Shared Account Problem in Super Apps

Yifeng Cai
caiyifeng@pku.edu.cn
Key Lab of HCST (PKU), MOE
SCS, Peking University
Beijing, China

Ziqi Zhang
ziqi_zhang@pku.edu.cn
Key Lab of HCST (PKU), MOE
SCS, Peking University
Beijing, China

Ding Li
ding_li@pku.edu.cn
Key Lab of HCST (PKU), MOE
SCS, Peking University
Beijing, China

Yao Guo
yaoguo@pku.edu.cn
Key Lab of HCST (PKU), MOE
SCS, Peking University
Beijing, China

Xiangqun Chen
cherry@pku.edu.cn
Key Lab of HCST (PKU), MOE
SCS, Peking University
Beijing, China

ABSTRACT

The rapid digitization of various services has led to the emergence of super apps, providing an array of utilities under one application. A common usage scenario of such platforms, such as Alipay, involves shared accounts by multiple users, typically within a family. However, this shared use poses a unique challenge to the security protocols designed to prevent unauthorized access, as they can misinterpret legitimate multi-user behavior as fraudulent activity. In this paper, we explore the complexities involved in accurately discerning such shared usage from potential security threats and investigate current solutions. It aims to stimulate discussion around a more flexible, adaptive, and user-inclusive approach to account security in the evolving landscape of super apps.

CCS CONCEPTS

• **Security and privacy → Software and application security**.

KEYWORDS

Super app; shared account problem; security protocol

ACM Reference Format:
Yifeng Cai, Ziqi Zhang, Ding Li, Yao Guo, and Xiangqun Chen. 2023. Shared Account Problem in Super Apps. In *Proceedings of the 2023 ACM Workshop on Secure and Trustworthy Superapps (SaTS '23), November 26, 2023, Copenhagen, Denmark*. ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3605762.3624426

1 INTRODUCTION

In the rapidly progressing digital age, the ubiquity of multi-functional applications, or 'super apps', has dramatically reshaped our quotidian activities [3]. These platforms amalgamate an array of services, transforming our smartphones into versatile tools that cater to our diverse digital needs [6]. Among the myriad of super apps, Alipay stands as a prime exemplar, embodying this transformative wave and emerging as an integral part of life for a significant populace not just in China, but across the globe [4]. However, with this growing integration of super apps into the fabric of our everyday routines, a host of new challenges and complexities associated with their use have begun to surface [1, 5, 8], necessitating a comprehensive analysis and understanding.

One prominent trend within the realm of super apps usage is the practice of shared accounts, particularly prevalent within familial contexts. Parents and children or couples often share a single account across various services offered by the platform, ranging from online payments to social networking and more. On the face of it, shared usage offers multiple practical benefits such as increased convenience, cost-effectiveness, and for some, a mechanism for parental control over younger users' online activities. However, it simultaneously ushers in complexities and hurdles in the sphere of account security.

The innate security protocols of these super apps, tailored to safeguard users against unauthorized access or fraud, scrutinize user behavior for any signs of inconsistency or unfamiliar patterns. In the traditional sense, such variations would raise red flags, indicating potential threats to account security. However, in a shared account setting, what the security algorithms interpret as 'irregular' is often a typical variation in the usage patterns across different users. As a result, these protocols can inadvertently mistake normal shared account activity as a security risk, prompting unnecessary security checks or account freezes, and consequently causing significant inconvenience to legitimate users.

Such a scenario underlines a nuanced dilemma. Super apps, on the one hand, need to uphold stringent security measures to safeguard user accounts, thereby preserving the trust and confidence of their user base - a key factor contributing to their continued success. However, these measures, on the other hand, also need to demonstrate flexibility and adaptability to accommodate shared usage patterns, thereby ensuring that their security protocols do not hamper user experience or functionality. Achieving this delicate balance between robust security and user-friendly operation forms the very crux of the challenge at hand.

In this paper, we dedicate an in-depth exploration of this multi-faceted issue. Specifically, We present results from a study of device account-sharing practices in super apps. Our study involved interviews with 50 participants about why and how account sharing

SaTS '23, November 26, 2023, Copenhagen, Denmark.

ACM ISBN 979-8-4007-0258-7/23/11…$15.00
https://doi.org/10.1145/3605762.3624426

occurred. Our key findings are that account sharing is common in super apps usages, even though users typically perceived super app accounts as personal information. Thus, we further study the complexities of shared account usage in super apps, the implications on their security protocols, and the effectiveness of solutions.

By shedding light on these critical aspects, we aim to underscore the pressing need for a more adaptive, flexible, and inclusive approach to account security in super apps. We believe it is important to recognize and adapt to the diverse and dynamic ways in which users use these super app platforms, and to enhance the robustness of security protocols.

