Account Recovery Challenges: Secure and Usable Authentication[*]

Mike Just

mike.just@ed.ac.uk

School of Informatics
University of Edinburgh
Edinburgh, UK

Abstract

Challenge questions represent the most popular practice today for supporting account recovery. In case a user forgets their *memorized* password, it is hoped that they'll be able to recall the answers to their challenge questions. In theory, it seems like a good idea: the answer to the questions should be information that is *already known* to the user. Challenge questions are even being used to complement password authentication; in addition to a password, users are asked for the answer to one of their questions. Despite their ubiquity, we know surprisingly little about the security and usability of challenge question authentication solutions. In this short article, we review the state-of-the-art in this area.

Keywords: Authentication, recovery, challenge questions

1 Introduction

Ensuring a user's authenticity is a key component of almost all business information systems. Without such protection, personal information would be readily available to numerous would-be attackers. However, over-zealous protection can also prove to be unusable for some and lead to insecure behaviour by users. For example, a system that requires users to choose a 40-character password might at first seem more secure than today's typical systems, but it would likely present users with a frustrating experience. And this experience might lead to insecure behaviour, for example, causing users to write down their password on a piece of paper next to their computer. Hence, systems require trustworthy and usable authentication solutions.

Figure 1 depicts the different classes of authentication credentials that are common to authentication systems. So-called *credentials* refer to components used by the user to authenticate themselves. The category of *Something You Have* refers to physical objects that a user must carry with them, such as smartcards. The card might require a reader interface, or perhaps provides a display screen from which the user uses the displayed information to authenticate. *Something You Are* refers to biometrics that rely upon physical properties of the user, such as fingerprints or retinal scans. A biometric interface is used to collect the biometric. While both preceding types of credentials have been studied for many years, and are increasing in their use, the most common category is that of *Something You Know*.

[*] The work of this author is supported by the Engineering and Physical Sciences Research Council (EPSRC) Grant No. EP/G020760/1.

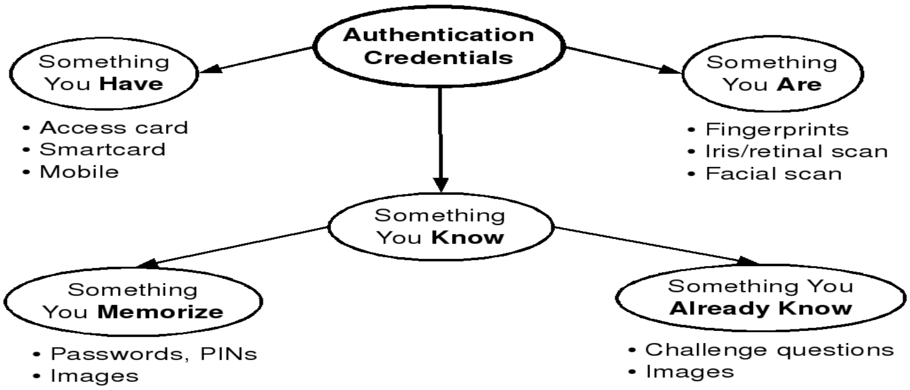

Figure 1: Types of Authentication Credentials

'Something You Know' refers to information the user knows such as a *memorized* password. One would expect that a reader of this article would be intimately familiar with passwords from their day-to-day experience, if not with their research. A typical user will remember, or more correctly, be required to remember, several passwords. So-called *power users* will have dozens of passwords to remember. Beyond passwords, it is also common today for information that is *already known*[1] to a user to be used for authentication purposes. In this instance, rather than requiring a user to choose and remember a new piece of information for authentication purposes, they'll be asked to leverage memories they already have. Most often, these take the form of challenge questions such as *"What is your Mother's Maiden Name?"* or *"What was the name of my first school?"*. Typically, such questions are used for the purpose of a *secondary* or *fallback* authentication. In other words, if you were to forget your password (your *primary* authentication credential), you might be asked one of your challenge questions, and required to provide the correct answer in order to access your account. As such, challenge questions would appear to offer a cost-effective way to support *account recovery.* In current practice, such questions are sometimes used *in addition* to password authentication.

