Design and Implementation of Image Based Web authentication System Using both Déjà Vu and SSL protocol

Ass. Lecturer Media Abdul Razak Ali
Computer and software Engineering Department
Al-mustansiriya University

Abstract

The (username/password) is a very common and widely authentication method still used up to now, but because of the huge advance in the uses of computer in many applications as data transfer, sharing data, login to emails or internet, drawbacks of normal password appear, like stolen the password, forgetting the password, week password, etc . In order to provide secure and user friendly authentication, the security experts are strongly recommending the new Graphical passwords, which consist of clicking or dragging activities on the pictures rather than typing textual characters which overcomes most of the problems that arise from the text-based passwords system. This paper presents the design of an online image based authentication system using Déjà vu , which authenticates a user through the ability to recognize previously seen images. D´ej`a Vu is more reliable and easier to use than traditional graphical based schemes, it has the advantage that it prevents users from choosing weak passwords and makes it difficult to write down or share passwords with others. The system applies the Secure Socket Layer (SSL) protocol to provide the required

web transmission security. The implementation of the design and related security analysis is also presented.

المستخلص :

تصميم وتنفيذ نظام توثيق لشبكة الويب باستخدام *Déjà vu* وبروتوكول امنية القابس

مدرس مساعد ميديا عبد الرزاق علي - هندسة الحاسبات والبرمجيات - الجامعة المستنصرية.

طريقة المصادقة (اسم المستخدم وكلمة السر) هي طريقة واسعة الاستخدام و على نطاق كبير ولا تزال تستخدم حتى الآن ، ولكن بسبب التقدم الهائل في استخدام الكمبيوتر في العديد من التطبيقات كنقل البيانات ، تبادل البيانات ، والدخول إلى رسائل البريد الإلكتروني أو الإنترنت فان مساوئ كثيرة لكلمة السر بدات بالظهور مثل سرقة كلمة السر ، نسيان كلمة المرور ، كونها غير مناسبة من الناحية الامنية ، الخ. من أجل توفير مصادقة آمنة وسهلة الاستعمال والتوثيق ، فان خبراء الأمنية ينصحون بشدة كلمات السر الرسومية الجديدة ، والتي تتكون من النقر أو سحب الأنشطة على الصور بدلا من كتابة الأحرف النصية .هذه الطريقة تتغلب على معظم المشاكل التي تنشأ من كلمات السر. يقدم هذا العمل تصميم وتنفيذ نظام توثيق لشبكة الانترنيت باستخدام طريقة التوثيق الصورية "Déjà Vu" الذي يصادق على المستخدم من خلال قدرته على اختيار نوع خاص من الصور تم اختياره سابقا من قبله .هذا النظام هو أكثر وثوقية وأسهل استخداما ، لديه ميزة أنه يمنع المستخدمين من اختيار كلمات سر ضعيفة ويجعل من الصعب كتابة كلمات السر أو مشاركتها مع الآخرين.النظام المصمم يستخدم بروتوكول امنية طبقة المقابس (SSL) لتوفير الأمن المطلوب لنقل البيانات على شبكة الإنترنت. التحليل الأمني للنظام هو ايضا مقدم .

Key Words: Image Based Authentication, Déjà vu, SSL Protocol , Apache Server.

1. Introduction

Authentication of humans is based on some combination of what you are (biometric), what you have (token), and what you know (password). Knowledge-based authentication, is by far the most common form. Due to the simplicity of single factor authentication mechanisms, most of the Web based services have been employing this mechanism. But these mechanisms are now not being considered secure enough for various reasons as there is a sharp increase in number of attacks on ID/password based mechanisms and users registered with various no. of online services have to remember pairs of ID/passwords for their respective accounts so they are either choosing easy to remember passwords which are weak and susceptible to dictionary attack, or choosing hard to guess alphanumeric passwords which are hard to remember and leads them to write it on paper , so a big necessity to have a strong authentication way is needed to secure all our applications as possible. Researches come out with advanced password called graphical password techniques where they tried to improve the password techniques and avoid the weakness of normal password. Today, many networks, computer systems and Internet-based environments used this technique to authenticate their users. It also designed to make the passwords more memorable, easier for people to use and therefore more secure. Based on the two assumptions; first, humans can remember pictures better than alphanumeric characters and second, a picture worth a thousand passwords; psychological studies and company software seem to agree with these assumptions [1].

