White paper (supporting material for Black Hat USA 2025)

Lost & Found: The Hidden Risks of Account Recovery in a Passwordless Future

Link to the Black Hat USA 2025 talk:
https://www.blackhat.com/us-25/briefings/schedule/#lost--found-the-hidden-risks-of-account-recovery-in-a-passwordless-future-46431

1. Introduction

Creating user accounts for online services has become an integral part of the Internet experience. User accounts enable online service providers to refine their services based on user behavior and enhance user interactions. Meanwhile, the users benefit from the tailored content, features, and services that may otherwise be restricted to anonymous users. Users create their accounts by providing basic information and setting up an authentication method that safeguards the website-specific user information against unauthorized access. The primary focus of our work in this paper is account recovery, a mechanism that allows users to reclaim control over their account when they forget or mislay the authentication credentials. Authentication using a username and password is the most common among the various methods that can be employed. Consequently, account recovery is widely referred to as a forgot password or password recovery mechanism.

Providing an account recovery mechanism is essential as users often forget or mislay their authentication credentials. There are also situations such as traveling abroad or losing personal devices during which the credentials are inaccessible to the user, which compels them to request access to the user accounts using account recovery. According to recent reports, 4 out of 5 users have forgotten at

least one credential within the last 90 days, with 25% experiencing the need for account recovery on a daily basis. These numbers highlight the prevalence and crucial role of account recovery mechanisms in ensuring continued access to user accounts.

Account recovery typically involves the service provider sending a recovery token (e.g., one-time password or link) to a channel or method that is pre-agreed with the user. Situated beyond the service provider's direct control, these channels inherently require the assumption that they remain uncompromised by adversaries, especially during recovery. The service providers have to blindly trust that the recovery channel is intact and reauthenticate someone claiming to be a benign user. Moreover, account recovery compels service providers to lower their security barriers by placing an inherent trust in a factor whose security is unknown or uncertain. Therefore, account recovery could be an attractive and relatively easy gateway for adversaries to gain control over user accounts.Due to the serious security implications, analysis of account recovery is an interesting research topic.

Our goal is to improve understanding of account recovery mechanisms by identifying security flaws and improvement opportunities. Previous research works have attempted doing this by following a generic analysis approach to highlight security flaws, e.g., due to poorly designed account recovery mechanisms. We follow a similar approach and conduct security analyses of account recovery of popular websites in the wild. However, we provide a new perspective by considering the availability of various authentication factors at the time of account recovery. Analyzing with respect to the account state from which recovery is carried out has two benefits. First, it helps to evaluate granular details of the recovery procedure that prior studies have overlooked while following a high-level or generic methodology. Secondly, it provides insights into the potential underutilization of security factors at the service provider's disposal during recovery.

The security issues highlighted in this work are not the typical software vulnerabilities. Instead, they are issues arising from inefficient security policies and processes that low-tech adversaries can exploit. Both research and practice seem to have overlooked this problem [28]. Security certification audits and penetration tests evaluate some aspects of security policies and processes. However, insights from such activities alone could become repetitive and less valuable over time.

One proposition is to conduct external validation of security policies and processes to identify research-practice gaps and overlooked best practices, as demonstrated in recent works on user authentication. We apply this strategy in our work — our auditing framework guides the analysis of security policies and processes by presuming an adversary's role from outside the system. Such an analytical approach can be regarded as an attack surface mapping activity focused on account recovery. The insights could complement those of penetration testing. Thus, our work carries both research merit and practical applications.

2. Background

Account Recovery Life Cycle: The account recovery life cycle comprises different stages. It begins when a user claims to be unable to log in to their account and ends when they regain control of the account and resume normal usage. We identify six steps in this life cycle, as described below and shown in Figure 1.

