Cognitive Authentication

Implementation and evaluation
of an image-based authentication method

N I K L A S P E D E R S E N

KTH Computer Science
and Communication

Bachelor of Science Thesis
Stockholm, Sweden 2010

Cognitive Authentication

Implementation and evaluation
of an image-based authentication method

N I K L A S P E D E R S E N

Bachelor's Thesis in Computer Science (15 ECTS credits)
at the School of Computer Science and Engineering
Royal Institute of Technology year 2010
Supervisor at CSC was Mikael Goldmann
Examiner was Mads Dam

URL: www.csc.kth.se/utbildning/kandidatexjobb/datateknik/2010/
pedersen_niklas_K10032.pdf

Royal Institute of Technology
School of Computer Science and Communication

KTH CSC
SE-100 44 Stockholm, Sweden

URL: www.kth.se/csc

Abstract

When it comes to authenticating a user on the Internet today, the de facto standard is to do so with an alphanumeric password. This scheme is easy to use both for the user and the developer, however there are growing threats to the security.

Some alternative schemes focuses on the users ability to remember and identify pictures, since humans are far superior to machines in that area.

Such a scheme is implemented in this thesis and a small study is performed on it. The results are not very promising, but the study is far too small to dismiss the scheme entirely.

Referat

Implementering och utvärdering av en bildbaserad autentiseringsmetod

För att autentisera sig på Internet finns det idag en de facto standard i att använda alfanumeriska lösenord. Detta är en metod som är enkel att använda både för användaren och utvecklaren, men det finns växande problem med säkerheten.

Några alternativa metoder fokuserar på användarens förmåga att minnas och identifiera bilder, eftersom människor är mycket överlägsna datorer inom det området.

I rapporten beskrivs en implementation av en bildbaserad inloggningsmetod, och en liten studie utförs på denna. Resultaten av studien är inte så lovande, men mer data behövs innan metoden kan förkastas.

Contents

Chapter 1

Introduction

1.1 Statement of the problem

This thesis aims to answer the question "Can an image-based authentication method replace the alphanumeric password scheme?". In order to do that an implementation of such a scheme was made, and a small study was made on that implementation to find out how well users perform when they have just received their "password".

1.2 Background

1.2.1 Authenticating on the Internet today

In order to authenticate yourself with an Internet-based service today you will most likely be asked to give your username and your password, a string of alphanumerical characters. The server will take the password, compare it with the value stored together with the username and if they are identical then the user is authenticated.

1.2.2 Security concerns

There is a big flaw in the security of alphanumerical passwords. It lies not so much in the scheme itself, but with those who use it. Most implementations of the scheme let the user choose the password, which means that the user will have a password that is easy to remember. In [IMP2010] are the results of a study over 32 million passwords used in real life. The results are astonishing - 20% of the users share 5000 passwords, all of which would be easy to guess for a hacker, and over 60% have passwords of 8 or less characters.

This implies that a hacker could easily get access to a lot of accounts by using a dictonary of common passwords. Passwords are also vulnerable to shoulder surfing attacks such as keyloggers, since they give away information about which keys the user pressed when writing the password.

1.3 Cognitive authentication schemes

An alternative to alphanumeric passwords is the cognitive authentication schemes, which focus on the human brains way of processing information, specifically the ability to remember and identify images. It was first mentioned in [BLO1995], where the user would authenticate by selecting different spots in an image in the correct order.

There are many variations of the scheme. One example is [Passfaces] where the user has to identify human faces, another examples is a system where the user has to identify a couple of images from a large set and align them in a line.

A couple of studies have been made on the cognitive authentication schemes, among them are [SAT2007] which analyses and proves that not all such schemes are secure. There is also [CAR2007] that analyses a scheme from the users point of view, with some promising results about the usability, and [ACM2005] that looked at the effects of tolerance and image choice in graphical password schemes.

Chapter 2

Implementing a cognitive authentication scheme

2.1 Description of the scheme

The scheme which I have chosen to implement was first proposed in [SOB2002] as a solution to the problem with shoulder surfing attacks. The password is a set of images, unique to each user. When the user want to authenticate a large set of random images will be displayed, a few of which belong to the users set. The user will have to find all of the images belonging to her set, and click somewhere within the convex hull that has its vertices in the centre of each such image. This procedure will be repeated a couple of timed until a desired probability of correctness has been achieved. The scheme is illustrated in figure 2.1.