Despite the widespread use and apparent acceptance of challenge questions as a form of authentication, they have received very little critical study. It would be fair question to ask whether they are actually a *secure* and *usable* form of authentication. In the remainder of this paper, we discuss the challenge of secure and usable account recovery, consider the role of challenge questions, and review the alternatives that exist today.

2 Account Recovery

The past decade has witnessed an explosion in online activity, and along with it, a need to manage the accounts of those online users. For the most part, time is taken up with routine, day-to-day activities. From the point of view of authentication, this simply means *login* after *login* after *login.* From an administrative point of view, maintenance of this account access is the most relevant (and costly!).

Account maintenance begins with the *registration* of the user. In some cases, this can be quite simple, involving only the assignment of an account to *some* user. For example, many email service providers and social networking sites have this behaviour; you register by choosing a username and password, perhaps provide some additional information, and an account is created. There is no need to ensure that you are who you claim to be.

In other cases, there is an important step of *identification* as part of the registration. In other words, before creating an account you must be properly identified that you are who you claim to be. For example, when registering for an online account with a bank, a user is required to first identify themselves by perhaps providing their account number and other information related to their account. Compare this to

[1] O'Gorman et al. [11] refer to the distinction between *memorized* and *already known* authentication information respectively as *push passwords* and *pull passwords* to hightlight how information is either "pushed" into user memory, or "pulled."

the Internet email provider who doesn't necessarily care who you are, though the account will be secure and accessible only to you once it is created.

Since registration is typically a one-time event per user, it is accepted that it can sometimes be a more time-consuming endeavour and thus be more costly. In some cases, the identification step might require that in-person identification using a physical ID card.

More common is the maintenance activity of account recovery. When a user forgets (or loses, in the case of *Something you Have*) their primary credential, a process for recovering their account needs to be created. In some cases, it would be reasonable to ask a user to simply re-register. However, since registration may be expensive, it might not be the most cost-effective option. And since there may not have been an initial identification stage, re-registration would not ensure that the account is being returned to the same, original user.

In support of an effecient and cost-effective, the practice of using information such as challenge questions has become quite common. Challenge questions rely upon information *already known* to the user. Thus, in theory, they should not be as susceptible to the same forgetfulness as passwords; if a user has forgotten their password, hopefully they still remember the answer to their challenge questions.

3 Challenge Questions

So-called *Challenge Questions* consist of a pair of items: a question and the corresponding answer. At registration, a user submits one or more question-answer pairs. The system stores the questions and answers for the user, with at least the answers protected for their confidentiality.[2]

When the account recovery process is initiated, a user will submit their username, afterwhich their questions will be retrieved and re-presented to them. The user is then asked to provide the original answers to all (or some) of the questions. In such a process, the *already known* information is the answer to each question, and the challenge question itself acts as a *cue* to aid the user in recalling their answer. Indeed, the question-answer pairing is similar to the concept of *word pairs* whereby two words are paired together if they have a special relationship. In fact, early study into the use of challenge questions for authentication focused on this aspect of word association.

There are different methods one can use to package a *challenge question authentication solution*. For example, the questions might be either *administratively-generated* or *user-generated*. Administrativel-generated challenge questions ("fixed questions" by Just [8, 9], and "selectable questions" by O'Gorman et al. [11]) are designed by the account owner so that the account user selects their questions from a pre-defined list. User-generated questions ("open questions" by Just [8, 9] and O'Gorman et al. [11]) are generated by the user, possibly with guidance from the authentication system.

Answers can refer to personal information, facts, beliefs, opinions, etc. More familiar examples, such as *"What is your Mother's Maiden Name?"*, *"What was the name of my first school?"*, or *"What was the name of your first pet?"* refer to personal information. A typical authentication solution will use a small number of authentication questions to authenticate an individual. Noting the lack of personal privacy regarding such information, O'Gorman et al. [11] focused on questions that solicit user opinions or "trivial facts" with questions such as *"What type of apple do you prefer?"* and *"Where do you carry your house keys?"*. Their solutions ask a larger number of such questions ($10 - 20$) in recognition of the smaller answer space for each question. Jakobsson et al. [7] furthered this model by focusing on binary responses (yes/no) to preference questions, for example *"Do I like cats?"*. In the sections below, we review the work that has been performed on determining the security and usability of all such instances of challenge question authentication.