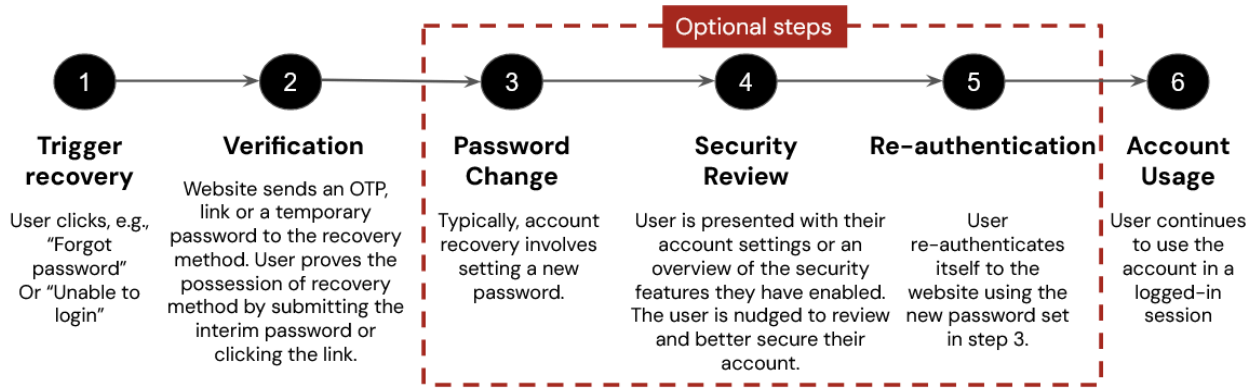

Figure 1: Different steps of an account recovery life cycle

Account states: The recovery process of a website may vary depending on the availability of the authentication factors—such as passwords, recovery methods, and two-factor authentication (2FA) methods—associated with a user account. We identified various account states based on the available authentication factors linked to a user account. These account states were used as a reference to design our test cases. Recovery can be initiated and potentially completed from any of these account states.

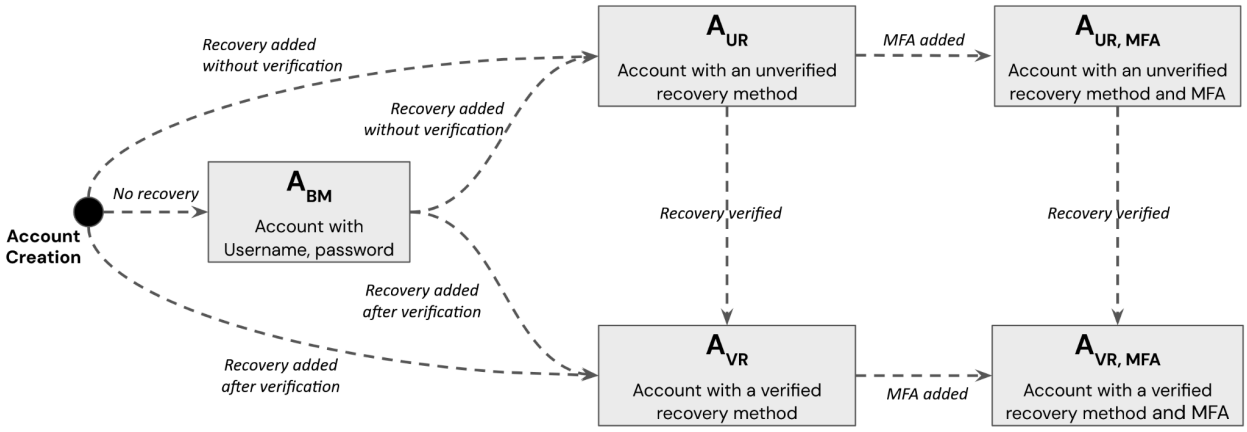

Figure 2: Various Account States and transitions

There are multiple possible account states when a user account is created, depending on the requirements and procedures for adding a recovery method during the account creation process. The account states transition from one to another as a result of user actions, as shown in Figure 2.

Adversary models: We consider three types of adversaries, namely, Eve, Mallory, and Chad. Eve and Mallroy have access to one of the recovery methods for the online account of a benign user, Alice. However, Chad only has knowledge of Alice's recovery method but no access to it.

- **Eve** aims to gain unauthorized access to Alice's account and maintain persistence without Alice's knowledge. She can achieve the goals through *skip password*, password *reuse*, and *parallel session* attacks.

- **Mallory** aims to take over the account and lock Alice out. Mallary achieves the goals through the *arms race, temporary and permanent lockout* attacks.

- **Chad** does not have access to any recovery method but knows what method Alice uses. His goal is to exploit the recovery system to spam Alice or prevent her from initiating a legitimate account recovery through the *recovery spam* and *recovery* lockout attacks.

3. Summary of analysis execution

We analyzed the behavior of our target websites under two scenarios.

- **Benign scenario**: We simulated an account recovery triggered from a trusted device, where the user has previously logged in and used the website. A recovery process in benign scenarios is usually straightforward, such as a password reset link being sent to the recovery email specified by the user.
- **Semi-malicious scenario**: Here, we simulated recovery from a device and location not previously used for logging in. We refer to this scenario as semi-malicious because the website has no straightforward means to detect whether the recovery is triggered by a benign user from a new device or location or by a malicious adversary who is attempting to take over the user account. In this scenario, the recovery process typically involves additional checks—such as requesting 2FA or typing the recovery email address—before successfully resetting the password.

