SECURITY PS

White Paper

Tips for Avoiding Bad Authentication Challenge Questions

By Bruce K. Marshall
Senior Security Consultant
bmarshall@securityps.com

July 2007

Tips for Avoiding Bad Authentication Challenge Questions:

About Bruce K. Marshall – bmarshall@securityps.com

Bruce K. Marshall, CISSP, NSA-IAM is a Senior Security Consultant for Security PS and works with clients to analyze and solve their information security challenges. He has made computer authentication threats and solutions a professional focus of his for more than a decade. Bruce is also the instructor for several Security PS classes and a popular speaker on information security topics at local and national events.

About Security PS – www.securityps.com

Security PS is a leading Midwest consulting firm that delivers application, host, and network security assessments to organizations committed to lowering their risk. Clients are provided with independent, expert reviews of their critical online assets through regular vulnerability scans and penetration tests. Security PS also offers hands-on training for topics like web application security threats and countermeasures.

SECURITY PS

Tips for Avoiding Bad Authentication Challenge Questions

As the threats to online applications evolve, so do the techniques adopted to guard these systems against attack. One recent trend, especially among financial institutions, has been to supplement traditional password authentication with "challenge questions". A challenge question asks a user for an answer to a personal question in an attempt to confirm their identity.

Challenge questions themselves are not a new creation. They have traditionally been used in customer service calls or account application processes to help authenticate people. The most famous of these challenge questions are "what is your mother's maiden name" and "what is your social security number".

In addition, challenge questions are referred to by a variety of different names. This causes some confusion and hurts efforts to establish a better understanding of them. We use the term "challenge questions" because it is one of the more popular options and is fairly descriptive. Listed below are a few alternative names:

- Secret Questions
- Recovery Questions
- Verification Questions
- Knowledge Based Authentication
- Question-and-Answer Passwords
- Secret Knowledge
- Query-Directed Passwords
- Personal Entropy

We saw the first application of challenge questions in IT when they were used for automated password recovery systems. These systems help users gain access to an application identity when they have forgotten their primary password, avoiding a more expensive help desk call. After receiving correct answers to one or more challenge questions the password recovery system either provides the user with their password or allows them to change it.

Now new attention is focused on challenge questions as an alternative to implementing true multi-factor authentication. In 2005 the Federal Financial Institutions Examination Council (FFIEC) responded to growing online threats by updating their security guidance to financial institutions [1]. FFIEC guidelines now require financial institutions to conduct a risk assessment of their online authentication controls. For applications that involve "high risk" transactions, the FFIEC declared single factor authentication to be inadequate.

Challenge questions can be presented to a user along with requests for a password, promising a greater level of security than a password alone. Some financial organizations have implemented challenge questions as a low cost solution intended to satisfy the FFIEC's requirements. However, security professionals are divided on whether this type of solution actually meets the guidelines.

During our assessments of web applications Security PS has found that many organizations are struggling to securely implement these new challenge question systems [2]. Designing a challenge question authentication system can be much like designing your own encryption algorithm. Failing to consider the quality

'Designing a challenge question authentication system can be much like designing your own encryption algorithm.'

of challenge questions selected and the controls implemented can actually expose applications to greater risks [3].

In this white paper, Security PS discusses the characteristics of good and bad challenge questions. In addition, we use our expertise to evaluate a sample of commonly used challenge questions and provide you with our feedback on their strengths and weaknesses.

A second, forthcoming white paper from Security PS will identify the technical controls in challenge question authentication systems that are needed to protect both organizations and their users against common threats. This paper will describe design and coding problems found in actual applications and offer recommendations to help you avoid making the same mistakes.

Challenge Question Implementation Approaches

Similar to passwords, challenge questions and their associated answers must be established prior to their use for authentication. Normally this is handled during the user enrollment process. An organization can manage the challenge question enrollment process in several different ways.

The first technique requires the organization to create a library of predefined challenge questions. During enrollment, a user selects a subset of these questions and enters their own answers.

