2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN)

Password Security system with 2-way authentication

Subhradeep Biswas
Computer Consultancy
Tata Consultancy Services
Calcutta, India
Subhradeep.biswas@gmail.com

Sudipa Biswas
Software Engineering
BITS Pilani
Bangalore, India
Sudipa16.india@gmail.com

***Abstract*—This paper proposes a password security system that allows the host not to store the passwords of its users at its end. Instead it creates and stores a derivative of the password with the help of a bitmap image uploaded by the user during the user creation process. During the login attempts of users, the user is required to enter the password and upload the same image. the proposed system verifies if the image uploaded during login matches with the original image that was provided during user creation by comparing their pixel information. Then, the system derives the password from the image with the help of the stored derivative. Then, the derived password is matched with the password entered by the user.**

***Index Terms*—graphical authentication, image authentication, text password, dual authentication, 2-way authentication.**

I. Introduction

In most of the password authentication systems, the graphical or text passwords are stored in host databases. The objective of the proposed authentication system is to provide means of password security that does not need to store the passwords in host database so that it can prevent passwords to be stolen in case of a database hacking incident. This solution allows the host not to store the passwords anywhere. At the time of every user login, the text password is derived using different information stored in different sources. Then, the password entered by user is authenticated against the derived password. The sources that are used to derive the passwords are [1] a bitmapped graphical image [2] pixel locations hidden in the program's algorithm and [3] password derivative stored in user record in host database. The solution combines the mechanisms of authenticating image and text passwords together. The password derivatives (can be considered as hashed passwords) that are stored at host cannot be decrypted either as this requires the image for the decryption. The system can also block unauthorized login attempts even when the text password is stolen until the image is not leaked.

II. Proposed System

A. User Creation

The proposed system requires a new user to provide a text password, a bitmapped graphic image and a secret key while signing up along with a unique user name and other details. The algorithm of the proposed system identifies two different sets of pixels on the bitmapped image. One set of pixels and the secret key are used to cater the image verification process. The other set of pixels is used to prepare the password derivative.

- Capturing image information for future verification: The secret key is stored in the user record in host database. The ASCII value of each character of the secret key is compared against the decimal (converted from binary) value of a specific color segment of a specific pixel (from the 1st set of pixels) identified by the algorithm. The difference (= ASCII of character – decimal value of color segment of a pixel) in value with less than (-ve) or greater than (+ve) sign for each character of the user's secret key is stored as the secret key derivative in a different column in the user record.
- Creating password derivative: The ASCII value of each character of the text password is compared against the decimal (converted from binary) value of a specific color segment of a specific pixel (from the 2nd set of pixels) identified by the algorithm. The difference (= ASCII of character – decimal value of color segment of a pixel) in value with less than (-ve) or greater than (+ve) sign for each character of the user's text password is stored as a distinct segment of the password derivative with the user record in the host database.

978-1-5386-1931-5/17/$31.00 ©2017 IEEE

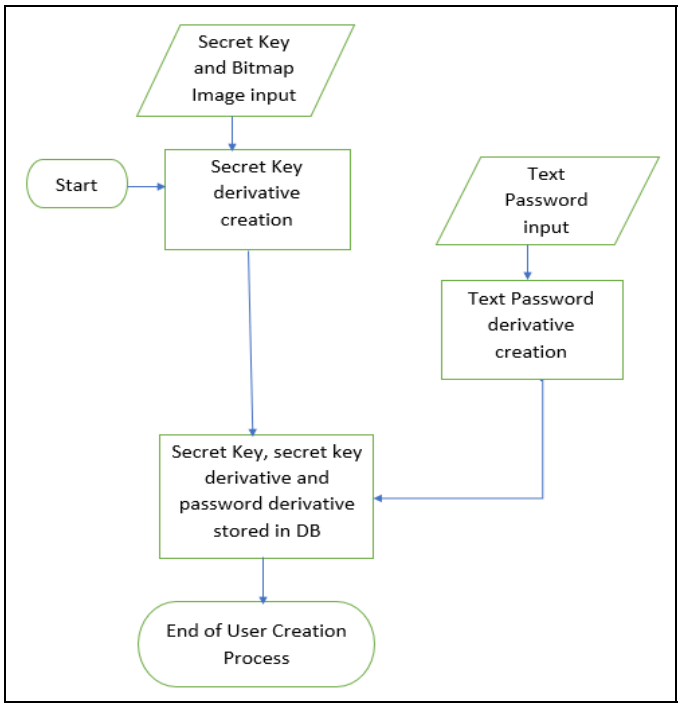

Fig. 1. User creation process flowchart.