2 BACKGROUND

2.1 Shared Account Usage

Typically, one account corresponds to a specific user in super apps, playing an essential role in the user's daily life. To be more precise, an account records a user's basic information, credit status, and facilitates quick payment through linked debit or credit cards. Therefore, it usually necessitates users to possess complete payment capabilities.

In the realm of super apps, shared account usage often manifests within family units, where one account is utilized by multiple members. This might occur for several reasons. Here, we give three typical cases with shared accounts.

Case 1. Minors. Super apps such as Alipay or WeChat require users to have their own bank account in order to complete real-name authorization and gain full transaction functionality. In reality, some users may not be able to use their accounts to make online payments. For example, in China, minors under the age of 16 are not eligible to apply for their own bank card. However, in daily life, there are many scenarios where minors need to scan codes to make payments. Therefore, minors usually use their parents' Alipay accounts to make payments, and it is easy for parents to monitor the payment records of minors.

Case 2. Elder Parents. In addition, due to their limited proficiency with smartphones or super apps, older people often refuse to apply for their own payment accounts and instead use their children's accounts. Similarly, children may argue that allowing their parents to use their own accounts is effective in preventing them from being scammed, due to the fact that large transfers require a more advanced form of authentication that can only be passed by themselves.

Case 3. Couples. In the above cases, the functionally-limited users share an account with family members. However, this last typical situation does not include functionally-limited users, but rather couples using a single account. Since some super apps, such as Alipay and Meituan, have low social attributes and are seldom used for sending messages, couples use the same account to make online purchases and order takeout to prevent duplicate purchases and to be able to manage money together.

To demonstrate the existence of this shared usage, we conducted a survey for 50 super app users aged between 35 and 50 years, with the issue of account sharing. The details are shown in Table 1. The survey revealed that 45 out of the 50 users shared their accounts, with 37 of them involved in long-term shared usage. Of these, 35 shared their accounts for their minor children, 10 for their elder parents, and 6 for their couple. It's worth clarifying that the question is a multi-option one, proving that there are users with more than one type of account sharing. Additionally, we investigated their initial intentions for using shared accounts. All users involved in account sharing believed that sharing accounts helped to circumvent the complexities of applying for bank accounts. Simultaneously, 26 users opined that direct account sharing aided them in supervising the other user's payment activities, preventing children or older adults from making unknown payments.

Table 1: A survey of shared accounts in super apps. (M) denotes a multi-option question.

Content	Total
Q1: Have you ever shared a super app account?	**50**
A1_1: Yes	45
A1_2: No	5
Q2: Has the account been shared for a long-term?	**45**
A2_1: Yes	37
A2_2: No	8
Q3: Who are you sharing the account with? (M)	**45**
A3_1: Children	35
A3_2: Parents	10
A3_3: Couple	6
Q4: What are your top considerations for using a shared account? (M)	**45**
A4_1: Children	**35**
A4_1_1: Children's inability to open bank accounts	25
A4_1_2: Supervision of children's daily expenses	16
A4_2: Parents	**10**
A4_2_1: Parents do not have their own payment accounts	7
A4_2_2: Preventing fraud	7
A4_3: Couple	**6**
A4_3_1: Joint management of finances	4
A4_3_2: Expressions of affection and trust	3
Q5: What's the problem you're facing when using a shared account? (M)	**45**
A5_1: Can't log in at the same time	35
A5_2: Duplicate authentication	31

2.2 Intersection of Shared Use and Security Risks

The challenge arises when shared usage intersects with security risks. Current security models are mainly based on the presumption of a single user per account. Thus, sudden changes in usage patterns, geographical location, transaction behavior, or interaction with different services could be interpreted as potential threats or intrusions. In shared accounts, however, such changes could merely reflect the switch from one legitimate user to another within the shared group.

Existing user authentication techniques also obey the above assumption that the model used in the app authenticates for a particular user. For example, the existing state-of-the-art technique AuthentiSense [2] uses a Siamese network to achieve user-senseless authentication in payment apps by sampling the action data of the user's daily operating behavior from the motion sensors. However, the technique is designed for single-user authentication and failed to accept multiple users. To demonstrate the limitation of the existing technique, we constructed a small experiment using data from users' daily usage of Alipay. Notably, we followed the assumption in AuthentiSense that the users are operating the same actions without any background noises. We compare the F1-Score of user

authentication between a single user and multiple users. When AuthentiSense only involves a single user, the F1-Score can reach 0.93, which is a desirable result. However, when multiple users are involved, the F1-Score of AuthentiSense drops to 0.68 significantly.

Table 2: Common authentication methods in super apps.

