Callback Authentication: A User Authentication Technique for Better Security

S. V. Patil, M. M. Sutar, P. R. Panari, A. A. Magar, G. S. Nakate

Abstract— a user can get access to its account only by means of username and password in this sense the security of user account is only dependent on the password of user. Hence it is important that user should keep his/her password confidential. In many systems people select their username and text passwords when registering accounts on a website. The matter becomes worse when users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might be unsafe. Therefore, it is important to take human factors into consideration when designing a user authentication protocol. In "callback authentication system" the user's registered cell phone number has been efficiently used for user authentication.

Keywords: Call, Status, Authentication.

I. INTRODUCTION

Over the past few decades, text password has been adopted as the primary mean of user authentication for websites. People select their username and text passwords when registering accounts on a website. In order to log into the website successfully, users must recall the selected passwords. Password reuse causes users to lose sensitive information stored on websites if a hacker compromises one of their passwords. In such systems only user passwords are used as a mean for authentication. In proposed "callback authentication system" cross verification of user is done on the basis of user's registered cell phone number. Call based authentication system provides security because authentication will be performed on the basis of user selected password as well as registered cell phone number[3].

Following are some limitations of user selected passwords:

1) Humans are not experts in memorizing text strings. Thus, most users would choose easy-to-remember passwords (i.e., weak passwords) even if they know the passwords might be unsafe.
2) Another crucial problem is that users tend to reuse passwords across various websites. Password reuse causes users to lose sensitive information stored on websites if a hacker compromises one of their passwords.
3) Human beings are error prone hence may make mistakes while manually typing authentication related code.
4) In the systems where login is fully dependent on user selected password, if hackers obtain respective password then can easily get access to the authorized user's account.
5) In text password based user authentication systems there is no way to easily capture the unauthorized use of account.
6) Using same password across various websites causes domino effect. In domino effect, when a weak system losses its password, some information will be revealed that will aid the hackers in infiltrating other systems which may cause loss of huge data.

Hence the systems which are using user selected passwords for authentication are more vulnerable. Therefore, it is important to take human factors into consideration when designing a user authentication protocol.

In "callback authentication system" user has to provide its cell phone number while registering with website. User will receive a call on registered number while login process, depending upon user's action after receiving call the further processing of authentication will be performed.

Different systems has been proposed for secure user authentication they are as follows:

Cell phone and short message service is used to thwart password stealing [3].User authentication protocol named oPass which leverages a user's cellphone and short message service to thwart password stealing and password reuse attacks. oPass only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through oPass, users only need to remember a long-term password for login on all websites. After evaluating the oPass prototype, we believe oPass is efficient and affordable compared with the conventional web authentication mechanisms. In One time password (OTP) [1] following steps are performed for system generated one time password for user to login. OTP only requires each participating website possesses a unique phone number, and involves a telecommunication service provider in registration and recovery phases. Through OTP, users only need to remember a long-term password for login on all websites.

II. LITERATURE SURVEY

The earlier systems use cell phone based authentication system but in different way, where they use sms (short message service) for user authentication. In sms based system user uses his/her selected text password for login, service provider is used for sms service. Where authentication code is sent to the user through sms. User has to manually enter the authentication code. Another system named one time password OTP [1] where sms system is used for one time password generation. In OTP the program asks the user to setup a long-term password. This long-term password is used to generate a chain of one-time passwords for further logins on the target server. Then, the program automatically sends a registration SMS message to the server for completing the registration procedure. The user uses his cell phone to produce a one-time password, server can verify and Authenticate user. The protocol starts when user wishes to log into her favorite web-server (already registered).

Manuscript Received on April 2015.

Mr. Suyog V. Patil, Assistant Professor in Department of Computer Science & Engineering, D. Y. Patil Technical Campus, Talsande, Kolhapur, Maharashtra, India

Mr. Milind M. Sutar, Department of Computer Science & Engineering, D. Y. Patil Technical Campus, Talsande, Kolhapur, Maharashtra, India.

Miss. Pooja R. Panari, Department of Computer Science & Engineering, D. Y. Patil Technical Campus, Talsande, Kolhapur, Maharashtra, India.

Mr. Avadhut A. Magar, Department of Computer Science & Engineering, D. Y. Patil Technical Campus, Talsande, Kolhapur, Maharashtra, India.

Miss. Gouri S. Nakate, Department of Computer Science & Engineering, D. Y. Patil Technical Campus, Talsande, Kolhapur, Maharashtra, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

III. System Structure

Call gateway provides a calling interface to the system where "callback authentication system" is to be used. Generally call gateways are provided by third party having special types of servers and hardware needed to implement calling and maintaining call logs along with call status.

