

Hao Cui

Email: cuihao.1eo@gmail.com
cuih7@uci.edu
 Telephone: +1 858-262-3756
 Website: <https://cvhc.cc/>
<https://www.ics.uci.edu/~cuih7>
 GitHub: @cuihao1eo
 LinkedIn: <https://www.linkedin.com/in/cvhc/>

Education

University of California, Irvine	2020–Today
<i>Ph.D.</i> in Networked Systems (GPA: 3.949/4.000)	
University of Science and Technology of China	2017–2020
<i>M.Eng.</i> in Electronics and Communication Engineering (GPA: 3.18/4.30)	
University of Science and Technology of China	2013–2017
<i>B.Eng.</i> in Computer Science and Technology (GPA: 3.71/4.30)	
<i>B.Sci.</i> in Geophysics (GPA: 3.47/4.30)	

Awards

UC Irvine EECS Department Fellowship	Sep. 2020 – Feb. 2021
Kaggle Deepfake Detection Challenge , 2 nd place / 300,000 USD	Jun. 2020
IJCAI-19 Alibaba Adversarial AI Challenge , 1 st place in defense track / 5,000 USD	Aug. 2019
China National Olympiad in Informatics in Provinces , 1 st prize / 4 th place in Henan Division	Oct. 2010

Work Experience

Software Engineering Intern, Google LLC	Summer 2023
<ul style="list-style-type: none"> Worked in the YouTube Shorts Ranking team. Built and tested new machine learning model architectures for short video recommendation. 	
Machine Learning Engineer Intern, Syntiant Corp.	Summer 2021
<ul style="list-style-type: none"> Conducted experiments to measure biases of keyword spotting models in gender, age and accents. Packaged PyTorch-based scripts into Docker containers to be used in the existing data pipeline. 	

Research Experience

UCI Networking Group & ProperData Lab, UC Irvine	2020–Today
<i>Graduate Student Researcher</i> / Ph.D. Advisor: Prof. Athina Markopoulou	
Automated privacy policy analysis	
<ul style="list-style-type: none"> Proposed PoliGraph, a novel framework that uses knowledge graphs to encode privacy policies. Built NLP tools based on spaCy and HuggingFace libraries that use various NLP techniques, notably zero-shot classification and coreference resolution, to extract information from privacy policies. 	
Understanding privacy norms through web forms	
<ul style="list-style-type: none"> Created a web form dataset using a customized crawler and large language models for annotation. Analyzed privacy norms embedded within the web forms, i.e., data collection patterns that match websites' functional necessities and legal obligations. 	

Inspecting privacy leakage in emerging platforms

- We decrypted network traffic on Oculus VR handsets by using Frida to bypass certificate validation.
- Compared network flows against privacy policies to audit flow-to-policy consistency of VR apps.
- We also applied the similar analysis to the Amazon Alexa voice assistant platform.

CAS Key Laboratory of Electromagnetic Space Information, USTC

2016–2020

Research Assistant / Advisor: Prof. Weiming Zhang

Multi-stage defense against adversarial examples for images

- Proposed a hybrid defense against adversarial attacks on CNN-based image classifiers that combines: adversarial training, model ensemble, multi-scale random filtering and abnormal result detection.
- 1st place in the defense track of the IJCAI-19 Alibaba Adversarial AI Challenge.

Covert screen-camera communication / Robust image watermarking against screen-shooting

- Proposed UnseenCode, an invisible on-screen barcode scheme for covert communication and image watermarking, which uses unobtrusive high-frequency color fluctuation on the screen to encode data
- Implemented the UnseenCode demo in C++ and Java that runs on desktop and Android phone.

Publications

- [1] U. Iqbal, P. N. Bahrami, R. Trimananda, **H. Cui**, A. Gamero-Garrido, D. Dubois, D. Choffnes, A. Markopoulou, F. Roesner, Z. Shafiq, "Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem," in *ACM Internet Measurement Conference 2023*, Montréal, Canada, Oct. 2023. (Best Paper Award)
- [2] **H. Cui**, R. Trimananda, A. Markopoulou and S. Jordan, "PoliGraph: Automated Privacy Policy Analysis using Knowledge Graphs," in *Proc. of USENIX Security Symposium 2023*, Anaheim, USA, Aug. 2023.
- [3] R. Trimananda, H. Le, **H. Cui**, J. T. Ho, A. Shuba and A. Markopoulou, "OVRseen: Auditing Network Traffic and Privacy Policies in Oculus VR," in *Proc. of USENIX Security Symposium 2022*, Boston, USA, Aug. 2022.
- [4] H. Bian, **H. Cui**, K. Liu, Z. Hang, D. Chen, W. Zhou, W. Zhang, and N. Yu, "CDAE: Color Decomposition-based Adversarial Examples for Screen Devices," in *Information Sciences*, 2021.
- [5] J. Zhang, D. Chen, J. Liao, H. Fang, W. Zhang, W. Zhou, **H. Cui**, and N. Yu, "Model Watermarking for Image Processing Networks," in *Proc. of the AAAI Conference on Artificial Intelligence*, New York, USA, Feb. 2020.
- [6] H. Fang, W. Zhang, Z. Ma, H. Zhou, S. Sun, **H. Cui**, and N. Yu, "A Camera Shooting Resilient Watermarking Scheme for Underpainting Documents," in *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 30(11), Nov. 2020.
- [7] **H. Cui**, H. Bian, W. Zhang, and N. Yu, "UnseenCode: Invisible On-screen Barcode with Image-based Extraction," in *Proc. of IEEE INFOCOM 2019*, Paris, France, Apr. 2019.
- [8] H. Fang, W. Zhang, H. Zhou, **H. Cui**, and N. Yu, "Screen-Shooting Resilient Watermarking," in *IEEE Transactions on Information Forensics and Security*, Vol. 14(6), Jun. 2019.
- [9] **H. Cui**, and X. Zha "Parallel Image Registration Implementations for GMTSAR Package," in *Seismological Research Letters*, Vol. 89(3), Feb. 2018.

Skills

Programming: proficient in Python, C/C++, Java, UNIX shell, JavaScript

Computer Vision: OpenCV, PyTorch, Tensorflow

NLP: spaCy, NLTK, HuggingFace

Web Development: Flask, NGINX, browser automation

Mobile & IoT: Android, Arduino

GPU Programming: CUDA, OpenCL, ArrayFire

DevOps: Linux, Git, Docker, Podman

Other Activities

Server Administrator of the CAS Key Laboratory of Electromagnetic Space Information

2017–2020

- Managed a computing cluster consisting of 14 Linux servers with 74 GPUs.
- Built the network infrastructure (routers/switches/VPN access) from scratch.

President of the USTC Linux User Group

2015–2016

CTO & Vice President of the USTC Linux User Group

2014–2015

- As one of the largest Linux user groups in China, we hold various events to promote free software to university students, and we provided online services like software mirrors to Chinese Linux users.