The user needs to remember the text password and keep the bitmapped image handy for future login.

B. *User verification*

The proposed solution asks the users to enter the text password and upload the bitmapped image for successful login. Once the required steps are completed, the image authentication is performed followed by the user authentication.

- Authenticating the image: The proposed solution fetches the pixel information for the 1st set of pixels that were identified for image authentication during the user creation process. The value stored in each segment of the secret key derivative is added or subtracted (according to the greater than/less than sign in the segment) with or from the decimal value (converted from binary) of a predefined color segment of the pixels. The resulting decimal values (considered as ASCII values) are converted into characters. The text formed by the characters is matched with the secret key that is stored at the user record. In case of a perfect match, the image is authenticated with success.
- Authenticating the user with password: Once the image authentication is successful, the proposed solution fetches the 2nd set of pixels that were identified for preparing the password derivative during the user creation process. The value stored in each segment of the password derivative is added or subtracted (according to the greater than/less than sign in the segment) with or from the decimal value (converted from binary) of a predefined color segment of the pixels. The resulting decimal values (considered as ASCII values) are converted into characters. The text formed by the characters is matched with the text password that has been entered by the user for login. In case of a match, the user is authenticated successfully.

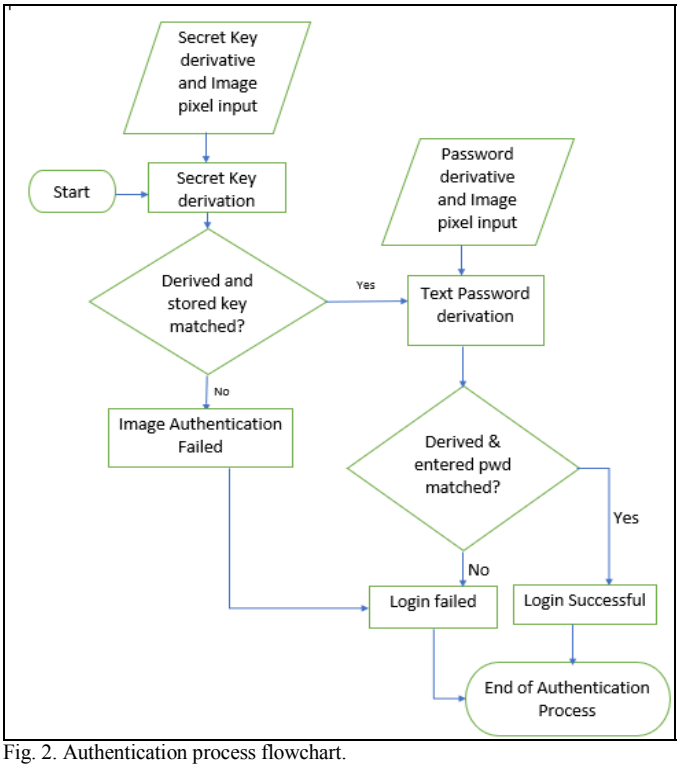

Fig. 2. Authentication process flowchart.

III. RESULTS

The proposed password authentication system has been implemented successfully. The scope of this system includes user creation and login authentication. The test results explain the system mechanisms as follows:

A. *User Creation:*

- Signing up on user interface: The system requires the user to enter a unique user name, a secret key (one-time use), a bitmapped image and a password.

