American Research Journal of Computer Science and Information Technology

Volume 7, Issue 1, 58-62 Pages
Research Article | Open Access
ISSN (Online)- 2572-2921
DOI : 10.21694/2572-2921.24013

AMERICAN RESEARCH JOURNALS
An Academic Publishing House

Enhancing Customer Account Security by Eliminating the Use of Security Questions

Raoul Hira
Principal Security Consultant, Vistra, USA.

ABSTRACT

Eliminating the use of security questions and answers as an authentication or password recovery method has become an important step in improving the security of client accounts. Traditional security questions and answers based on user knowledge are criticized because of their vulnerability to guessing, social engineering attacks, or past security breaches. Such threats undermine their reliability as a means of protecting account access. Instead, modern approaches such as biometric authentication, multi-factor authentication (MFA), and password-free methods, including Magic Link, offer a higher level of security, reducing the risks of account compromise. The implementation of these methods requires a careful and step-by-step approach to minimize risks and increase the stability of security systems in the face of ever-increasing threats and technological changes.

KEYWORDS: *information security, authentication, security questions, biometric authentication, multi-factor authentication, password-free technologies, Magic Link.*

INTRODUCTION

In recent years, information security has become one of the key priorities for organizations providing online services. With the rise in cyberattacks and data breaches, the issue of securing user accounts has come to the forefront. Traditional authentication methods, such as using security questions, are increasingly criticized for their low reliability and vulnerability. These knowledge-based methods can easily be compromised through guessing or obtaining information from public sources, creating significant risks for data security.

Despite their long-standing use, security questions have proven to be ineffective in modern conditions, where attackers can easily access personal information through social networks and other online resources. As a result, the need to find and implement more reliable authentication methods that can ensure a high level of protection for user accounts has become increasingly relevant.

Modern alternatives, such as biometric authentication, multi-factor authentication (MFA), and passwordless methods, including Magic Link, offer significant advantages in terms of security. These approaches provide more robust protection against hacking and credential compromise, reducing the reliance on easily exploitable knowledge-based factors. However, their implementation requires careful analysis and a phased approach to minimize potential risks and ensure a smooth transition to new technologies.

The goal of this paper is to analyze modern authentication methods, their advantages and disadvantages, and assess the feasibility of abandoning the use of security questions to enhance the security of client accounts.

Limitations of Using Security Questions

Authentication is the process of verifying the identity of a user or client. In a world where web resources are accessible to anyone with an internet connection, effective authentication systems are critically important for ensuring the security of web applications.

The classification of authentication types is presented below in Table 1.

Table 1. Classification of authentication types [1].

Type of Classification	Description
Knowledge	This type of authentication involves using information such as a password or the answer to a security question that the user knows. These methods are often referred to as "knowledge factors."
Possession	In this case, verification is based on the user possessing a physical object, such as a mobile phone or a special token. These methods are known as "possession factors."
Identity	Here, authentication is based on unique characteristics of the user, such as biometric data or behavioral patterns. These methods are called "inherence factors."

Authentication systems use various technologies to verify one or more of the factors listed above. Security questions and answers are well-known authentication or account password recovery methods that many users encounter when interacting with various online platforms. When registering for an online service, users are often asked to provide answers to security questions and answers, which are later used to recover access to the account. These questions and answers typically serve to reset the password—correctly providing the answer confirms the user's identity and allows them to change the password. Security questions can also be used as an additional authentication factor during login.

Security questions can be divided into two main types:

- Custom questions: These questions allow users to choose from a list of options the one they want to answer. The implementation of such questions is relatively simple, but their effectiveness depends on how complex and unique the user's chosen answer is.

- System-generated questions: These questions are based on information that the service already knows about the user (e.g., birth date or address). Such questions assume that the system has sufficient data about the user and that the answer is difficult for third parties to discover.

Below in Table 2 are examples of secret questions that are leveraged by some web-based applications for authentication or account recovery.

Table 2. Examples of questions considered unreliable [2].

