Volume : 2 | Issue : 4 | Apr 2013 • ISSN No 2277 - 8179

Research Paper

Three Level Approach for E-Banking

Engineering

KEYWORDS : Security, Authentication, OTP, Image Passwords, Shoulder Attacks, Brute Force Attacks.

Tapan. A. Darekar | Parvatibai Genba Moze College of Engineering, University of Pune, Pune

Priyanka. S. Jadhav | Parvatibai Genba Moze College of Engineering, University of Pune, Pune

ABSTRACT

Security has always been an issue since web development came into existence. Any of the login systems solely depends on passwords requiring no other public or private participant's specific information to be stored. As the passwords are predictable or there is a constant threat of losing the password to someone with a venomous intent, hence there is a need of a system which is more esoteric, thereby being more user-friendly and unique as passwords, to make a system which is secure and equally difficult to hack. This system offers a 3 level security approach, which will definitely improve and increase the security level consisting of text based password, image based authentication along with OTP(one-time password), thus increasing the security for E-Banking.

1. INTRODUCTION

The internet is based on an open network architecture, so information can be transferred freely and efficiently. While this greatly facilitates the development of e-commerce applications, it also raises many security concerns. If anything is bought over the internet before following worries may occur :

Worry 1: If a credit card information is transmitted over the internet people other than the recipient may read it.

Worry 2: People agree to pay say. 200$ for the purchased goods this payment information may be changed or captured by someone on the internet.

Worry 3: The company that claims itself to be legitimate may not be the one.

Fortunately, by using modern encryption techniques e-commerce transactions can be made secure in fact more secure than conducting commerce in the physical world.

In general the aforementioned worries can be summarized into three security requirements namely
1) Confidentiality,
2) Integrity and
3) Authentication.

Confidentiality makes sure that a message is kept confidential or secret such that only the intended recipient can read it. This eliminates the first worry because even if an intruder captures the credit card information on the internet he cannot read the information. To provide this data confidentiality encryption is used. Integrity makes sure that if the content of the message is altered, the receiver can deduct it. This addresses the second worry because if the payment information is changed, the message is no longer valid. A digital signature is commonly used to ensure data integrity. Finally authentication is about verifying identity this elements the third worry as the identity of the company can be verified before carrying out a transaction in an open e-commerce system, a digital certificate is employed to satisfy the authentication requirement. Further, there is also requirement of non repudiation. This ensures the involved party cannot deny the occurrence of a transaction in general if integrity and authentication can be ensured, the non repudiation requirement can also be satisfied.

Figure 1. Facilities given by E-Commerce

This paper is an unique and an esoteric study of using images as password and implementation of an extremely secured system, employing 3 levels of security (Text Password, Image Password, and One-Time automated generated password). A scrupulous research is being done for choosing image sets, involving images that curb attacks like Shoulder Attack, Tempest Attack, and Brute Force Attack at the client side.

2. LITERATURE OVERVIEW

1.SECURITY ANALYSIS AND PROPOSAL FOR IMAGE-BASED AUTHENTICATION

Most human authentication systems have been text-based. Recent psychological studies show users' inability to recall random character sequences. Image-based authentication systems have shown promise in circumventing this problem. In addition, they are more intuitive and user-friendly. This paper presents and analyzes a user authentication technique using images that can be used in local as well as remote authentication. TEMPEST and other forms of attacks are also considered.

2. ONE-TIME PASSWORD

Every time the OTP (one time password) is typed it follows a mathematical function that is known to the legitimate user and the system only i.e it keeps on changing at each entry.

Instead of assignment of a phrase that does not change (static) , the system assigns a mathematical function.

The system and the user know a common one-to-one function like $f(x)=x^2+1$.

The system provides user an argument say '5' and the user replies with password '26' and hence the user is authenticated.

Such systems are also known as challenge response system, because the system presents a challenge to the user and judges the authenticity of the user by the user's response.

One time passwords are very important for authentication because an intercepted static password is useless because it cannot be reused.

