Analysis of fallback authentication mechanisms

Satenik Hovsepyan
satenik.hovsepyan@aalto.fi

Tutor: Siddharth Rao

Abstract

Reclaiming access to an account after the password is lost plays a major role in the security of authentication systems. Different authentication systems implement a wide variety of account recovery mechanisms. Most prevalent ones include security questions, SMS and email-based recovery, social authentication and manually checking credentials.

In this paper, we analyze the usability and security of those mechanisms, in particular, different types of security questions, their comparison with each other as well with alternative techniques.

KEYWORDS: security, fallback authentication, security questions

1 Introduction

Mainstream authentication systems develop and apply numerous methods to ensure the security of the system. They commonly use passwords, biometrics, physical tokens or private keys as the main authenticator. However, users forget passwords, lose tokens and private keys, biometric features become temporarily or permanently unavailable. This raises the requirement of having a secondary authentication scheme (also referred to as fallback authentication, backup authentication or account recovery).

Clearly, the overall security of the fallback authentication scheme should be at least as high as that of the main authentication scheme. Unfortunately, in practice this is not always viable. Secondary authentication schemes oftentimes have security weaknesses that substantially decrease the overall security of the system.

Since fallback authentication is not used every day, it must have better memorability. For this reason, various authentication systems take advantage of the knowledge users already have, in contrast with the information they purposefully memorize, through the use of security questions. Others use a predefined email address or phone number to deliver a one time recovery token. In some particular cases, manual check of credentials or social authentication is used.

The goal of this paper is to examine currently applied and proposed fallback authentication mechanisms, compare them based on their security, usability and deployability features.

The rest of the paper is structured as follows: section 2 describes general ideas behind authentication schemes and motivation for the study; section 3 is the main study, that presents several types of security questions (predefined, user-chosen, preference-based, activity-based and location-based) and their comparison, after which it presents several other fallback authentication schemes such as SMS and email-based authentication, social authentication and manually checking credentials as well as the use of machine learning in authentication; finally, section 4 summarizes the discussed topics and concludes the paper.

2 Background and Motivation

Authentication is the process of verifying that someone or something is, in fact, who or what it declares itself to be. In general, authentication can involve verifying user's identity based on identity documents, known secrets, biometrics and other factors [13]. Authentication is important as it allows organizations to keep their resources secure and share them only with authorized users. In contrast with authentication - the process of verifying the identity of the user, authorization is the process of verifying user's permissions. Users may be authenticated, but fail to perform specific actions if they are not authorized, i.e., given specific permissions. Although terms authentication and authorization are often used interchangeably, they have two distinct functions [13].

In order to authenticate to the system, users should present a piece of evidence that only they own and the server can verify. This piece of evidence is called an authentication factor. Most commonly used authentication factors include

- *Knowledge factor:* Something the user knows. This can be a password, pin or any other information that the user possesses.
- *Possession factor:* Something the user has. This can be an ID card, a physical token, one-time password token or any other item that only the user can own and can carry with him/her.
- *Inherence factor:* Something the user is. This can be any biometric data, such as fingerprint, facial recognition or any other biometric identification.

The above-listed factors are typically combined in order to improve the security of the system.

The problem, however, is that none of those factors are persistent. In case of knowledge-based authentication, secrets can be forgotten; in case of possession-based authentication, owned evidence can be lost or stolen; in case of inherence-based authentication, biometrics can be temporarily or permanently unavailable (e.g., fingerprint changed by a cut, voice changed because of illness) [9]. In order to address the issue, authentication systems develop **fallback authentication mechanisms**. Fallback authentication provides a means to regain access to the account after the loss of the primary authenticator.

Fallback authentication usually involves two stages. During the first stage, enrollment, users provide some information, such as answers to security questions, email address or phone number and biometrics. This information is used during the second stage, recovery, when a password reset is required. Oftentimes, the time range between the two stages is very long. Thus, memorability and durability of the provided information are major aspects to be considered in the usability of the mechanism. Another aspect affecting usability is the duration of enrollment and recovery stages.

