YAN LONG

(+1)7348815577 yanlong@umich.edu

SUMMARY

Ph.D. candidate specialized in developing emerging embedded systems with better security&privacy and novel sensing functionalities. Skilled in processing information in audio, video, and general data types using DSP and AI/ML techniques. Experienced in Android and micro-controller development.

Research Interest: My research spans the intersections of embedded system security, sensing, and mobile computing. The core research question I explore is how to use existing sensors to sense extra modalities of signals using data-driven approaches informed by sensor physics. My dissertation focuses on (1) the gap between existing computation abstractions and actual hardware/software implementations in embedded sensing systems, and (2) the downstream security and privacy problems as well as the new opportunities in biometric data collection and digital forensics.

EDUCATION

EECS Department, University of Michigan (UMich), Ann Arbor September 2019 - Present
Expected Degree: Ph.D. in Electrical and Computer Engineering

- Research Advisor: Kevin Fu
- Overall GPA: 4.0/ 4.0
- Courses: Computational Data Science & Machine Learning. Computer Vision. Estimation, Filtering, Detection. Computer Security. Electrical Biophysics. Probability & Random Process. Stochastic Processes.

College of Electrical Engineering, Zhejiang University (ZJU), Hangzhou, China September 2015 - June 2019
Degree: B.Eng in Electronic and information Engineering

- Research Advisor: Wenyuan Xu
- Overall GPA: 3.93/4. GPA Ranking: 5/121
- Courses: Interface Technology of Microprocessors, Signal Analysis & Processing, Computer Network & Communication, Information Theory & Coding, Operating System, Modern Sensors

RESEARCH EXPERIENCE

Exfiltrating Speech Information From Camera Side Channels July 2021 - August 2022
Ph.D. Research @ UMich, Project Leader

- Investigated the technique of exfiltrating speech information from silent smartphone videos without microphone access using DSP techniques and deep learning models.
- Uncovered how sound is embedded into image streams by modeling the rolling shutter imaging process and CMOS camera's movable lens structures.

Preventing Screen Content Leakage in Video Conferencing March 2021 - August 2022
Ph.D. Research @ UMich, Project Leader

- Characterized the limits and security consequences of screen content leakage through eyeglass reflections in webcam videos in daily video conferencing settings.
- Created video filtering tools based on dlib's facial landmark recognition models to demonstrate a short-term mitigation methodology. Proposed long-term infrastructural improvement to video conferencing platforms such as Zoom to provide usable security.

Protecting Temperature Sensors From IEMI Threats November 2020 - June 2021
Ph.D. Research @ UMich, Project Leader

- Identified the susceptibility of vaccine cold-chain temperature monitors to the threats of controlled false temperature reading excursions posed by intentional electromagnetic interference disruptions.

– Proposed accessible administrative controls to help cold chain logistics mitigate the risks to a tolerable level.

Wireless Sensor Platform for Automated Mask Decontamination Verification June 2020 - June 2021
Ph.D. Research @ UMich, Project Leader

– In response to the global N95 mask shortage, created an open-source platform "VeriMask" that consists of nRF52-based wireless sensor nodes and an Android tool for automated verification of environmental conditions during N95 masks' moist-heat decontamination processes.
– Reduced the cost of safe N95 mask decontamination from $100k range to $1k range.

Motion Sensor Based Acoustic Eavesdropping and Protection October 2019 - February 2020
Ph.D. Research @ UMich, Project Collaborator

– Investigated how low privacy level motion sensors in Android smartphones could be exploited to eavesdrop highly sensitive ambient audio information with the help of machine learning classifiers.
– Systematically investigated existing countermeasures and proposed new software-level defenses that achieve the best attack accuracy reduction while maintaining maximum usability.

Flexible Control and Waveform Generation Algorithms for Neurostimulation July 2018 - October 2018
Internship @ UCLA, Project Collaborator

– Developed a wireless neural stimulation system with Android control interfaces and wireless micro-controllers based on TI SimpleLink.
– Outperformed prevalent commercial neuromodulation research stimulators (8 channels, square wave only) with 32 concurrent stimulation channels and arbitrary waveform generation.

