# Using Avatars for Improved Authentication with Challenge Questions

Nicholas Micallef
*School of Informatics*
*University of Edinburgh*
*Edinburgh, UK*
*nicholasmicallef@gmail.com*

Mike Just
*School of Engineering & Computing*
*Glasgow Caledonian University*
*Glasgow, UK*
*mike.just@gcu.ac.uk*

***Abstract*—We present a novel method for improving the security of challenge question authentication, which traditionally requires a user to answer questions such as *"What is your Mother's Maiden Name?"*. In our method, users create an Avatar representing a fictitious person, and later use the Avatar's information to authenticate themselves. The Avatar Profile consists of basic identifying information (e.g., name, address) as well as personality information (e.g., pets, interests). This info is pseudo-randomly generated from a large corpus of information. For authentication purposes, a small amount of the Avatar Profile information is used to respond to *challenge questions*. In terms of security, the use of information that is not personally associated with the user is intended to thwart *observation* attacks such as, for example, knowing the user's mother's maiden name. In terms of usability, our design establishes a bond between the user and their Avatar using graphical images and periodic associations by, for example, presenting an image of the Avatar at each login. This *nurturing* of the bond between a user and their Avatar leverages known psychological phenomena. At the same time it also provides a novel adaptation to security of the emotional investments that users exhibit in *virtual worlds* and *massively multi-user online graphical environments*. In this paper, we describe our work-in-progress towards an Avatar Authentication design, partially guided by an initial pilot experiment. Our initial results are promising and point to a possible future for the use of avatars for authentication.**

***Keywords*-authentication; avatar; security; usability.**

## I. Introduction

A secure and usable authentication system is of critical importance for applications nowadays. A secure system prevents impersonation, which otherwise could lead to monetary loss, embarrassment, inconvenience, and other problems. A usable system not only encourages more secure behaviour, but also results in a more enjoyable user experience and can increase user enrolment.

Password authentication is the most ubiquitous authentication method used today, yet its security and usability weaknesses have been known for many years [1][2][3]. It is also important to note that with increases in attacker capabilities and an ever-increasing quantity of accounts that users must manage, these problems are further exacerbated. Alternatives such as biometrics and smartcards continue to present usability issues and deployment challenges [4].

Recently, significant research effort has been focused on alternatives to *text* passwords. Numerous graphical password systems have been developed and tested, and recent research suggests good potential, and a path toward more consistent evaluation [5]. Challenge question authentication is as ubiquitous as passwords, and is often used as a form of secondary authentication in case a user forgets their original password. Their use of personal information and memories, as opposed to *memorized* passwords, has been the main focus of the latest research [6][7][8][9]. Unfortunately, in their basic implementation, the answers to challenge questions are most vulnerable to *observation attacks* in which the information and memories used by a user to authenticate, are also known to (or easily determined by) attackers.

Our approach to authentication uses an *Authentication Avatar* which represents the identity, including personality, of a fictitious person that is almost randomly generated from minimal user input. An Avatar Profile (AP) contains information about the avatar, and a subset of the AP information is used by the user to respond to challenge questions such as *"What is your Avatar's pet's name?"*, or *"What was your Avatar's secondary school?"*. In this way security might be improved since, unlike the user's own information, the avatar information is not as easily determined by an attacker. In terms of usability, since such fictitious information is likely to be more challenging for a user to recall (than their own, personal information), our design uses techniques such as repeated exposure and graphical imagery whereby, for example, a user might be exposed to an image of their avatar at every login in order to improve the memory association. Such images can be associated with the avatar itself, and also with elements of the AP, e.g., a picture of the Avatar's pet. From our early designs, it appears that such methods can be seamlessly integrated into the authentication process. In this way, as with avatars used in *virtual worlds* and *massively multi-user online graphical environments*, our authentication avatar design attempts to build upon the degree of emotional investment that users exhibit with avatars.

In Section II we describe several factors influencing our design. In Section III we describe our current, prototype implementation and highlight some possible design variations. In Section IV we describe some plans for our final design,

ISBN: 978-1-61208-010-9

and discuss our plans for measuring security and usability. Section V provides some concluding remarks and direction for future work.

