

Yan Long

2260 Hayward Street, Ann Arbor, MI, 48105

yanlong@umich.edu \diamond <https://yanlong.site/> \diamond (734) 881-5577

RESEARCH

My research is broadly in the area of **embedded and cyber-physical systems security** with a particular focus on **protecting sensing-based computation** in various forms of embedded and mobile information systems using hardware-software co-design and physics modeling. I work toward hardware-ensured information authenticity in critical infrastructures and consumer electronics, as well as innovative privacy-preserving sensing in emerging IoT, AI, and healthcare technologies.

EDUCATION

University of Michigan, Ann Arbor, MI Sep 2019 - Present

- Ph.D. in Electrical and Computer Engineering
- Thesis: Modeling and Mitigating Side Channels in Optical & Embedded Sensing Systems
- Dissertation committee: Kevin Fu (chair), Mingyan Liu (co-chair), Alanson Sample, Pei Zhang, Jean-Baptiste Jeannin

Zhejiang University, Hangzhou, China Sep 2015 - June 2019

- B.S. in Electronic and Information Engineering
- Thesis: Sound Field-based Liveness Detection in Voice Authentication
- Advisors: Wenyuan Xu, Xiaoyu Ji

WORK EXPERIENCE

University of Michigan, Ann Arbor, MI Sep 2019 - Present

Lead Graduate Research Assistant, Security and Privacy Research Group

Zhejiang University, Hangzhou, China Sep 2017 - June 2019

Undergraduate Research Assistant, Ubiquitous System Security Lab

UCLA, Los Angeles, CA July 2018 - Sep 2018

Summer Visiting Researcher, Biomimetic Research Lab

Thundercomm, Chongqing, China June 2017 - Sep 2017

Embedded Development Intern

AWARDS & HONORS

UMich Graduate Student Research Grant (\$3000 maximum, role: PI) 2023

UMich Towner Prize for Outstanding Graduate Instructor Finalist 2023

Rackham Predoctoral Fellowship (top 6 PhD candidates of UM CS&ECE) 2023

NSF/NSPW Student Travel Grant 2022

ACM SIGMOBILE Research Highlight on GetMobile 2022

Best Poster Runner-up – SenSys COVID-19 Response Research (top 8%) 2020

Outstanding Undergraduate Thesis of Zhejiang University 2019

UCLA Cross-disciplinary Scholarship in Science and Technology 2018

Zhejiang Provincial Government Scholarship (top 3% of school) 2018

Samsung Scholarship (top 5% of school) 2018

Refereed Conference & Workshop Publications

- C10 **EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras**
Yan Long, Qinhong Jiang, Chen Yan, Tobias Alam, Xiaoyu Ji, Wenyuan Xu, Kevin Fu
Network and Distributed System Security Symposium (NDSS) 2024
[historical acceptance rate = 16.2%, 18 pages]
- C9 **GhostType: The Limits of Using Contactless Electromagnetic Interference to Inject Phantom Keys into Analog Circuits of Keyboards**
Qinhong Jiang, Yanze Ren, Yan Long, Chen Yan, Yumai Sun, Xiaoyu Ji, Kevin Fu, Wenyuan Xu
Network and Distributed System Security Symposium (NDSS) 2024
[historical acceptance rate = 16.2%, 18 pages]
- C8 **Characterizing and Mitigating Touchtone Eavesdropping in Smartphone Motion Sensors**
Connor Bolton, Yan Long*, Jun Han, Josiah Hester, Kevin Fu
26th International Symposium on Research in Attacks, Intrusions, and Defenses (RAID) 2023
[acceptance rate = 50/213 = 23.5%, 14 pages]
- C7 **Side Eye: Characterizing the Limits of POV Acoustic Eavesdropping from Smartphone Cameras with Rolling Shutters and Movable Lenses**
Yan Long, Pirouz Naghavi, Blas Kojusner, Kevin Butler, Sara Rampazzi, Kevin Fu
44th Annual IEEE Symposium on Security and Privacy (IEEE S&P) 2023
[acceptance rate = 195/1147 = 17%, 18 pages]
- C6 **Private Eye: On the Limits of Textual Screen Peeking via Eyeglass Reflections in Video Conferencing**
Yan Long, Chen Yan, Shilin Xiao, Shivan Prasad, Wenyuan Xu, Kevin Fu
44th Annual IEEE Symposium on Security and Privacy (IEEE S&P) 2023
[acceptance rate = 195/1147 = 17%, 18 pages]
- C5 **Position Paper: Space System Threat Models Must Account for Satellite Sensor Spoofing**
Benjamin Cyr, Yan Long, Takeshi Sugawara, Kevin Fu
Workshop on Security of Space and Satellite Systems (SpaceSec) 2023
[acceptance rate = 10/19 = 52.6%, 6 pages]
- C4 **Side Auth: Sensor Side Channels Considered Beneficial by Synthesizing Virtual Sensors for Authentication**
Yan Long, Kevin Fu
ACM/ACSA New Security Paradigms Workshop (NSPW) 2022
[acceptance rate = 38%, 8 pages]
- C3 **VeriMask: Facilitating Decontamination of N95 Masks in the COVID-19 Pandemic: Challenges, Lessons Learned, and Safeguarding the Future**
Yan Long, Alexander Curtiss, Sara Rampazzi, Josiah Hester, Kevin Fu
ACM International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp) 2021
[acceptance rate = 22%, 29 pages]

C2 The Catcher in the Field: A Fieldprint based Spoofing Detection for Text-Independent Speaker Verification

Chen Yan, Yan Long*, Xiaoyu Ji, Wenyuan Xu

26th ACM Conference on Computer and Communications Security (ACM CCS) 2019

[acceptance rate = 149/934 = 16%, 15 pages]

