American Journal of Engineering Research (AJER)
e-ISSN : 2320-0847 p-ISSN : 2320-0936
Volume-03, Issue-08, pp-353-361
www.ajer.org

Research Paper Open Access

Web based authentication scheme using images

Viswa Subramanian Sekar[1]
Department of Computer Science and Engineering, PSG College of Technology, Coimbatore - 641004, India.
.

ABSTRACT: *The most common computer authentication method is to use alphanumerical usernames and passwords. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. In the developing world of technologies, Security breaching has become more popular. The more and more amount of data being stored in the networks, the more security is needed. On the other side of world, there arises a community called "Hackers"- a person who involves most of his time in breaking the security. They find the vulnerabilities, break your password, and try to steal the information in your database. The main idea of this "Image Password" is an authentication technique based on pictures as a possible solution to the most important problems concerning traditional passwords. The concept is having unique sequence of pictures for a user, by this way the attacker will not be aware of what the password is. This work brings together the technical (crypto logical) and non-technical (psychological) awareness into the research on passwords. Security issues of any authentication mechanism (relying on knowledge) should not be considered without analysis of the human factor − since the users' human nature was identified as a source of major weaknesses of conventional authentication. The "Image Passwords" brings out statistically significant superiority of picture passwords over alphanumerical. There is a resistance to 'key logging' and 'mouse tracking'. This method guarantees that users choose dissimilar, personalized and cryptographically strong graphical passwords.*

KEYWORDS: *Security, Image, Password, Picture passwords, graphical password, web authentication, browser password.*

I. INTRODUCTION

According to recent reports, many researches and statistics from real systems, there are many vulnerabilities and threats typical of alphanumerical passwords. As usual, the users are 'the weakest link in the security chain'. One of the major problems is the difficulty of remembering passwords, the other, ignoring security requirements. Users tend to create either too short passwords or passwords that though long enough are easy to guess. There is an informal rule stating that passwords easy to remember, are mostly also easy to break. According to Schneier [1], passwords' length distribution based on 34,000 users shows that 65% of passwords have only up to 8 characters and almost 95% up to 10 characters. Other research [2] shows that only 17% of the inquired IT professionals use complex passwords (including letters, numbers and symbols) and 72% stated that they almost never or never change their access codes. 52% of professional users tend to share their passwords and 65% of them have only one or two passwords to access the majority of services. A study of information contained within the passwords [3] shows that 66% of users' passwords are designed making use of personal characteristics thereof, where 32% contained names of people, places or things. The common constructions involve full information in the passwords – 75%, partial – 13.5%, or combined – 7.5%. Almost all respondents reuse passwords – on average 4.45 passwords are used in 8.18 systems. On the other hand, strong passwords imposed on users bring no solution as well – people cannot and/or would not remember strong passwords and write them down instead. According to [4] we can say: there will be either about 80% remembered but weak passwords (created by users) or 80% strong passwords (generated by the system) but written down. Many alternative authentication solutions have been invented and developed to ensure the proper security level – in order to avoid weaknesses of traditional methods. One group of techniques (involving a physical factor in the authentication process – 'something you have') focuses on utilizing all kinds of tokens, one-time passwords, magnetic stripes and proximity cards, iButtons, cryptographic cards, etc. The other kind of research makes use of methods (called ‘something you are’) based on biometric information like fingerprints, voiceprints, the patterns of blood vessels on the eye retina, the topography of the eye iris, the geometry of the hand, facial patterns, DNA codes or even thoughts (cerebral waves).

However, all of the aforementioned solutions have two significant disadvantages. First, they may become unacceptably expensive when a large number of users are involved. Second, access to the system is strongly dependent on the suitable interfaces – which makes such methods comparatively less universal (in the context of mobility) and in some cases, impossible to use. Additionally, biometrics is extremely vulnerable to a replay attack – the personal information is hard to hide (face, fingerprints) and cannot be changed. In the past few years we have been observing a growing interest in graphical authentication techniques – those of knowledge-based methods, which include graphical aspect(s) in the authentication process. There are a few distinct grounds, which aroused the interest in graphical techniques. There are methods particularly useful for mobile devices and/or systems that have no keyboards, methods resistant to shoulder-surfing attacks (enabling to log in ‘in the crowd’), there are also advantages coming from resistance to malicious software (malware). Notwithstanding, the leading inclination is still to construct a system, which will prevent from choosing trivial passwords and which will allow to remember passwords with the cryptographically proper length.

