闫琛

助理研究员
浙江大学 先进技术研究院/电气工程学院 系统科学与工程系
智能系统安全实验室 (USSLab)
地址：浙江省杭州市西湖区浙大路 38 号第二教学大楼 303 室
邮箱：yanchen@zju.edu.cn 个人主页：https://cyansec.com

研究方向

主要研究方向为物联网安全，聚焦于其中的感知环节。博士期间的研究主要围绕信号在物理、模拟、数字形态之间转换的可信性和安全问题，对各类智能设备和系统进行安全脆弱性分析与防护，例如手机等个人智能设备、各类传感器、自动驾驶汽车、医疗设备、语音助手等，旨在提升智能系统在真实物理环境中的安全性。此外，研究也涉及生物认证、设备指纹、侧信道、机器学习安全、声学等方面。在自动驾驶和智能语音方面的研究曾得到来自特斯拉汽车、华为、苹果、谷歌、三星、亚马逊等公司的致谢。

教育经历

博士：浙江大学 （2015 年 9 月— 2021 年 3 月） 中国杭州
专业：控制理论与控制工程
论文题目：声音感知安全机理与攻击和防护关键技术研究
导师：徐文渊 教授
研究课题：感知安全、语音安全、自动驾驶汽车安全、医疗设备安全、机器学习安全、设备指纹、生物认证、非线性声学等

本科：浙江大学 （2011 年 9 月— 2015 年 6 月） 中国杭州
主修专业：自动化（辅修专业：英语）
论文题目：汽车后装胎压传感器安全分析
导师：徐文渊 教授

学术访问

密歇根大学 美国安娜堡
访问学者（2016 年 7 月— 2016 年 8 月）
访问实验室：Security and Privacy Research Group（SPQR）
导师：Kevin Fu 教授
参与研究：硬盘声音攻击、医疗设备安全

加州大学伯克利分校 美国伯克利
暑期学校（2013 年 7 月— 2013 年 8 月）

发表论文

1. Qinhong Jiang, Xiaoyu Ji, **Chen Yan**, Zhixin Xie, Haina Lou, and Wenyuan Xu. “GlitchHiker: Uncovering Vulnerabilities of Image Signal Transmission with IEMI”, To appear, In *Proceedings of the USENIX Security Symposium (USENIX Security)*, 2023.【CCF A 类，四大安全顶会之一】

2. Ruochen Zhou, Xiaoyu Ji, **Chen Yan**, Chaohao Li, and Wenyuan Xu. “DeHiREC: Detecting Hidden Voice Recorders via ADC Electromagnetic Radiation”, To appear, In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2023.【CCF A 类，四大安全顶会之一】
3. Zizhi Jin, Xiaoyu Ji, Yushi Cheng, Bo Yang, **Chen Yan**, and Wenyuan Xu. “PLA-LiDAR: Physical Laser Attacks against LiDAR-based 3D Object Detection in Autonomous Vehicle”, To appear, In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2023.【CCF A 类，四大安全顶会之一】
4. Yan Jiang, Xiaoyu Ji, Kai Wang, **Chen Yan**, Richard Mitev, Ahmad-Reza Sadeghi, Wenyuan Xu. “WIGHT: Wired Ghost Touch Attack on Capacitive Touchscreens”, In *Proceedings of the IEEE Symposium on Security and Privacy (S&P),* 2022.【CCF A 类，四大安全顶会之一】
5. **Chen Yan**, Xiaoyu Ji, Kai Wang, Qinhong Jiang, Zizhi Jin, Wenyuan Xu. “A Survey on Voice Assistant Security: Attacks and Countermeasures”, *ACM Computing Surveys*
6. **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.【CCF A 类，四大安全顶会之一】
7. 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.【CCF A 类，四大安全顶会之一】
8. 徐文渊，郭世泽，冀晓宇，**闫琛**. “从带内到带外——智能系统的脆弱性体系演变”，中国计算机学会通讯, 18, 2 (2022), 46-52.
9. 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.【CCF A 类，四大安全顶会之一】
10. 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).* 【CCF A 类，SCI 收录】
11. **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. 【CCF A 类，四大安全顶会之一】
12. **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%) 【CCF A类，四大安全顶会之一】
13. **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).* 【CCF A 类，SCI 收录】
14. 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. 【CCF A 类】
15. **Chen Yan**, Kevin Fu, Wenyuan Xu. “On Cuba, Diplomats, Ultrasound, and Intermodulation Distortion.” *Computers in Biology and Medicine* 104 (2019): 250-266. 【SCI 收录】

16. 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. 【中科院一区，SCI 收录】
17. **Chen Yan**, Kevin Fu, and Wenyuan Xu. "On Cuba, Diplomats, Ultrasound, and Intermodulation Distortion." *Technical report*. 2018.
18. 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%). 【CCF A 类，四大安全顶会之一，**最佳论文奖**】
19. Kevin Fu, Harold Thimbleby, Wenyuan Xu, and **Chen Yan**. "勒索软件：我们如何爬出泥沼." 中国医疗设备, 32, 7 (2017), 167-168.
20. 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.
21. **Chen Yan**, Wenyuan Xu, and Jianhao Liu. "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles." *DEF CON 24,* 2016.【国际黑客大会】
22. **闫琛**, 徐文渊. "汽车智能化的安全思考." 中国计算机学会通讯, 12, 1 (2016), 20-27.