2. GRAPHICAL AUTHENTICATION TECHNIQUE

Knowledge based technique include both text based and picture based technique. The picture based techniques can further be divided into two categories of graphical techniques: Recall based and Recognition based .

2.1 Recall-based Graphical Password Systems

In the Draw-A-Secret (DAS) scheme by Jermyn[2]. The password is a simple picture drawn on a G × G grid. This approach is alphabet independent, users do not have to remember any kind of alphanumeric string. Each grid cell is denoted by two dimensional coordinates (x, y) 2 [1...G] × [1...G]. In order for a user to authenticate he is asked to re-draw the picture, which must have the same encoding. Two drawings having the same encoding which means crossing the same sequence of grid cells with pen-up events in the same places in the sequence are considered equivalent. The procedure of enrollment and authentication with a DAS implementation on a PDA is shown in figure 1.

Blonder designed a graphical password scheme Passlogix[3] , figure 2, in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall, which is the case with a text-based password.

The PassPoints system by Wiedenbeck [4] (see figure 3) is a graphical password scheme based on Blonder's original idea which overcomes its limitations of needing simple, artificial images, predefined regions, and consequently many clicks in a password. In

order to authenticate, the user must click in the correct sequence within the tolerance of his previously chosen pixels. The tolerance is needed because the user's click point is literally a single pixel, which is too precise for a user to click on successfully.

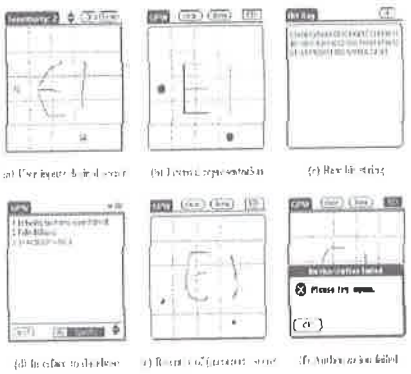


Figure 1: A password is created by drawing the secret on the display as shown :

Figure 2: Passlogix's graphical-password system

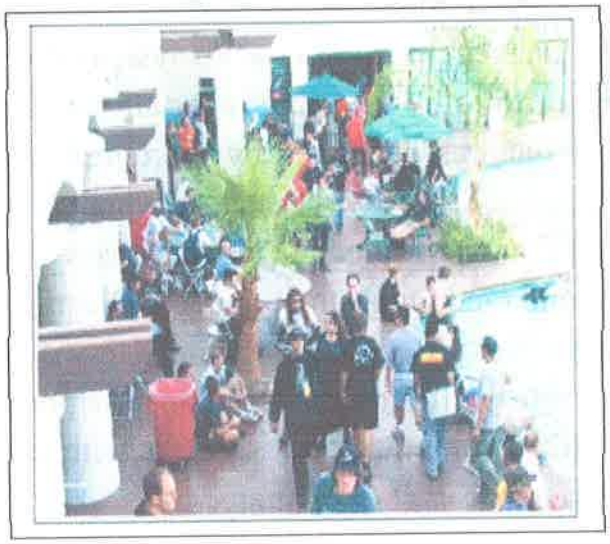
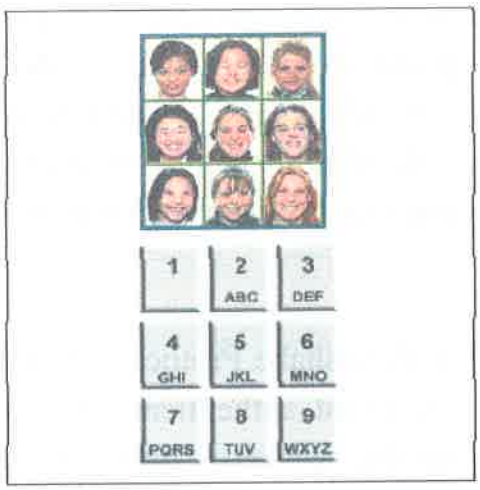


Figure 3: Every pixel on an image used in the Pass Points system can be used for the password.