II. BACKGROUND

Alpha-numeric passwords were first introduced in the 1960s as a solution to security issues that became evident as the first multi-user operating systems were being developed. As the name indicates, an alpha-numeric password is simply a string of letters and digits. Although almost any string can serve as a password, these passwords only offer good security as long as they are complicated enough so that they cannot be deduced or guessed. Commonly used guidelines for alpha-numeric passwords are:

1) The password should be at least 8 characters long.
2) The password should not be easy to relate to the user (e.g., last name, birth date).
3) The password should not be a word that can be found in a dictionary or public directory.
4) Ideally, the user should combine upper and lower case letters and digits.

Since the best password would be a completely random one, people have devised ways to create pseudo-random passwords. One such method is to take a common word and perform certain actions on it. Using the word Dinosaur as an example, users often create passwords such as DiNoSaUr (by alternating upper and lower case), rUaSoNiD (by reversing the string), oSNaiUDr (by shuffling the string), D9n6s7u3 (combining numbers and letters). However, the better the password is, the harder it is to remember.

Another drawback of alpha-numeric password is the dictionary attack. Because of the difficulty in remembering random strings of characters, most users tend to choose a common word, or a name. Unfortunately, there are several tools that allow an individual to crack passwords by automatically testing all the words that occur in dictionaries or public directories. This attack will usually not uncover the password of a predetermined user; but studies have shown that this attack is usually successful in finding valid passwords of some users of a given system.

Because human beings live and interact in an environment where the sense of sight is predominant for most activities, our brains are capable of processing and storing large amounts of graphical information with ease. While we may find it very hard to remember a string of fifty characters, we are able easily to remember faces of people, places we visited, and things we have seen. These graphical data represent millions of bytes of information and thus provide large password spaces. Thus, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security.

Dictionary attacks are infeasible, partly because of the large password space, but mainly because there are no pre-existing searchable dictionaries for graphical information. It is also difficult to devise automated attacks. Whereas we can recognize a person's face in less than a second, computers spend a considerable amount of time processing millions of bytes of information regardless of whether the image is a face, a landscape, or a meaningless shape.

III. PROPOSED IDEA

The idea is implemented for web service. Each user will have unique set of pictures, where user will select a unique sequence in selecting the order of the password.

Modules:

1. Creation of User account
2. Uploading pictures/setting sequence
3. Deploying in Web page

Creation of User Account

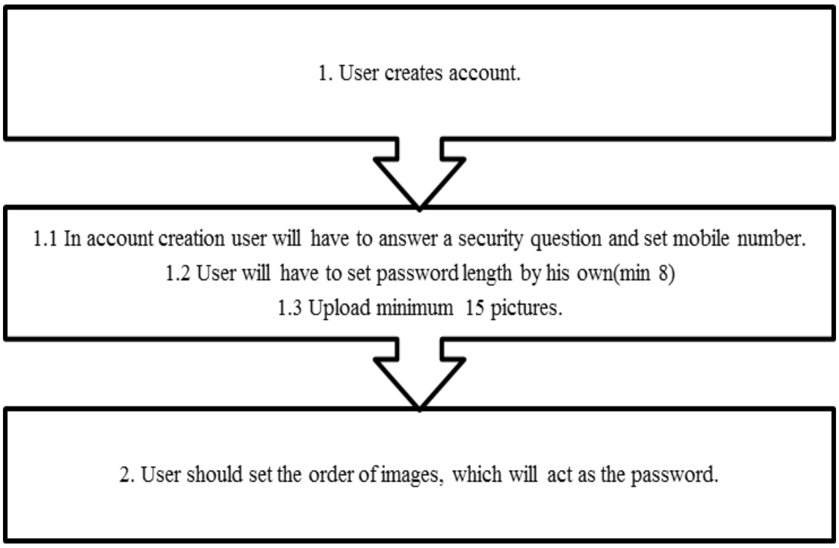

1. User creates account.
1.1 In account creation user will have to answer a security question and set mobile number.
1.2 User will have to set password length by his own(min 8)
1.3 Upload minimum 15 pictures.
2. User should set the order of images, which will act as the password.