Authentication Type	Security Level	Support for Multi-users
Device built-in touch/face ID	0	Yes
PIN/Password	1	Yes
Sensors	2	No
Face recognition service (server)	3	No
Voiceprint	4	No
Live video	5	No

When a user's identity is difficult to be authenticated, more advanced authentication methods, such as face recognition, voiceprint, or live videos, will be invoked for security purposes. The common authentication methods are illustrated in Table 2. In the second column, a higher number indicates a higher security level. However, more advanced authentication methods require users to make longer and more complex actions, which significantly reduces the user experience. In addition, since an account can only be tied to the information of one natural person, more advanced authentication will surely be a complete loss of access to the app for the user of the shared account. Hence, our solution should lie in developing a system that can differentiate between these instances of legitimate shared usage and actual instances of account misuse or hacking.

In the following sections, we will delve into the strategies currently in place to tackle this issue, their limitations, and the potential for future development. We will also propose possible modifications to better accommodate shared account usage.

3 METHODS

In super apps, service providers often want to ensure a higher user experience while keeping user accounts as secure as possible. First, the model deployment strategy needs to be adapted when confronted with shared accounts. That is, from one account corresponding to one feature or one model, it is adjusted to one device, or one possible trusted user corresponding to one feature or model. Therefore, in Alipay, we developed the following technologies that mainly judge from the login device, payment behavior, actions, etc., whether there is account sharing.

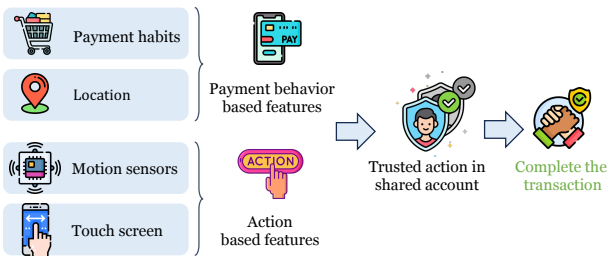

Figure 1: The framework of identifying shared accounts and completing the trusted transaction.

3.1 Naive Idea: Login Device Features

When a super app needs to determine whether an account is being simultaneously accessed by multiple individuals, the most straightforward approach is to examine changes in the login devices and their long-term access permissions. Specifically, upon the initial login of a new device, the server records unique identifiers for that device (e.g., IMEI, MAC address, etc.), logs out the account from the original device, and prompts the user with relevant information such as "If this is not your action, please promptly change your password." After the account has been successfully accessed multiple times from the new device, it can be considered as an authorized action and categorized as a normal behavior for shared accounts, allowing for a reduction in risk control measures. Additionally, as Alipay currently prohibits multiple device logins for the same account, only the latest login device will be permitted for regular usage.

Limitations. In cases where malicious attackers gain control over a particular device, they can easily log into the account from another device and acquire the "allowed" status. Consequently, the super app server will recognize this as an authorized new device, inadvertently permitting unauthorized actions. This poses potential risks to payment security and legal compliance. Hence, a more secure method of verification is required.

3.2 Payment Behavior-based Features

One viable approach involves utilizing payment habits for modeling purposes. In other words, risk assessment can be based on users' consumption patterns. In common scenarios of shared accounts, there is often a significant disparity in consumption habits between the main user and the shared user. For example, in a parent-child shared account scenario, the main user's spending habits are usually more complex, encompassing various aspects of life, travel, and shopping, which can be modeled as adult consumption behavior. On the other hand, the shared user, typically a child, tends to make smaller transactions, primarily in the retail industry, which can be modeled as minor's consumption behavior. Moreover, by considering the geographical location of completed payments, consumption patterns can be further identified. Consequently, by combining these characteristics, the risk level of the shared account device can be determined. When an inconsistency with the corresponding consumption pattern of the current device occurs, advanced identity authentication can be triggered.

3.3 Action-based Features

Another feasible approach involves modeling the action-based characteristics of each user. This method entails capturing sensor readings generated during the operation of the super app through mobile sensors and touch screen sensors. Advanced technologies such as deep learning can then be employed to recognize whether the user is the legitimate account holder. Different users exhibit distinct action preferences while using the app, such as variations in tapping intensity, shaking amplitude, and other patterns. Leveraging these differences, it becomes possible to determine whether the user is the legitimate account holder. Unlike previous methods, this model is designed to encompass all shared users of an account and can integrate multiple sensors, achieving a more robust outcome.

By combining payment behavior-based features with action-based features, it becomes possible to identify shared accounts to a certain extent without disrupting user experience. Effective modeling of multiple users enables risk identification. In Alipay, we have devised the following framework to assess account risks, as shown in Figure 1.

4 EVALUATION

4.1 Evaluation Protocol

Data Collection. We collected the daily usage characteristics of 10,000 accounts from the Alipay-dev application, among which 2,000 accounts were shared. The ground truth regarding these accounts was determined by other departments within Alipay through user surveys and analysis of user usage patterns, ensuring the reliability of the results. Each data entry contains the following information:

Device information includes IMEI and geographical location.

User information includes the user's identity information.