Many websites employ the Risk-Based Authentication (RBA) method to determine whether an authentication request (i.e., log-in or recovery) is benign. We wanted to ensure that RBA is not triggered during benign scenarios so that we could assess whether the recovery process differs in non-benign scenarios. We achieved this by following a vetted method: for each site we tested, we logged in 10 times from the same location on a single machine to mark the device as trusted. This ensured that RBA would not trigger additional checks. This approach approximates a benign scenario as closely as possible without knowing the internal details of the RBA implementation.

We designed 9 comprehensive test cases. These test cases involved triggering recovery and adding/removing recovery and MFA methods to analyze the behavior of a website. Naturally, such security actions could be interpreted as suspicious hacking attempts by the websites, potentially leading to account lockouts. To minimize the chances of lockouts, **we designed a test process** that could guide in executing the test cases with only the required number of security actions, ensuring smooth transitions between account states. A website can reach a set of account states, and our test process ensures that all test cases corresponding to each state are executed. Drafting this process allowed us to test each website, irrespective of

its recovery life cycle, in a consistent and coherent manner without disrupting the flow.

> The auditing framework that we build as part of the research project is available on Github for public use as a free and open source project**.**
>
> **Account Recovery Threat Heuristic Auditing (ARTHA) Framework: https://github.com/Nokia-Bell-Labs/Account-Recovery-Threat-Heuristic-Auditing-Framework**
>
> We encourage you to contribute and use the project, as well as give us feedback.

4. Summary of findings

Our analysis revealed serious security concerns stemming from the exploitation and misuse of account recovery methods and mechanisms, which undermine user data protection and access control. On a high-level, our findings can be classified into design flaws, missing best practices, and security vulnerabilities.

Design flaws

- **Problems with verification for recovery methods:** Unverified methods and their use for recovery could be leveraged by an adversary for typosquatting attacks and account hijacking. In some cases, they may also lead to stale accounts that cannot be recovered.
- **Insufficient session handling:** Users are typically not informed of concurrent login or recovery sessions, and session termination mechanisms lack consistency, leaving room for unnoticed parallel access.
- **Inconsistent treatment of recovery methods:** recovery methods are often treated with varying levels of security while adding, deleting or using them without any logical reasoning. Also, the recovery methods are not handled with the same prudence of visibility and access control as MFA factors.

- **Incomplete activity logs:** Most platforms fail to provide users with a clear audit trail of security-critical events, such as recovery attempts, password resets, or change of account states during recovery.

Missing Best Practices

- **Inadequate alerting for sensitive actions:** Key changes—like modifications to MFA settings or the removal of recovery methods—often go unreported to the user.
- **Unclear or insecure recovery communications:** Recovery-related messages sometimes contain vague or misleading instructions that compromise user security. There is no clear and comprehensive knowledge on how to alert about account recovery-related events. For example, the recovery method will be the sole communication channel that may have been compromised or used for an attack, leaving no scope for proactive or post-compromise actions to combat account hijacking or hidden observer attacks.
- **No clear guidance on forced re-authentication for critical changes:** Users are often allowed to make sensitive changes, such as adding recovery methods, without being asked to re-authenticate. Best practices have no clear guidance on the course of actions post account recovery from a benign user or regaining access after the recovery method is compromised.

Security Policy Weaknesses

- **Risk of account hijacking and lockout:** The use of unverified recovery methods enables attackers to take over accounts or permanently lock out legitimate users.
- **Weaknesses in password reuse policies:** Permitting the reuse of old or similar passwords during recovery creates opportunities for credential-based attacks.

- **Exposure to parallel session attacks:** The lack of controls and alerts for simultaneous recovery or login sessions allows attackers to exploit timing-based vulnerabilities.
- **Persistent access via trusted devices:** Some systems preserve trusted device status even after recovery, bypassing MFA and enabling continued unauthorized access.

5. Conclusion

It appears that online service providers are generally focused on ensuring the security of account recovery methods and procedures. However, many service providers prioritize a quick account creation process to onboard users swiftly, often overlooking simple yet crucial steps which could significantly enhance account security.

Our findings highlight the critical need for greater awareness of the security risks posed by poorly designed account recovery procedures. By systematically reviewing recovery mechanisms from the perspective of an external adversary, our work demonstrates how such analysis can uncover significant vulnerabilities. We believe our auditing framework and best-practice recommendations provide valuable guidance for both security researchers and practitioners.

As password-based authentication gives way to passwordless systems—where device-specific cryptographic credentials are securely backed up and restored via cloud services—recovery will still rely on traditional methods when users lack access to trusted devices. Therefore, our recommendations remain relevant in future authentication ecosystems.

For more information

- Visit the Github repository
- Contact Sid (email: sid.rao@nokia-bell-labs.com and Gaby (email: gabriela.sonkeri@wolt.com)