3.1 The Security of Challenge Questions

The security of challenge questions has been studied by several researchers. And while the typical security questions that relate to the entropy of the answers are easy to calculate, the security of the answers based upon their potentially wide availability has often proved elusive.

[2] The questions might also be protected for confidentiality, though it is not necessary.

Haga and Zviran [5] performed early tests to determine the ability of family or friends to determine a user's challenge question answers. Similar to a user's own abilities, family or friends wouldn't necessarily provide the answers with perfect accuracy, but the results should performance rates of just under 50%; perhaps not too surprising, especially in the case of personal questions.

Just [8, 9] defined high-level security criteria of *Guessability* and *Observability*, that respectively referred to one's difficulty in guessing the corresponding answer to a question, and one's difficulty to observe or retrieve the answer. Rabkin [13] further refined the notion of observability to identify answers that were either *Attackable* in which case the answer is known to friends or family and can be determined with substantial probability, or *Automatically Attackable* where the answer could be mined from social-networking, or other public sources. And Rabkin then applied these criteria to a review of the questions from 20 online banking sites. His analysis suggests that many of the administratively-generated questions in use today are potentially insecure. Unfortunately, the results don't include recommendations for constructing more secure challenge questions.

Jakobsson et al. provide some initial security analysis as part of their preference-based solution [7] and have followed-up with some re-design and further security analysis [6]. Their analysis measures for "too high" correlations between questions and works to design a solution that is resistant to attack.

3.2 The Usability of Challenge Questions

Unfortunately, there has been very little study into the usabilty of challenge question systems, especially with environments closely related to those found in practice today. However, some results exist and there appears to be a renewed interest in discovering the usability of these techniques. Below, we highlight several of the results that do exist today.

Just [8, 9] identified the following criteria for the usability of challenge questions. These criteria reflect the testing of earlier studies as well.

- *Applicability* - The question is applicable, or relevant, to users. For example, the question *"What was the name of your first pet?"* would not be applicable to those users that have never owned a pet. This criterion would only apply to administratively-generated questions (and not user-generated questions).
- *Memorability* - The answer to the question is easy to recall. Since the purpose of challenge questions are to aid in the recall of *already known* information, a key criterion is that the answers to the questions are memorable by (at least a significant portion of) users.
- *Repeatability* - A subset of memorability, the answer to a question needs to be repeatable. This typically refers to two such aspects. First, the syntax of the answer should be repeatable over time. For example, for the question *"Where was my first home located?"*, the answer might include any one of the words *"Street"*, *"St."*, *"Avenue"*, etc., and systems today require 100% accuracy with such individual responses. Secondly, the *original* answer to a question is required. For example, in response to the question, *"Who is my favourite actor?"*, the user is not being asked to provide their current favourite, but rather their favourite when they first registered the question and such preferences can change over time,

Haga and Zviran [5, 19] examined the memorability of so-called *cognitive passwords* and *associative passwords* where the former generally refer to challenge questions that ask for personal information, opinions, preferences etc., and the latter refer strictly to sets of word pairs (where one word is *associated* with the other). Their results report reasonably high levels of recall, though their data reveals that few users were able to recall their answers with 100% recall.

Pond et al. [12] examined users' ability to recall 20 word association pairs and after only a 2-week retention interval, had poor recall rates of only 60% in some cases (even worse for some portions of their experiment). They note, however, that their results should be replicated in a more traditional computer security setting, aligned with some of the questions we've noted above. However, their result does speak to the difficulty for users to recall even already known information with accuracy.

Ellison et al. [2] and Frykholm and Juels [3] both describe cryptographic techniques for tolerating errors on behalf of users. Specifically, they employ secret sharing techniques [15] to tolerate forgetful users so that from n questions posed, only $t < n$ correct answers would be requires, as with a (t, n) threshold-based secret sharing scheme.

More recently, Just [8, 9] performed some focus group testing on a challenge question authentication solution developed for the Government of Canada. Results indicated that users were distracted by inapplicable (administratively-generate) questions, had difficult remembering dates and "first-time" events, but were comfortable with being asked more than one challenge question. Rabkin [13] analyzed the usability of the questions from 20 online banking sites and found significant numbers of questions that might prove difficult to use. He also noted the trade-offs with security as there appeared to be a strong inverse relationship between those questions that were secure and those that were emorable. Jakobsson et al. [7] have studied the usability of their solutions based upon user preferences and obtained relatively positive results.