3 Main Study

Numerous implementations of fallback authentication mechanisms are deployed in practice in different systems. However, there is no single established standard for it [5].

Below, we discuss some of the commonly used techniques.

3.1 Security questions

Perhaps one of the most widely known techniques for fallback authentication is **security questions**.

In this scheme, the user selects several questions that the website provides (e.g., "Mother's maiden name" and "Frequent flyer number") and gives correct answers to them. Later, during the recovery, the user should provide the same answers in order to regain access to the account. The advantage of this method over regular passwords is that the answers are supposed to be something the user already knows, in contrast with the specifically created and memorized passwords. In addition, questions give hints about the answers. However, it has been shown that these answers have poor memorability which decreases over time, and they are vulnerable to guessing attacks [14]. The reason for this vulnerability is that some questions have common answers shared by many users. For example, if the attacker guesses "Maria" for "Mother's maiden name" question, there is a high chance that it is the victim's mother's maiden name. Other questions, such as "Who is your favorite superhero?", have very few plausible answers. Another notable reason for security questions' low entropy is that users often try to make their answers harder to guess by providing untruthful responses. However, research shows that users "harden" their answers in a predictable way. A study was conducted at Google to analyze the motivation for untruthful responses [3]. Figure 1 illustrates the goals of users who admitted having provided fake answers to security questions.

The study shows that the majority of users claim to fake the answers to improve the security or to make the answers easier to remember, though the outcome is the exact opposite. This happens since when trying to give an incorrect answer to a questions people tend to choose answers that other users are also prone to choose. For example, when answering the question "What city were you born in?", a lot of people may choose Paris making it a popular choice between truthful and untruthful responses.

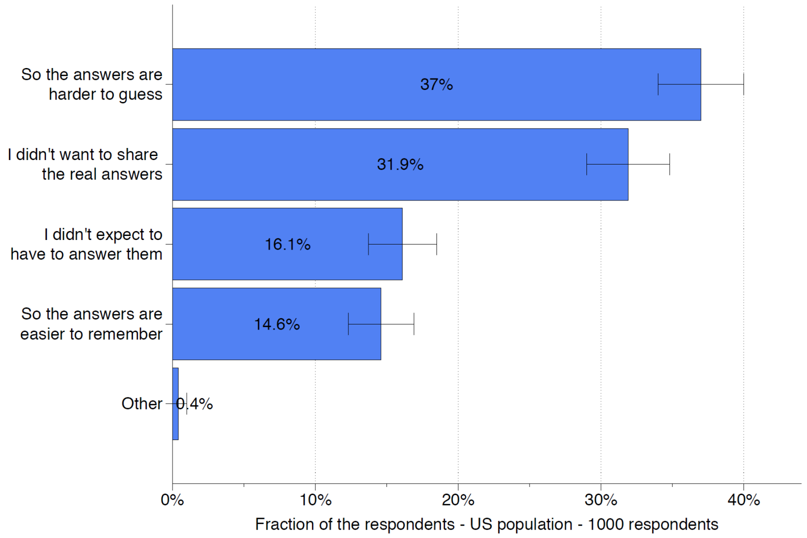

Figure 1. Survey answers for the question "Why did you provide fake answers to your password recovery question?" [3]

In other cases, people may decide to give a completely irrelevant answer such as "Megatron” or, even better, “NvX8z4yJzmu”. While the second approach is secure in contrast with the first one, it still decreases the usability drastically, since the answer is no more a true memory the user holds.

Nonetheless, personal knowledge questions are acceptable in cases when the security risk is low or if they are combined with other methods [3].

In order to address memorability and security issues of personal knowledge questions, some authentication schemes support **user-chosen security questions**. In this design, users are supposed to choose questions themselves. It is assumed that this way questions will be more applicable to the user and thus be harder to guess. However, research shows that unguided user-chosen questions still have poor memorability and low entropy [10].