2.2 Recognition-based Graphical Password Systems

Passface method use faces as an object for password. During enrolment procedure, the users select whether their Passface consist of male or female picture. Then they choose four faces from the database as their future password. On the next step, a trial version starts for user in order to learn the real login process. During trial, the users taken twice through the Passface login procedure with their Passface which is shown to them. The enrolment will be completed by correctly identifying their four Passfaces twice in a row with no prompting, entering an enrolment password. During login phase which is been shown in figure 4, a grid that contain 9 pictures is shown to the user. This grid only contains one of the user's passwords, and the other eight pictures are selected from the database[5,6].

Dhamija and Perrig developed, D´ej`a Vu, a recognition-based authentication system (figure 5), which authenticates a user through his ability to recognize previously seen images [7]. Similar to most other graphical password systems, it is based on the observation that people have an excellent memory for images .In the D´ej`a Vu system, the user is asked to create an image portfolio by selecting a certain number of images from a set of random pictures generated by a program. Later, the user will be required to correctly identify the images which are part of his portfolio in order to be authenticated. D´ej`a Vu uses Andrej Bauer's Random Art to generate random abstract images. Dhamija and Perrig believe that if the system was based on photographs, it would be easy for users to pick predictable portfolios, to describe their portfolio images and to write down this information and share it with others. This is the reason why they use random abstract images.



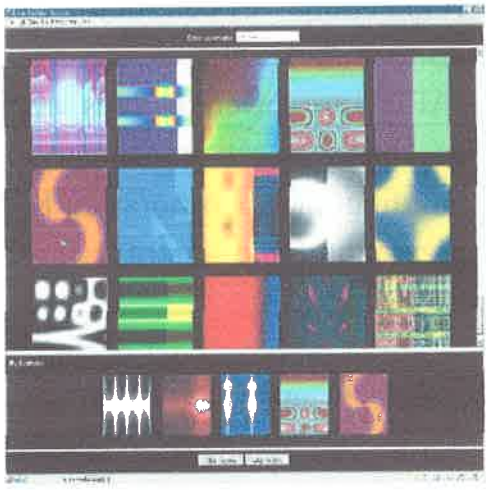


Figure 4: Passfaces and eight decoy faces

Figure 5: D´ej`a Vu, Random Art selection

3. Secure Socket Layer Protocol

SSL stands for Secure Sockets Layer protocol developed by Netscape and is the standard Internet protocol for secure communications. The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. HTTPS is http using a Secure Socket Layer (SSL). A secure socket layer is an encryption protocol invoked on a Web server that uses HTTPS.

SSL is a type of sockets communication and resides between TCP/IP and upper layer applications, requiring no changes to the application layer SSL is used typically between server and client to secure the

connection. A common TCP/IP sockets call is substituted for a call to SSL sockets and a variety of application programming interfaces (APIs) are offered. This approach of "plugging in" security at the socket layer can significantly reduce development time in contrast to building and incorporating the necessary cryptographic components to assure the same security.

Three protocols lie within SSL, the Handshake Protocol, the Record Protocol, and the Alert Protocol. The client authenticates the server during the Handshake Protocol. When the session is initiated and the handshake is complete, the data transfer is encrypted during the Record Protocol phase. If there are any alarms at any point during the session, the alert is attached to the questionable packet and handled according to the Alert Protocol (refer to figure 6).This exchange of messages is designed to facilitate the following actions[8]:

- Authenticate the server to the client.
- Allow the client and server to select the cryptographic algorithms, or ciphers, that they both support.
- Optionally authenticate the client to the server.
- Use public-key encryption techniques to generate shared secrets.
- Establish an encrypted SSL connection.