However their utility is restricted by the algorithm complexity which people can be expected to remember.

3. PROPOSED SYSTEM

This solitary system offers a 3-level approach providing better security along with feasibility and convenient use.

1. Level 1 :

This level requires the user to pop in a simple text based user name and password based on the traditional technique of authentication. If the entered username and passwords match only then the next level is attained.

2. Level 2 :
This is the most crucial level of this system. Here the security is provided using images. At this level, three image grids are provided. From each of the three grids the user has to select one image.

3. Level 3 :
Level 3 is further divided into two sublevels :

Sub level 1
At this sub level a transaction password is received by the user which is generated by the system. The transaction password is generated during the registration of the new user itself. This password is common for all transactions of the user.

Sub level 2
At this sub level if the entered transaction password is correct then system generates an OTP (one time password). This generated password is valid just for that login session. This one time password will be informed to the authentic user by mailing the same on his/her signed up email-id. This makes the system tougher to attack unless the attacker has access to the user's original email-id.

The authentication of the user is proved only after completing these three levels successfully.

4. WORKING MECHANISMS
At the initial stage, the user is required to register himself on the system by providing all the login details to the system. The login details include user id password that are distinct for each user. This user id and password is used during the log-in session of the user.

After the registration is complete the user gains a transaction password. This transaction password is common for all transaction sessions of the respective user.

Figure 2. Architecture

Level 1:
This level involves the use of a text based user id and password which requires to be individually distinct to each user. No two ids should be same. The selection of a password should be done appropriately that is it should not be easily guessed. It may involve adoption of special characters and symbols.

We use sha-1algorithm at this level for encryption purpose.

A frequently used cryptographic hash function is SHA 1. It is used in digital signature standard (DSS) .

Let x ϵ {0,1}*. Assume that the length |x| of x is smaller than 264. The hash value of x is computed as follows.

First , x is padded such that the length of x is a multiple of 512.

This works as follows.

1) The symbol is appended to x: x← x o 1.
2) A minimal number of zeroes are appended to x such that |x| = k (512 - 64).
3) The length of k is written as a 64-bit number.

The password entered by the user is hashed by using the SHA algorithm and stored in the database.

This prevents the attacker to obtain the password as it is being hashed even if attacker gains control over the database.

Level 2:
At this level security is imposed by using image authentication. There are 3 image grids provided . Each grid contains images in a random sequence. This sequence of images is changed at every login session.

The user has to select an image from each grid. The image position is no where related to previous image set that was generated at an earlier point of time, i.e. during the previous signup or login process.

By doing this, the system protects itself from many security problems. This helps in preventing the keystroke logging attacks where in the attacker observes the pattern of the user's key strokes and hence he tries to obtain the password.

But here the user is required to select one of the different coloured images which will be placed at different places at each login session.

Light is an electromagnetic radiation that stimulates our visual response. Light received from an object can be written as

$$i(\lambda) = e(\lambda)\, l(\lambda)$$

Where e(λ) represents reflectivity and l(λ) is the incident energy distribution.

The retina of the human eye contains two types of photoreceptors, called rods and cones. The rods, about 100 million in number are relatively long and thin. They provide scotopic vision which is the visual response at lower orders of magnitude of illumination.

The cones few in number are short and thick and are less sensitive than rods . They provide photopic vision. The cones are also responsible for colour vision.

Colour representation is based on the classical theory by Thomas Young . He stated that - any colour can be reproduced by mixing an appropriate set of three primary colours. Maxwell in this theory has stated - that there are three different types of cones in human retina with absorption spectra.

Colour representation in different colour spaces
We can perceive only a dozen gray levels while we have an ability to distinguish between thousands of colours. Different colours spaces are used to represent colours. Resolution of colour difference is different in different colour spaces. The CIE chromaticity diagram ,XY coordinates, NTSC transmission colour coordinate system, lightness , hue and saturation colour space, lab colour space and SML colour space are some of the colour spaces presented. Choice of colour space depends upon application.