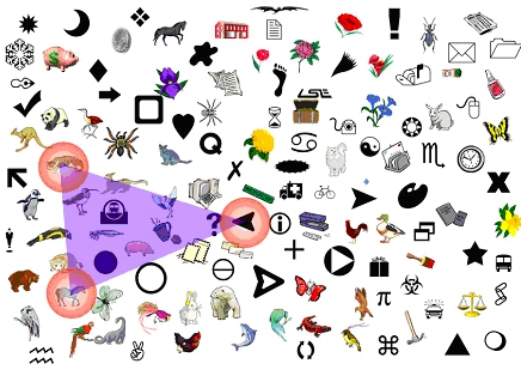

Figure 2.1. The image used by Sobrado and Birget to illustrate the scheme

2.2 My implementation

I chose to do my implementation as a java applet, since that seemed easiest to develop and works the same on all major browsers and operative systems. For images I used a large set of Clipart images, which I transformed and converted so that every image was exactly 50x50 pixels and in the JPG format. A slightly simplified version of the scheme was used, where the images are displayed in a 16x10 matrix and contains exactly three images from the users set.
My prototype was designed as a test for users short term memory of images, as it might look when a user first registers at a service which has this scheme as its authentication method.

2.2.1 Registration

The first thing a user get to do is choose the size of its set. Values between 4 and 20 were accepted, with the default being 6 images. On the screen were two buttons, one to generate a new set of images and one to proceed to the next stage.

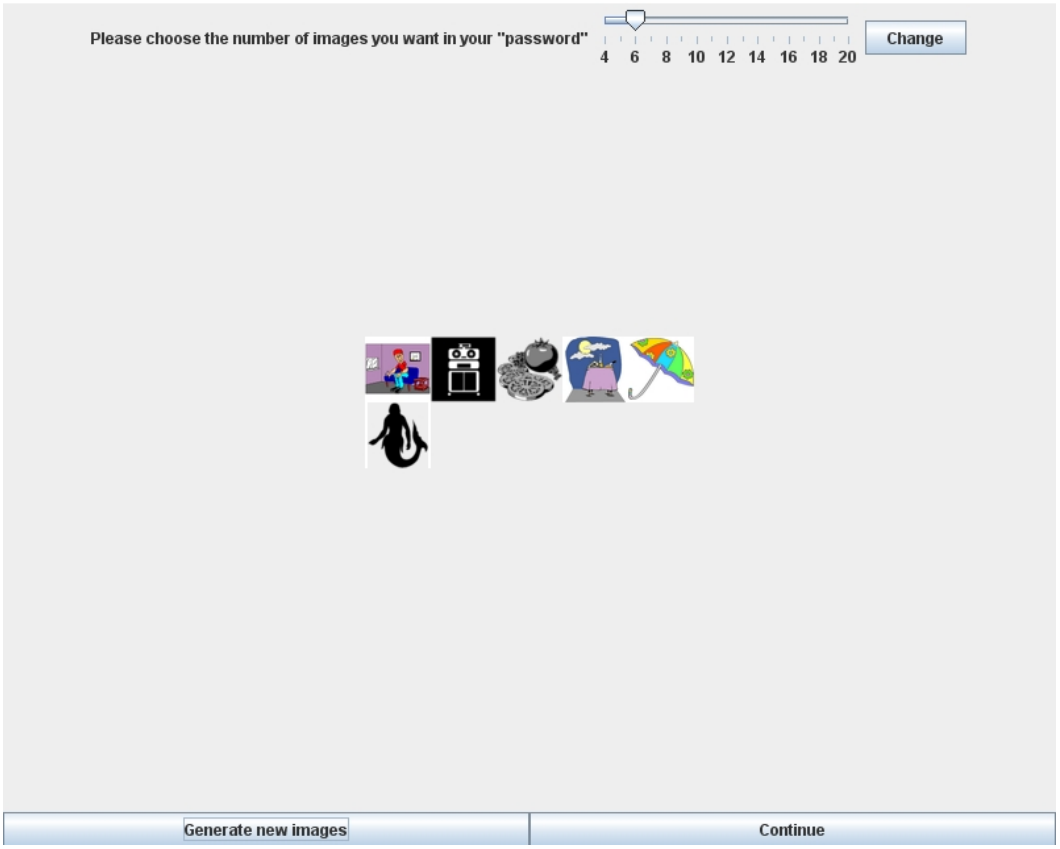

Figure 2.2. A registration screen with six images

2.2.2 Example

After a set of images had been generated for the user, an example of how the authentication works was shown. It only differed from a "real" authentication screen by the fact that the users images were marked with a red border and that the triangle to click within was drawn on the screen.