Figure 6. SSL Protocol Stack

SSL uses digital certificates to authenticate servers. (SSL also includes an optional authentication for clients). SSL uses X.509 certificates to validate identities as the certificate authority then validates this certificate. Digital certificates are based on public-key cryptography. A digital certificate can securely bind your identity, as verified by a trusted third party, with your public key . An SSL certificate contains the following information [9]:

- The domain for which the certificate was issued.
- The owner of the certificate (who is the also the person/entity who has the right to use the domain).
- The physical location of the owner.
- The validity dates of the certificate.

4. Designed authentication System

The designed system is a web-based prototype system (figure 7), follows the déjà vu authentication [7],consisting of authentication web server hosting the database server "image bank" ,a secure hyper text

transmission link achieved by the applied Secure Socket Layer (SSL) protocol ,and an end user . Using D´ej`a Vu, the user creates an image portfolio, by selecting a subset of p images out of a set of sample images. To authenticate the user, the system presents a challenge set, consisting of n images. This challenge contains m images out of the portfolio. The remaining n - m images is called decoy images. To authenticate, the user must correctly identify the images which are part of her portfolio. D´ej`a Vu has three phases: portfolio creation, training, and authentication.

Figure 7: Designed authentication System

5. System Implementation

The system is implemented as a collection of PHP programs hosted by an SSL enabled Apache web server . The configuring of the used Apache server mod SSL includes (figure 8):

1. Installing OpenSSL
2. Creating Self-Signed Certificate; several files related to the SSL certificate are created in this phase , so a common base name was chosen , https://www.mypserver.com .Using a command prompt and

the OpenSSL directory , the following command is executed to create a new certificate, the request follows the SSL configuration to points the SSLCertificateFile at a PEM encoded certificate. :

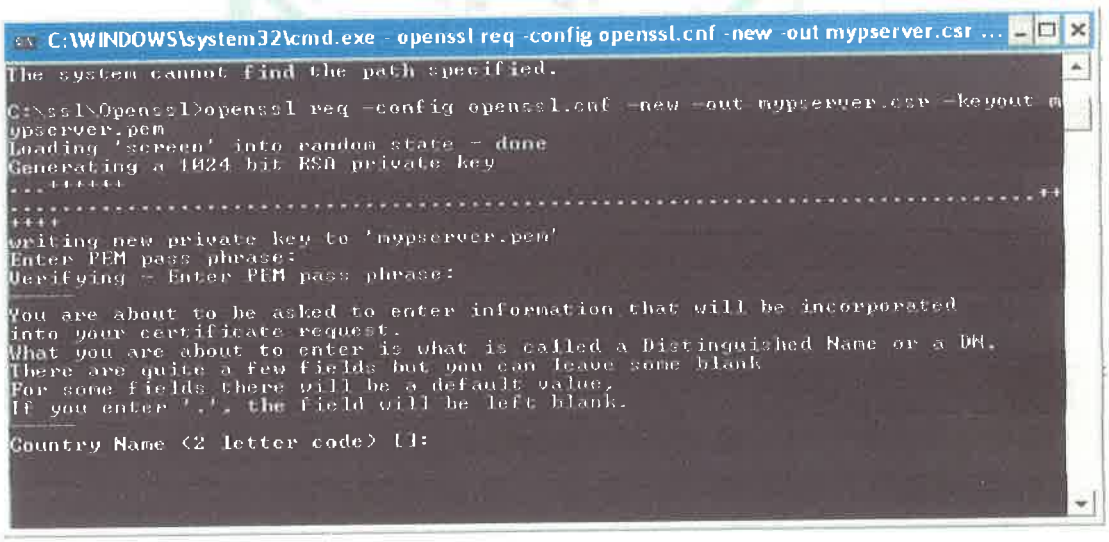
openssl req -config openssl.cnf -new -out mypserver.csr -keyout mypserver.pem

