Graphical Authentication - An Alternative to Text Based Authentication

Review

This paper reflects quite a good understanding of the topic, An alternative to Text Based Authentication, especially Graphical Authentication. The author has tried to provide a clear overview of why we at all need alternative means of authentication or where does the year old textual methods fall short. The entire text consists of several different systems based on Graphical Password, their strengths, drawbacks etc. The author has given an honest effort to clarify the current scenario of recent researches on the topic. It is quite easy for a newbie to understand the text. Recognition and Recall based schemes are described quite well. But there are some points that should be mentioned:

• The title of the paper is, “Graphical Authentication - An authentication to textual based authentication”. It should either be “... textual authentication” or “text based authentication”.

• The Author has used the term “Dual Coding Theory” in a few places. A brief definition of the theory would be appreciable.

• In the first page, 2nd column, under the subheading, “A. Token based Authentication”, the first line has two references, but the first paragraph merely defines or describes the general idea of Token Based Authentication. Here one reference would be sufficient. Two references may be used with two different contexts or definitions, otherwise they are just increasing the number of references.

• The previous point is applicable to the next subheadings, “B. Biometric Authentication” and “C. Knowledge Based Authentication” also and to all other similar occurrences.

• In some places as In page 4, while starting the description of “Deja Vu”, the author has cited thrice like [3], [7], [8], where only one reference [8] refers to the original “Deja Vu” paper. The other two are just referring to the original paper as the author is trying to do. So [3], [7] should not be cited here. This is again increasing the number of references unnecessarily. Similar things are there in other places also. The author can easily find those out.

• Under “B. Biometric Authentication” at page 2, the author has stated about VeriFace by Lenovo. Though the name VeriFace is quite intuitive, a couple of sentences about how the scheme verifies users would be good.

• References may not be given in headings or subheadings as given in “Password Creation [3]”, “Login[3]” etc. under “B. Usability” at page 3.
In the section “Password reset and password change [3]” the author has stated, “Biddle et al. [3], claimed that such type of verification is difficult in implementing in graphical password systems, as it would pose social-engineering attacks. So, as a solution, they have proposed to use temporary non-graphical password during resetting process.” But according to Biddle et. al. [3] the concept is completely opposite. They have stated that Graphical Passwords cannot be easily communicated over phone or email so they give a protection against Social Engineering Attacks. But as they cannot be communicated easily they have usability issues. To counter this usability challenge they have proposed the assignment of temporary non-graphical password. The author should take a look at this.

Apart from considering Security and Usability issues the author might have considered Reliability and Storage and communication issues also as described by Suo et. al. [2].

In page 4, while describing “Deja Vu”, the author has given a mathematical notation comprising of N and M which appears to be taken from [3] page 11, last line. So this notation may have a reference to [3]. Apart from that some reader may be unfamiliar to that particular notation and may not understand the calculation properly. It is basically a combination of M objects out of a total N objects as stated in [8] in section 4.3, Formal User Testing. The author may think to include that statement.

In page 6, in the Critical Analysis section of Man et. al. [11], the author has written that even if the login session is observed it is difficult to find the exact password. In the paper [11], at section 3.2 Security it is shown that even if the login session is filmed S times then also how small is the probability to find the exact password for the attacker. In [2] it is clearly written that even if somebody sees the codes, as no mouse click is associated it is not possible to find at each step that which pass object is presented at that particular stage, where it is located on screen. Therefore the mapping between the code given by the user and a pass object at each step is unknown to the attacker and it is to be calculated which is problematic for large pass object space. The author also has written that clearly. Therefore the sentence “But I think ... vulnerable to shoulder surfing attacks” does not seem to be correct. The author may think a bit about it.

Under PassFace in Critical Analysis in page 8, the author has written “I think the possibility of brute force attack is $1/2^{13}$.” Any claim for mathematical formulation or result should be concrete. It should not start with “I think…”.

In page 9, at the last section of Q-DAS, before starting Critical Section the author may include a description of “Dynamic Grid Transformation” and how it differs from DAS. Also before writing the password space as $2.8*10^{14}$ at least how it is calculated and what parameters are involved may be stated.

In the last paragraph in page 12, in the section “Proposed Solutions/Modifications” the author has stated that the user may be allowed to modify the images themselves. This
may have deployability issues because for a merely commercial software, say a core banking application, it is an extra overhead to provide a drawing panel (an MS Paint or Adobe Photoshop extension) with the registration page or screen. It will increase the licensing cost also.

- The author has focused on a lot of systems so all of them could not be given proper justice and for a reviewer it is difficult to go through all the original papers and understand and analyse them. A few systems would have been better to discuss and understand.

- Almost everywhere in Critical Sections, the author has given her own view starting as “I think...”. It would be better if these things can be written in passive voice.

- A section could have been added on which systems the author is recommending to use and why. More than one systems could be combined to address common problems.

- For a particular context only one reference is encouraged to use. Two or more references are welcome if they really correspond to different contexts and also ‘which reference is used for what’ might have been clearly written. Otherwise for a reviewer it is very difficult sometimes to find out which paper originally reflects the concepts. This issue is reported earlier also and it is emphasized on a few times because it led to confusions while reviewing.

There might be other issues which could have been found out as in a case the author is contradicting to the original idea of the author of the system. The author may carefully remove those issues in the final version. If the author tries to resolve these issues given above it would become a nice piece of work.

Apart from that there are minor english construction problems which are highlighted in the reviewed pdf file.

I wish good luck for the author.