A potentially more secure alternative form of authentication questions is called **preference-based authentication** [8]. In this scheme, users answer a large set of personal preference questions (e.g., "Do you like country music?" and "Do you like game shows?"). Later, during authentication, users are presented with a preset of the original list and, if their answers are close enough to their initial preferences, they are authenticated. In particular, the approach distinguishes between small and big errors, i.e., if the answer initially was "Really like" in 3-point Likert Scale, while later it is changed to "Really dislike", the error is considered big. A small error is accounted if the answer is changed by one point, i.e., from "Really like" to "Don't care". A few minor deviations like this are allowed.

This scheme prevents statistical guessing since an illegitimate user can only guess the answers to the questions for which the user has strong opinions. Thus, an illegitimate user will make a significant amount of big errors. Listed claims are backed by experiments [8].

The approach is motivated by the higher durability of people's likes/dislikes compared to their memory, and the absence of preferences in public records or online databases.

Nevertheless, what prevents preference-based questions from being widely deployed in practice is that they are more time-consuming at the enrollment stage than individual questions.

An nonintrusive approach with no user friction at the enrollment stage is based on **activity-based personal questions** [2]. It benefits from the massive amount of data that is already stored on servers or user's devices and dynamically generates activity-based ephemeral authentication questions. Correct answers to them are automatically extracted from user's web activities without user's participation (e.g., the answer to "Who was the last person you sent mail to today?" is retrieved from the mail server). Proposed activity-based security questions are divided into three categories:

- *Network Activity*: Questions that focus on user's online activity (browsing history, emails)
- *Physical Events*: Questions based on user's planned events from emails, calendars, social networks
- *Conceptual Opinions*: Questions that take advantage of user's opinions extracted by analyzing user's browsing history, read articles and email content.

Overall security of the approach depends on the popularity of the websites user visits, the popularity of the events user attends and the number of people who know about it, the possibility of randomly guessing an answer to opinion-based questions and several other factors. Security improvements can be reached by requiring users to answer multiple questions. It is also important to note that types of activity-based questions should be carefully analyzed and selected since the questions themselves can leak information about the user's activity.

Similar research suggests using dynamic security questions for fallback authentication on smartphones using their app usage, calls or text messages [6].

Another design addressing fallback authentication security and usability issues uses **location-based security questions** [7]. This approach resembles traditional security questions in the sense that it is based on personal information. However, it differs from the later in question types and its form of providing the answers. Questions focus on episodic memories such as "Where did your first kiss take place?" with location-based answers. In contrast with the traditional approach where users type answers as a text, here, users select a location on a map. The hypothesis behind this approach is that episodic memories are easier to remember than personal facts. Selecting the location, on the other hand, prevents issues such as repeatability and error-proneness. Experiments show that adversaries (both close friends/family and strangers) are unable to guess the answers with required accuracy most of the time.

Experiment results of the concept lead the authors to believe that the approach has the potential to replace traditional security questions in the future [7].

A limitation of this concept is that security questions should be thoroughly designed and evaluated.

An even more optimal solution proposes a combination of the last two approaches. It generates **dynamic location-based challenge questions** based on users' tracked locations. After tracking users' locations for an extended period of time, the algorithm detects locations that are more "interesting", i.e., are rarely visited and so are more likely to be remembered by the legitimate user and less likely to be guessed by an adversary, and asks different kinds of questions about them (e.g., locations visited at a certain date and the order and time gap between visiting several locations). To further improve the security, the approach applies Bayesian classifier to authenticate legitimate users based on their performance/success rate patterns [1].

The study concludes that an accurate design of the approach can significantly raise the overall security and usability of an authentication system.

3.2 Comparing security question types

Investigations show that question styles greatly affect users' performance in account recovery [1].

In this section, we compare above-discussed question types from security, usability and deployability points of view. *Security* considers robustness against attacks from adversaries such as strangers, close friends and family as well as brute force guessing attacks. Privacy concerns are also considered in the overall security level.

Usability is discussed by *memorability* and *ease-of-enrollment* points of view separately. In *ease-of-deployment* we consider how effortful the development and deployment process of the system is and how widely it can be deployed.