Lightness , hue and saturation colour space :
Hall states that brightness is the primary visual sensation , whose corresponding psychophysical variable is luminance. Hue is attribute given to different colour sensation such as red, green, blue. The centre of the circle is considered to be achromatic and most saturated colours lie on the perimeter of the circle.

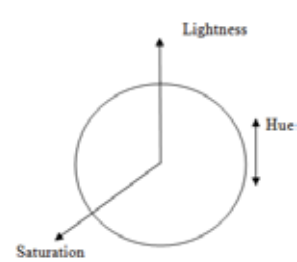

Figure 3. Colour attribute lightness , hue and saturation.

Different hues are indicated as shown in figure. Lightness provides an achromatic centre axis., on which the hue circle can be positioned at various light levels.

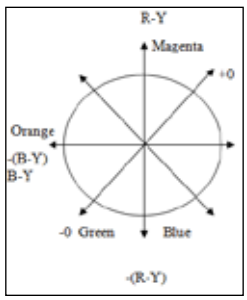

Figure 4. Different hues in YIQ and HIS colour space.

The SML colour space.

There are three types of cones present in the human eye these are labelled as S, M and L. These three cones respond differently

To luminance wavelength (hue) and saturation. According to surveys m and l cones respond to luminance.

Fig shows SML colour space . SML colour space is being used to test the colour deficiency of the human vision. This colour space can differentiate the shades , that can be differentiated by human vision. Thus it matches with the model of human eye.

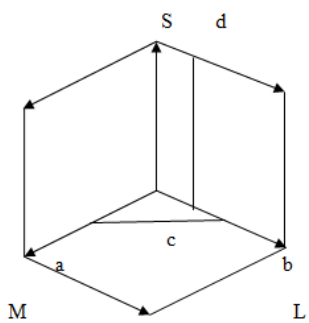

Figure 5. SML colour space

The transformation equations of RGB to SML are :
S= 0.00004r + 0.0019g + 0.173b
M= 0.0447r + 0.2637g + 0.0487b
L= 0.1752r + 0.4208b + 0.0469b

Grid 1(hue grid):
Therefore, taking into account these above mentioned concepts we have added the image grid with randomly sequenced same images with different colours.

Figure 6. Different images are formed due to changes in hue

Grid 2:
The indigo colour is placed on the electromagnetic spectrum between about 420 and 450 nm in wavelength, placing it between blue and violet. This colour is many times confused for being blue violet or purple. This fact enhances the idea of adding the indigo colour in the grid. By doing this adds up to the attacker's confusion. The user is required to remember jut a single colour. This makes the usage user friendly for the user and at the same time difficult for an attacker to remember such a confusing colour.

This prevents attacks like shoulder surfing as even if the attacker tries to seek any information from behind it will be difficult for him to give the required exact input to the system.

Figure 7. Indigo Grid

Grid 3:
The third grid is a combination of colours such as white blue turquoise. All these colours in the grid appear to have a very close similarity.

The similarities among the colours aggregate for the confusion of the attacker. It becomes all the more complex to the attacker for remembering the colour. This point proves to be an indisputable factor for the user. Thus, making the system simple and convenient to use and at the same time tough for the attacker. The restriction provided, where the attacker is blocked from using the system further after he has reached the maximum number of wrong attempts, piles up for the security of the system. It helps in preventing attacks like shoulder surfing, brute force attacks limited to a certain range in the worst case scenario even if the attacker is successful in the selection of the exact colour and successfully completes the grid levels then there is a provision of an one time password too which is discussed broadly in level 3 security.

Figure 8. Grid with combination White and Turquoise

Level 3:
This level is broadly classified into 2 levels

Sublevel 1:
When a new user begins to use the system he is asked to register himself on the system by providing his login details. After the user is successfully registered in the system he is provided with a transaction password during the first login session itself. This password has to be entered correctly in order to proceed with the transaction.