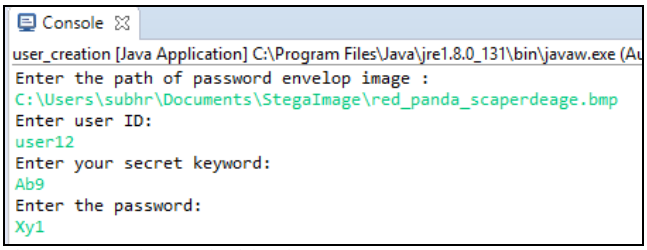

Fig. 3. Information required for sign up process.

- Generating Secret Key Derivative: A set of pixels and a specific color segment are identified by the algorithm. The binary value of that color segment of each pixel is converted into decimal. The ASCII value of each character of secret key is fetched. The difference in value between the ASCII value and the converted decimal value is derived. The result is stored as a segment of secret key derivative. In the given test case, the ASCII value of 'A' (1st character of secret key) is 65, The decimal value of the identified color segment is 191. The difference in value is (= 65 – 191) -126. Hence, for the first character of secret key, the 1st segment of the secret key derivative is '0-126'. Likewise, all other segments for all the characters of secret key is derived.

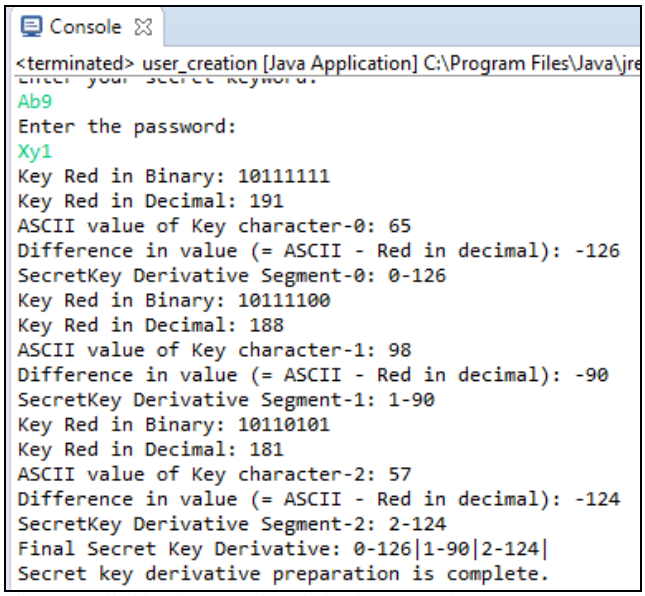

Fig. 4. Detailed log for secret key derivative generation

- Generating Password Derivative: This follows the same process as the Secret Key derivative generation mechanism does. A different set of pixels is identified and used by the program algorithm.

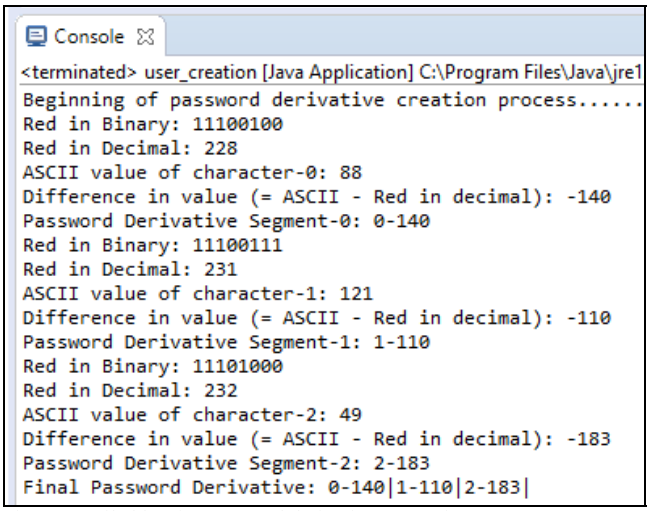

Fig. 5. Detailed log for password derivative generation

- User Record stored in Database: The system stores user id, password derivative, secret key and secret key derivative in the database. The highlighted user record in Fig. 6 has been created for the test case.