Figure 2 represents a comparison of personal-knowledge, activity-based, preference-based and location-based questions. The chart is created based on discussions from [2], [3], [6], [7], [8]. Note that user-chosen security questions are omitted since their overall security, usability and deployability are similar to predefined personal-knowledge questions. In addition, dynamically generated location-based questions are considered under activity-based questions category.

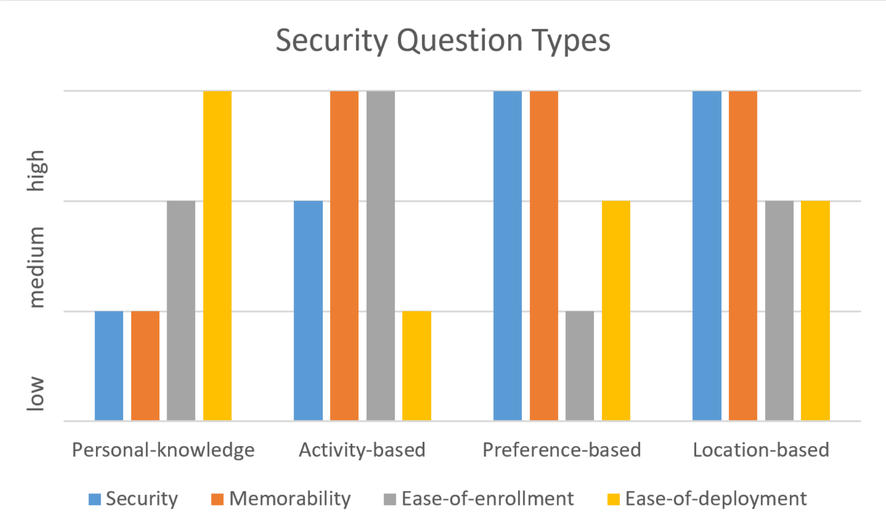

Figure 2. Security, Memorability, Ease-of-enrollment and Ease-of-deployment comparison of different types of security questions

As we can see, none of the discussed types is ideal.

The lowest *security* is achieved by personal-knowledge questions. Other three methods have higher *security*, activity-based questions being medium, because of privacy reasons (the information may be leaked by the questions and, based on the architecture, the service may need to track additional user activity). From *memorability* point of view, the last three types achieve higher results than personal knowledge questions. *Ease-of-enrollment* is the highest for activity-based questions since no user action is required at that stage. Preference-based questions recede in *ease-of-enrollment* measure because of the need to answer a multitude of questions during enrollment. Considering the *ease-of-deployment*, personal-knowledge questions beat the others since the implementation, deployment and usage is rather straight forward and applicable to most of the systems. Activity-based questions have a lower rate of *ease-of-deployment* since some of the planned questions may not be relevant to the user or it may be complicated to find the answer.

Although based on the chart the highest overall grade is achieved by location-based questions, we believe that the nonintrusiveness of activity-based questions at the enrollment stage makes them the better option from the usability point of view. By accurately addressing privacy issues, this method can achieve advantageous results in security as well.

3.3 SMS and Email-based recovery

An alternative recovery method with higher reliability than security questions is authentication by email or SMS (Short Message Service). In this approach, a temporary password or a recovery URL is sent to a predefined email address or phone number. Figure 3 shows the success rate of SMS and email-based recovery compared to security questions [3]. Success rate of a fallback authentication mechanism is defined as the fraction or percentage of success among the total number of attempts to recover access using the mechanism.