Creating non-password protected key for Apache 2.0.X by executing the following command, the Server Private Key is not combined with the certificate:

openssl rsa -in mypserver.pem -out mypserver.key

Finally, creating X.509 certificate form for the above with the required validity date, (figure 9):

openssl x509 -in mypserver.csr -out myperver.cert -req -signkey mypserver.key -days 365



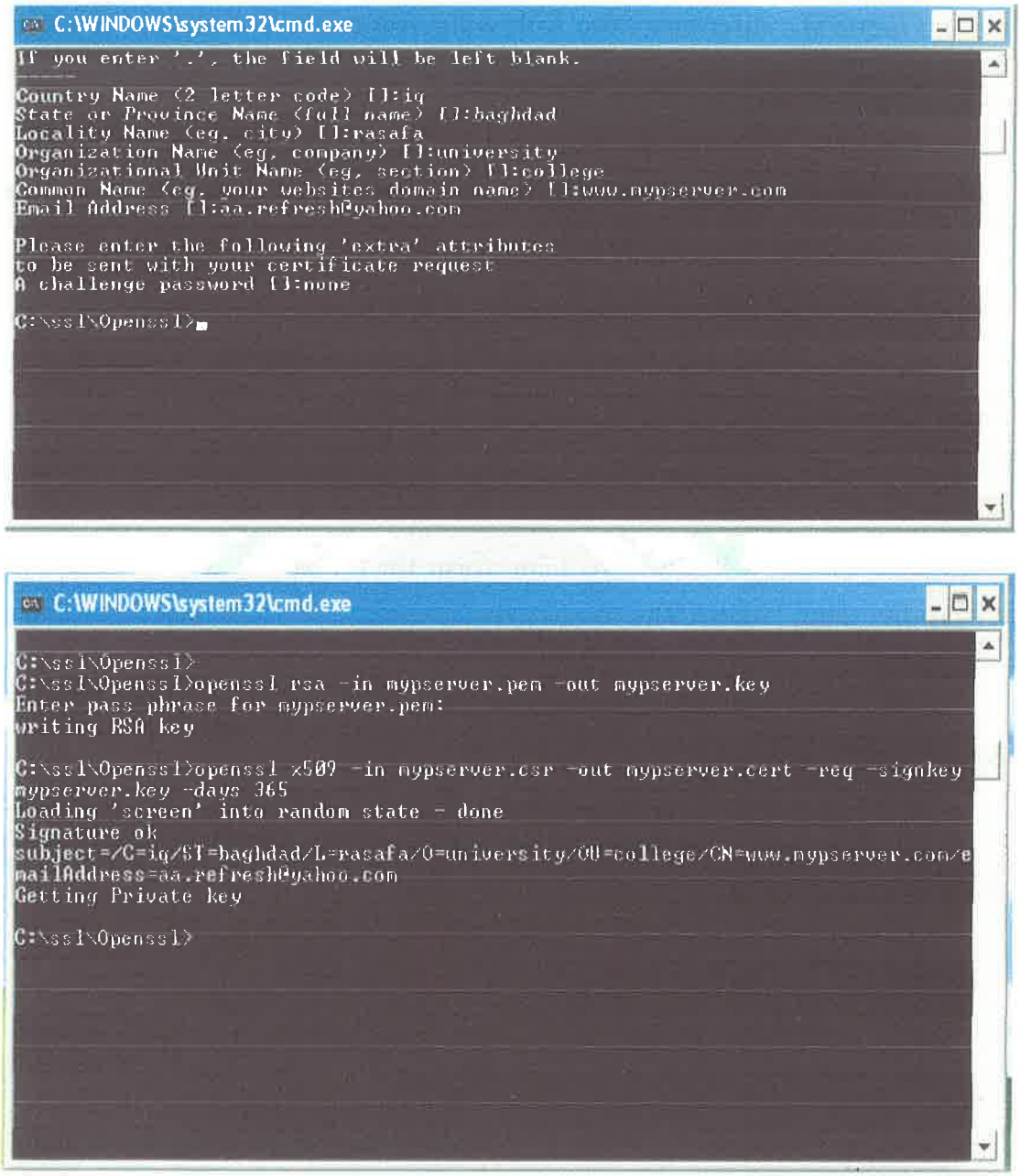


Figure 8: Apache server configuration

Figure 9: Generated x.509 certificate

3. Installing Apache 2.0.X w/ mod_ssl.so

4. Enabling SSL in Apache 2.0.X by editing conf file by the following steps:

A. load SSLmodule by

LoadModule ssl_module modules/mod_ssl.so

B. Including SSL configuration file

<IfModule mod_ssl.c>

Include conf/ssl.conf

</IfModule>

C.Creating a directory under conf file called **ssl** to store the mypserver.key and mypserver.cert files there; the ones created in step 2.Using the self-signed certificate by changing the

SSLCertificateFile and **SSLCertificateKeyFile path** to point to the CERT and KEY files respectively.

6. The Authentication Procedure

1 .Portfolio Creation Phase

To set up a D´ej`a Vu image portfolio, the user selects a specific number of images from a larger set of images presented by a server. Therefore, the approach was to store a large library of random art images in a 'trusted image-bank" hosted by the application server, which is also the authentication server.

2.Training Phase

After the portfolio selection phase, we use a short training phase to improve the memorability of the portfolio images. During training, the user points out the pictures in his portfolio from a challenge set containing decoy images. The selection and the training phase need to occur in a secure environment, such that no other person can see the image portfolio this is provided by the used SSL channel.

3 .Authentication Phase

For each authentication challenge, the server creates a challenge set, which consists of portfolio and decoy images. If the user correctly identifies all portfolio images, s/he is authenticated. (Figure 10 describe the authentication system).