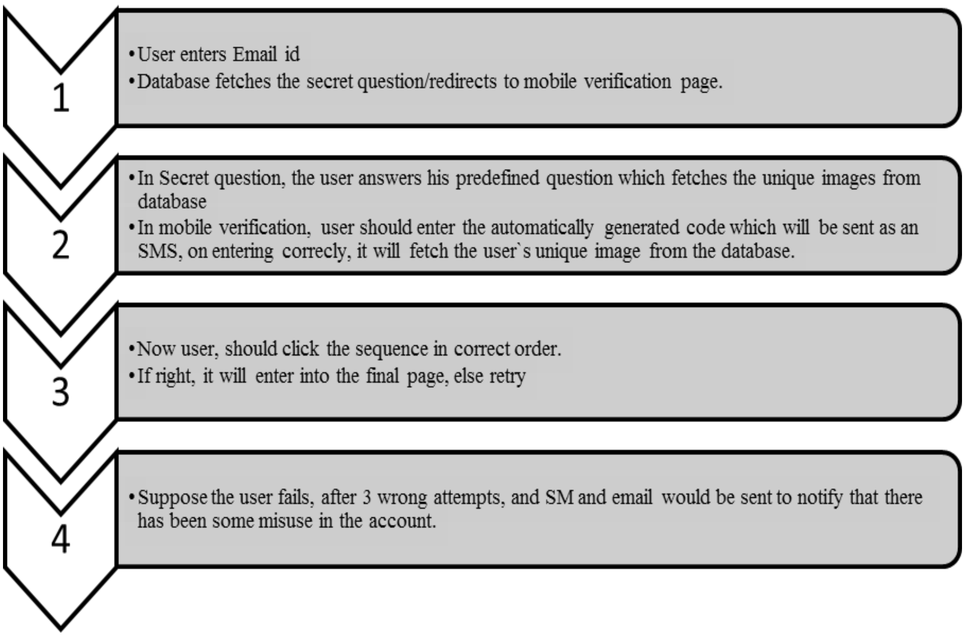
Fig 1: Flow of User account creation

Process

This module is the webpage where user will have the options to create a new user account. All mandatory questions will be included such as DOB, Age, Primary email address. Here the user will be specially asked to set a security question which will be the first phase of authentication. Next the user will be asked to upload images for the authentication. Once uploaded, the images will be scaled down to reduce the size. This will save the space required to store the images in the database. After setting up of picture sequence the password is now set. Now, when user logins, firstly the user will be interfaced to type in their mail id. Once typed, the page will fetch their secret question and display it. Once displayed, user will have to answer to that question, if answered rightly, the page will fetch respective user`s pictures and display them. Here user will have to drag the mouse and click the sequence. In order to escape from mouse tracing, or shoulder sniffing, each time the images are shuffled. The order is highlighted as a thin line around the picture box, which will not be visible to the person standing beside.

Features

Say the password is given wrongly for 3 times, a counter will be working behind to know the number of wrong attempts. If it exceeds, the page will send an SMS to the prescribed number and email id stating that there was exceeded number of try`s. Instead of security question, user can set mobile verification, where user will have to type the code that he receives in his mobile. The sequence and pictures can be changed. This method will not take much space of database, because, once the picture is uploaded, it is scaled down and reduced to lower size for storage efficiency.



- User enters Email id
- Database fetches the secret question/redirects to mobile verification page.

- In Secret question, the user answers his predefined question which fetches the unique images from database
- In mobile verification, user should enter the automatically generated code which will be sent as an SMS, on entering correcly, it will fetch the user`s unique image from the database.

- Now user, should click the sequence in correct order.
- If right, it will enter into the final page, else retry

- Suppose the user fails, after 3 wrong attempts, and SM and email would be sent to notify that there has been some misuse in the account.

Fig 2: Flow of Login Process

This type of password is superior and safe, because the set of images is unique for each user. There are 2 Gateways to enter into final page. The hacker to find the password, must first find a way to break the first gateway.

Here brute force technique is difficult because, each user will have different set of images. So it is really hard to create a dictionary. No keylogging, because of images.

Mouse tracking is impossible because the hacker should know what is there in the screen to get the mouse traces.

Scope

1. This type of authentication can be used in military purposes, where high amount of security is needed.
2. To protect medical database.
3. To protect confidential information.

Advantages

1. There are possibilities of significant enlargement of the picture passwords space. In the traditional passwords, the base does not exceed one hundred (b n – password space, b – base, n – password length). Picture passwords offer the password base up to ten times larger – technically, the only limitation is the resolution of the screen.
2. There is technical possibility to prevent users from choosing trivial passwords. Through the permutation of the set (only once – after the password creation) the users are forced to remember their passwords regarding only the meaning of elements and not the topological placement of elements (like row or column).
3. It's possible to personalize the passwords, which can prevent from (common) dictionary attacks. After removing irregular elements and pairs from the set, chosen passwords will depend only on individual thoughts, associations with one's past and personal feelings – in contrast to the common language dictionaries and attacks based on universal strings.
4. There is a possibility to make the authentication process resistant to 'key logging' and 'mouse tracking'. The first resistance is obvious (due to not using the keyboard). The second one is achieved (again) due to the permutation of the set. But in this case, the permutation table should be individual for each login name (and/or workstation). As a matter of fact the sequence of the screen coordinates (users' clicks) will be meaningless without the view of the screen.
5. Sharing passwords with other users as well as noting them down or giving them away as a result of a social engineering attack are much more difficult. While traditional passwords can be easily written down or spelled out, giving a picture password out is very troublesome. The effect can be especially intensive when the keypad consists of ambiguous symbols or symbols having similar names.
6. Passwords incrementation effect (i.e. recurrent and obvious changes made to the passwords – e.g. change from "2nd*SIS#07" to "3rd*SIS#08") can be neutralized. It is because there are no sequences

