Google Apps [redacted]

Acknowledgement for the review I wrote

4 messages

[redacted] Wed, Dec 20, 2023 at 10:59 PM
To: Qi Alfred Chen <alfchen@uci.edu>

Hi Alfred,

According to the emails you sent to me, you have been assigning your paper review tasks to me through email since 2/2/21. I reviewed in total 62 papers for you, see the table below.

Please help me confirm
1) You, as the original reviewer, assigned these papers to me as internal research tasks, and I wrote reviews for these papers
2) Whether I was acknowledged publicly/externally for the reviews I wrote (e.g., credited in a way that other people can see), and if not, why
3) How my reviews were used for your review task, e.g., you submit my review after minor changes (like fixing typos, grammatical errors, and formatting issues), or you submit the review after merging the contents with reviews from other students, etc.

Best,
[redacted]

Table of papers I have written reviews for you.

Venue	Year	File name	Paper title
Infocom	2023	1570831468 paper.pdf	Loong: Generic Neural Network Automation for Multi-Objective Networking Classification Tasks
Infocom	2023	1570831854 paper.pdf	Privacy-Preserving Video Analytics System with Trajectory Prediction: Foresee and Protect You
Infocom	2023	1570831978 paper.pdf	FingerFaker: Spoofing Attack on COTS Fingerprint Recognition Without Victim's Knowledge
AutoSec	2022	AutoSec_2022_paper_12.pdf	The Adaptability of Sybil Attack Detection Mechanisms in Vehicular Fog Computing
ICRA	2023	ICRA23_1550_MS.pdf	kollagen: A Collaborative SLAM Pose Graph Generator
IROS	2023	IROS23_0304_MS.pdf	An Attentional Recurrent Neural Network for Occlusion-Aware Proactive Anomaly Detection In Field Robot Navigation
ECCV	2022	Submission 1666.zip	Physical Attack on Monocular Depth Estimation with Optimal Adversarial Patches
TDSC	2022	TDSC-2022-11-1040_Proof_hi.pdf	Towards Automatic Detection of Vulnerabilities in Robot Operating System 2
TOSN	2021	TOSN-2021-0145_Proof_hi.pdf	Optimizing Base-Station's Anonymity with PID-Controlled Fake Packets and Data Aggregation
ACM CCS	2021	ccs2021-a-paper110.pdf	Risk Analysis and Policy Enforcement of Function Interactions in Robot Apps
ACM CCS	2021	ccs2021-a-paper140.pdf	Protecting Smart Homes from Unintended Application Actions
ACM CCS	2021	ccs2021-a-paper336.pdf	All Your Checkpoints (are) Belong to Us! Stealthy Data-Driven Attacks Against Control Invariant Defense in Robotic Vehicles
ACM CCS	2021	ccs2021-b-paper14.pdf	CADD: Context-Aware Anomaly Detection for Vehicle Dynamics
ACM CCS	2021	ccs2021-b-paper238.pdf	I Can See the Light: Attacks on Autonomous Vehicles Using Invisible Lights
ACM CCS	2021	ccs2021-b-paper306.pdf	SPARTA: Signal Propagation-Based Attack Recognition and Threat Avoidance for Automotive Networks
ACM CCS	2021	ccs2021-b-paper326.pdf	Who's In Control? On Security Risks of Disjointed IoT Device Management Channels
CPSIOTSEC	2022	cpsiotsec22-paper12.pdf	Secure Reboots for Real-Time Cyber-Physical System
escarUSA	2022	escarUSA_2022_paper_13.pdf	Electric Vehicle Charging Cybersecurity and Intrusion Detection
ACSAC	2022	hotcrp-paper134.pdf	CARdea: Practical Anomaly Detection for Connected and Automated Vehicles
ACSAC	2022	hotcrp-paper313.pdf	SLOPT: Bandit Optimization Framework for Mutation-Based Fuzzing
iccps	2022	iccps2022-paper175.pdf	A Physics-Aware Software Approach to IoT Safety under Cyber-Physical Threats
iccps	2022	iccps2022-paper28.pdf	Real-time Detection of Sensor Replay and Controller Integrity Attacks in Cyber-Physical Systems
NDSS	2022	ndss22-fall-paper180.pdf	GradFuzz: Fuzzing Deep Neural Networks with Gradient Vector Coverage for Adversarial Examples
NDSS	2022	ndss22-fall-paper303.pdf	AVMon: Securing Autonomous Vehicles by Learning Control Invariants and Residual Prediction
NDSS	2022	ndss22-fall-paper329.pdf	RAB: Provable Robustness Against Backdoor Attacks
NDSS	2022	ndss22-fall-paper360.pdf	G2AUTH: Secure Mutual Authentication for Drone Delivery Without Special User-Side Hardware
NDSS	2022	ndss22-fall-paper72.pdf	Evil Robots in the Warehouse: Mitigating Plan-Deviation Attacks with Co-Observations and Horizon-Limiting Announcements
NDSS	2022	ndss22-summer-paper135.pdf	Towards Systematic Defense Testing with Optimal Attack Generation in Cyber-Physical Systems