However, as noted earlier, there remains a lack of rigorous, long-term study into the practical usability of challenge question answers, whether they be personal information, preferences, opinions, etc., so that the long-term benefits or issues of such solutions remain to be seen.

4 Concluding Remarks

Challenge questions alone do not provide sufficient security and account protection. Indeed, early results from Just and Aspinall [10] suggest that use of only a single question-answer pair provides very little security. Thus, prudent designers will ask multiple questions and leverage additional security precautions. One such example is to include an email to the user as part of the overall recovery process [17].

Despite the ubiquity of challenge question authentication solutions and their use as either a secondary authentication mechanism, or as a complement to a primary authentication system, our knowledge of their security and usability is sorely lacking.

Refernces

[1] F. Asgharpour, M. Jakobsson, "Adaptive Challenge Questions Algorithm in Password Reset/Recovery," in *First International Workshop on Security for Spontaneous Interaction (IWIISI '07)*, Innsbruck, Austria, (2007).

[2] C. Ellison, C. Hall, R. Milbert, B. Schneier, "Protecting Secret Keys with Personal Entropy," *Journal of Future Generation Computer Systems*, **16(4)**, (2000), 311-318.

[3] N. Frykholm, A. Juels, "Error-Tolerant Password Recovery," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS '01), ACM Press*, (2001), 1-9.

[4] V. Griffith, M. Jakobsson, "Messin' with Texas, Deriving Mother's Maiden Names Using Public Records," *RSA CryptoBytes*, **8(1)**, (2007), 18-28.

[5] W. Haga, M. Zviran, "Question-and-Answer Passwords: An Empirical Evaluation," *Information Systems*, **16(3)**, (1991), 335-343.

[6] M. Jakobsson, L. Yang, and S. Wetzel. "Quantifying the Security of Preference-Based Authentication." DIM '08.

[7] M. Jakobsson, E. Stolterman, S. Wetzel, L. Yang. "Love and Authentication," in *Proceedings of ACM Human/Computer Interaction Conference (CHI)*, (2008).

[8] M. Just, "Designing and Evaluating Challenge Question Systems," in *IEEE Security & Privacy: Special Issue on Security and Usability, (L. Faith-Cranor, S. Garfinkel, editors)*, (2004), 32-39.

[9] M. Just, "Designing Authentication Systems with Challenge Questions," in *Designing Secure Systems that People Can Use, O'Reilly, L. Faith-Cranor, S. Garfinkel, editors*, (2005).

[10] M. Just, D. Aspinall, "Challenging Challenge Questions," to appear in *Proceedings of Trust 2009*, 6-8 April 2009, Oxford, UK.

[11] L. O'Gorman, S. Begga, J. Bentley, "Call Center Customer Verification by Query-Directed Passwords," in *Proceedings of Financial Cryptography '04, International Financial Cryptography Association*, (2004).

[12] R. Pond, J. Podd, J. Bunnell, R. Henderson, "Word Association Computer Passwords: The Effect of Formulation Techniques on Recall and Guessing Rates," *Computers and Security*, **19(7)**, (2000), 645-656.

[13] A. Rabkin. "Personal knowledge questions for fallback authentication: Security questions in the era of Facebook." in *Proceedings of the Symposium On Usability, Privacy and Security (SOUPS '08)*, (2008).

[14] B. Schneier, "The curse of the secret question," *Computerworld*, (February 2005).

[15] A. Shamir, "How to share a secret," *Communications of the ACM*, Vol. 22, No. 11, Nov. 1979, pp. 612-613.

[16] C. E. Shannon, A mathematical theory of communication. *Bell System Technical Journal*, 1948, vol. 27, pp. 379–423.

[17] S. Garfinkel, "Email-Based Identification and Authentication: An Alternative to PKI?," *IEEE Security and Privacy*, vol. 1, no. 6, pp. 20-26, Nov. 2003,

[18] Y. Spector, J. Ginzberg, "Pass-Sentence - A New Approach to Computer Code," *Computers and Security*, **13(2)**, (1994), 145-160.

[19] M. Zviran, W. Haga, "A Comparison of Password Techniques for Multilivel Authentication Mechanisms," *The Computer Journal*, **36(3)**, (1993), 227-237.