Username	Password	SecretAns	secretKeywrdderi
subhra123	0+77|1-37|2-36|3-18|4	maharaj	0+109|1-23|2-20|3-8
subhradeep	0-23|1+38|2-25|3+69|4	kelo	0+2|1+83|2+85|3+46
sudipa	0-148|1-134|2-117|3-12	secret123	0-76|1-87|2-82|3-43
sudipa123	0-148|1-134|2-117|3-12	secretKey	0-76|1-87|2-82|3-43
User1	0-140|1-110|2-175|	Ab1	0-126|1-90|2-132|
user12	0-140|1-110|2-183|	Ab9	0-126|1-90|2-124|

Fig. 6. User records stored in database.

B. User authentication:

- Login on user interface: The system requires the user to enter the user name, the image the user registered at sign in and the password.

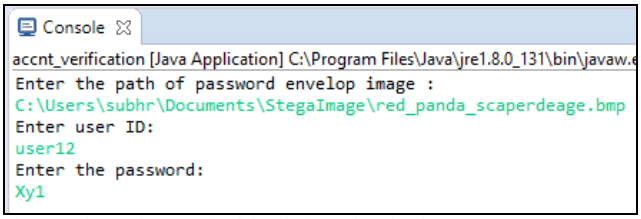

Fig. 7. Information required for login authentication

- Image authentication using Secret Key: Secret key and the secret key derivative are fetched from user record. As shown in Fig. 8, each segment of the derivative provides the value to be subtracted or added with the decimal value of the predefined color segment of specific pixel to get the ASCII value of secret key characters. All the characters form the secret key together and matched against the secret key retrieved from database.

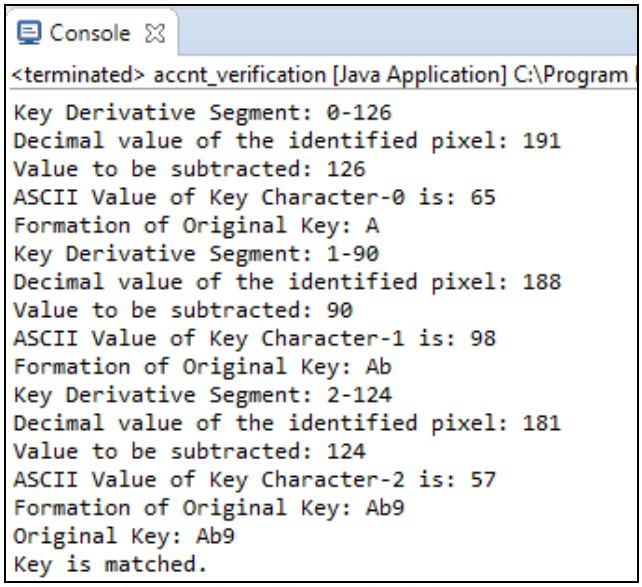

Fig. 8. Secret key formation and image authentication

- Password authentication: Password derivative is fetched from database. As shown in Fig. 9, password authentication process follows the same mechanism as the secret key formation to form the password. Then the derived password is matched against the password entered by the user for login.

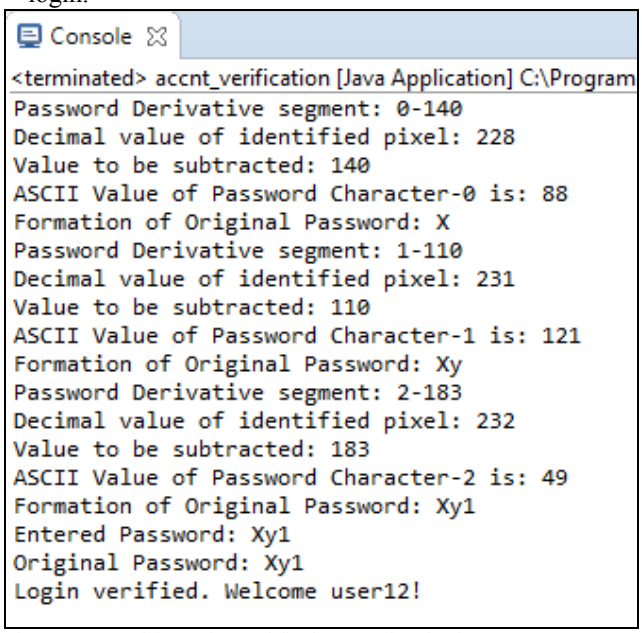

Fig. 9. Password formation and final user authentication

C. Negative Scenario Testing:

- Incorrect image used for authentication: During signing in, if the user enters the username and text password correctly, but, provides the wrong image as shown in the screenshot below, the user authentication should fail.