Ineffective Security Question	Reason
What is your date of birth?	Easy for others to guess—this is not confidential.
What was the name of your favorite teacher?	Childhood topics may be too distant for people to remember.
What is your favorite movie?	Preferences are likely to change over time.
What was your first car?	It's unclear what level of detail should be included in the answer.
What is your zodiac sign?	The range of possible answers is narrow, and others may guess or discover it easily.

Since the compromise of customer accounts can negatively affect company operations or compromise sensitive personal information, these issues will be discussed further in Section 2.

Vulnerabilities in Secret Questions and Answers: Methods of Compromise in Authentication Systems

Cybersecurity risks represent just one of the many threats organizations face worldwide, making the need for preparedness increasingly pressing. Issues of physical and digital security can lead to significant disruptions and chaos. Frequent data breaches are gradually becoming commonplace, with the incident involving Yahoo Inc. setting a new record by compromising over one billion user accounts. Although some cyberattacks are unavoidable, this case highlights the importance of implementing additional security measures and taking steps to protect data. In 2013, a major database breach at Yahoo allowed attackers to access information from more than one billion users. This incident, along with another that affected approximately 500 million accounts, underscores the vulnerability of email and personal data in today's world. Among the stolen data were names, birth dates, encrypted passwords, and answers to security questions, such as a mother's maiden name or the name of a first pet.

Below in Table 3 are examples on how secret questions are compromised.

Table 3. examples of methods used to compromise secret questions and answers [3]

Compromise Method	Reason
Social Engineering	Obtaining answers through manipulation or research
Data breaches	Accessing databases of secret questions and answers from compromised systems
Guessing attacks	Exploiting the limited range of common answers
Credential stuffing	Using answers from one breached site to access accounts on other sites

Social Engineering

Social engineering is a sophisticated psychological manipulation technique used to exploit human vulnerabilities in security systems. In the context of secret questions and answers, attackers employ various strategies to extract sensitive information directly from the target or their associates. These methods often involve impersonation, pretexting, and exploiting cognitive biases. For instance, an attacker might pose as a customer service representative and use persuasive communication techniques to elicit answers to security questions. According to the 2021 Verizon Data Breach Investigations Report, 85% of breaches involved a human element, with social engineering playing a significant role. Techniques like phishing (36% of breaches) often incorporate social engineering elements to gather security question answers.

Data Breaches

Data breaches pose a severe threat to the integrity of secret questions and answers by exposing vast amounts of personal information. When an organization's database is compromised, attackers can obtain not only usernames and passwords but also the answers to security questions. This information is often sold on dark web marketplaces, creating a ripple effect that extends far beyond the initially breached organization. For example, the 2013 Yahoo data breach exposed security questions and answers for 3 billion user accounts. The compromised data included easily guessable questions like "What is your mother's maiden name?" or "What was your first pet's name?". Security architects must consider the implications of such large-scale breaches when designing authentication systems.

Guessing Attacks

Guessing attacks on secret questions exploit the often limited entropy of user-chosen answers. These attacks can be broadly categorized into two types: blind guessing and informed guessing. Blind guessing involves attempting common answers to popular security questions. For example, a 2009 study by Microsoft Research found that 20% of people used one of the top three most common answers for the question "What is your favorite sports team?". Informed guessing leverages publicly available information about the target, often gleaned from social media or public records, to make educated guesses about likely answers.

Credential Stuffing

Credential stuffing is an automated attack method that leverages large sets of compromised username and password pairs, often obtained from previous data breaches, to gain unauthorized access to user accounts across various platforms. While primarily focused on password-based authentication, credential stuffing can also be applied to secret questions and answers. Attackers exploit the tendency of users to reuse the same security questions and answers across multiple accounts. According to a 2019 Google/Harris Poll, 52% of users reuse the same password for multiple accounts, and this behavior often extends to security questions.

Modern Alternatives to Security Questions and Answers

Before selecting the best protection method for employees and customers, it is important to carefully evaluate the potential risks and benefits of each approach and determine which one provides the highest level of security for recovering access to accounts. Methods based on user knowledge (such as security questions or passwords) offer a low level of reliability. In contrast, methods that rely on physical attributes or specific identifiers of the user demonstrate a significantly higher level of security.