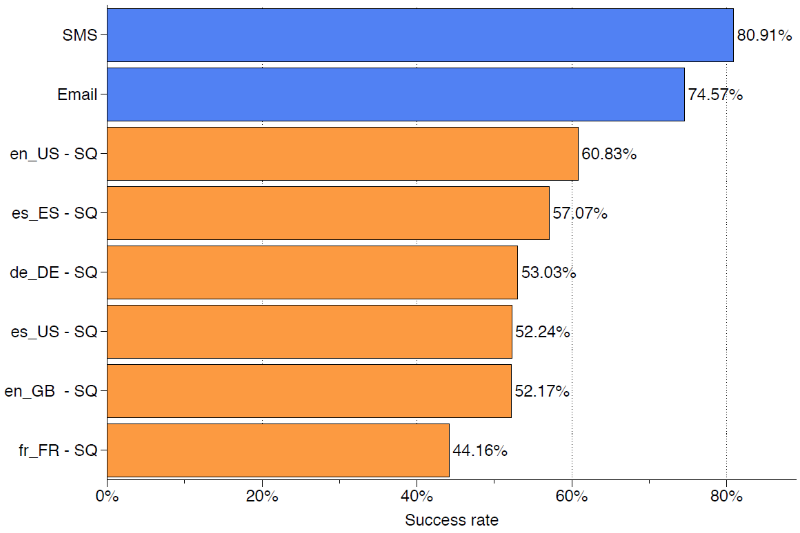

Figure 3. Success rate of different recovery methods [3]

The data was collected by Google based on recovery claims during a month. It shows that email increases the success rate of recovery by 13.74% over the most successful security questions. An even higher success rate is achieved by SMS-based recovery, due to some potential drawbacks of email-based recovery. The drawbacks include the likelihood of losing access to the email along with the other account (e.g., because of using the same password for both accounts or because of losing the browser cache where both passwords were stored).

In addition, both phone numbers and secondary emails may be recycled by service providers due to inactivity. Telecommunications service providers have different policies on phone number recycling that can typically be after 3-6 months of inactivity. Email providers generally recycle emails after longer periods of inactivity (e.g., Microsoft accounts are closed in 5 years of inactivity [4]). It was estimated that in 2014 7% of users' secondary emails were recycled, becoming available for anyone to register and use them again [3].

The figure also shows that cultural differences considerably impact the success rate of security questions. Different language/culture groups have different memorability for the same question and top-performing groups change depending on the question type. For example, the gap between US-English speaking users' and UK-English speaking users' recall for the question "Father's middle name?" reaches 10% after 12 months: 74.43% vs 64.12%. Shifts like this are hard to predict and impose a challenge for designing an international recovery system [3].

3.4 Social authentication

Another recently developed approach for fallback authentication is called social authentication [9]. Here users choose a set of trusted contacts that, in case of forgotten password, need to delegate them one-time secrets, which combined allow the users to reset their password.

In practice, social authentication can be realistically implemented in social network sites. Although the approach is promising, several studies found vulnerabilities in all social authentication mechanisms applied by social network sites. In particular, a relatively new attack against Facebook's social authentication mechanism, called Trusted Friend Attack, circumvents the security of the scheme. The attack is implemented by adding fake accounts to the victim's friends list and then using these accounts to obtain the secret code for the recovery [9].

3.5 Manually checking credentials

Some websites utilize the approach of manually checking the credentials. Here, the users need to either personally meet the authorities or send in a copy of their passport. This method can be useful when security demands are high and in corporate settings, where users are in near proximity. The disadvantage of it is that it scales badly in interned-wide services.

3.6 Machine Learning for authentication

Each of the above-discussed methods have their advantages/disadvantages, usability-security trade-offs and their use cases. However, all of them require some kind of user action. Some of the approaches are substantially more difficult (such as manually checking credentials) or more time-consuming (such as preference-based authentication).

With the accelerating growth of machine learning, a new approach of **implicit authentication** (also referred to as continuous authentication, active authentication and transparent authentication) is emerging [12]. Implicit authentication helps to minimize user friction while ensuring higher security for authentication.

Continuous authentication approaches include touch dynamics, face recognition, gait dynamics and behavior-based profiling. In case of using one of those approaches, methods that are otherwise used for primary authentication can be used for fallback authentication (e.g., a user may be required to enter a pin, in case of behavior recognition failure).

Furthermore, several studies suggest using machine learning for designing **risk-based authentication systems** [11]. This design suggests an improvement over static authentication methods by adjusting the method with the user's risk profile. Parameters affecting the level of risk include login time, location, IP address, number of failed attempts and some other contextual information. The approach provides higher level of security without harming usability, in contrast with the traditional approaches that make a trade-off between the two.