The second technique requires the user to create their own challenge questions and provide the answers to these questions during enrollment.

A third technique involves the use of challenge questions derived from private information databases. This approach asks the user personal questions, such as "what company services your current mortgage" or "what was the balance on your previous bill." Some organizations prefer to use a third-party service to compile and provide access to this information rather than managing it themselves. In this scenario, the user does not initially select or answer any challenge questions since this information has already been gathered.

Based on our experience, the first and second techniques are most popular for use with online authentication. Organizations may prefer these techniques over the third approach due to their lower cost.

Of the two main challenge question approaches, Security PS recommends that organizations use the first and create a predefined library of questions for their users. We believe that most users will create unsatisfactory challenge questions on their own and, accordingly, should not be allowed to do so. In part, this is because we have seen organizations make little effort to educate users on how to come up with good challenge questions. However, even security professionals struggle to create good challenge questions, so education of users alone isn't sufficient. More analysis of the problems with user defined challenge questions can be found in the Security PS blog [4].

Once the challenge questions are selected and answers are provided, the user can complete the enrollment process. When the user returns to use the application, these challenge questions may or may not be asked,

depending on how the authentication system was implemented. In many cases, challenge questions are used in conjunction with a password for authentication. Users can be prompted to answer challenge questions during every login or only under specific conditions. Certain risk-based authentication (RBA) systems only present challenge questions when the user logs in from a different computer.

Users can be prompted to answer challenge questions in one of two ways. A user can either type in their answer free-form or they can select their answer from the multiple choices presented by the authentication system.

When required to type their answer, a user's greatest challenge is remembering the exact answer provided during enrollment. If they cannot remember their answer they must blindly submit guesses or contact the organization to reset their questions. In this respect, challenge questions with free-form answers are similar to passwords.

The multiple choice approach offers users a better chance to remember their answer because it will be one of only four to six options listed on the page. Unfortunately, this also greatly decreases the number of answers an attacker must guess before determining the correct answer. The uniqueness of a user's answer when compared to the alternatives might further distinguish it to an attacker as the correct choice. Among the choices for 'favorite animals', a user supplied answer of "unicorn" would stand out from "cat", "dog", and "rabbit".

Due to this threat, Security PS does not recommend implementing multiple choice answers for challenge question authentication.

Now that we have described the fundamental challenge question formats, we will introduce an approach for evaluating potential challenge questions.

Selecting Proper Challenge Questions

Since the goal of challenge questions is to help authenticate users they must do an effective job of doing so. We have worked with several organizations that started to implement challenge question authentication and realized they did not have criteria for distinguishing good challenge que stions from bad challenge questions. They were stuck either copying the questions of other organizations or coming up with their own. In some cases poor challenge questions hurt the overall security of the application.

One certainty is that any single challenge question is going to be weaker (e.g. less secure) than any single password. This is due to the fact that challenge question answers tend to be logical while passwords are completely free-form. Challenge questions make requests like "tell me your favorite food", which differs from the password approach of saying "tell me anything". One has a limited number of expected answers and one does not.

'One certainty is that any single challenge question is going to be weaker (e.g. less secure) than any single password.'

The type of answers requested by challenge questions also differ in some respects, depending on the question asked. Some questions are fact-based, like "what hospital were you born in". Answers to this

type of question will not change over time and should be easier for a user to remember. Unfortunately, they may also be easier for an attacker to research and abuse.

Other questions are more belief-based (such as "who was your favorite teacher") or selection-based (such as "Who is a memorable person from your childhood"). These answers are useful because they are more open ended and may allow more possible answers. However, they also increase the chance of users forgetting the answer (e.g. a 'favorite') they provided during enrollment.

Either type of question can be appropriate in a challenge question system, but the inherent risks of each must be understood.

Evaluating the security provided by challenge questions can be difficult without a structured approach for identifying strengths and weaknesses. Several years ago I developed a framework that focused on these five fundamental characteristics of all authenticators. These characteristics are:

- Usability
- Uniqueness
- Integrity
- Affordability
- Accuracy

A challenge question can be evaluated for these same characteristics. In the following sections we provide you with our feedback on the qualities of different challenge questions.