or numbers when the keypad pictures were properly chosen (e.g. avoiding signs). Even when user changes only one element of the password - it is still hard to guess which one and which is the new one. Moreover, there is always a way of forcing users to change their passwords significantly by modifying (entirely or partially) the set of pictures.

7. There is a possibility for undemanding and inexpensive implementation (in comparison to biometrics and cryptographic hardware).
8. To prevent shoulder sniffing, each time the set of pictures displayed are shuffled.
9. There are many prospective possibilities (manipulation of the pictures colours, meanings of the elements, personalizing passwords sets) of achieving even better memory abilities and/or constructing much stronger mnemonics.

Disadvantages

1. Graphical interface is required - which means that the graphical authentication methods will be less universal (in terms of mobility) and troublesome in implementation (in comparison to traditional passwords).
2. We should not forget about visually impaired and blind people (who are using common internet services as well), for whom something like graphical authentication interface will be impassable or hard to get through.

IV. IMPLEMENTATION

The system is implemented using html with java and php, mysql as database. The snapshots shown below explain the idea.

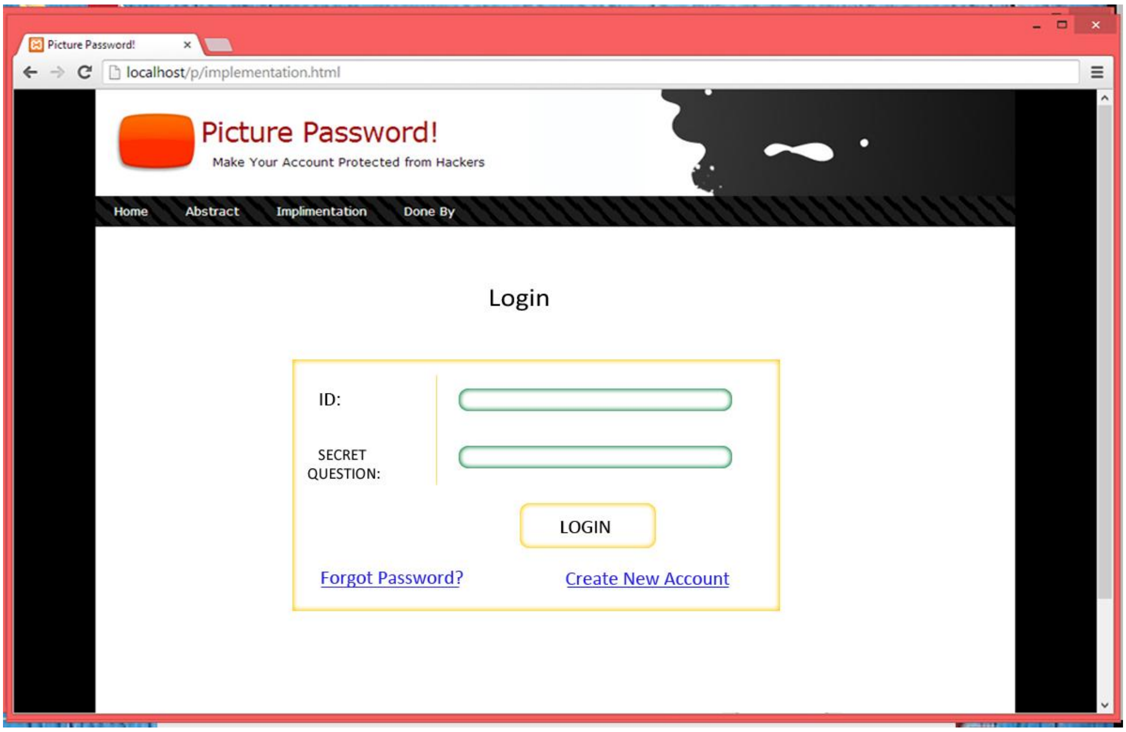
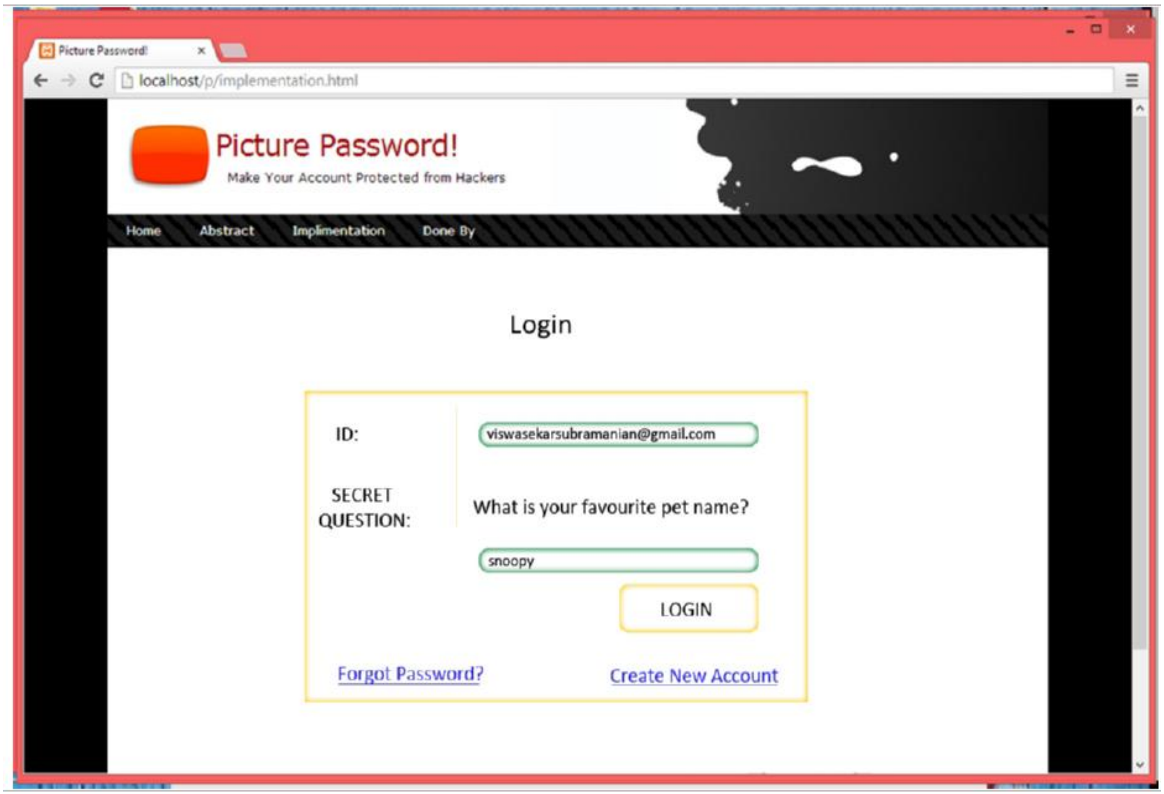