NDSS	2022	ndss22-summer-paper162.pdf	EMS: History-Driven Mutation for Coverage-based Fuzzing
NDSS	2022	ndss22-summer-paper2.pdf	NWADE: A Neighborhood Watch Mechanism for Attack Detection and Evacuation in Autonomous Intersection Management
NDSS	2022	ndss22-summer-paper71.pdf	SemperFi: Anti-spoofing GPS Receiver for UAVs
NDSS	2022	ndss22-summer-paper77.pdf	PoF: Proof-of-Following for Vehicle Platoons
NDSS	2023	ndss23-fall-paper1176.pdf	We Will Know You by Your Undercarriage: Distinguishing Vehicles Through Wireless Fingerprinting
NDSS	2023	ndss23-fall-paper348.pdf	MetaWave: Attacking mmWave Sensing with Meta-material-enhanced Tags
NDSS	2023	ndss23-fall-paper375.pdf	PHADE: Practical Phantom Spoofing Detection Targeting Unseen Domains for Autonomous Vehicles
NDSS	2023	ndss23-summer-paper13.pdf	Jigsaw Puzzle: Selective Backdoor Attack to Subvert Malware Classifiers
NDSS	2023	ndss23-summer-paper165.pdf	RoVISQ: Reduction of Video Service Quality via Adversarial Attacks on Deep Learning-based Video Compression
SafeThings	2023	safethings2023-paper23.pdf	Software Updates in Vehicles Current Concerns and Future Consideration
USENIX Security	2021	sec21winter-paper335.pdf	CARdea: Practical Anomaly Detection and Prevention for Connected and Automated Vehicles
USENIX Security	2021	sec21winter-paper397.pdf	Same Coverage, Less Bloat: Accelerating Binary-only Fuzzing with Coverage-preserving Coverage-guided Tracing
USENIX Security	2022	sec22fall-paper109.pdf	Physical Attack on Monocular Depth Estimation in Autonomous Driving with Optimal Adversarial Patches
USENIX Security	2022	sec22fall-paper305.pdf	TPatch: A Triggered Physical Adversarial Patch
USENIX Security	2022	sec22fall-paper488.pdf	NEEDLE: Towards Non-invertible Backdoor Attack to Deep Learning Models
USENIX Security	2022	sec22fall-paper501.pdf	OVERTON: A Misbehavior Detection and Trust Framework for Vehicular (V2X) Networks
USENIX Security	2022	sec22summer-paper277.pdf	Adversarial Attack Detection for Deep Learning Driving Maneuver Classifiers in Connected Autonomous Vehicles
USENIX Security	2022	sec22summer-paper442.pdf	Rolling Colors: Adversarial Laser Exploits against Traffic Light Recognition
USENIX Security	2022	sec22winter-paper125.pdf	AVMon: Securing Autonomous Vehicles by Learning Control Invariants and Residual Prediction
USENIX Security	2022	sec22winter-paper138.pdf	Exorcising "Wraith": Protecting LiDAR-based Object Detector in Automated Driving System from Appearing Attacks
USENIX Security	2022	sec22winter-paper254.pdf	DeLorean: Replay-based Recovery for Autonomous Robotic Vehicles from Sensory Deprivation Attacks
USENIX Security	2022	sec22winter-paper504.pdf	AUTOSLAYER: Discovering Adversarial Driving Maneuvers against Autonomous Vehicles
USENIX Security	2023	sec23fall-paper362.pdf	Fides: An Efficient Framework for Client-side Result Verification of Outsourced Machine Learning Workloads via Trusted Execution Environment
USENIX Security	2023	sec23summer-paper234.pdf	Evaluating Compressive Sensing on the Security of Computer Vision Systems
USENIX Security	2023	sec23winter-paper310.pdf	DarkneTE: Trusted Deep Learning Inference on Heterogeneous Edge Devices with TEE
USENIX Security	2023	sec23winter-paper472.pdf	RoboRebound: Multi-Robot System Defense with Bounded-Time Interaction
USENIX Security	2024	sec24summer-paper100.pdf	Experimental Security Analysis of DNN-based Adaptive Cruise Control under Context-Aware Perception Attacks
USENIX Security	2024	sec24summer-paper1096.pdf	Tossing in the Dark: Practical Bit-Flipping on Gray-box Deep Neural Networks for Runtime Trojan Injection
IEEE S&P	2024	sp2024summer-paper355.pdf	Simon says, enchanted — Sensor Deprivation Attacks on UAVs via serial device reconfiguration
IEEE S&P	2024	sp2024summer-paper538.pdf	Rethinking Invariants and Estimators: A Robust Diagnosis Filter for Securing Robotic Aerial Vehicles
VehicleSec	2023	vehiclesec-paper30.pdf	TrainSec: A Simulation Framework for Security Modeling and Evaluation in CBTC Networks
WiSec	2023	wisec23-paper50.pdf	Vulnerability Analysis of Vehicular Coordinated Maneuvers
WiSec	2023	wisec23-paper59.pdf	PoolSecArch: Secure Carpooling in Connected Autonomous Vehicular Networks
WiSec	2023	wisec23-winter-paper15.pdf	OPINION: Future-proofing VANET Security and Resilience