Usability

The usability characteristic measures how effectively people can utilize a challenge question to successfully authenticate. Usability is also concerned with any human or environmental factors that might impede the use of a challenge question.

Every environment has a percentage of users that will be unable to utilize a particular challenge question, or at least use it without difficulty. One of your goals is to minimize the number of people in this group. You can improve usability by identifying challenge questions which will pose this problem and either avoid them or offer alternatives to them.

One important consideration is whether the challenge question can be answered by all users. Maybe a person has never had a pet, doesn't have a favorite author, or wasn't born in a hospital. Logically, they can't answer challenge questions asking for these answers.

Another common problem is questions that ask for a ZIP code or other regionalized piece of information that is not applicable to all users of the system. This doesn't mean these questions must be avoided, but users should be able to choose alternative questions that they can answer.

Since challenge questions are knowledge-based authenticators, a user's ability to remember their answers is also important. The attractiveness of challenge questions is that they ask personal questions which should be easier to remember than a less personal password.

You may notice that some challenge questions ask for childhood memories rather than recent ones. The theory behind this childhood focus is to improve usability. If the memory from years ago is still distinct enough to answer during account enrollment, a user may be more likely to remember it during subsequent authentications.
Another usability benefit of challenge questions is that users don't require much training prior to use since they have been answering questions their entire life. However, as we will discuss in the Integrity section, you still should educate users on how to avoid supplying answers that weaken the security of the system.

Finally, keep in mind potential privacy concerns about the information collected using challenge questions. Challenge questions, by their very nature, run a higher risk of raising privacy concerns because they are designed to ask for personal information.

Stay away from asking questions that are too personal (e.g. "what is your race") and you shouldn't have many objections. You can also avoid some user objections if you inform them about your organization's policy for protecting their answers to these questions.

Uniqueness

The uniqueness characteristic examines the distinctness of proof used to confirm an identity. If an answer isn't unique then we lose faith that it provides any reliable authentication of the user's identity. An attacker may attempt to impersonate a legitimate user by predicting their answers.

Passwords also present a challenge to ensure adequate uniqueness. However, password controls can be implemented that require users to make better choices. Similar controls are difficult to implement for challenge questions. You can't tell a user to choose a different favorite author because "Grisham" is too popular. Accordingly, you must consider both the numbers of possible answers and likely answers when evaluating the uniqueness of challenge questions [5].

For example, the challenge question "what color are your eyes" offers very few possible answers because of the natural limitations of human eye color. The question "what is your favorite color" offers more possible answers, but still has only a small amount of likely answers. More users will answer with the most common, and therefore predictable, colors (e.g. blue, green, red).

Names also present a uniqueness challenge. Questions asking for any type of name (people, pets, streets, cars, sports teams) will have answers that tend to be more popular than others. Intelligent attackers will compile lists of the more likely answers and guess these first rather than attempting a more random, and time consuming, brute force approach.

Predictability of answers is an inherent weakness for any authenticator where users are asked to generate their own secrets. Organizations choosing to implement challenge questions will have to choose questions with both the greatest number of possible and likely answers, as well as manage the threat of guessing attacks with technical monitoring controls.

Integrity

The integrity characteristic serves as a measure of how well a challenge question resists attempts to impersonate a user's identity over time. Good integrity provides resistance to challenge question disclosure or duplication, thereby ensuring that answers are available only to the genuine user. This will rely, in part, on the user's commitment to keeping the challenge question answers a secret.

Use of challenge questions may pose a paradigm shift for some security professionals. Many of us discouraged users from creating a password using a family name, sports team, or other personal information due to the increased potential of an attacker guessing it. Now we ask users to authenticate (at least in part) using this very same information.

'Be sure to introduce challenge questions as a supplement to a good password, not as a replacement for it.'

These contradictory practices require organizations to emphasize the differences between passwords and challenge questions in security awareness material to avoid undermining the quality of passwords. Be sure to introduce challenge questions as a supplement to a good password, not as a replacement for it.