## II. Motivation and Design Considerations

In designing an avatar for authentication purposes, we were motivated by existing work in secure and usable authentication, and also reflective of avatars designed for other purposes, such as virtual worlds. Our goal was to build a structure containing information that could be used by a user to authenticate in such a way that the structure holds some meaning for the user, but not for attackers. For the authentication protocol, we chose to base our solution upon challenge question authentication, and note that avatars may similarly prove useful for other security methods.

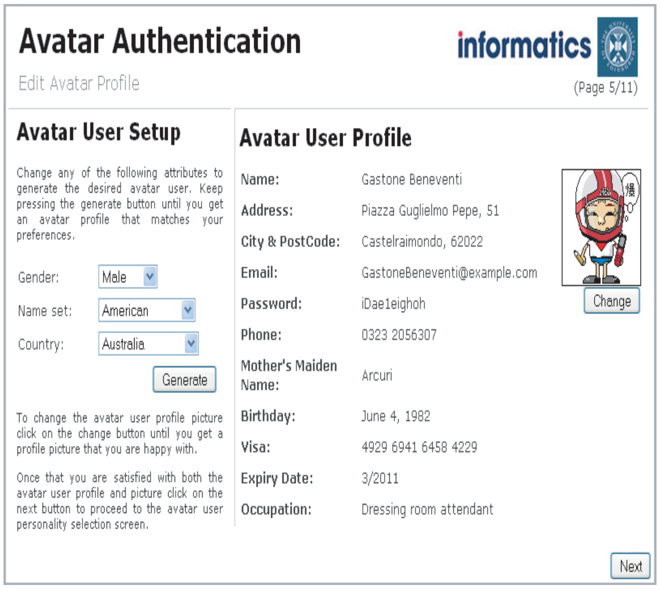
There are two main issues to securing challenge question authentication. Firstly, answers with inherently small, or non-uniform answer spaces should be avoided [7][8]. And while most questions share this risk, it can be partially mitigated with appropriate question selection, and the enforcement of a requirement to use multiple authentication questions. Secondly, the answers to challenge questions are often *observable*, so that a determined attacker can observe or recover answers to challenge questions with relative ease [6][9]. For this reason our design introduces a proxy for the answers to the challenge questions: an Avatar.

In terms of usability, the same research indicates that users struggle in recalling their own answers to challenge questions, despite the fact that the answers are *already known* to the user (and shouldn't require additional memorization). There are several potential reasons for this, including a user's changing or conflicting memories. In this sense, it may be that current designs have relied too heavily upon users to accurately and specifically recall one of their various memories, especially when it is likely that the memory originated in some other other context. The potential of authenticating with an avatar is to create new memories, but in such a way that users establish a close, personal bond with this information. The idea of creating this information in the context of their authentication application is to make the information more memorable when re-used in that same context to later authenticate. For our solution we attempt to build this relationship through nurturing, where an electronic pet is used as a daemon [11]. In our solution, the user is consistently exposed to their avatar through a representative image, ideally forming an association that improves the recall of the answers to the related challenge questions. We also apply some additional memory techniques at registration such as story writing and repetition [12].

In terms of the data upon which the AP is constructed, we collected a large corpus of profile and personality information based upon existing sources, often used for different purposes, such as registering for aggregate news sites [13][14][15]. Whereas such sites are often used for "one time" registrations (e.g., when information is collected for marketing purposes), it is a portion of our AP information that is used for repeated and consistent authentication.

## III. An Authentication Avatar Implementation

From these considerations, we can begin to design, implement and evaluate an avatar authentication system. Below, we describe some additional detail involved in this design, and include a couple of screen-shots from our current prototype implementation. The design focuses on the creation of an *Avatar Profile* during user registration. The AP includes information that would likewise be associated with a real person, e.g., name, family. From this information, the user will then choose three challenge questions where the answers relate to the information contained in the AP. The AP which builds upon elements used elsewhere for fake name generation [14], consists of two parts: the Avatar User Profile (AUP), and the Avatar Personality (APY). We now describe the process for building this profile in more detail.



Avatar Authentication

Edit Avatar Profile

(Page 5/11)

Avatar User Setup

Change any of the following attributes to generate the desired avatar user. Keep pressing the generate button until you get an avatar profile that matches your preferences.

Gender: Male

Name set: American

Country: Australia

To change the avatar user profile picture click on the change button until you get a profile picture that you are happy with.