Passkeys

Passkeys represent a significant advancement in authentication technology, offering a more secure and user-friendly alternative to traditional passwords and secret questions. Based on the FIDO2 and WebAuthn standards, Passkeys leverage public key cryptography to provide phishing-resistant authentication. In a Passkey system, a cryptographic key pair is generated during account creation, with the private key securely stored on the user's device (often in a hardware-backed secure enclave) and the public key stored on the server. During authentication, the server sends a challenge, which the device signs with the private key. This signed response proves possession of the private key without ever transmitting it. Passkeys should be adopted for several compelling reasons: they eliminate the vulnerabilities associated with password reuse and guessable secret questions; they're resistant to phishing attacks as the cryptographic exchange is bound to the legitimate website; they offer a seamless user experience, often integrating with biometric authentication on devices; and they reduce the cognitive burden on users by removing the need to remember complex passwords or answers to secret questions. Furthermore, Passkeys can be synchronized across a user's devices through end-to-end encrypted channels, providing both security and convenience. For developers and security architects, implementing Passkeys significantly enhances the overall security posture of applications while potentially reducing account recovery and support costs associated with forgotten passwords or compromised secret questions

OAuth

Another popular option for account recovery is the use of the OAuth protocol and social media for login. This method allows authentication through accounts on third-party platforms such as Google, Facebook, or Apple. It significantly reduces the amount of information that needs to be remembered and entered manually, providing an additional level of security due to the trusted protection mechanisms of these platforms.

One-Time Passwords (OTPs) and Magic Links

OTPs are temporary codes delivered via authentication apps, email, or SMS, while magic links are unique URLs sent to the user's email for automatic authentication. These methods provide temporal security, uniqueness per session, and out-of-band verification, making them more resilient to various attacks.

The security of these methods varies significantly based on the delivery channel. Authentication apps are the most secure for OTPs, followed by email-based methods (for both OTPs and magic links). SMS-based OTPs are the least secure due to vulnerabilities such as SIM swapping attacks and SS7 protocol exploits.

Magic Link authentication is gaining popularity among developers due to its simplicity, enhanced security, and convenience. This method allows users to log in without the need to enter traditional passwords, significantly simplifying the process and making it more secure.

Some additional alternatives are Multi-Factor Authentication for reduced recovery needs, offline backup codes for emergency access, trusted contacts for assisted recovery, blockchain-based verification for decentralized security, progressive identity proofing for risk-based authentication, and biometric authentication for unique physical identifiers, each offering distinct advantages in security and user experience.

Below in Table 3, the advantages and disadvantages of the primary recovery method will be described.

Table 3. Advantages and disadvantages of access recovery methods

Method	Advantages	Disadvantages
Passwordless authentication (WebAuthn / FIDO2)	- No need to remember complex passwords; - Reduces the likelihood of credential attacks (phishing, password guessing); - Enhances user experience through simplicity and convenience.	- WebAuthn/FIDO2 technology requires compatible devices and software and set up across multiple devices - Complex recovery in cases where primary authentication method fails
OAuth and social authentication	- Utilizes robust security mechanisms of major platforms; - Simplifies recovery and data management; - Intuitive for users and widely adopted.	- Dependence on third-party services for authentication; - Potential risks associated with access denial due to issues with the account on an external platform.
One-Time Passwords (OTP) and magic links	- Short-lived relevance reduces the time for attacks; - Using additional channels enhances security; - Possibility of generating new codes multiple times.	- Vulnerability to SIM swap attacks when using SMS; - Dependence on access to phone or email; - Possible delays in receiving codes via SMS or other channels.

CONCLUSION

The National Institute of Standards and Technology (NIST) has proposed new guidelines in its Digital Identity Guidelines draft SP 800-63-4, aimed at eliminating outdated and counterproductive password requirements. The proposed changes include removing mandatory periodic password changes, abandoning complex character composition rules, and discontinuing the use of security questions. NIST argues that these long-standing practices often lead to weaker passwords and compromised security [11].