One aspect of authenticator integrity is whether a user can detect that their authenticator has been stolen. All knowledge-based authenticators suffer from the fact that they can be easily copied (if exposed) and subsequently used by an attacker. The user may never have any indication that their identity was stolen. This highlights the need for organizations to monitor application logs for unauthorized account use rather than waiting for a user complaint.

Challenge questions are especially susceptible to theft because they are not inherently secrets. They are simply questions that should be difficult to answer without personal knowledge of the user.

Unfortunately, these answers can be exposed in a number of different ways. A user may share the information with others before or after they have established it as an answer to a challenge question. A friend or family member of the user may share the personal information with others, unaware that it is being used for authentication.

Unless a user is constantly aware of the impacts of sharing their personal information they may unwittingly put challenge question answers at risk. We believe it is unreasonable to assume that most users would maintain this level of awareness. Therefore we should assume that a determined attacker will be able to overcome challenge question authentication.

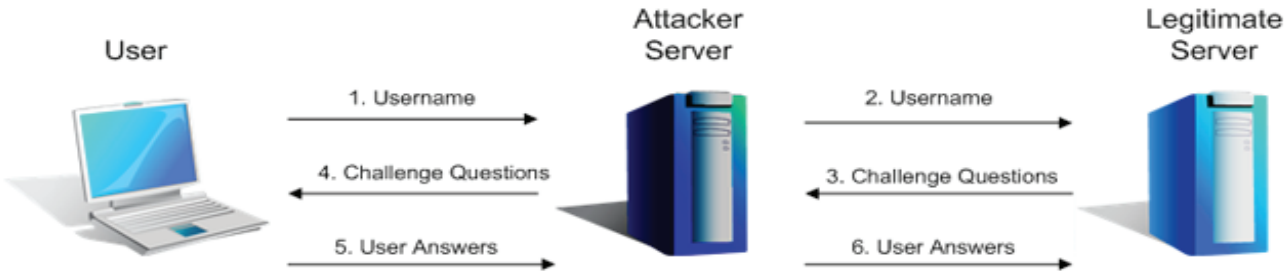
The susceptibility of a challenge question to guessing attacks will increase when the attacker has personal familiarity with the user. Survey results from Javelin Strategy and Research showed that when a victim of identity theft could identify the person responsible for obtaining their personal information, 15% of the time it was friends, acquaintances, relatives, or in-home employees [6].

While identity theft isn't the only outcome of a compromised online identity, this statistic supports the idea that a portion of attacks against challenge questions will come from people familiar with the user.

In fact, in a 1996 study John Podd, Julie Bunnell, and Ron Henderson found that a worrying percentage of "significant others" (such as a parent, partner, or friend) could guess the answer to the user's challenge question within four tries or less [7]. For example, the user's favorite school teacher was guessed 15% of the time and their favorite actor was guessed 13% of the time. This was without allotting time for the significant other to surreptitiously pry the answers out of the user during normal conversations.

Fortunately, the majority of attackers will not know much about a user when they begin their attempt to gain unauthorized access to the user's account. In addition to online guessing attacks (refer back to the Uniqueness section), we expect two other attacks to be popular: man-in-the-middle attacks and question duplication attacks.

This type of man-in-the-middle attack involves the interception of data between the user's computer and the legitimate web server. Similar to a site spoofing attack, it requires a user to access an attacker's site while believing they are actually accessing a legitimate site. Attackers can redirect users to their malicious site using phishing, DNS poisoning, malicious proxy software, or other approaches. People may be deceived if the appearance and behavior of the attacker's site is similar enough to the legitimate site.



Steps in a man-in-the-middle attack against challenge question authentication

As users input their account credentials on the attacker's site, this web server creates a session with the legitimate site. Using this session it can present the user's account credentials, retrieve their specific challenge questions, and then display the questions on its own pages. The user answers the challenge question, allowing the attacker to record the answers for later use. They may even pass the user onto the legitimate site to avoid suspicion about the attack.