Call gateways are available which provide the service of sending a voice message to a user's cell phone and maintain logs of all details of call status with its unique id. After completion of voice message call is rejected automatically. The call gateway is API (Application programming interface) which is integrated in the system to provide calling functionality. It contains all required functionality to provide call status with respect to each call generated. The system receives this status about each call generated by call service provider and according to this status it performs further redirection of links.

The same call gateway has been used in "callback authentication system" but with a blank message because in "callback authentication system" we need to be only call status. Log details consist of further mentioned call status queued, ringing, in-progress, completed, no-answer, busy, failed. The code has been written in JavaScript to check the call status and redirect the link. Different conditions are given in the JavaScript for redirecting the link. As it is required in "callback authentication system" that user should get access if call is accepted by him/her the conditions are given accordingly.

The conditions are dependent of the status provided by the call service provider. According to status received the further redirecting is performed. If status received is in-progress then this indicates that user has accepted the call. Condition is given in JavaScript code that, if status is completed the redirect the link to the user profile. If status is not in-progress that in all other cases redirect the link to homepage.

Architecture of callback authentication technique:

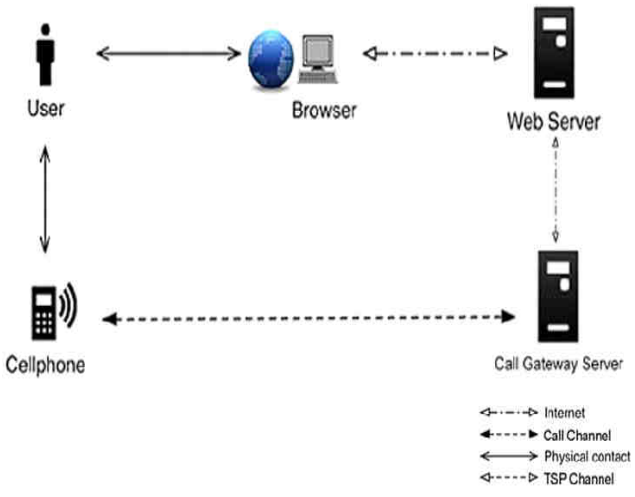

Fig.1: Architecture diagram of callback authentication technique.

User is directly interact with Browser and its personal cell phone. Browser (i.e. website) is connect to web server and phone call Gateway by internet and cell phone is connect with Telecommunication Service Provider (TSP) channel.

Flow chart of callback authentication technique:

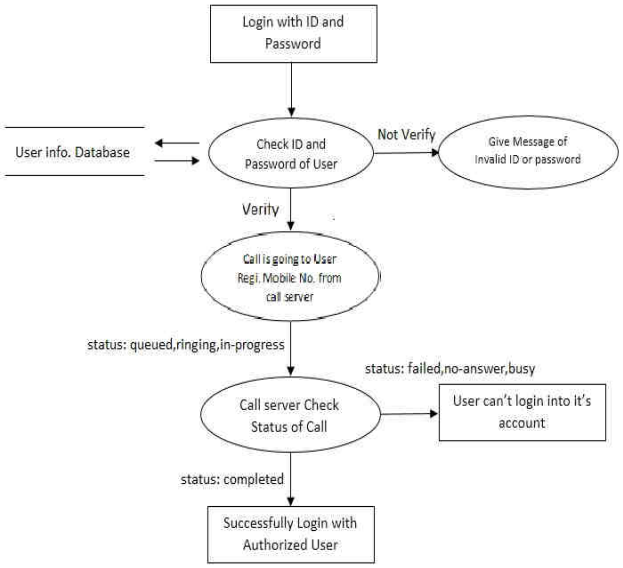

Fig.2: flow chart of callback authentication technique.

IV. Methodology

The call service providers provide calling gateways to integrate the calling functionality in the system. All the status generated by call service provider will be displayed on the user's screen. This indicates that "callback authentication process"

"Callback authentication system" performs following steps to authenticate user. User requires their own selected password and cell phone which is registered with the system.

First users recall their text password along with their id while getting access to their respective account. After entering text password server checks to see if it's valid id and password.

If the id and password entered by user is valid then further processing is performed. The next step is the call generation. After performing this validation step call service provide which has been integrated with the system generates call to the user's registered cell phone number. If the password and id entered by the user is invalid then server sends invalid password and id message to user.

