Yunhan (Jack) Jia

1195 Bordeaux Dr, Unit 16725
Sunnyvale, CA 94089
United States

Email: jack0082010@gmail.com
Homepage: **http://jiayunhan.com**
Tel: (+1) 650-267-9477

RESEARCH INTERESTS

Recently focusing on adversarial learning and the robustness of AI models.
Always interested in approaching system security problems.

EDUCATION

University of Michigan, Ann Arbor 09/2013-04/2018
PhD student in Computer Science and Engineering
- Advisor: Professor **Z. Morley Mao**
- Thesis: Program Analysis based Approaches to Ensure Security and Safety of Emerging Software Platforms

Shanghai Jiaotong University, Shanghai, China 09/2009-06/2013
Bachelor of Engineering in Software Engineering
- Advisor: Professor **Haibo Chen**

WORK EXPERIENCE

Senior Security Scientist 04/2018-present
X-Lab, Baidu USA, US

Threat Research Engineer Intern 05/2017-08/2017
Threat Research Team, Palo Alto Networks, US

Research Intern 06/2015-08/2015
QoE Lab, T-Mobile, US

Research Intern 06/2014-08/2014
QoE Lab, T-Mobile, US

Intern 08/2012-09/2012
CSS Lab, Microsoft APGC

PUBLICATIONS

Yunhan Jia, Yantao Lu, Junjie Shen, Qi Alfred Chen, Zhenyu Zhong, Tao Wei, Fooling Detection Alone is Not Enough: First Adversarial Attack against Multiple Object Tracking, CVPR Adversarial Machine Learning in Real-World Computer Vision Systems Workshop (**AdvMLCV**), 2019 [**Oral**] [PDF]

Yunhan Jia, Yantao Lu, Senem Velipasalar, Zhenyu Zhong, Tao Wei, Enhancing Cross-task Transferability of Adversarial Examples with Dispersion Reduction, CVPR Adversarial Machine Learning in Real-World Computer Vision Systems Workshop (**AdvMLCV**), 2019 [PDF]

Yunhan Jia, Yantao Lu, Junjie Shen, Qi Alfred Chen, Zhenyu Zhong, Tao Wei, Attacking Multiple Object Tracking using Adversarial Examples, ICML Security and Privacy of Machine Learning Workshop (**SPML**), 2019 [Poster]

Yunhan Jia, Zhenyu Zhong, Yulong Zhang, Qian Feng, Tao Wei, The Cost of Learning from the Best: How Prior Knowledge Weakens the Security of Deep Neural Networks, Blackhat Asia (**BHASIA**), 2019 [Slides]

Yunhan Jia, Zhenyu Zhong, Weilin Xu, Tao Wei, Perception Deception: Physical Adversarial Attack Challenges and Tactics for DNN-based Object Detection, Blackhat Europe (**BHEU**), 2018 [Slides]

Shichang Xu, Yunhan Jia, Z. Morley Mao, Subhabrata Sen, Dissecting HAS VOD Services for Cellular: Performance, Root Causes and Best Practices, Proceedings of the 17th Internet Measurement Conference (**IMC**), 2017 [PDF]

Ding Zhao, Yaohui Guo, Yunhan Jia, TrafficNet: An Open Naturalistic Driving Scenario Library, Proceedings of the 20th IEEE International Conference on Intelligent Transportation System Conference (**ITSC**), 2017 [PDF]

Yunhan Jia, Ding Zhao, Qi Alfred Chen, Z. Morley Mao, Towards Secure and Safe Appified Automated Vehicles, Proceedings of the 28th IEEE Intelligent Vehicles Symposium (**IV**), 2017 [PDF]

Yunhan Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Z.Morley Mao, Atul Prakash, ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms, Proceedings of the 24th Network and Distributed System Security Symposium (**NDSS**),2017 [PDF]

Yunhan Jia, Qi Alfred Chen, Yikai Lin, Chao Kong, Z.Morley Mao, Open Port for Bob and Mallory: Open Port Usage in Android Apps and Security Implications, Proceedings of the 2nd IEEE European Symposium on Security and Privacy (**EuroS&P**),2017 [PDF]

Yuru Shao, Jason Ott, Yunhan Jia, Zhiyun Qian, and Z. Morley Mao, The Misuse of Android Unix Domain Sockets and Security Implications, Proceedings of the 23th ACM Conference on Computer and Communications Security (**CCS**),2016 [PDF]

Yunhan Jia, Qi Alfred Chen, Z. Morley Mao, Jie Hui, Kranthi Sontineni, Alex Yoon, Samson Kwong, and Kevin Lau, Performance Characterization and Call Reliability Problem Diagnosis for Voice over LTE, Proceedings of the 21th ACM Annual International Conference on Mobile Computing and Networking (**MobiCom**),2015 [PDF]

Qi Alfred Chen, Zhiyun Qian, Yunhan Jia, Yuru Shao, and Z. Morley Mao, Static Detection of Packet Injection Vulnerabilities – A Case for Identifying Attacker-controlled Implicit Information Leaks, Proceedings of the 22nd ACM Conference on Computer and Communications Security (**CCS**), 2015. [PDF]

TALKS

(06/2019, CVPR workshop) Attacking Multiple Object Tracking using Adversarial Examples

(03/2019, Blackhat Asia) The Cost of Learning from the Best: How Prior Knowledge Weakens the Security of Deep Neural Networks

(11/2019, Blackhat Euro) Perception Deception: Physical Adversarial Attack Challenges and Tactics for DNN-based Object Detection

(04/2019, UC Irvine) Threat to Real-world Deep Learning Systems: Practical Attacks and Security Measures

(08/2018, Usenix Security) From Memory Safety to AI Security

(07/2017, Palo Alto Networks) Lessons Learnt from Securing Modern IoT and Autonomous Vehicle Platform

(06/2017, IEEE IV) Towards Secure and Safe Appified Automated Vehicles

(04/2017, IEEE EuroS&P) Open Port for Bob and Mallory: Open Port Usage in Android Apps and Security Implications

(02/2017, NDSS) ContexIoT: Towards Providing Contextual Integrity to Appified IoT Platforms

(01/2017, SJTU) SmartPhone, SmartHome, and SmartCar: Lessons Learnt from Securing Modern Appified Platform

(09/2015, MobiCom) Performance Characterization and Call Reliability Problem Diagnosis for Voice over LTE

HONORS & AWARDS

Internet of Things (IoT) Technology Research Award, Google	2016
CSE Fellowship, University of Michigan	2014
Excellent Participation in Research Program of Shanghai Jiao Tong University	2011

HOBBIES Playing guitar, jam with the band, play basketball and travel.