Variations of this attack have already been reported [8] [9].

A question duplication attack requires more time and patience on the part of an attacker. The attacker must create a site which independently attracts people to visit and create a user account. They may lure users by providing access to funny videos, free software, pornography, or other attractive content. During the account creation process the attacker's site asks users the same challenge questions used by one or more other sites targeted by the attacker. The attacker then uses the supplied username, password, and challenge questions answers during their attempts to impersonate users on the targeted sites.

We have observed criminals carry out similar attacks against passwords and it is likely that they will adopt this same tactic with challenge questions.

A final integrity shortcoming of challenge questions is that once an answer is known by bad guys it shouldn't ever be trusted again. In other words, once their 'favorite pet's name' is known, it no longer serves as a good authenticator. If it is still used, the same attacker (or attackers with whom the information was shared) may be able to continue infiltrating the user's accounts.

Unless a user is aware that an attacker has knowledge of their challenge question answers they will probably continue to choose similar questions when enrolling for an account on other systems. Even with this awareness, some users will undoubtedly fail to connect the risk of using the same answers on different sites.

Affordability

The affordability characteristic measures the cost to buy and maintain the challenge question. With challenge questions, the initial costs are limited. The typical expense is the money needed to develop or purchase the security software that handles challenge question enrollment, authentication, and management.

The low implementation cost of challenge questions is undoubtedly a big reason they have become so popular when compared to true multi-factor authentication alternatives.

However, challenge questions also incur customer support expenses any time a user has to contact an organization to deal with forgotten or compromised information. If you ask for challenge question answers that are difficult for people to remember, the solution's affordability will suffer.

'The low implementation cost of challenge questions is undoubtedly a big reason they have become so popular when compared to true multi-factor authentication alternatives.'

Accuracy

The accuracy characteristic measures the frequency of authentication mistakes that limit use by legitimate users. Accuracy of answers to challenge questions is an important factor in reducing the false rejection of legitimate users.

Figures from a basic study published by Lawrence O'Gorman, Amit Bagga, and Jon Bentley indicate that users forget the answer to a challenge question about 5% of the time when presented with multiple choice answers [10]. Notice that this data applies to multiple choice answers and not the free form answers we advocate using. We actually expect a higher percentage of forgotten answers when using free form answers.

In addition, accuracy should improve when users are allowed to select their challenge questions from a pool of 10 to 20 available questions. Presumably they will choose questions during enrollment with an answer they feel most likely to remember in the future.

Finally, consider that accuracy may suffer when you ask belief based challenge questions instead of fact based challenge questions. Beliefs or selections change over time. During enrollment a user's favorite

movie may have been Borat, but several months later it may be Transformers. Users can face difficulty trying to remember how they answered a challenge question, especially if it has been some time since they were last prompted for an answer.

Examples and Analysis of Challenge Questions

Now that we have examined the characteristics of challenge questions, we want to demonstrate how real challenge questions can be evaluated against these criteria.

The following questions were compiled from actual applications that implemented challenge question authentication. Common variations of the challenge question are included for comparison. These variations may offer a better or worse alternative, depending on the quality of the question.

We have also included feedback from our own evaluation of each challenge question. This feedback offers a general description of what we saw as the question's strengths and weaknesses. Your particular environment or user population may produce a different evaluation.

Finally, we assigned each challenge question a rating using the following labels to describe the overall authentication quality from worst to the best: Poor, Fair, Ok, Good, Excellent.

This rating system is intended to allow comparison of challenge questions against any other type of authenticator evaluated using our authenticator characteristics framework. Accordingly, even the best challenge question may not receive an "Excellent" rating since there are better alternative authenticators available.

Keep in mind that the integrity of challenge question answers will probably decrease with time as more personal data becomes publicly available. Expect attackers to continue improving their techniques to take advantage of new data. Due to this trend, ratings assigned to these same questions in five years time may be worse.