Fig 3: Login page – 1st step

This is the 1st page where user sees. When the user enters the mail id, the database fetches the secret question. When the user enters the correct answer for the secret question it fetches the user defined set of images



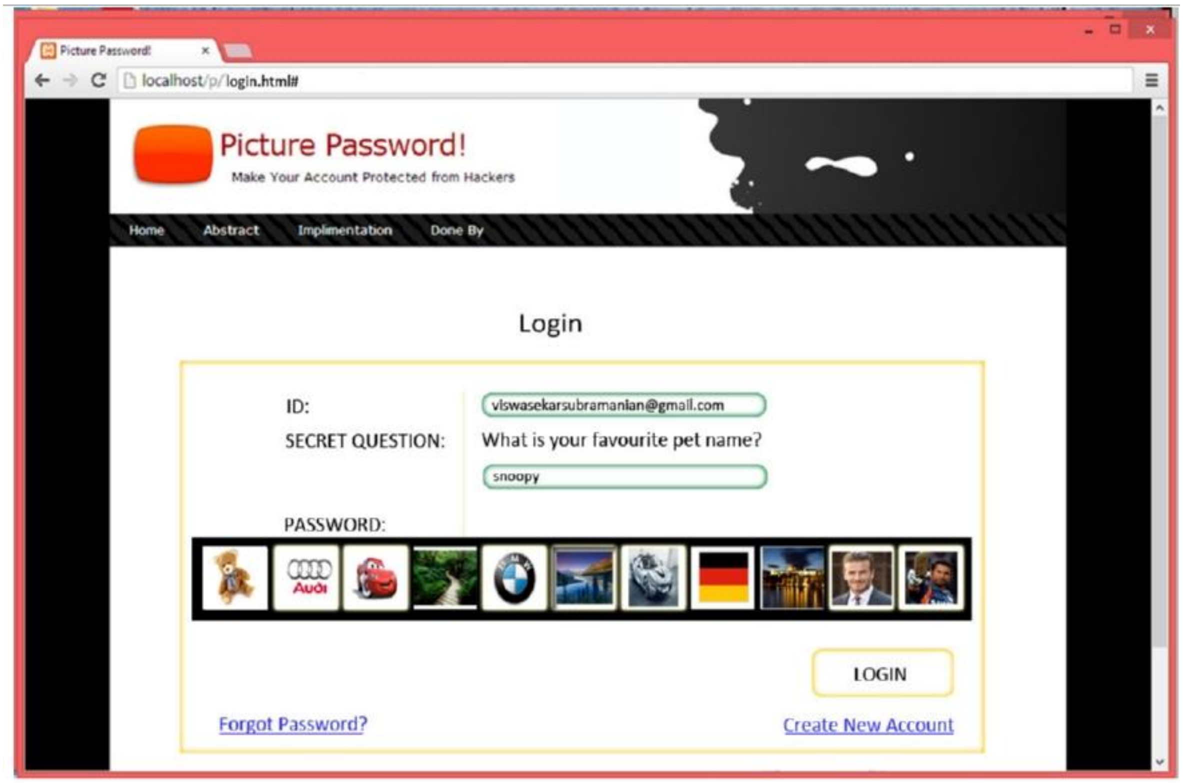
Login

ID: viswasekarsubramanian@gmail.com

SECRET QUESTION: What is your favourite pet name?

snoopy

Fig 4



Login

ID: viswasekarsubramanian@gmail.com

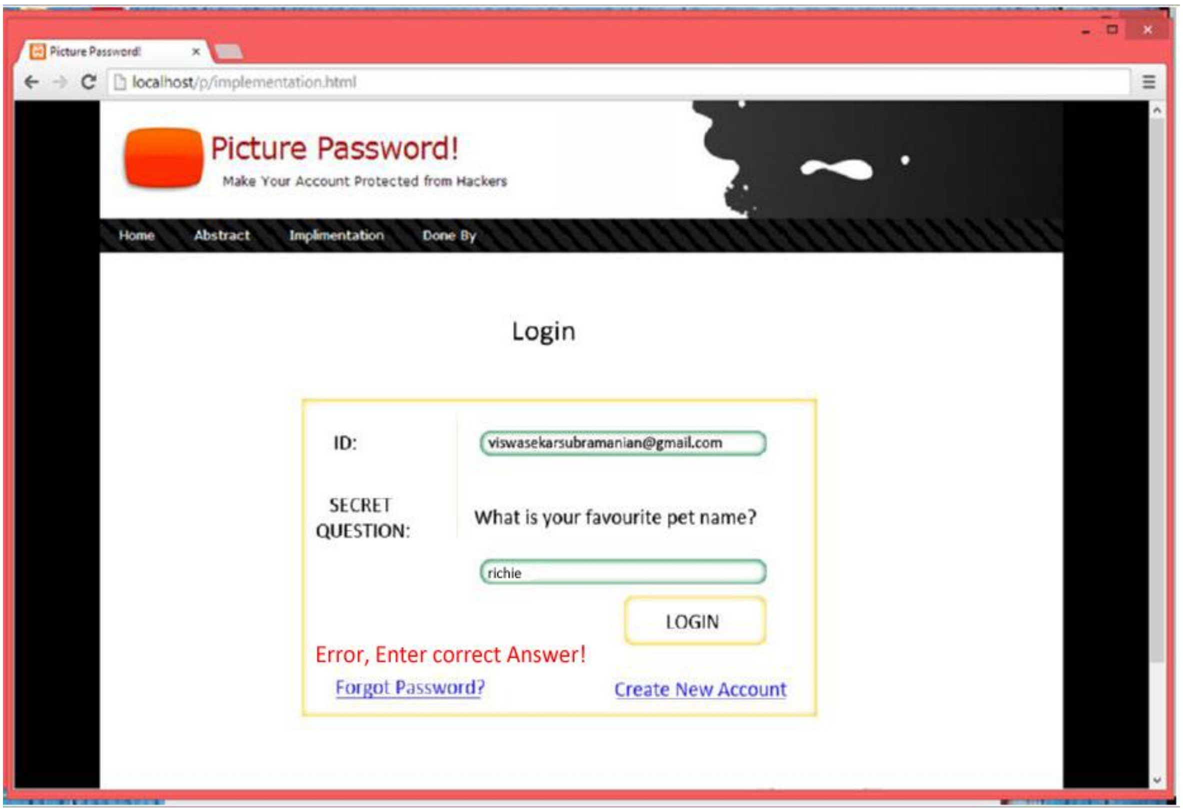
SECRET QUESTION: What is your favourite pet name?

snoopy

PASSWORD:

Fig 5: Correct answer for Secret question

In the above image, we can notice that user has entered the correct answer for the secret question, so the page fetches the user defined images stored already and displays it. Now the user should select the sequence of the images for the correct password.