Once that you are satisfied with both the avatar user profile and picture click on the next button to proceed to the avatar user personality selection screen.

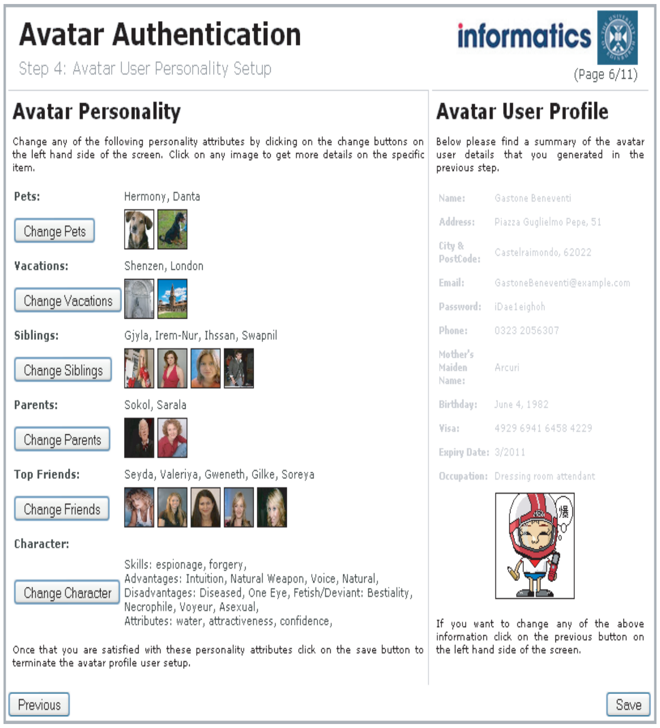
Avatar User Profile

| | |
|---|---|
| Name: | Gastone Beneventi |
| Address: | Piazza Guglielmo Pepe, 51 |
| City & PostCode: | Castelraimondo, 62022 |
| Email: | GastoneBeneventi@example.com |
| Password: | iDae1eighoh |
| Phone: | 0323 2056307 |
| Mother's Maiden Name: | Arcuri |
| Birthday: | June 4, 1982 |
| Visa: | 4929 6941 6458 4229 |
| Expiry Date: | 3/2011 |
| Occupation: | Dressing room attendant |

Figure 1. Avatar User Profile Setup

Figure 1 shows the first stage of user registration. The user *seeds* the AUP with information about the avatar, selected from three drop-down lists: the avatar's *gender*, *name set*, and *country of birth*. In our current implementation, the gender choice is either male or female, the name set is one of 18 different cultures (e.g., American, Arabic, Hispanic), and the country is one of 19 countries, where details for the latter two were taken from Fake Name Generator [13]. The generated AUP information includes a name, address, city & postcode, email address, password, phone number, mother's maiden name, birthday, credit card number & expiry date, and occupation for the Avatar, in addition to a random image.

To continue, the user populates the *Avatar Personality (APY)* as depicted in Figure 2, consisting of information about pets, vacations taken, family (siblings & parents), friends, as well as various character traits. In our current implementation, rather than seeding from user input, the APY information is initially chosen randomly, and a user is thereafter able to toggle the selections in each category. Also notice that for many of the elements of the APY, an image is associated with the Avatar information.



Avatar Authentication

Step 4: Avatar User Personality Setup

(Page 6/11)

Avatar Personality

Change any of the following personality attributes by clicking on the change buttons on the left hand side of the screen. Click on any image to get more details on the specific item.

Pets: Hermony, Danta

Vacations: Shenzen, London

Siblings: Gjyla, Irem-Nur, Ihssan, Swapnil

Parents: Sokol, Sarala

Top Friends: Seyda, Valeriya, Gweneth, Gilke, Soreya

Character:

Skills: espionage, forgery,
Advantages: Intuition, Natural Weapon, Voice, Natural,
Disadvantages: Diseased, One Eye, Fetish/Deviant: Bestiality, Necrophile, Voyeur, Asexual,
Attributes: water, attractiveness, confidence,

Once that you are satisfied with these personality attributes click on the save button to terminate the avatar profile user setup.