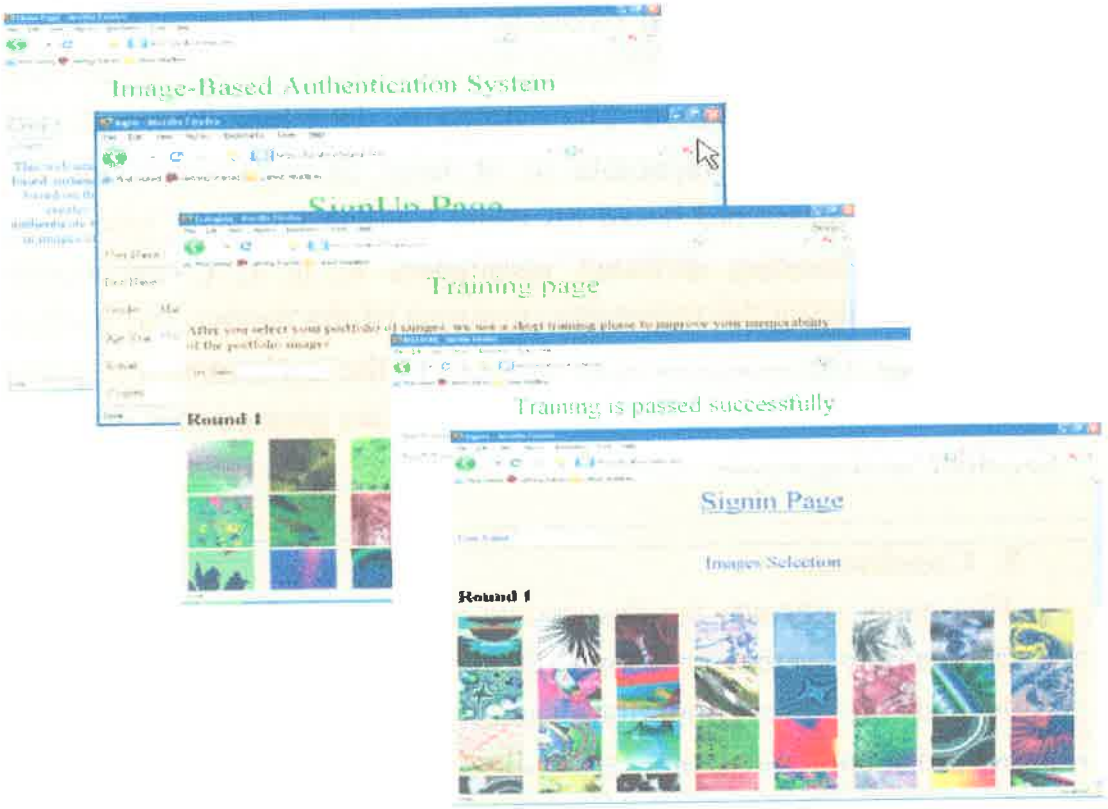


Figure 10: Implemented web sits examples

7. Security Analysis

All the transmitted data between the system components are transmitted in encrypted form through the secure channel achieved by the Secure Socket Layer protocol to avoid attacks such as interception, modification, interruption, and fabrication.

The entropy of a randomly selected graphical password conforming to this policy is $r \cdot \log_2 t$, where $t = c(n,k)$ equals $n!/k!(n-k)!$ Where r is the number of rounds of the graphical password verification. For each round, a challenge set n , and k the number of images selected as the

graphical password. As an example, consider r = 1, n = 36, k = 5, meaning one round of verification by selecting 5 images in any order from a portfolio of size 36. The entropy is 18.5 bits. This makes the password strength comparable to at least an eight character long alphanumeric password based on usual English language letter usage frequency. Choosing different parameters k, n, r, t can increase security. Changing the respective positions of the decoys and portfolio pictures on the authentication screen(s), the authentication pattern cannot be inferred by observing which keys are pressed thus defending shoulder surfing attack.

8. Conclusion

This paper presents the design and implementation of a web based authentication system .The used Déjà vu image based authentication withstand the most important security risk "guessing attack" that password authentication and the other considered Passface authentication suffer from as the knowledge of a user's personal interests and