The conducted research particularly relates to primary authentication schemes. However, similar approaches can be applied to ensure the security and usability of fallback authentication schemes. Such an approach was represented in [1] that, in addition to checking the answers to location-based security questions, uses a machine learning classifier to authenticate real users based on their recall rate and performance patterns.

4 Summary

Achieving high level of security in fallback authentication remains a crucial aspect in designing an authentication system. In this paper, we reviewed several approaches that are widely applied in existing systems as well as approaches that are at the research stage. Overall, none of the approaches is perfect.

It is confirmed that security questions have poor memorability and their security level if far lower than that of user-chosen passwords [14].

Although SMS and Email-based recovery are proven to be more secure and are the preferred approach by large service providers such as Google, they still have their limitations and security questions remain useful [3].

Possible improvements to traditional personal-knowledge security questions (such as preference-based, activity-based and location-based questions) can increase their overall security and usability. In addition, security questions provide a satisfactory experience when the risk-level is considered low or if they are combined with other methods.

Less common approaches, that are beneficial in particular cases are social authentication and the manual check of credentials.

Finally, integrating machine learning to authentication system designs gives the ability to improve both security and usability without harming either.

References

[1] Yusuf Albayram, Mohammad Maifi Hasan Khan, Athanasios Bamis, Sotirios Kentros, Nhan Nguyen, and Ruhua Jiang. Designing challenge questions for location-based authentication systems: a real-life study. *Human-centric Computing and Information Sciences*, 5(1):17, Jun 2015.

[2] Anitra Babic, Huijun Xiong, Danfeng Yao, and Liviu Iftode. Building robust authentication systems with activity-based personal questions. pages 19–24, 01 2009.

[3] Joseph Bonneau, Elie Bursztein, Ilan Caron, Rob Jackson, and Mike Williamson. Secrets, lies, and account recovery: Lessons from the use of personal knowledge questions at google. In *WWW'15 - Proceedings of the 22nd international conference on World Wide Web*, 2015.

[4] Microsoft Corporation. Microsoft Services Agreement. https://www.microsoft.com/en/servicesagreement/, 2018. [Online; accessed 05-April-2019].

[5] The OWASP Foundation. Cheatsheetseries. https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets, 2019.

[6] Alina Hang, Alexander De Luca, and Heinrich Hussmann. I know what you did last week! do you?: Dynamic security questions for fallback authentication on smartphones. 04 2015.

[7] Alina Hang, Alexander De Luca, Michael Richter, Matthew Smith, and Heinrich Hussmann. Where have you been? using location-based security questions for fallback authentication. 07 2015.

[8] Markus Jakobsson, Erik Stolterman, Susanne Wetzel, and Liu Yang. Love and authentication. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '08, pages 197–200, New York, NY, USA, 2008. ACM.

[9] Ashar Javed, David Bletgen, Florian Kohlar, Markus Durmuth, and Jorg Schwenk. Secure fallback authentication and the trusted friend attack. pages 22–28, 06 2014.

[10] Mike Just and David Aspinall. Personal choice and challenge questions: A security and usability assessment. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, pages 8:1–8:11, New York, NY, USA, 2009. ACM.

[11] M. Misbahuddin, B. S. Bindhumadhava, and B. Dheeptha. Design of a risk based authentication system using machine learning techniques. In *2017 IEEE SmartWorld, Ubiquitous Intelligence Computing, Advanced Trusted Computed, Scalable Computing Communications, Cloud Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pages 1–6, Aug 2017.

[12] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbello. Continuous user authentication on mobile devices: Recent progress and remaining challenges. *IEEE Signal Processing Magazine*, 33(4):49–61, July 2016.

[13] Margaret Rouse. authentication. https://searchsecurity.techtarget.com/definition/authentication, 2018. [Online; accessed 27-February-2019].

[14] S. Schechter, A. J. B. Brush, and S. Egelman. It's no secret. measuring the security and reliability of authentication via "secret" questions. In *2009 30th IEEE Symposium on Security and Privacy*, pages 375–390, May 2009.