

Who Moved My Transaction? Uncovering Post-Transaction Auditability Vulnerabilities in Modern Super Apps

Junlin Liu
Peking University
Beijing, China
jlinliu@pku.edu.cn

Mengyu Yao
Peking University
Beijing, China
mengyuyao@stu.pku.edu.cn

Ziqi Zhang*
University
of Illinois Urbana-Champaign
Champaign, IL, USA
ziqi24@illinois.edu

Zhaomeng Deng
Peking University
Beijing, China
infinityedge@pku.edu.cn

Yifeng Cai
Peking University
Beijing, China
caiweifeng@pku.edu.cn

Yao Guo
Peking University
Beijing, China
yaoguo@pku.edu.cn

Ziming Wang
Peking University
Beijing, China
wangzim@stu.pku.edu.cn

Yutao Hu
Huazhong
University of Science and Technology
Wuhan, China
yutao@hust.edu.cn

Ding Li*
Peking University
Beijing, China
ding_li@pku.edu.cn

Abstract

Super apps are the cornerstones of modern digital life, embedding financial transactions into nearly every aspect of daily routine. The prevailing security paradigm for these platforms is overwhelmingly focused on pre-transaction authentication, preventing unauthorized payments before they occur. We argue that a critical vulnerability vector has been largely overlooked: the fragility of post-transaction audit trails. We investigate the ease with which a user can permanently erase their transaction history from an app's interface, thereby concealing unauthorized or sensitive activities from the account owner. To quantify this threat, we conducted an empirical study with 6 volunteers who performed a cross-evaluation on six super apps. Our findings are alarming: all six applications studied allow users to delete transaction records, yet a staggering five out of six (83+%) fail to protect these records with strong authentication. Only one app in our study required biometric verification for deletion. This study provides the first concrete evidence of this near-ubiquitous vulnerability, demonstrating a critical gap in the current mobile security landscape and underscoring the urgent need for a paradigm shift towards ensuring post-transaction audit integrity.

CCS Concepts

• **Security and privacy** → **Usability in security and privacy**; *Mobile platform security*.

*Corresponding author(s).

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

SaTS '25, Taipei, Taiwan (Province of China)

© 2025 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM ISBN 979-8-4007-1912-7/2025/10

<https://doi.org/10.1145/3733824.3764877>

Keywords

Super Apps, Mobile Payment Security, Post-Transaction Auditability, Empirical Study

ACM Reference Format:

Junlin Liu, Zhaomeng Deng, Ziming Wang, Mengyu Yao, Yifeng Cai, Yutao Hu, Ziqi Zhang, Yao Guo, and Ding Li. 2025. Who Moved My Transaction? Uncovering Post-Transaction Auditability Vulnerabilities in Modern Super Apps. In *Proceedings of the 2025 Workshop on Security and Privacy of AI-Empowered Mobile Super Apps (SaTS '25)*, October 13–17, 2025, Taipei, Taiwan (Province of China). ACM, New York, NY, USA, 3 pages. <https://doi.org/10.1145/3733824.3764877>

1 Introduction

In many digital economies, super apps are not merely applications but are foundational operating systems for daily life. They seamlessly integrate communication, social media, e-commerce, and, most critically, financial services, processing trillions of dollars in transactions annually [9, 10]. Consequently, securing these platforms is a matter of paramount importance.

The current security focus, however, exhibits a crucial blind spot. The industry has invested immense resources in a strategy that can be termed pre-transaction defense [2, 11]. This approach involves erecting sophisticated fortifications, such as biometric authentication and AI-driven fraud detection, with the explicit goal of stopping illicit payments before they happen. While essential, this raises a vital question: what happens if an unauthorized transaction gets through? Can we guarantee its discovery?

This paper argues that the integrity of the post-transaction audit trail is a dangerously neglected aspect of security. This record is a cornerstone of user trust and control, yet it can often be easily erased, allowing malicious actors or even family members to conceal their activities. To address this gap, we introduce the principle of Post-Transaction Auditability and provide the first empirical study to measure this vulnerability in dominant super apps. Our findings

are alarming: while all six tested applications allow record deletion, a staggering five out of six do so without strong authentication.