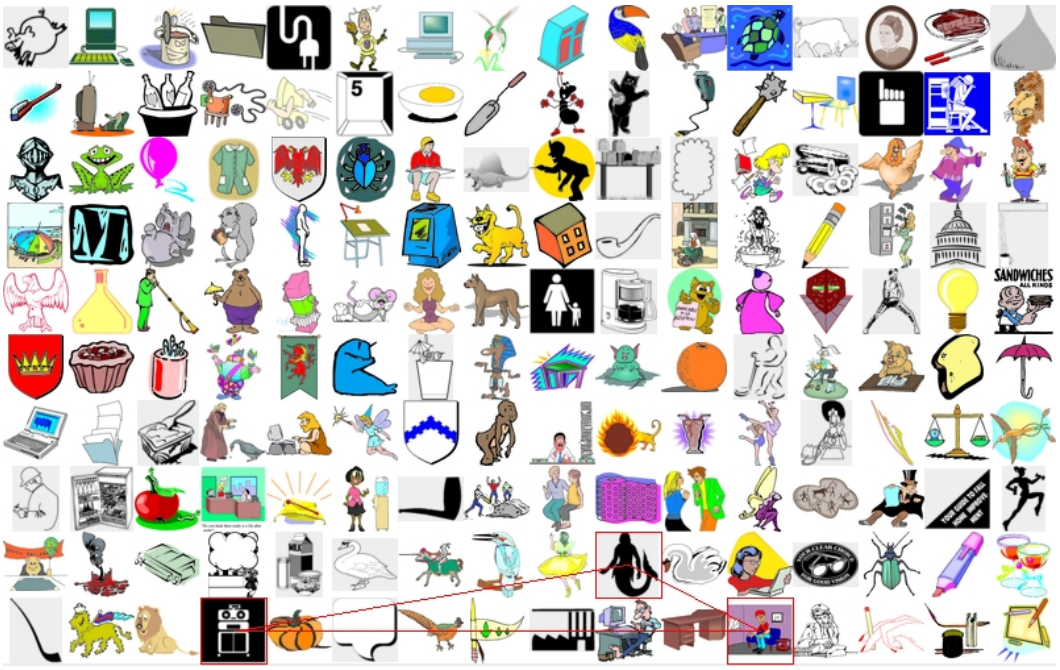

Figure 2.3. An example illustrating where the user is supposed to click

2.2.3 Authentication

Matrices like those in figure 2.4 were shown to the user five times before the test was over. Each matrix contained 160 images, three of which belonged to the users set. The user was supposed to click within the triangle that her images formed, the result of this was logged and displayed when the test was over.

Figure 2.4. A typical authentication screen

2.3 Implementation problems

2.3.1 Images

Images are naturally a big part of the implementation of any cognitive authentication scheme. There are many parameters to take into consideration, for example the images should be distinct from one another and easy to identify at low resolutions.

How the images are arranged is another concern. The area which the user has to click should be within some boundary values to make sure that it is not too hard for the user to hit it, and not too easy for someone else to hit it by chance.

In [SOB2002], where the scheme was first proposed, the images are arranged in a random scatter. Developing a system which does that could be quite hard, and puts some more constraints on the images which are used. For example the images should be in a format that allows transparency if the corners are to overlap.

2.3.2 User interaction

For the scheme described in section 2.1, capturing the location of the users mouseclick is a vital part. The program has to evaluate if the click was within the triangle the images form, in order to know if the user should be allowed into the system.

This is not as easy as it might sound since most programming languages for the web were not designed for this kind of user interaction. There are ways of doing it

with html, see for example [W3CIMGM], and the support of scripting languages, but Java has one of the easiest ways of doing it with the MouseListener interface.