Alfred Chen <alfchen@uci.edu> Wed, Dec 20, 2023 at 11:48 PM
To: [redacted]

The list is long and it will take time for me to review and confirm. I do not think this can really help your green card application. [redacted] I believe what they are looking for in these review services is evidence that you are viewed as an expert in a research community, by being invited by these top community venues as a reviewer/PC. Here, I am the invitee, not you. Getting review assignment by me does not give you evidence that YOU are the expert viewed by the community; it's just a research assignment that any PhD student can get.

Alfred
[Quoted text hidden]
--
Stay safe,
Alfred Chen

Assistant Professor,
Department of Computer Science,
University of California, Irvine
Tel: 1-734-834-2916
Alt. Email: adios737@gmail.com
Homepage: https://www.ics.uci.edu/~alfchen

[redacted] Thu, Dec 21, 2023 at 12:04 AM
To: Alfred Chen <alfchen@uci.edu>

Since I've done all these, I think adequate acknowledgement is what I deserve. Please let me know when you think you can finish.

Best,
[redacted]

> On Dec 20, 2023, at 23:49, Alfred Chen <alfchen@uci.edu> wrote:
>
> [Quoted text hidden]

Alfred Chen <alfchen@uci.edu> Thu, Dec 21, 2023 at 8:40 PM
To: [redacted]

Finishing research tasks assigned by your advisor is your duty, [redacted], and any PhD student should do that. I do not think getting confirmation that you can finish your duties is something that can make you standout in green card applications. But anyway, since you insist:

1) You, as the original reviewer, assigned these papers to me as internal research tasks, and I wrote reviews for these papers
Yes, I am the original reviewer/PC who got invited by these top venues as a domain expert to judge tthese papers. I assigned these papers to [redacted] as a common internal research task as part of the PhD training. All PhD students in my group get such internal review task assignments. [redacted] did write reviews for these papers.

2) Whether I was acknowledged publicly/externally for the reviews I wrote (e.g., credited in a way that other people can see), and if not, why
As said above, this is a common internal research task as part of the PhD training. Thus, there are no public/external acknowledgements for him to finish these tasks.

3) How my reviews were used for your review task, e.g., you submit my review after minor changes (like fixing typos, grammatical errors, and formatting issues), or you submit the review after merging the contents with reviews from other students, etc.
I do not think I should give you information on these. This is on how I finish my assignment tasks, not on how you finish yours assigned by me. I do not think I should confirm to you how I finish my tasks.

Alfred
[Quoted text hidden]