Question: What is your birth date?
Variations: What is your year of birth?
Evaluation: Usability and uniqueness are fairly good. Uniqueness suffers if you ask only for the year of birth. Integrity is poor since it is so frequently disclosed either in person or through Internet sites. Affordability is fairly good. Accuracy problems may result if the user enters "Jan 1" during enrollment and later try to use "January 1" or "1/1/1970".
Rating: Poor

Question: What is your social security number?
Variations: What are the last four digits of your social security number?
Evaluation: Usable by most people residing in the U.S., but not by an international user population. Uniqueness is fairly good. Integrity is only fair since it is so frequently disclosed, and follows a partially predictable format. Affordability and accuracy are fairly good.
Rating: Fair

Question: What is your mother's maiden name?
Variations: What is your father's middle name? What is your spouse's middle name? What is your first child's middle name? What is your youngest sibling's middle name?
Evaluation: Usability is fairly good. The variations of this question listed above are less usable for people without a spouse, sibling, or children. Names can be unique, but the popularity of some choices will increase predictability. Integrity problems arise when the user's surname is the same as their mother's maiden name. Internet genealogy databases also supply information that can decrease integrity. Affordability and accuracy are fairly good.
Rating: Fair

Question: What was the total on your most recent bill?
Variations: What was the account balance on your most recent statement?
Evaluation: Usability is okay, although it may require the user to have physical access to their most recent statement. This will reduce usability when away from home. Uniqueness may or may not be good, depending on the associated service. Charges for monthly cable service may be less unique than the balances in users' bank accounts. Integrity is fairly good as long as the user is instructed not to share the information. Affordability and accuracy suffer because of the changing monthly answers that increase the likelihood of a wrong answer and the need for customer support.
Rating: Fair

Question: What high school did you attend?
Variations: What middle school did you attend? What grade school did you attend? What was the name of your high school mascot?
Evaluation: Usability tends to be good except for people who were home schooled or did not attend high school. Names can be unique, but the popularity of some choices (e.g. Washington or Kennedy) will increase the predictability of choices. Integrity tends to be poor since this information isn't considered a secret by most users, and Internet sites (such as Classmates.com) make school history public. Affordability and accuracy are fairly good.
Rating: Fair

Question: Where were you born?
Variations: In what city were you born? In what state were you born? Where did you live when you were age 14?
Evaluation: Usability is fairly good. Uniqueness is good, but the popularity of some cities will increase the predictability of choices. The limited number of states offers poor uniqueness for this question variation. Integrity tends to be poor since this information isn't considered a secret by most users, and Internet sites (such as MySpace.com or Facebook.com) may make this information public. Some people also live in the same city their entire life. Affordability and accuracy are fairly good.
Rating: Fair

Question: What is your favorite TV show?
Variations: Who is your favorite TV character? Who is your favorite TV actor?
Evaluation: Usability is good for most people, but excludes those who don't watch TV. Uniqueness is okay, but the popularity of some shows will increase the predictability of choices. Integrity can be poor since this information isn't considered a secret by most users, and Internet sites (such as MySpace.com or Facebook.com) may make this information public. Affordability is fairly good. Accuracy may be affected over time if the user's favorites change.
Rating: Fair

Question: What is your favorite book?
Variations: Who is your favorite character in a book? Who is your favorite author?
Evaluation: Usability is good for most people, but excludes those who don't read books. Uniqueness is okay, but the popularity of some books will increase the predictability of choices. Integrity can be poor since this information isn't considered a secret by most users, and Internet sites (such as MySpace.com or Amazon.com) may make this information public. Affordability is fairly good. Accuracy may be affected over time if the user's favorites change.
Rating: Fair

Question: What is your favorite animal?
Variations: What is your favorite type of mammal? What is your favorite type of fish? What is your favorite type of bird?
Evaluation: Usability is good. Uniqueness is okay, but the popularity of some types of animals (e.g. dogs, cats, dolphins) will increase the predictability of choices. Some of the question variations further reduce uniqueness. Integrity can be poor since this information isn't considered a secret by most users. Affordability is fairly good. Accuracy may be affected over time if the user's favorites change.
Rating: Fair