Login

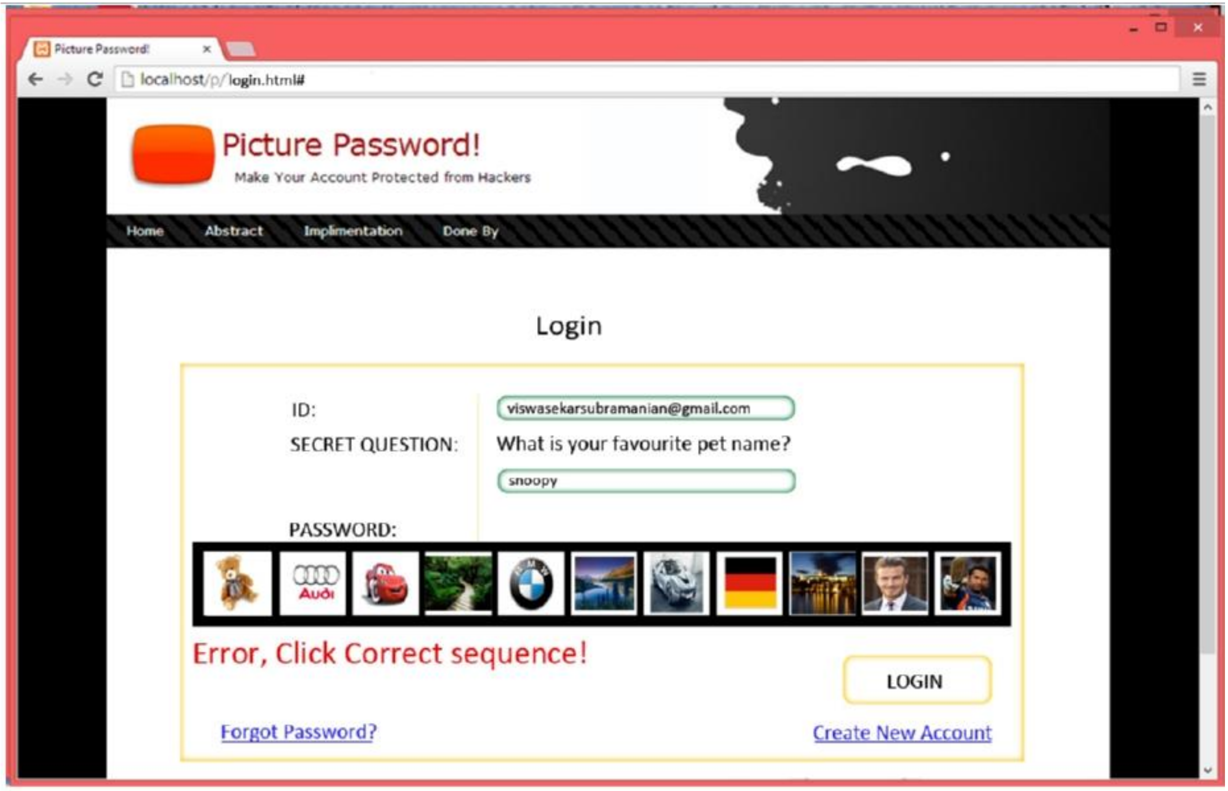
ID: viswasekarsubramanian@gmail.com

SECRET QUESTION: What is your favourite pet name?

richie

Error, Enter correct Answer!

Fig 6



Login

ID: viswasekarsubramanian@gmail.com

SECRET QUESTION: What is your favourite pet name?

snoopy

PASSWORD:

Error, Click Correct sequence!

Fig 7: Incorrect sequence of images

In the above image we can notice that the user does not click the correct sequence of images, so it shows an error and the login is not successful.

V. RESULTS AND DISCUSSIONS

Is a graphical password as secure as textbased password?

Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. Here we briefly exam some of the possible techniques for breaking graphical passwords and try to do a comparison with text-based passwords.

Brute force search

The main defense against brute force search is to have a sufficiently large password space. Text-based passwords have a password space of 94^N, where N is the length of the password, 94 is the number of printable characters excluding SPACE. Some graphical password techniques have been shown to provide a password space similar to or larger than that of text-based passwords. Recognition based graphical passwords tend to have smaller password spaces than the recall based methods. It is more difficult to carry out a brute force attack against graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human input, which is particularly difficult for recall based graphical passwords. Overall, we believe a graphical password is less vulnerable to brute force attacks than a text-based password.

