/wireless/164318.html
- DolphinAttack (2017):
  - Wired: https://www.wired.com/story/security-roundup-germany-election-software-is-hackable
  - BBC: http://www.bbc.com/news/technology-41188557
  - MIT Technology Review: https://www.technologyreview.com/s/608825/secret-ultrasonic-commands-can-control-your-smartphone-say-researchers/
  - Xinhua News, http://www.xinhuanet.com/fortune/2017-10/31/c_1121881819.htm
  - Zhejiang University, http://www.zju.edu.cn/2017/0911/c578a637706/page.htm
- Can you trust autonomous vehicles (2016):
  - dailySECU: http://www.dailysecu.com/news/articleView.html?idxno=16945
  - Wired: https://www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles/
  - Forbes: http://www.forbes.com/sites/thomasbrewster/2016/08/04/tesla-autopilot-hack-crash/#235519f6dc93