专利

1. 徐文渊，郭世泽，冀晓宇，闫琛，王凯. "一种基于功能域的终端设备安全威胁模型的构建方法"，中国发明专利: ZL202011209933.0
2. 冀晓宇，徐文渊，程雨诗，张月鹏，王凯，闫琛. "一种基于声波的图像对抗样本生成方法及系统"，中国发明专利: ZL202011124293.6
3. 冀晓宇，龙颜，徐文渊，闫琛. "一种语音认证系统的重放攻击检测方法"，中国发明专利: ZL201910303649.3
4. 徐文渊，冀晓宇，张国明，闫琛，张天晨，张泰民. "基于机器学习的防御无声指令控制语音助手的方法"，中国发明专利: ZL201711374668.2

荣誉与奖励

省部级：

- 北京市科学技术进步一等奖, **北京市人民政府**, *2020*

学术：

- 优秀博士论文奖, **ACM 中国**, *2021*
- 学术新星培养计划, **浙江大学**, *2019*
- 2017 年十大学术进展奖, **浙江大学**, *2018*
- 最佳论文奖, **ACM CCS**, *2017* （中国大陆地区首次）
- 会议学生奖金/旅行奖：**ACM CCS 2019、CHES 2016、AsiaCCS 2016**

行业：

- 安全研究人员名人堂奖章 (No. 094/6831), **Tesla Motors**, *2016*
- HackPwn 冬季汽车破解大赛一等奖, **Syscan 360**, *2016*
- HackPwn 破解大赛一等奖, **奇虎 360**, *2015*

学业：

- 浙江大学：优秀研究生奖学金（2019）、“罗慈-林文震”奖学金（2019）、学业优秀一等奖学金（2014）、优秀学生奖学金（2014）、得克萨斯仪器奖学金（2014）等

特邀学术报告

- **Bench Council 国际大数据与人工智能线上峰会，** 线上，2020 年 3 月
  “智能语音系统安全”
- **牛津大学系统安全实验室，** 英国牛津，2019 年 2 月
  “Analog Security of Cyber-Physical Systems: A Trust Crisis in Sensors”
- **中国互联网安全大会（ISC），** 中国北京，2017 年 9 月
  “Deceiving Eyes: Analog and Sensing Security”
- **XCon 2017，** 中国北京，2017 年 8 月
  “汽车传感器的信任危机”
- **第二届中国汽车网络信息安全峰会，** 中国上海，2017 年 2 月
  “智能汽车感知安全”
- **POC 2016，** 韩国首尔，2016 年 11 月
  “Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles”
- **PacSec 2016，** 日本东京，2016 年 10 月
  “Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles”
- **DEF CON 24，** 美国拉斯维加斯，2016 年 8 月
  “Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles”
- **IEEE TrustCol 2015，** 中国杭州，2015 年 10 月
  “Security and Privacy Challenges of Smart Vehicles”
- **极棒 GeekPwn 2015 公开课，** 中国上海，2015 年 6 月
  “针对后装汽车胎压传感器的逆向工程”
- **山西省政府安全研讨会，** 中国太原，2015 年 6 月
  “汽车系统安全”

学术活动

国际学术会议程序委员会（TPC）：

- ACM CCS 2021, ACM SenSys 2022 (Shadow PC)

论文审稿人：

- 期刊：IEEE Transactions on Dependable and Secure Computing (TDSC)、IEEE Transactions on Information Forensics and Security (TIFS)、IEEE Vehicular Technology Magazine、IEEE Transactions on Cognitive and Developmental Systems (TCDS)、IEEE Intelligent Transportation Systems Magazine、IEEE Transactions on Instrumentation & Measurement (TIM)
- 会议：ACM IMWUT 2021、IEEE Sensors 2019

会议服务：

- 主席助理：NDSS 2022、NDSS 2023
- 志愿者：DEF CON 24 Car Hacking Village，美国拉斯维加斯，2016 年 8 月
- 主席助理：2015 年中国互联网安全大会（ISC）物联网分会，中国北京，2015 年 9 月

新闻报道（部分）

- 基于充电线注入的电容式触摸屏鬼手攻击（2022）：

    - Forbes: https://www.forbes.com/sites/daveywinder/2022/05/28/how-this-shocking-hack-remotely-swipes-iphone--android-touchscreens-using-charging-cables/?sh=6c4bf6b5d3b1
- 交通灯识别激光对抗攻击（2022）：
    - NewScientist: https://www.newscientist.com/article/2315634-driverless-cars-can-be-tricked-into-seeing-red-traffic-lights-as-green/#ixzz7RM1L01V2
- 古巴大使馆声波攻击事件分析（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
- 海豚音攻击（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/
    - 新华社：http://www.xinhuanet.com/fortune/2017-10/31/c_1121881819.htm
    - 浙大首页：http://www.zju.edu.cn/2017/0911/c578a637706/page.htm
    - 雷锋网：https://www.leiphone.com/news/201803/lSnmZ6pgjhrccYZP.html
- 特斯拉自动驾驶汽车安全分析（2016）：
    - 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
    - dailySECU: http://www.dailysecu.com/news/articleView.html?idxno=16945
    - 雷锋网：https://www.leiphone.com/news/201608/yty43tdMp3K2gclo.html