The main contributions of this paper are:

- We are the first to identify and formalize the threat of post-transaction record tampering in super apps, presenting a realistic threat model that considers both opportunistic insiders and malicious software.
- We introduce Post-Transaction Auditability as a new, critical security principle for financial applications, shifting focus from merely preventing bad transactions to ensuring they can always be discovered.
- We present the first empirical study that quantifies this vulnerability across six dominant super apps, demonstrating that the lack of protection is a systemic and widespread issue (83+% of tested apps are vulnerable).

2 Background

Existing Research on Payment Security. Extensive research in mobile payment security has concentrated on pre-transaction vulnerabilities. This body of work covers critical topics such as defeating biometric sensors [1, 8], phishing attacks for credentials [4, 7], and analyzing risks in NFC and QR code protocols [3, 5]. Similarly, UI security research has often focused on preventing tapjacking or other overlay attacks [6, 12]. However, the specific threat of a legitimate (or seemingly legitimate) user intentionally corrupting the audit trail after a successful transaction remains a significant and unaddressed research gap. Our work distinguishes itself by focusing on *preserving the record*.

Threat Model. We formalize our investigation with a clear threat model: the attacker’s primary goal is to permanently hide one or more transaction records from the user interface, thereby preventing the legitimate account owner from detecting the activity. We consider two representative attacker profiles, i.e., an opportunistic insider or a malicious software.

3 Empirical Study Demo

Methodology. To assess the real-world prevalence of this vulnerability, we conducted a controlled empirical study designed to answer a specific research question: What level of security do leading super apps implement to protect their transaction records from user-initiated deletion? We selected six of the world’s most dominant super apps. These platforms are representative of the ecosystem, each boasting hundreds of millions of daily active users and featuring a deeply integrated payment system.

The study involved six volunteers, and was conducted in a controlled lab setting. We prepared six smartphones, each pre-configured with a test account for one of the target applications. Each volunteer was randomly assigned a device at the beginning of the experiment. We employed a cross-evaluation design where participants rotated among the devices, ensuring that every volunteer systematically evaluated all six applications. For each app, the designated task was to locate the most recent transaction record, attempt to delete it, and meticulously document the UI path and any authentication challenges encountered during the process.

Results. Our study revealed a critical and widespread security vulnerability regarding how leading super apps handle the deletion of financial records. The most alarming finding is the near-complete absence of strong authentication for this sensitive action, allowing for the easy concealment of transactions.

Table 1: Authentication Requirements for Deleting Transaction Records in Six Dominant super apps.

App	Verification Level	App	Verification Level
AliPay	Biometrics	WeChat	Pop-up Only
Taobao	Pop-up Only	JD	Pop-up Only
TikTok	Pop-up Only	MeiTuan	Pop-up Only

The detailed findings of our experiment are summarized in Table 1. The central conclusion is that a staggering five out of six applications tested (approximately 83%) permit users to permanently erase transaction histories without requiring a password, PIN, or biometric verification.

As shown in Table 1, only a single application, AliPay, has implemented a robust biometric safeguard. The vast lack of protection demonstrates that the risk is not an isolated oversight but appears to be a systemic issue and the de facto standard for the majority of the market leaders we investigated. While the existence of a deletion feature in all six apps highlights user demand for such functionality, it has clearly been implemented at the expense of fundamental audit integrity.

Findings. In conclusion, the absence of strong verification mechanism for deleting financial records indicates a systemic failure in design philosophy. It suggests that a majority of super app developers prioritize UI convenience over the fundamental security principle of audit integrity. This is a dangerous trade-off that leaves billions of users exposed.

For users, this study highlights a hidden risk. The assumption that their transaction history is a secure and reliable record is false. For the industry, our work is an urgent call to action. Implementing strong authentication for record deletion is not a complex engineering challenge; it is a matter of acknowledging the risk and prioritizing user security.

Meanwhile, as a preliminary study, our sample size of six super apps and six volunteers is small. However, the result provides a strong signal that this is a widespread issue worthy of immediate attention and larger-scale investigation.