Avatar User Profile

Below please find a summary of the avatar user details that you generated in the previous step.

| | |
|---|---|
| Name: | Gastone Beneventi |
| Address: | Piazza Guglielmo Pepe, 51 |
| City & PostCode: | Castelraimondo, 62022 |
| Email: | GastoneBeneventi@example.com |
| Password: | iDae1eighoh |
| Phone: | 0323 2056307 |
| Mother's Maiden Name: | Arcuri |
| Birthday: | June 4, 1982 |
| Visa: | 4929 6941 6458 4229 |
| Expiry Date: | 3/2011 |
| Occupation: | Dressing room attendant |

If you want to change any of the above information click on the previous button on the left hand side of the screen.

Figure 2. Avatar Personality (APY) Setup

For the AUP and APY, we chose elements with large answer spaces, and random selection should produce relatively flat distributions (to be verified as part of our experiments).

Once the Avatar Profile (including the AUP and APY) has been populated, there are at least two options for selecting the challenge questions. Firstly, the user could be presented with a list of candidate challenge questions and be asked to choose three questions from the list, providing the answers that correspond to the information from the AP.[1] This is the option that we have currently implemented for our prototype design. Alternatively, the user could select three categories of information from the AP, and then challenge questions associated with this information could be presented to the user. Based upon early results from our pilot experiment (see Section IV) we plan to implement the second option in our next prototype version as it should allow the user to more clearly focus on elements of the AP that are most relevant (and ideally, memorable) to them.

As noted above, our current implementation associates images with most of the elements of the AP. For example, our sample Avatar is represented by a small character with a red and white helmet, and family members such as pets and siblings are also represented with images. These images can serve as *cues* to the AP information, and can help to prompt the user for their answer. For example, if the user registers the challenge question *"What is the name of my sister?"*, an image of the Avatar's sister would be associated with the answer. When later authenticating, the user would be presented with the question *and the image cue*, and be asked to provide the answer.

If challenge questions are used as a user's primary form of authentication, then the user would regularly be presented with the images at login, reinforcing the answers at each login as a form of nurturing [11]. If, as is more typical today, the challenge questions are less regularly used for situations such as recovery due to a forgotten password, then the images could still be regularly presented to the user as a way of reinforcing the memory of the answers. For example, at password login the user could be shown the image of their Avatar as a reminder of their Avatar's character. This regular engagement with the avatar images will (hopefully) encourage improved recall of the avatar information, and has a side benefit of contributing to the authentication of the server to the user. We plan to validate these hypotheses as part of an experiment on our final design.

## IV. Fine Tuning our Implementation

To inform our final design we conducted a pilot experiment of our initial prototype with approximately 100 staff and students from the University of Edinburgh. Participants configured an Avatar Profile, registered a set of three challenge questions and corresponding answers, and then returned after two weeks to attempt to authenticate with the answers to the challenge questions.

In terms of security, our design supports a random population of the AP information suggesting that for a challenge question with $n$ possible answers, an attacker would have a guessing probability of $1/n$. However, the answers aren't completely random due to the impact of user choice in their selection. For example, in the pilot experiment, while almost 75% of participants used the Avatar Profile information to populate answers to their challenge questions, 25% did not (and possibly used their own personal information). For this reason, we are implementing the aforementioned modification in which users will be presented challenge questions based upon their identification of preferred information from the AP. In addition, we need to determine whether users exhibit a bias in choosing the Name Set or Country for their Avatar User Profile, or similar bias with the Avatar Personality (APY), e.g., users might toggle to choose more

[1] The answer information could be automatically populated, but requiring the user to enter the information would help to improve answer retention.

familiar pet or sibling names. Such effects weren't noticed in our pilot experiment, but need to be confirmed with a larger set of diverse users.

In terms of usability, even though we had not yet implemented the nurturing features of our system, more than one-third of the challenge questions were answered correctly by our participants – a surprisingly positive result in that some users were able to recall newly memorized information for a fictitious person, giving us further hope when we implement our methods to increase this bond. We expect this number to increase significantly upon implementation of our nurturing features and will compare the recall results of users with baseline results for existing challenge question systems [6][7].

