Image Based Authentication For One Time Password

Authors
Sheetal Shinde, Chetana Ratnparakhi, Uttam Chormale
Corresponding Author
Sheetal Shivaji Shinde
Email: sheetal.kharatmol@gmail.com

ABSTRACT
Image based authentication is applying for OTP to provide more security of user’s personal account. Along with the username and password providing a valid image for authentication. Image authentication is using database in a pixel format and application process will written in java. In previous concept there is a problem of stealing password attacks is when users type passwords to untrusted public computers. This system state that user can log in into conventional computers for authentication using image as a username and password. Including a cell-phone, which is used to generate a one time password and new communication channel, SMS is used to transmit an authentication message. The aim of this system is to develop a model that provide a better security, easy to use on any web browser. This process become an efficient and user friendly.

Keywords- image based authentication (IBA), one time password (OTP), SMS

INTRODUCTION
In previous system text based passwords have problem that peoples are not experts to memorizing text string so that they are choose simple text for easy-to-remember. So this system propose an authentication which prevent password stealing and password reuse attacks. OPASS is an android application used at client side. This OPASS application is installed on user’s cell-phone. Through Wi-Fi connection sever and users cell-phone are connected. OPASS involves a new component to the cell phone used to generate OTP and new communication channel.

In this system software component is used android cell for creating communication between any web browser and server. After establishment of connection user enters image as user-name and password and get message from server that login is successful. Server generates an OTP and send on user’s cell-phone. For security purpose application uses pin number. After entering a pin number OPASS asks for IP address of client’s machine. The system share this information with the server. This technique is used for many application system such as banking, online shopping card system etc. This system is used for real-estate billing application. After sharing IP address information it establish a connection between server and real-estate billing application via verification code. This verification code is send by the server on users cell-phone. This verification is enter on application window. After successful verification of code it opens billing application.

Real-estate application provides more functions such as adding new projects and customers, updating customer’s data, payment mode. If SIM card or mobile has been lost from user for that
purpose system provides one more application that particular account will be block within 24 hrs. In previous system there is possibility of screen capturing and keyboard tracing, so third party will hack this account. On that image password is one of the solution.

RELATED WORK

OPASS adopts an one time password strategy. In system we describing features of SMS channel with the explanation of why SMS is trusted. Introduce the 3G connection used in registration, login, and recovery phase.

One Time Password

The one-time password system is two-factor authentication system where the password constantly alternates. This greatly reduces the risk of unauthorized intruder gaining access to the account.

SMS channel

SMS is a text based authentication service system provided by telecommunication system. It represents most successful data transmission of telecommunication system. It spreads mobile service all over the world. It protect the exchanging messages between users and the server.

3G Connection

Password reuse is a serious problem in the present user authentication systems. So 3G connection provides data confidentiality of users data and the signal data and also provides data integrity. Using 3G connection user can securely transmit and receive all the information or data.

PROPOSED SYSTEM

To perform secure login on an un-trusted computer, OPASS consists of a trusted cell-phone, a browser on an un-trusted computer, and a web server that users wish to access. The user operates his cell-phone and the un-trusted computer directly to accomplish secure logins to the web server. The communication between the cell-phone and the web server is through the SMS channel. The web browser interacts with the web server via the Internet also server checks image that it updated on every 15 days if yes then proceed further otherwise it sends image on user account. Every user has a different image for his account. In our protocol design, require the cell-phone interact directly with an un-trusted computer. The general approach is to select available interfaces on the cell-phone, Wi-Fi, hotspot.

System can provide more security to the confidential information stored into web-accounts. Using this software, industry people can store their confidential information on web accounts more securely. Instead of username and password image authentication is used for security purpose. User authentication is performed using image verification at server side. On the server side image is stored in database. There is a two layer scenario. In the first basement part pixels are put on image resolution according to X and Y co-ordinates, colors with RGB code and intensity of that image. These selected pixel are joined together and this will generate one type of shape like polygon, circle etc. On this shape user’s image is imposed and that will
be stored on server. After sending image at client side browser will match the pixels, colors, and intensity. For security purpose the intensity will be different for different users. If the pixels, colors, and intensity are matched, authentication is done.

Design Overview

**Fig. architecture**

In the figure: User signs up for registration of account on a server with login image as username and the password. After successful login, user can open any web browser for accessing his account and send that image to server. Server validates that image which is sent from user. After validating it sends an OTP on cell-phone and forwards it to the web-browser, web-browser sends OTP to the server. Server validates OTP and user’s login successfully for a system.

### Procedures for image creation

**Step 1:** Get time and date of system

When user login into account and for verification image is sent to the server, it checks time and date of image. After 15 days it checks on what date and which time it updated.

**Step 2:** apply function to get image points.

Every user has a unique image. In this method addition of year, day, month, hour, minute, seconds is used. This function determines how many points are to be plotted on image.

Function:-

\[ f(\text{point}) = (yy + dd + mm + hh + mm + ss) \mod 1000 \]

**Step 3:** function to calculate (X,Y) co-ordinates of each point

Following method is used to calculate X and Y co-ordinates of the pixels for the image. Any random number is used to get the co-ordinates by taking its mod with the screen resolution (400 X 600)

Function:-

\[ f(\text{to calculate x}) = (\text{random number})\mod 400 \]
\[ f(\text{to calculate y}) = (\text{random number})\mod 600 \]

**Step 4:** Apply color of each point

Similar to finding co-ordinates of pixels, random numbers are used to get the RGB values for the pixel color.

Function:-

\[ f(\text{to calculate R}) = (\text{random number})\mod 255 \]
\[ f(\text{to calculate G}) = (\text{random number})\mod 255 \]
\[ f(\text{to calculate B}) = (\text{random number})\mod 255 \]

### Advantages and limitations

#### Advantages

It is more secure for users personal account for account registration and recovery. Best for internet enabled Android phone. Easy password recovery
when user lose their cell phone, the protocol is able to recover OPass setting on her new cell-phone assuming user still uses the same phone number (Apply a new SIM card with old phone number).
Compatible with any web browser such as internet explorer, Mozilla,chrome etc. No manual interface for login. It can be used for both industrial and commercial application to where data confidentiality and secure data transfer is the major concern.

Limitations

Internet connection is must after 90 days. Not yet widely used, current graphical password technique are still immature.

CONCLUSION

On the possibility of hacking passwords graphical /image password are an alternative to textual alphanumeric password. Many solutions have been proposed. Process is user friendly.

REFERENCES