Dictionary attacks

Since recognition based graphical passwords involve mouse input instead of keyboard input, it will be impractical to carry out dictionary attacks against this type of graphical passwords. For some recall based graphical passwords, it is possible to use a dictionary attack but an automated dictionary attack will be much more complex than a text based dictionary attack. Overall, we believe graphical passwords are less vulnerable to dictionary attacks than text-based passwords.

Spyware

Key logging or key listening spyware cannot be used to break graphical passwords. It is not clear whether “mouse tracking” spyware will be an effective tool against graphical passwords. However, mouse motion alone is not enough to break graphical passwords. Such information has to be correlated with application information, such as window position and size, as well as timing information.

Shoulder surfing

Like text based passwords, most of the graphical passwords are vulnerable to shoulder surfing. But since that the order in which the image is selected is shuffled, it is difficult for attacker to remember the sequence of the images in that short period of time.

Social engineering

Comparing to text based password, it is less convenient for a user to give away graphical passwords to another person. For example, it is very difficult to give away graphical passwords over the phone. Setting up a phishing web site to obtain graphical passwords would be more time consuming.

Overall, we believe it is more difficult to break graphical passwords using the traditional attack methods like brute force search, dictionary attack, and spyware. There is a need for more in-depth research that investigates possible attack methods against graphical passwords.

What are the major design and implementation issues of graphical passwords?

Security

In the above section, we have briefly examined the security issues with graphical passwords.

Usability

One of the main arguments for graphical passwords is that pictures are easier to remember than text strings. Preliminary user studies presented in some research papers seem to support this. However, current user studies are still very limited, involving only a small number of users. We still do not have convincing evidence demonstrating that graphical passwords are easier to remember than text based passwords. A major complaint among the users of graphical passwords is that the password registration and log-in process take too long, especially in recognition-based approaches. For example, during the registration stage, a user has to pick images from a large set of selections. During authentication stage, a user has to scan many images to identify a few pass-images. Users may find this process long and tedious. Because of this and also because most users are not familiar with the graphical passwords, they often find graphical passwords less convenient than text based passwords.

Reliability

The major design issue for recall-based methods is the reliability and accuracy of user input recognition. In this type of method, the error tolerances have to be set carefully – overly high tolerances may lead to many false positives while overly low tolerances may lead to many false negatives. In addition, the more error tolerant the program, the more vulnerable it is to attacks.

Storage and communication

Graphical passwords require much more storage space than text based passwords. Tens of thousands of pictures may have to be maintained in a centralized database. Network transfer delay is also a concern for graphical passwords, especially for recognition-based techniques in which a large number of pictures may need to be displayed for each round of verification.

VI. CONCLUSION

The past decade has seen a growing interest in using graphical passwords as an alternative to the traditional text-based passwords. In this paper, we have conducted a comprehensive survey of existing graphical password techniques. The current graphical password techniques can be classified into two categories: recognition-based and recall-based techniques. Although the main argument for graphical passwords is that people are better at memorizing graphical passwords than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our preliminary analysis suggests that it is more difficult to break graphical passwords using the traditional attack methods such as brute force search, dictionary attack or spyware. However, since there is not yet wide deployment of graphical password systems, the vulnerabilities of graphical passwords are still not fully understood. Overall, the current graphical password techniques are still immature. Much more research and user studies are needed for graphical password techniques to achieve higher levels of maturity and usefulness.

REFERENCES

[1] Schneier B. Real-World Passwords. Crypto-Gram Newsletter, December 15, 2006.

[2] Magalhaes S. T., Revett, K., Santos, H.D. Generation of Authentication Strings From Graphic Keys. IJCSNS, Vol. 6 No. 3 pp. 240-246, 2006.

[3] Brown A. S., Bracken E., Zoccoli S. and Douglas K. Generating and remembering passwords. Applied Cognitive Psychology 18, 641-651, (2004).

[4] Zviran, M., Haga, W. J., User authentication by cognitive passwords: an empirical assessment, 5 JCIT, 137-144, 1990.

[5] Jansen W., Gavrila S., Korolev V., Ayers R., Swanstrom R. Picture Password: A Visual Login Technique for Mobile Devices. NIST, NISTIR 7030.

[6] Zhi L., Qibin S., Yong L., Giusto D. D. An Association-Based Graphical Password Design Resistant To Shoulder-Surfing Attack. IEEE, ICME, 2005.