In conclusion, the analysis confirms the necessity of abandoning the use of security questions and answers in favor of more modern and secure authentication and account recovery methods. Security questions and answers, despite their widespread use, exhibit significant vulnerabilities, especially in the face of increasing information security breaches. In the transition away from the use of security questions in online protection systems, password managers play a key role in simplifying the process. Although the primary goal is to eliminate security questions, password managers provide a temporary solution that enhances both security levels and user convenience during the transition period.

One of the significant advantages of using password managers is their ability to generate random answers to security questions. Such answers consist of long strings of random characters, significantly increasing the difficulty of guessing them. This method mitigates the risks associated with users selecting weak or easily predictable answers, such as personal information or common phrases. Moreover, users are not required to remember these random answers, as they are securely stored in the password manager.

Additionally, modern password managers offer cross-platform access, allowing users to retrieve necessary information for recovery from various devices, regardless of their location. This feature is particularly important in the context of widespread multi-platform environments, where users may encounter the need to recover data from different devices.

While password managers can reduce certain risks associated with the use of security questions, it should be acknowledged that they do not eliminate the fundamental vulnerabilities of

this system. Consequently, the use of password managers in this context should be viewed as a temporary measure on the path to implementing more reliable authentication methods.

REFERENCES

1. Karl M. et al. Keys to the kingdom are not required: a comprehensive study of common authentication vulnerabilities //Proceedings of the 22nd ACM Internet Measurement Conference. – 2022. – pp. 619-632.
2. Olade I. et al. Exploring vulnerabilities and benefits of swipe or pattern authentication in virtual reality (VR) //Proceedings of the 4th International Conference on Virtual and Augmented Reality Modeling, which will be held in 2020. - 2020. – pp. 45-52.
3. Alharbi F. S. Dealing with Data Breaches Amidst Changes In Technology //International Journal of Computer Science and Security (IJCSS). – 2020. – T. 14. – №. 3. – C. 108-115.
4. Mom's Maiden Name? The Right Way to Answer Security Questions and More Online Safety Advice. [Electronic resource] Access mode: https://www.wsj.com/articles/moms-maiden-name-the-right-way-to-answer-security-questions-and-more-online-safety-advice-1481838744 (accessed 08/31/2024).
5. What you should do if you were hit by the Yahoo hack. [Electronic resource] Access mode: https://www.cbsnews.com/news/yahoo-hack-what-you-should-do-change-password/ (accessed 08/31/2024).
6. Equifax data breach FAQ: What happened, who was affected, and what was the impact? [Electronic resource] Access mode: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (accessed 08/31/2024).
7. Reddy H. B. S. et al. Analysis of unexplored security issues common to all types of NoSQL databases //Asian Journal of Computer Science Research. – 2022. – vol. 14. – No. 1. – pp. 1-12.
8. Seven Epic Cases of Companies That Failed Internationally. [Electronic resource] Access mode: https://www.firmex.com/resources/blog/seven-epic-fails-by-businesses-that-tried-expanding-into-foreign-markets / (accessed 08/31/2024).
9. Saini D. K., Kumar K., Gupta P. [Withdrawn] Security problems in models of Internet of Things and cloud computing services with proposed solutions //Security and communication networks. – 2022. – T. 2022. – No. 1. – S. 4943225.
10. Liu K. H. et al. A reliable authentication scheme for personal medical records in cloud computing //Wireless networks. – 2024. – vol. 30. – No. 5. – pp. 3759-3769.
11. NIST Releases Second Public Draft of Digital Identity Guidelines for Final Review. [Electronic resource] Access mode: https://www.nist.gov/news-events/news/2024/08/nist-releases-second-public-draft-digital-identity-guidelines-final-review (accessed 08/31/2024).

Citation: Raoul Hira, "Enhancing Customer Account Security by Eliminating the Use of Security Questions", American Research Journal of Computer Science and Information Technology, Vol 7, no. 1, 2024, pp. 58-62.