2.3.3 Java-specific problems

Implementing the scheme as a Java applet has it's pros and cons. The major pros, compatibility and good support for user interaction has already been mentioned. The reason for these pros, and some of the cons, are that the applet is executed on the client and not on the server.

Loading time is a big problem since the applet has to be downloaded to the client, ans then executed. If you compare it to scripting languages like PHP, then Java has a very long execution time.

The biggest problem lies however in loading the images, since they have to be downloaded individually by HTTP requests which can take some time to initiate. An alternative is to include all images in the applet, but that would greatly increase the time it takes before the applet starts running.

Due to security concerns applets are running in a sandbox, which for example does not allow the applet to access local files or connect to other servers unless it is signed with a certificate that the user trusts. This is more of an inconvenience then a problem, since most tasks can still be done but get harder to implement.

Chapter 3

Usability study

A small scale usability study was performed on my implementation. The focus was on the users short-term memory, specifically on the registration phase.

3.1 Method

The study was done remotely by visiting a web page made for this purpose. On the web page were some instructions on how to participate in the study, as well as the applet described in section 2.2 and a link to the survey which is included in appendix A.

The aim was to provide a test in a realistic environment in order to study how users would perform when they have to use this scheme for the first time. On the web page were instructions on how to use the scheme, however they were a bit sparse and contained no images to illustrate the process.

3.2 Result

Below are the results of the study. The test was completed 19 times, however only 6 persons chose to answer the survey.

Number of images	Successfull/total attempts	Percent
4	7/25	28%
6	17/55	30.9%
8	0/5	0%
20	1/10	10%
Total:	25/95	26.3%

Table 3.1. Results from the test on my implementation

Each time someone took the test their result was logged with information about how many images that were in their set and on how many authentication screens they clicked within the triangle made by their images. The result of the tests are displayed in table 3.1.

The survey consisted of four questions about different aspects of the scheme and the test which the user just took. The questions are found in appendix A, the results are in table 3.2.

Question 1 - What did you think about the images that were used?

1 - Worthless	0	0%
2	3	50%
3	1	17%
4	2	33%
5 - Perfect	0	0%

Question 2 - Which of the following sentences can be used to describe your problems with the test?

It took too long to load the images	3	50%
I found it very hard to remember my images	4	67%
I could not find my images in the matrix	4	67%
I did not understand what I was supposed to do	2	33%
I am concerned about the security with this method	1	17%

Question 3 - Could you see this type of authentication as a replacement for "normal" passwords?

Yes, it is better in every way	0	0%
Yes, but only on sites with important data	2	33%
Yes, but only on sites that does not hold sensitive data	0	0%
No	4	67%

Question 4 - How likely is it that you could improve your performance to successfully login 95% of the time?

1 - Not likely at all	0	0%
2	2	33%
3	2	33%
4	2	33%
5 - Very likely	0	0%

Table 3.2. Results from the survey

Chapter 4

Discussion

Unfortunately the study did not receive enough data to draw any conclusions that can be considered statistically secure. The lack of data is mainly due to the limited budget assigned to this project, since I did not have enough time to find more people to take the test. It is also possible that some potential testers did not understand what they were supposed to do and because of that failed to provide any data, which is partially supported by the results of the survey where 2 of the 6 people answered that they did not understand the instructions.

The data generated by the tests are not very promising. Even with 6 or less images in the set, the average user clicked in the correct area only about 30% of the time. There were only three attempts with more then 6 images, all of which had even worse results.

Among the 19 sets of testdata, only two can be considered to have successfully passed the test. One of those clicked in the correct area on all five attempts, the other had four correct clicks. Both used sets of six images.

In [SOB2002] the authors did some calculations and came to the conclusion that if the user had 10 images in their set and there were a total of 1000 images, the possible "passwords" would exceed the number of alphanumerical passwords of length 15. They used the binomial coefficient, $\binom{N}{K}$, to calculate the number of possible passwords. For my implementation I had about 35 000 images in total, so 6 images in the users set would generate a large enough number of possible passwords, since $\binom{35000}{6}$ is more then ten times larger then 36^{15}, the amount of alphanumerical passwords at length 15.

Just having a lot of possible passwords is not enough to make the scheme secure. One of the main arguments for this specific scheme is that it is secure even if an attacker knows what is displayed on the screen and where you click. If there are few images in the users set and the number of images displayed each time is small in comparison with the total number of images, it would be quite easy to find out the users images just by looking at a couple of authentication attempts and see which

images that are displayed multiple times. Should the user have only 6 images in their set, it would probably be possible to find out which those images are just by looking at the five matrices from one authentication attempt.