tastes might be a vital piece of information that an attacker may best exploit. Unlike DAS The system requires no external hardware or special graphical interface to display images, pictures or drawings nor needs a device to input his drawing. The system is suitable on PDAs as there is no problem with image size as there is no restriction on predefined regions as Passlogix and Passpoints do.

References:

1. Ali Mohamed Eljetlawi, Norafida Bt.Ithnin, **"Graphical Password: Usable Graphical Password Prototype"** , Journal of International Commercial Law and Technology Vol. 4, Issue 4 -2009.
2. I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin. "**The Design and Analysis of Graphical Passwords**," Proceedings of the 8th USENIX Security Symposium , 1999.
3. G. E. Blonder, "**Graphical password**," U.S. Patent 5559961, Lucent Technologies, Inc. (Murray Hill,NJ), Aug. 30, 1995.
4. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, and N. Memon, "**PassPoints: Design and longitudinal evaluation of a graphical password system**", International Journal of Human Computer Studies, 2005.
5. RealUser Corporation. http://www.realuser.com.
6. Farnaz Towhidi, Maslin Masrom,"**A Survey on Recognition-Based Graphical User Authentication Algorithms**" , (IJCSIS) International Journal of Computer Science and Information Security,Vol. 6, No. 2, 2009.
7. Rachna Dhamija, Adrian Perrig," **D´ej`a Vu: A User Study Using Images for Authentication",** 9th Usenix Security Symposium ,2000.
8. Stephen Thomas ,**"SSL AND TLS Essentials Securing the Web",**2000.
9. Cisco Systems, "**Introduction to Secure Sockets Layer"** , 2002.