SELECTED PUBLICATION

- Connor Bolton*, **Yan Long***, Jun Han, Josiah Hester, and Kevin Fu. "Characterizing and Mitigating Touchtone Eavesdropping in Smartphone Motion Sensors" In the 26th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2023). (Acceptance rate 23.5%) (To appear)

- Benjamin Cyr, **Yan Long**, Takeshi Sugawara and Kevin Fu. "Space System Threat Models Must Account for Satellite Sensor Spoofing" In Workshop on Security of Space and Satellite Systems (SpaceSec). 2023

- **Yan Long**, Pirouz Naghavi, Blas Kojusner, Kevin Butler, Sara Rampazzi and Kevin Fu. "Side Eye: Characterizing the Limits of POV Acoustic Eavesdropping from Smartphone Cameras with Rolling Shutters and Movable Lenses." In Proceedings of the 44th Annual IEEE Symposium on Security and Privacy (IEEE S&P). 2023. (Acceptance rate 17%)

- **Yan Long**, Chen Yan, Shilin Xiao, Shivan Prasad, Wenyuan Xu, and Kevin Fu. "Private Eye: On the Limits of Textual Screen Peeking via Eyeglass Reflections in Video Conferencing." In Proceedings of the 44th Annual IEEE Symposium on Security and Privacy (IEEE S&P). 2023. (Acceptance rate 17%)

- **Yan Long**, and Kevin Fu. "Sensor Side Channels Considered Beneficial: Synthesizing Virtual Sensors to Verify Authenticity of Measurands". In Proceedings of the 2022 ACM/ACSA New Security Paradigms Workshop (ACM/ACSA NSPW). 2022. (Acceptance rate 38%)

- **Yan Long**, Sara Rampazzi, Takeshi Sugawara, and Kevin Fu. "Protecting COVID-19 Vaccine Transportation and Storage from Analog Cybersecurity Threats." Biomedical Instrumentation & Technology (AAMI BI&T). 2021.

- **Yan Long**, Alexander Curtiss, Sara Rampazzi, Josiah Hester, and Kevin Fu. "VeriMask: Facilitating Decontamination of N95 Masks in the COVID-19 Pandemic: Challenges, Lessons Learned, and Safeguarding the Future." In Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (ACM IMWUT/UbiComp). September 2021. (Impact Factor 4.16, acceptance rate 22%)

- **Yan Long**, Alexander Curtiss, Sara Rampazzi, Josiah Hester, and Kevin Fu. "Automating decontamination of N95 masks for frontline workers in COVID-19 pandemic: Poster Abstract." In Proceedings of the 18th Conference on Embedded Networked Sensor Systems (SenSys). 2020. (Best poster runner-up award: top 8%)
- 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 2019 ACM Conference on Computer and Communications Security (ACM CCS). 2019. (Acceptance rate 16%)
- Wang, Po-Min, Stanislav Culaclii, William Yang, **Yan Long**, Jonathan Massachi, Yi-Kai Lo, and Wentai Liu. "A Novel Biomimetic Stimulator System for Neural Implant." In 2019 9th International IEEE/EMBS Conference on Neural Engineering (IEEE/EMBS NER), 2019.

TECHNICAL STRENGTH

MATLAB:	Audio and video signal processing & analysis, machine learning prototyping
Python:	Data analysis, PyTorch, interface for embedded systems
Java + Android Studio:	Android user interface, sensor data acquisition & processing, networking
C + Assembly:	Driver & application layer of embedded systems
Linux + Bash:	OS and fast file manipulations
Wireshark + Nmap:	Network traffic analysis & auditing

Service & Award

Graduate Student Instructor:

- EECS 598 Special Topics in Embedded Security (**co-designed the brand-new course**) 2022
- EECS 505 Computational Data Science & Machine Learning 2021
- EECS 501 Probability & Random Process 2021

Academic Services:

- Journal reviewer: ACM TOPS (2023), IEEE TDSC (2023), ACM IMWUT/UbiComp (2021), IEEE TIE (delegate, 2020), IEEE TIFS (delegate, 2020)
- Conference delegate reviewer: ACM MobiCom (2023), USENIX Security (2020), ACM CCS (2019).
- Panelist: 2nd Annual Embedded Security Workshop (2020)

Awards:

- University of Michigan Rackham Predoctoral Fellowship 2023
- NSF/NSPW Travel Support Award 2022
- ACM SIGMOBILE Research Highlight (GetMobile) for "VeriMask: Facilitating Decon..." 2022
- China Invention Patent for "A Fieldprint..." 2021
- SenSys Best Poster Runner-up Award for "Automating Decon..." 2020
- Outstanding Undergraduate Thesis of ZJU 2019
- UCLA Cross-disciplinary Scholars in Science and Technology 2018
- Zhejiang Provincial Government Scholarship 2018
- Samsung Scholarship 2018