Initially after validation phase user will get to see status "queued" on the screen.

At the time of actual serving of call request from queue, the status is changed to "ringing". At this stage server check a mobile connection as it is range on not. If it is in coverage area then user gets a call on his/her registered number.

If user accepts the call then status provided by call service provider will be changed to "In-process". After receiving authentication call it reject automatically and status is change to 'completed'

If user rejects or not answer the call then server send a no-answer status and authentication process will be going failed. If user's cell phone is out of coverage area then initially status provided by call service provider will be "queued". After then status will be changed to "ringing". Eventually as user is out of coverage area the status will be changed to "failed".

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

V. ADVANTAGES

Following are the advantages of using callback authentication technique:

1) In call based user authentication technique users don't need to manually type any code except password for authentication purpose.
2) Users are free to choose their own password because authentication will be on the basis of password as well as cell phone number.
3) In case if someone has stolen registered user's password and trying to get access to the account then it will get detected. If any third person enters stolen username and password then call will get generated on registered user's cell. Ultimately registered user will get to know that his/her password has been compromised and third person is trying to get access to his account.
4) As login is fully dependent of call it will be ensured that correct user is getting access to its respective account.

VI. CONCLUSION

This paper represents a user authentication system named "callback authentication" which leverages cell phones to thwart unauthorized access of user account. We assume that each user register their unique cell phone number with system. We also assume that a telecommunication service provider participates in the login phase. SMS delay occupies more than 40% of total execution time, with "callback authentication system" this delay can be significantly reduced. Users are free from manually typing the authentication code which is provided through sms in sms based authentication system.

"Callback authentication system" concept can be used in embedded systems like BMS (building monitoring system) where it can be implemented in door access control. It can also be used in banking sector, datacenter environment to thwart unauthorized access of accounts. Along with these above mentioned systems it can also be used in the systems where user authentication is crucial.

ACKNOWLEDGMENT

Support from work received from Department of Computer Science and Engineering of D. Y. Patil Technical Campus, Talsande Kolhapur, Maharashtra, India.

REFERENCES

1. "OTP: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks" by Hung-Min Sun, Yao-Hsin Chen and Yue-HsunLin proceeding IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, September 21, 2011.
2. A Survey on Password Security Systems" by Ms. A. G. Khairnar [1], Prof. N. L. Bhale [International Journal of Electronics and Computer Science Engineering]
3. oPass: A User Authentication Protocol Resistant toPassword Stealing and Password Reuse Attacks[IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 7, NO. 2, APRIL 2012]by Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin.
4. A Perrig and D. Song, "Hash visualization: A new technique to improve real- world security," in Proc. Int.Workshop Cryptographic TechniquesE-Commerce, Citeseer, 1999, pp. 131–138.
5. S. Gawand E. W. Felten, "Password management strategies for online accounts," in SOUPS '06: Proc. 2nd Symp. Usable Privacy. Security,New York, 2006, pp. 44–55, ACM.
6. D. Florencio and C. Herley, "A large-scale study of web password habits," in WWW '07: Proc. 16th Int. Conf. World Wide Web., New York, 2007, pp. 657–666, ACM


Asst.Prof.Suyog V. Patil

Asst. Prof.Suyog V. Patil received the BE Degree in Computer Science & Engineering from the SETI Panhala in 2012, He appear M.E. degree in Computer Science &Engineering in Shivaji university Kolhapur. He is currently Assistant Professor in the Department of Computer Science & Engineering, D. Y. Patil Technical Campus, Talsande, Kolhapur .His research interests include Data mining, Web mining.


Mr.Milind M. Sutar

Mr.Milind M. Sutar is final year BE (CSE) student of D. Y. Patil Technical Campus, Talsande, Kolhapur, Maharashtra, India.


Miss.Pooja R. Panari

Miss. Pooja R. Panari is final year BE (CSE) student of D. Y. Patil Technical Campus, Talsande, Kolhapur, Maharashtra, India.


Mr.Avadhut A. Magar

Mr. Avadhut A. Magar has received Diploma in Computer Engineering From D.Y.Patil Polytechnic Kasaba-Bawada, Kolhapur in 2012.and is final year BE (CSE) student of D. Y. Patil Technical Campus, Talsande, Kolhapur, Maharashtra, India.


Miss.Gouri S. Nakate

Miss. Gouri S. Nakate is final year BE (CSE) student of D. Y. Patil Technical Campus, Talsande, Kolhapur, Maharashtra, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.