## V. Conclusion and Future Work

*Avatar authentication* is a new way to view information-based authentication which utilizes fake personas (an *Avatar*) that can be created by users in order to authenticate themselves. The use of an Avatar is intended to thwart attackers who are otherwise able to obtain personal information about a user. We describe how *nurturing* of the bond between the user and the Avatar leverages known psychological phenomena and provides a novel adaptation to security of the emotional investments that users exhibit in *virtual worlds* and *massively multi-user online graphical environments* in order to better recall information associated with the Avatar. We described our initial prototype design and some plans for improvement following a pilot experiment with 100 participants in which participants showed a surprising ability to recall information associated with their Avatar (despite the fact that our initial prototype had not yet included key nurturing features).

Looking to future work, there may be other ways to set-up a fake persona for authentication purposes, for example, by randomly gathering information from disparate users on a social network, or even by gathering information related to digital objects [16]. Also, there are likely different ways to build the bond between the user and the Avatar, perhaps more fully leveraging components of a virtual world.

## VI. Acknowledgments

Thanks to Bill Cheswick for initially suggesting the use of *false information* for authentication.

## References

[1] E. H. Spafford, "Observing reusable password choices," in *In Proceedings of the 3rd Security Symposium. Usenix*, pp. 299–312.

[2] D. V. Klein, "Foiling the cracker: A survey of, and improvements to, password security," in *Proceedings of the 2nd USENIX UNIX Security Workshop*.

[3] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *IEEE Security and Privacy*, vol. 2, no. 5, pp. 25–31, 2004.

[4] L. Ballard, S. Kamara, and M. K. Reiter, "The practical subtleties of biometric key generation," in *SS'08: Proceedings of the 17th conference on Security symposium*. Berkeley, CA, USA: USENIX Association, 2008, pp. 61–74.

[5] R. Biddle, S. Chiasson, and van Oorschot P.C., "Graphical Passwords: Learning from the First Twelve Years," *ACM Computing Surveys*, 09 2009.

[6] S. Schechter, A. J. B. Brush, and S. Egelman, "It's no secret. measuring the security and reliability of authentication via 'secret' questions," in *SP '09: Proceedings of the 2009 30th IEEE Symposium on Security and Privacy*. Washington, DC, USA: IEEE Computer Society, 2009, pp. 375–390.

[7] M. Just and D. Aspinall, "Personal choice and challenge questions: a security and usability assessment," in *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*. New York, NY, USA: ACM, 2009, pp. 1–11.

[8] J. Bonneau, M. Just, and G. Matthews, "What's in a name? evaluating statistical attacks on personal knowledge questions," in *Proceedings of Financial Cryptography 2010*. N/A: SpringerLink, 2010.

[9] A. Rabkin, "Personal knowledge questions for fallback authentication: security questions in the era of facebook," in *SOUPS '08: Proceedings of the 4th symposium on Usable privacy and security*. New York, NY, USA: ACM, 2008, pp. 13–23.

[10] N. Yee, "The psychology of massively multi-user online role-playing games: Motivations, emotional investment, relationships and problematic usage," in *Avatars at Work and Play*, ser. Computer Supported Cooperative Work, R. Schroeder and A.-S. Axelsson, Eds. Springer Netherlands, vol. 34, pp. 187–207.

[11] P. Briggs and P. Olivier, "Biometric daemons: authentication via electronic pets," in *UPSEC'08: Proceedings of the 1st Conference on Usability, Psychology, and Security*. Berkeley, CA, USA: USENIX Association, 2008, pp. 1–5.

[12] A. D. Baddeley, *Essentials of Human Memory*. Psychology Press, 1999.

[13] CorbanWorksLLC, "Generate a random name, last accessed: 2010-08-18, http://www.fakenamegenerator.com/gen-female-sw-us.php," 2006. [Online]. Available: http://www.fakenamegenerator.com/gen-female-sw-us.php

[14] WikiHow, "Create a fake real person, last accessed: 2010-08-18, http://www.wikihow.com/create-a-%22fake-real-person%22," 2009. [Online]. Available: http://www.wikihow.com/Create-a-%22Fake-Real-Person%22

[15] ——, "How to make an imaginary friend, last accessed: 2010-08-18, http://www.wikihow.com/make-an-imaginary-friend," 2009. [Online]. Available: http://www.wikihow.com/Make-an-Imaginary-Friend

[16] R. Biddle, M. Mannan, van Oorschot P.C., and T. Whalen, "User Study, Analysis, and Usable Security of Passwords Based on Digital Objects," School of Computer Science, Carleton University., Tech. Rep., 10 2010.

ISBN: 978-1-61208-010-9