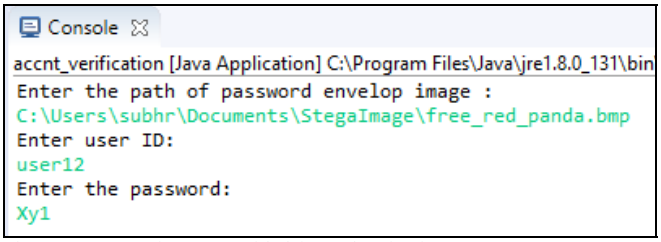

Fig. 10. Incorrect image provided for authentication

- Derived secret key not matched with stored secret key: The secret key and the secret key derivative are fetched from user record for user: "user12". As shown in Fig. 11, each segment of the derivative provides the value to be subtracted or added with the decimal value of the predefined color segment of specific pixel to get the ASCII value of secret key characters. All the characters form the 'derived' secret key and matched against the secret key stored in the database. As the stored and derived keys are not matched as shown in Fig. 11, the user authentication fails.

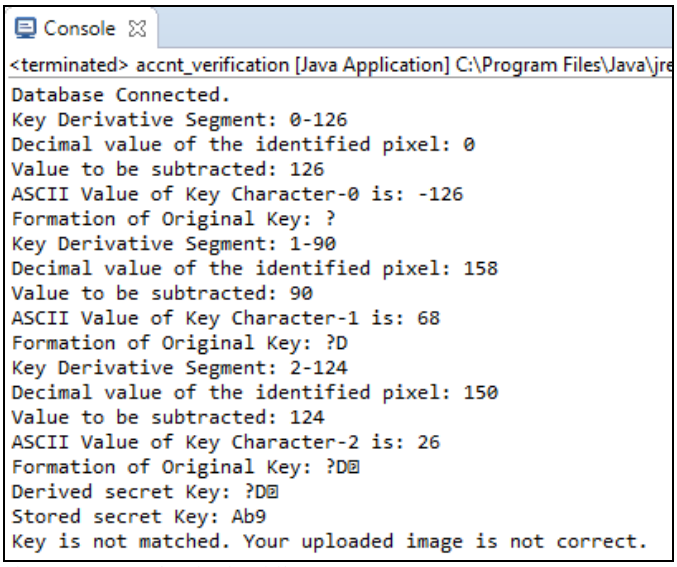

Fig. 11. Image authentication fails

- Incorrect text password entered for authentication: During signing in, if the user enters the username and bitmap image correctly, but, enters the wrong password as shown in the screenshot below, the user authentication should fail.

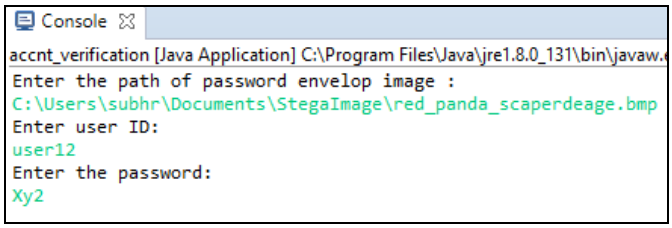

Fig. 12. Incorrect password provided for authentication

- Derived password not matched with entered password: The secret key matching and image authentication is done successfully for this login attempt. Then, the password derivative is fetched from user record for user: "user12". As shown in Fig. 13, each segment of the derivative provides the value to be subtracted or added with the decimal value of the predefined color segment of specific pixel to get the ASCII value of text password characters. All the characters form the 'derived' password and matched against the text password entered by the user. As the derived and entered passwords are not matched as shown in Fig. 13, the user authentication fails.

