International Journal of Computer and Communication Technology

Volume 7 | Issue 1 Article 12

January 2016

THREE –WAY SECURITY USING IMAGE BASED AUTHENTICATION SYSTEM

SARIKA KHALADKAR
Department of Information Technology, Bharati Vidyapeeth College Of Engineering for Womens, University of Pune, Sarika.khaladkar@gmail.com

SARITA MALUNJKAR
Department of Information Technology, Bharati Vidyapeeth College Of Engineering for Womens, University of Pune, saritamalunjkar22@gmail.com

POOJA SHINGOTE
Department of Information Technology, Bharati Vidyapeeth College Of Engineering for Womens, University of Pune, poojashingote2@gmail.com

Recommended Citation

KHALADKAR, SARIKA; MALUNJKAR, SARITA; and SHINGOTE, POOJA (2016) "THREE –WAY SECURITY USING IMAGE BASED AUTHENTICATION SYSTEM," *International Journal of Computer and Communication Technology*: Vol. 7 : Iss. 1 , Article 12.
DOI: 10.47893/IJCCT.2016.1335
Available at: https://www.interscience.in/ijcct/vol7/iss1/12

THREE –WAY SECURITY USING IMAGE BASED AUTHENTICATION SYSTEM

SARIKA KHALADKAR[1], SARITA MALUNJKAR[2] & POOJA SHINGOTE[3]

[1,2&3]Department of Information Technology, Bharati Vidyapeeth College Of Engineering for Womens, University of Pune
Email:Sarika.khaladkar@gmail.com, saritamalunjkar22@gmail.com, poojashingote2@gmail.com

Abstract- Secure environments protect their resources against unauthorized access by enforcing access control mechanisms. So when increasing security is an issue text based passwords are not enough to counter such problems. The need for something more secure along with being user friendly is required. This is where Image Based Authentication (IBA) comes into play. This helps to eliminate tempest attack, shoulder attack, Brute-force attack. Using the instant messaging service available in internet, user will obtain the One Time Password (OTP) after image authentication. This OTP then can be used by user to access their personal accounts. The image based authentication method relies on the user's ability to recognize pre-chosen categories from a grid of pictures. This paper integrates Image based authentication and HMAC based one time password to achieve high level of security in authenticating the user over the internet.

***Keywords**- Image Based Authentication System, Tempest Attack, Shoulder Attack, Brute-force Attack.*

I. INTRODUCTION AND MOTIVATION

Authentication plays a crucial role in protecting resources against unauthorized and illegal use. Authentication processes may vary from simple password based authentication system to costly and computation intensified authentication systems. Passwords are more than just a key. They serve several purposes. They ensure our privacy, keeping our sensitive information secure. Passwords authenticate us to a machine to prove our identity-a secret key that only we should know. They also enforce non repudiation, preventing us from later rejecting the validity of transactions authenticated with our passwords.

Our username identifies us and the password validates us. But passwords have some weaknesses: more than one person can possess its knowledge at one time. Moreover, there is a constant threat of losing your password to someone else with venomous intent.

II. RELATED WORK

The main Objective of of 3-Level Security system is a unique and an esoteric study of using images as password and implementation of an extremely secured system, employing 3 levels of security.

1) Level 1
Security at level 1 has been imposedby simple text-based password.

2) Level 2
Security at this level has been imposed by using image based authentication(IBA) which helps to eliminate shoulder attack ,tempest attack and brute-force attack. User has to select three images from the respective grid.