4 Conclusions and Future Work

This paper provides the first empirical evidence of a critical vulnerability in modern super apps: the lack of strong authentication for deleting post-transaction audit trails. Our finding that 83.3% of dominant platforms are vulnerable decisively challenges the current pre-transaction security paradigm. The integrity of a financial record is a fundamental security requirement, not a convenience.

Building on this preliminary study, which provides a strong signal of a widespread issue, our future work will proceed in two directions. First, we will develop an automated testing pipeline to perform a comprehensive, large-scale market analysis. Second, we plan to formalize our criteria into a public “Post-Transaction Auditability” benchmark to empower developers and allow for standardized comparison of apps.

Acknowledgments

We would like to thank the anonymous reviewers for their valuable feedback. This work was supported by the National Science and Technology Major Project of China (2022ZD0119103).

References

- [1] Yifeng Cai, Ziqi Zhang, Jiaping Gui, Bingyan Liu, Xiaoke Zhao, Ruoyu Li, Zhe Li, and Ding Li. 2024. {FAMOS}: Robust {Privacy-Preserving} Authentication on Payment Apps via Federated {Multi-Modal} Contrastive Learning. In *33rd USENIX Security Symposium (USENIX Security 24)*. 289–306.
- [2] Yifeng Cai, Ziqi Zhang, Mengyu Yao, Junlin Liu, Xiaoke Zhao, Xinyi Fu, Ruoyu Li, Zhe Li, Xiangqun Chen, Yao Guo, et al. 2025. I Can Tell Your Secrets: Inferring Privacy Attributes from Mini-app Interaction History in Super-apps. *arXiv preprint arXiv:2503.10239* (2025).
- [3] Dennis Giese, Kevin Liu, Michael Sun, Tahin Syed, and Linda Zhang. 2019. Security analysis of near-field communication (NFC) payments. *arXiv preprint arXiv:1904.10623* (2019).
- [4] Urvashi Kishnani, Naheem Noah, Sanchari Das, and Rinku Dewri. 2022. Privacy and security evaluation of mobile payment applications through user-generated reviews. In *Proceedings of the 21st Workshop on Privacy in the Electronic Society*. 159–173.
- [5] Steffen Klee, Alexandros Roussos, Max Maass, and Matthias Hollick. 2020. {NFCGate}: Opening the Door for {NFC} Security Research with a {Smartphone-Based} Toolkit. In *14th USENIX Workshop on Offensive Technologies (WOOT 20)*.
- [6] Luka Malisa, Kari Kostiaainen, and Srdjan Capkun. 2017. Detecting mobile application spoofing attacks by leveraging user visual similarity perception. In *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*. 289–300.
- [7] Yutian Tang, Yulei Sui, Haoyu Wang, Xiapu Luo, Hao Zhou, and Zhou Xu. 2020. All your app links are belong to us: understanding the threats of instant apps based attacks. In *Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering*. 914–926.
- [8] Chao Wang, Yanjie Zhao, Jiapeng Deng, and Haoyu Wang. 2025. Born with a silver spoon: On the (in) security of native granted app privileges in custom android roms. In *2025 IEEE Symposium on Security and Privacy (SP)*. IEEE, 4267–4283.
- [9] Yuqing Yang, Chao Wang, Yue Zhang, and Zhiqiang Lin. 2023. Sok: Decoding the super app enigma: The security mechanisms, threats, and trade-offs in os-alike apps. *arXiv preprint arXiv:2306.07495* (2023).
- [10] Yuqing Yang, Yue Zhang, and Zhiqiang Lin. 2025. Understanding Miniapp Malware: Identification, Dissection, and Characterization. In *Proceedings 2025 Network and Distributed System Security Symposium. San Diego, CA, USA*.
- [11] Yue Zhang, Yuqing Yang, and Zhiqiang Lin. 2023. Don't leak your keys: Understanding, measuring, and exploiting the appsecret leaks in mini-programs. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*. 2411–2425.
- [12] Hao Zhou, Ting Chen, Haoyu Wang, Le Yu, Xiapu Luo, Ting Wang, and Wei Zhang. 2020. Ui obfuscation and its effects on automated ui analysis for android apps. In *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*. 199–210.