Sublevel 2:
This level provides with an OTP that stands for - one time password.

Passwords are dangerous because the attacker can learn the passwords by tapping the connection between the prover(the one who proves his authentication to the system) and the verifier(the one who checks for authentication of the user). With one time passwords this attack does not work. One time passwords are used for one time identification. For the next identification, a new one time password is used. A simple way of implementing one time passwords is the following:

The verifier has a list f(w1),f(w2).....f(wn) of images of passwords w1,w2.....wn.. The prover knows this list of passwords and uses its elements for the identifications. Since the prover must store all passwords in advance, an attacker could learn some or all of them.

It is also possible that the prover and verifier share a secret function f of an initial string w . Then the one time passwords are wi =fi(w), i ≥ 0. The prover can put the current password w1 and the one- way function f in a system. He does not need a large password file.

In this system if the transaction password is entered correctly then user is received with an OTP this is valid only for that session. The OTP is unique for a single session. This OTP is mailed

to the user's mail id which has been provided by the user into the system at the time of registration. This helps in avoiding brute force attack, as this unique one-time password will be send on user's email-id saved in the database.

Considering the worst level scenario if the user successfully crosses the first two levels then he cannot access the OTP and the transaction password unless he has an access to the user's signed up email id provided during the registration process. This is somehow difficult to go through the first two levels easily. The system thus looks for the authentication of the user and allows the transaction process to be completed only after the successful completion of all these above mentioned levels.

5. CONCLUSION

The 3 level approaches for improving the security proves to be effective and useful under areas where high security is given more significance than time consumption. This system takes more time to complete the whole authentication process but at the same time it proves to be a better option that provides higher security. It helps to avoid attacks such as Shoulder Surfing, Key Stroke Logging Attack, Tempest Attack, Brute Force Attack (to some extent).

6. FUTURE SCOPE

This system can be improved further by adding features:-

Eye Blink Technique:

This is an extra feature which can be added in the first level during login session of a user. In this feature the face of the user is captured and for unlocking purpose the user has to blink his eyes the blinking time is decided by the user solely as to blink once or twice. This can prevent from many security breaches.

Scalability:

More number of image grids can be added as per the required security.

Suppose if high security is needed then 5 image grids can be selected. for example for very high security purposes like military purposes, 10 image grids can be selected and 1 image from each has to be selected. This adds up to confusion of the attacker.

REFERENCE

[1].Security analysis of and proposal for image-based authentication Richard E. Newman, Piyush Harsh, and Prashant Jayaraman. [2] Security Analysis and Implementation of *JUIT–Image Based Authentication System using Kerberos Protocol [3] Nitin, Durg Singh Chauhan, Sohit Ahuja, Pallavi Singh, Ankit Mahanot,Vineet Punjabi, Shivam Vinay, Manisha Rana, Utkarsh Shrivastava and Nakul Sharma, Security Analysis and Implementation of JUIT-IBA System using Kerberos Protocol, Proceedings of the 7th IEEE International Conference on Computer and Information Science,Oregon, USA, pp. 575-580, 2008 [4] Nitin, Durg Singh Chauhan and Vivek Kumar Sehgal, On a Software Architecture of JUIT-Image Based Authentication System, Advances in Electrical and Electronics Engineering, IAENG Transactions on Electrical and Electronics Engineering Volume I-Special Edition of the World Congress on Engineering and Computer Science, IEEE Computer Society Press, ISBN: 978-0-7695-3555-5, pp. 35-46, 2009. [5] International journal of network security & Its applications (ijnsa), vol.3, no.3, may 2011 authentication schemes for session passwords Using color and images M sreelatha , m shashi , m anirudh , Md sultan ahamer , v manoj kumar [6] Security analysis of and proposal for image-based authentication richard e. Newman, piyush harsh, and prashant jayaraman cise dept., university of florida, gainesville fl 32611-6120 {nemo, pharsh, pjayaram}@cise.ufl.edu