C1 A Novel Biomimetic Stimulator System for Neural Implant

Wang, Po-Min, Stanislav Culaclii, William Yang, Yan Long, Jonathan Massachi, Yi-Kai Lo, Wentai Liu

9th International IEEE/EMBS Conference on Neural Engineering (IEEE/EMBS NER) 2019

[4 pages]

(* denotes co-first authors)

Refereed Journal & Magazine Publications

J2 VeriMask: Sensor Platform for Decontamination of N95 Masks

Yan Long, Alexander Curtiss, Sara Rampazzi, Josiah Hester, Kevin Fu

Mobile Computing and Communications (GetMobile). June 2022, Vol. 26 Iss. 2. pp 25-28

[4 pages]

J1 Protecting COVID-19 Vaccine Transportation and Storage from Analog Cybersecurity Threats

Yan Long, Sara Rampazzi, Takeshi Sugawara, Kevin Fu

Biomedical Instrumentation & Technology (AAMI BI&T) 55, no. 3, Oct 2021

[6 pages]

Posters & Demos

P2 Limiting the Optical-Electromagnetic Side Channel Leakage of Smartphone Cameras

Yan Long, Kevin Fu

NSF CHEST Meeting 2023

P1 Automating Decontamination of N95 Masks for Frontline Workers in COVID-19 Pandemic

Yan Long, Alexander Curtiss, Sara Rampazzi, Josiah Hester, Kevin Fu

18th ACM Conference on Embedded Networked Sensor Systems (SenSys) 2020

[Best Poster Award Runner Up – COVID-19 Response Research (Top 8%)]

Submissions in Review

S3 SampleGuard: Enabling Lightweight Runtime Monitoring and Characterization of Android Zero-permission Sensor Usage from User Space

Yan Long, Tobias Alam, Kevin Fu

Undergoing revision at 24th Privacy Enhancing Technologies Symposium (PETS) 2024

[14 pages]

S2 WIP: Threat Modeling Laser-Induced Acoustic Interference in Computer Vision-Assisted Vehicles

Nina Shamsi, Kaeshav Chandrasekar, Yan Long, Christopher Limbach, Kevin Fu

Submitted to 2nd ISOC Symposium on Vehicle Security and Privacy (VehicleSec) in Dec. 2023

[8 pages]

S1 **From Virtual Touch to Tesla Command: Unlocking Unauthenticated Control Chains From Smart Glasses for Vehicle Takeover**

Xingli Zhang, Yazhou Tu, Yan Long, Liquan Shan, Mohamed A Elsaadani,
Kevin Fu, Zhiqiang Lin, Xiali Hei

Submitted to 45th Annual IEEE Symposium on Security and Privacy (**IEEE S&P**) in Dec. 2023
[17 pages]

TALKS

Security of Computer Systems with Non-Computational Sensor Side Channels

MIT CSAIL Security Seminar, Oct 4, 2023

Host: Mengjia Yan

Protecting Health Care and Cyberphysical Systems

University of Washington CSE Security Seminar (joint talk with Dr. Kevin Fu), Oct 11, 2023

Host: Franziska Roesner and Joshua Smith

PATENTS

Acoustic Eavesdropping Using A Smartphone Camera

Yan Long et al.

US Patent, application filed, 2023

A Method for Detecting Voice Replay Attacks

Xioayu Ji, Yan Long, Wenyuan Xu, Chen Yan

China Invention Patent, ZL 2019 1 0303649.3

TEACHING EXPERIENCE

EECS 498/598 Embedded Security (~10 undergrad and ~25 graduate students)	Fall 2022
EECS 505 Computational DS & ML (~250 graduate students)	Fall 2021
EECS 298 Applied Comp. ML for Sci. & Eng. (~150 undergrad students)	Fall 2021
EECS 501 Probability & Random Process (~80 graduate students)	Winter 2021

SERVICE

Professional Activities

Technical program committee member:

- USENIX Security 2024
- ISOC Symposium on Vehicle Security and Privacy (VehicleSec) 2024, Poster/Demo Session
- International Conference on Mobility, Sensing and Networking (IEEE MSN) 2023
- International Workshop on Security and Privacy of Sensing Systems (Sensors S&P) 2023
- Annual Embedded Security Workshop (EmSec) 2020

Reviewer:

- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Internet of Things Journal (IoTJ)
- IEEE Transactions on Wireless Communications (TWC)
- ACM Transactions on Privacy and Security (TOPS)
- ACM Proceedings on Interactive, Mobile, Wearable and Ubiquitous Tech (IMWUT)

Sub-reviewer:

- IEEE Transactions on Industrial Electronics (TIE)
- IEEE Security & Privacy Journal
- ACM Conference On Mobile Computing And Networking (MobiCom) 2023
- USENIX Security Symposium 2020
- Network and Distributed System Security (NDSS) Symposium 2020
- ACM Conference on Computer and Communications Security (CCS) 2019

Student Advising

Sarah Bargfrede	B.S. Computer Science	2023-Present
Jiaming Yao	M.S. Data Science	2023-Present
Emiko Sano	High-school student	2023-Present
Tobias Alam	B.S. Computer Science (papers at NDSS'24 and PETS'24)	2022-Present
Yumai Sun	M.S. Electrical and Computer Engineering (paper at NDSS'24)	2022-2023
Haoliang Cheng	B.S. Computer Engineering (now: ECE master's at CMU)	2022-2023
Shivan Prasad	B.S. Computer Science (paper at IEEE SP'23)	2021-2022
Mia Li	B.S. Computer Science (now: Salesforce)	2020
Weikun Lyu	B.S. Computer Science (now: Meta)	2020