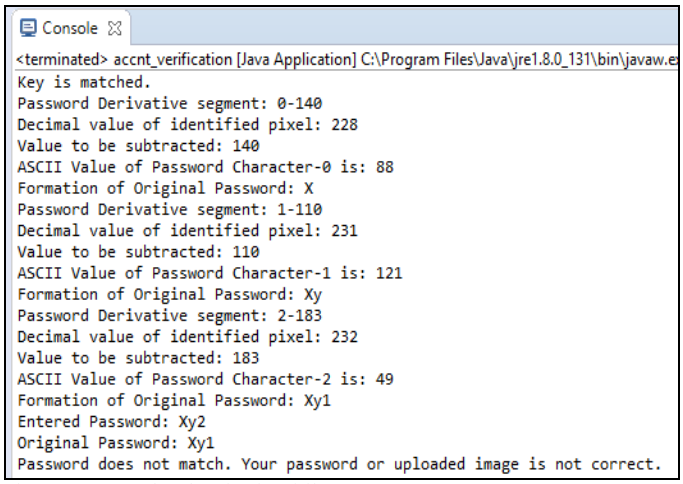

Fig. 13. Password authentication fails

IV. Evaluation

The proposed authentication system provides two layers of security. Hence, it is more resistant against the unauthorized login attempts as compared to most of the authentication systems that rely solely on either text password or graphical authentication.

The image authentication layer provides the security against common hacking techniques like monitoring or recording users' key strokes or attacks using shoulder-surfing and hidden camera.

In the proposed system, as the password is not stored anywhere and it is derived from the image the user is to provide during signing in, it mitigates the possibilities of user data security getting compromised in case of host database hack.

The solution can be implemented in any real-time online or offline applications to enable a robust password security mechanism.

The drawback of this solution is it increases the complexity of the user authentication process. The users need to remember the alphanumeric text passwords along with the image used while signing in.

V. Conclusion

The proposed authentication system provides security over attacks by monitoring or recording users' key strokes, shoulder-surfing and hidden camera. Even if the password is leaked and the host database is hacked, any random bitmapped image cannot be modified accordingly as the sets of pixels (used in authentication process) are identified by the algorithm. Thus, the pixel locations are not stored in the database. The unauthorized access cannot be prohibited if both the text password and the image are compromised.

The user needs to keep the image handy for login which should not be a big deal in the age of easy and secured file portability provided by the cloud based file storage systems.

References

[1] Alaa A. Jabbar Altaay, Shahrin Bin Sahib and Mazdak Zamani, "An Introduction to Image Steganography Techniques", IEEE Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference.

[2] Hung-Min Sun, Shiuan-Tung Chen, Jyh-Haw Yeh, Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical AuthentiationSystem", IEEE, IEEE Transactions on Dependable and Secure Computing (Volume: PP, Issue: 99)

[3] Ahmad Almulhem, "A Graphical Password Authentication System", IEEE, Internet Security (WorldCIS), 2011 World Congress.

[4] P. Sriramya and R. A. Karthika, PROVIDING PASSWORD SECURITY BY SALTED PASSWORD HASHING USING BCRYPT ALGORITHM, ARPN Journal of Engineering and Applied Sciences, Vol. 10, No. 13.

[5] Ziran Zheng, Xiyu Liu, Lizi Yin, Zhaocheng Liu, "A Stroke-Based Textual Password Authentication Scheme", IEEE, First International Workshop on Education Technology and Computer Science, 2009. ETCS '09.

[6] Amol Bhand, Vaibhav Desale, Swati Shirke, Suvarna Pansambal Shirke, "Enhancement of password authentication system using graphical images", IEEE, 2015 International Conference on Information Processing (ICIP).

[7] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme," in 21st International Conference on Advanced Information Networking and Applications Workshops(AINAW 07), vol.2. Canada, 2007, pp. 467- 472.

[8] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Basic results," in Human-Computer Interaction International(HCII2005). Las Vegas, NV, 2005.

[9] G. E. Blonder, "Graphical passwords," in United States Patent, vol.5559961, 1996.