Question: What is your pet's name?
Variations: What is your favorite pet's name? What was the name of a childhood pet?
Evaluation: Usability is good. Uniqueness is okay, but the popularity of some pet names will increase the predictability of choices. Some of the question variations further reduce uniqueness. Integrity can be poor since this information isn't considered a secret by most users. Affordability is fairly good. Accuracy may be affected over time if the user's pet, or favorite pet, changes.
Rating: Fair

SECURITY PS

Question: Who is a memorable person from your childhood?
Variations: Who was your childhood hero? Who is a memorable person to you?
Evaluation: Usability is fairly good. Uniqueness tends to be good except for cases where the user selects a well known public figure (such as a president, athlete, or celebrity), which increases the predictability of choices. Fairly good integrity except for cases where the user makes their admiration for the person well known (again, usually in the case of an athlete or celebrity). Affordability and accuracy are fairly good.
Rating: Ok

Conclusion

Implementing challenge question authentication requires careful analysis of both the user population and the question being considered. With proper planning, an organization can decrease the risk of attacks against challenge question authentication and, in turn, the identities of their users. Our authenticator characteristics evaluation framework can provide security professionals with a structured approach for conducting this analysis and avoiding bad challenge questions.

As you can observe from our ratings of the sample challenge questions, Security PS believes that it is difficult for individual challenge questions along to provide adequate authentication of users. Challenge questions can be attractive based on their usability and affordability, but these advantages can't eliminate the shortcomings of other characteristics. We believe that most challenge questions are deserving of only a "fair" overall rating, with "ok" at best. While requiring users to answer multiple challenge questions during the authentication process can improve overall security, some residual risk will remain.

We hope organizations recognize that challenge questions do not adequately address the authentication needs of every application. Alternatives like one-time passwords, private keys and certificates, biometrics, or even other knowledge-based authenticators may better combat threats against high value online services. While low cost authentication solutions are tempting, customer account security and trust are better preserved by implementing the right authentication solution for your specific application.

For assistance in properly implementing challenge question authentication or assessing alternatives, contact the author of this white paper at bmarshall@securityps.com or 913-888-2111. Visit the Security PS blog (blog.securityps.com) to read or share comments about this white paper.

SECURITY PS

References

1. Authentication in an Internet Banking Environment, FFIEC, October, 2005, http://www.ffiec.gov/pdf/authentication_guidance.pdf

2. Multi-Factor and Risk-Based Authentication, Kris Drent, The App Security Advisor Blog, June 2007, http://www.appsecadvisor.com/podcast/multi-factor-and-risk-based-authentication/

3. Designing Authentication Systems with Challenge Questions, Mike Just, August 2005, http://hornbeam.cs.ucl.ac.uk/hcs/teaching/GA10/lec5extra/ch08just.pdf

4. When to Assign Users Responsibility for Security, Bruce K. Marshall, April 2006, http://blog.securityps.com/2007/04/when-to-assign-users-responsibility-for.html

5. Using Secret Questions, Mark Burnett, OWASP, November 2006, http://www.owasp.org/index.php/Using_Secret_Questions

6. 2006 Identity Fraud Survey Report, Javelin Strategy & Research, 2006, http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf

7. Cost-effective Computer Security: Cognitive and Associative Passwords, John Podd, Julie Bunnell, and Ron Henderson, Proceedings of the 6th Australian Conference on Computer-Human Interaction, 1996

8. Citibank Phish Spoofs 2-Factor Authentication, Brian Krebs, Washington Post blog entry, July 10, 2006, http://blog.washingtonpost.com/securityfix/2006/07/citibank_phish_spoofs_2factor_1.html

9. ABN Amro Compensates Victims of 'Man-In-The-Middle', Finextra, February 2007, http://www.finextra.com/fullstory.asp?id=16750

10. Call Center Customer Verification by Query-Directed Passwords, Lawrence O'Gorman, Amit Bagga, Jon Bentley, Proceedings of Financial Cryptography 04, 2004

SECURITY PS