If the scheme is to be used in a real environment the developer would have to maintain a good balance between the size of users sets and the total number of images.

If we look at the survey, it is clear that those who answered did not consider the images to be very good. The majority of the answers claimed that they had problem remembering and finding their images, and marked their general impression of them at or below average.

On the positive side, only one person was concerned with the security of the scheme and two could see it as an alternative to normal passwords on sites with sensitive data.

What does all this mean for the future of the scheme? Can it replace the alphanumeric passwords?
It is still too early to say whether the scheme has a future or not. The results from my study were not very promising, but it would require a lot more research to say something for certain. Different variations of the scheme should also be studied before it can be dismissed.

It is however clear that there are a couple of problems with the scheme, among them that you have to keep a good balance between the total number of images and the number you want a user to have in their set. Getting a large set of images that are suitable for this kind of scheme is also a problem since every image should be easily distinguished from the other as well as easy to remember.

4.1 Future research

For future research in this area it is important to do larger studies in order to get some statistically secure data, instead of speculating about the results. It would also be interesting to answer the following questions:

- Do users recognize the images given to them after a week? After a month?
- Is it more effective to initially give the user a small set and then add images at certain intervals, instead of giving the user a large set right away?
- Does the arrangement of the images affect the users peformance? In explicit, is it more effective to arrange the images in a matrix or a random scatter?

Bibliography

[IMP2010] Imperva - Consumer Password Worst Practices
Last accessed 2010-05-04
http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

[BLO1995] G. E. Blonder - Graphical Password
US Patent 5559961, filed 1995-08-30
http://www.freepatentsonline.com/5559961.html

[SOB2002] L. Sobrado, J-C. Birget - Graphical Passwords
Published in the Rutgers Scholar, volume 4 2002
Last accessed 2010-05-04
http://rutgersscholar.rutgers.edu/volume04/sobrbirg/sobrbirg.htm

[Passfaces] Passfaces
Last accessed 2010-05-04
http://www.realuser.com

[SUO2005] X. Suo, Y. Zhu, G. S. Owen - Graphical Passwords: A Survey
Published by ACSAC 2005
Last accessed 2010-05-04
http://www.acsac.org/2005/papers/89.pdf

[ACM2005] S. Wiedenbeck, J. Waters, J-C. Birget, A. Brodskiy, N. Memon - Authenticating using graphical passwords: effects of tolerance and image choice
ACM International Conference Proceeding Series, Volume 93
http://portal.acm.org/citation.cfm?id=1073001.1073002

[SAT2007] P. Golle, D. Wagner - Cryptoanalysis of a Cognitive Authentication Scheme
Last accessed 2010-05-04
http://crypto.stanford.edu/~pgolle/papers/sat.pdf

[CAR2007] S. Chiasson, R. Biddle, P.C. van Oorschot - A Second Look at the Usability of Click-Based Graphical Passwords
Carleton University, 2007
Last accessed 2010-05-04
http://hotsoft.carleton.ca/~sonia/content/Chiasson_SOUPS2007_Click_based_GP.pdf

[W3CIMGM] W3C Recommendations for HTML 4.0
Last accessed 2010-05-04
http://www.w3.org/TR/REC-html40/struct/objects.html#h-13.6

Appendix A

Survey

What did you think about the images that were used?
Give your general impression on a scale from 1-5. Consider for example if the images were too small, if it was hard to see what was on them and if it a lot of images looked alike.

Worthless - 2 - 3 - 4 - Perfect

Which of the following sentences can be used to describe your problems with the test?
Multiple choices are possible.

x It took too long to load the images
x I found it very hard to remember my images
x I could not find my images in the matrix
x I did not understand what I was supposed to do
x I am concerned about the security with this method

Could you see this type of authentication as a replacement for "normal" passwords?

o Yes, it is better in every way
o Yes, but only on sites with important data
o Yes, but only on sites that does not hold sensitive data
o No

How likely is it that you could improve your performance to successfully login 95% of the time?
Consider a better implementation where you could use the same set of images every time.

Not likely at all - 2 - 3 - 4 - Very likely