Payment behavior information covers historical payment data, such as timestamps, amounts, merchant types, and locations.

Action information encompasses touchscreen data (click timestamps, locations, duration, and pressure) and motion sensor data (timestamps, accelerometer, magnetometer, and gyroscope).

It is essential to note that all users of the Alipay-dev have consented to provide this sensitive information, and the data is strictly protected within Alipay's internal servers.

Evaluation Metric. We mainly report the Area Under ROC Curve (AUC) metric. Specifically, the AUC metric is based on four major metrics: the True Positive, False Negative, True Negative, and False Positive results in detecting the shared account usage problem under different thresholds.

The AUC depends on the various thresholds that decide whether the account is shared. The Receiver Operating Characteristic (ROC) curve plots the True Positive Rate ($TPR = \frac{TP}{TP+FN}$) against False Acceptance Rate ($FAR = \frac{FP}{TN+FP}$) in different thresholds.

The resulting area between such curve and the X-axis at an interval of [0, 1] is termed AUC and evaluate the performance in detecting shared account.

Implementation Details. We implement the detection framework with Python 3.7 and PyTorch 1.8. The framework runs on a server with Ubuntu 20.04.6, 128 GB memory, 48 cores provided by Intel Xeon CPUs, and 4 NVIDIA GeForce GTX 2080Ti GPUs. All experiments are repeated by 3 times and reported the average performance.

4.2 Result

To demonstrate the effectiveness of detecting shared account problems, we present in Table 3 the performance of detecting shared accounts using payment behavior features, action features, and their combination. When combining both features, the AUC reaches 0.88, which represents the best performance. Moreover, using payment behavior features (0.79) or action features (0.78) separately shows little difference, but when compared to their combination, there is a significant drop in performance.

Table 3: AUC of detecting shared accounts.

Features	Payment	Action	Payment+Action
AUC	0.79	0.78	0.88

5 RELATED WORK

Super apps have emerged as an innovative and convenient platform that offers a wide range of services within a single application [6]. While these apps bring numerous benefits to users, they also introduce unique security and privacy challenges. Researchers have explored various methods and mechanisms to enhance trust and accountability, such as user authentication techniques [2], Cross-miniapp allowlisting [7], and API restrictions [5]. However, the security concerns surrounding super apps become even more critical. one of which is the shared account problem. Detecting timely and ensuring safety in shared accounts is crucial for maintaining user satisfaction and preventing misuse.

6 CONCLUSION

In conclusion, shared account problem presents security challenges. Current security protocols may misinterpret normal variations in multi-user behavior, causing inconveniences for legitimate users. In this paper, we underscore the need for an adaptive, user-inclusive approach to account security. By studying device account-sharing practices and implications on security protocols, we emphasize the importance of striking a delicate balance between robust security and seamless user experience. Developers must enhance security measures to accommodate shared usage while maintaining user trust. Moreover, we propose a shared account detection mechanism, which uses the payment behavior features and action features to detect the possibility of accounts whether shared with multiple users. Evaluation demonstrates the proposed solution achieves respectable performance.

ACKNOWLEDGMENTS

Ding Li and Yao Guo are corresponding authors. This work was sponsored by CCF-AFSG Research Fund (RF20220006).

REFERENCES

[1] Supraja Baskaran, Lianying Zhao, Mohammad Mannan, and Amr Youssef. 2023. Measuring the Leakage and Exploitability of Authentication Secrets in Super-apps: The WeChat Case. *arXiv:2307.09317* (2023).

[2] Hossein Fereidooni, Jan König, Phillip Rieger, Marco Chilese, Bora Gökbakan, Moritz Finke, Alexandra Dmitrienko, and Ahmad-Reza Sadeghi. 2023. AuthentiSense: A Scalable Behavioral Biometrics Authentication Scheme using Few-Shot Learning for Mobile Platforms. *arXiv:2302.02740* (2023).

[3] Marc Hasselwander. 2023. Digital platforms' growth strategies and the rise of super apps.

[4] Lerong Lu. 2018. Decoding Alipay: mobile payments, a cashless society and regulatory challenges. *Butterworths Journal of International Banking and Financial Law* (2018), 40–43.

[5] Chao Wang, Yue Zhang, and Zhiqiang Lin. 2023. Uncovering and Exploiting Hidden APIs in Mobile Super Apps. *arXiv:2306.08134* (2023).

[6] 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:2306.07495* (2023).

[7] Yuqing Yang, Yue Zhang, and Zhiqiang Lin. 2022. Cross miniapp request forgery: Root causes, attacks, and vulnerability detection. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*. 3079–3092.

[8] Yue Zhang, Yuqing Yang, and Zhiqiang Lin. 2023. Don't Leak Your Keys: Understanding, Measuring, and Exploiting the AppSecret Leaks in Mini-Programs. *arXiv:2306.08151* (2023).