2.1 SCREENSHOTS OF SECOND-LEVEL

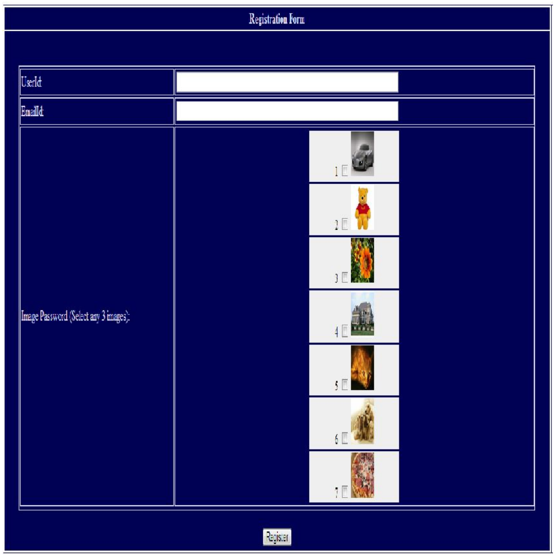

Fig 1 : Registration Form

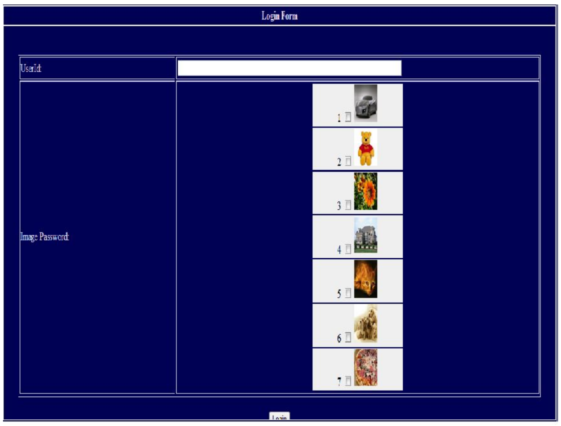

Fig 2. Login Form

3) Level 3
After the successful clearance of the above two levels, the 3-Level Security System will then generate a one-time numeric password that would be valid just for that login session. The authentic user will be informed of this one time password on his email-id.

III. PROPOSED SYSTEM

3.1 HMAC-Based One-Time Password Algorithm

This paper describes an algorithm which is used to generate Time-synchronized OTP values, based on SHA-1 based Hash Message Authentication Code (HMAC). This is called as the HMAC-Based One-Time Password because here OTP is generated based on HMAC. One-Time Password is obviously one of the easiest and most popular forms of two-factor authentication that can be used for securing access to accounts. One-Time Passwords are often referred to as a secure and stronger forms of authentication, and allowing them to installed across multiple machines including home computers, mobile phones etc. When the user selects the pre-selected images to login an OTP is generated and sent to the corresponding mobile phone. The user is then directed to next page where the user is asked to enter the OTP. The user gets the OTP using the e-mail account and enters it. If the OTP is verified the user succeeds in logging in the system.

3.2 Algorithm Requirements

A - The algorithm MUST be time synchronized.
B - The algorithm SHOULD be economical to implement by reducing the amount of hardware required.
C - The algorithm MUST work with any sort of code generating tokens.
D - The value displayed on the token or any mail message should be easy to read and entered by the user. For this the OTP value should be of reasonable length such as a 8-digit value. It is desirable for the OTP value to be a numeric digit so that it can be easily entered.
E - User-friendly mechanisms should be available to resynchronize the time.

Algorithm

The notations used in OTP algorithm-
T- It is the Time value, the changing Factor.
Key -Shared secret between client and server, i.e. Username and Image Based Password.
Digit-Number of digits in an HOTP value.

Description

The OTP algorithms are based on an increasing time value function and a static symmetric key known only to client and server. In order to create the OTP value, a HMAC- SHA-1 algorithm is used. Since the output of the HMAC-SHA-1 calculation is 160 bits, we have to truncate this value
to a smaller digit so that it can be easily entered.
OTP(Key,T)=Truncate(ToHex(HMAC-SHA-1(Key,T)))
Where –Truncate converts the value generated through HMAC-SHA-1to an OTP value.

3.3 Generation of OTP Value

The algorithm can be described in 3 steps:

Step 1: Generate the HMAC-SHA-1 value Let HMK = HMAC-SHA-1(Key, T) // HMK is a 20-byte string
Step 2: Generate a hex code of the HMK. HexHMK=ToHex (HMK)
Step 3: Extract the 8-digit OTP value from the string OTP = Truncate (HexHMK) The Truncate function in Step 3 does the dynamic truncation and reduces the OTP to 8-digit.

IV. CONCLUSION

A new type authentication system, which is highly secure has been proposed in these paper. This system, is also more user friendly.This system will definitely help thwarting Shoulder attack, Tempest attack and Brute-force attack at the client side.Though 3-Level Security system is a time consuming approach, it will provide strong security where we need to store and maintain crucial and confidential data secure. Such systems provide a secure channel of communication between the communicating entities. The ease of using & remembering images as a password also support the scope of
these systems.

REFERENCES

[1] 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.

[2] Richard E. Newman, Piyush Harsh and Prashant Jayaraman, “Security Analysis of and Proposal for Image Based Authentication,” 2005.

[3] Chiasson, S., R. Biddle, R., and P.C. van Oorschot. A Second Look at the Usability of Click-based Graphical Passwords. ACM SOUPS, 2007.

[4] Haichang Gao, Zhongjjie Ren, Xiuling Chang, Xiyang Liu Uwe Aickelin, A New Graphical Password Scheme Resistant to Shoulder-Surng.

[6] Z. Zheng, X. Liu, L. Yin, Z. Liu A Hybrid password authentication scheme based on shape and text Journal of Computers, vol.5, no.5 May 2010.

[7] Chris Ullman and Lucinda Dykes, Beginning Ajax (Programmer to Programmer), Paperback, March 19, 2007.

◈◈◈