Secured Authentication Using Mobile Phone as Security Token

Monalisa P. Kini, Kavita V. Sonawane, Shamsuddin S. Khan

Abstract— The inherent challenges of the security issue have become a top priority in every organization that makes use of information. Securing digital identities is getting more and more crucial. For authentication the usage of passwords is no longer sufficient because it faces most modern means of attacks and thus stronger authentication schemes are needed. Strong authentication solutions having two identification factors require often an additional device, which could be difficult for the user and costly for the service providers. In order to avoid the use of additional device, mobile phone is adopted as security token. This paper introduces a concept where mobile miss call is used as an additional password to the application. For lot of security reasons one generally requires a very secure password, to implement the same the focus of this paper is on Authentication using mobile phone as security token and a mobile missed call is a unique one.

Index Terms— Strong Authentication, Security token, Two-factor authentication

1. INTRODUCTION

In many areas such as banks, governmental applications, educational institutions, healthcare industry, military organization, etc. security has become an important aspect. The systems today depend on static passwords to authenticate the user's identity. However, management of static password has major security concerns. However, static passwords have some major management security concerns. Mostly the users make a choice of using password that are easy-to-guess passwords and write the passwords or store them on their machines, makes use of the same password in multiple accounts, etc. Furthermore, hackers have the option of using many techniques to steal passwords such as shoulder surfing, sniffing, guessing, snooping, etc.

Authentication is the use of one or more mechanism to prove that you are who you claim to be. The four levels of authentication defined by NIST (National Institute of Standards and Technology) as follows [2]:

1. Little or no confidence in the asserted identity's validity. There is no need for identity proofing on this level, but the authentication mechanism provides some assurance that the same user is accessing the data each time. It allows a wide range of authentication technologies to be used and all the token methods of the upper levels can be used. Authentication requires that the user proves to have control of the key. For example, simple password challenge-response protocols are allowed.

2. Some confidence in the asserted identity's validity. "Level 2 provides single factor remote network authentication [3]". At this level there is a need for identity proofing and need for a secure authentication protocol to prove the identity.

3. High confidence in the asserted identity's validity. "Level 3 provides multi-factor remote network authentication [3]". Identity proofing is required and authentication is based on proof of possession of key or one-time password through a cryptographic protocol. Level 3 authentication requires that the token is protected by a strong cryptographic mechanism. This prevents eavesdropping, replay, online guessing, verifier impersonation and man-in-the-middle attack. A minimum of two authentications factors are required. Soft token, hard token and one-time password token can be used.

4. Very high confidence in the asserted identity's validity. "Level 4 is intended to provide the highest practical remote network authentication assurance [3]". This level requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that both parties prove that they have control of the token. Eavesdropping, replay, online guessing, verifier impersonation and man-in-the-middle attack are prevented.

From above levels it cannot be predicted which level is strong but level 3 with multi-factor authentication is definitely considered a strong authentication. Also strong authentication does not have to be multi-factor. According to [4] strong authentication can start with two-factor authentication which combines two of the following authentication options:

- **Something you know:**
  Passwords
  Knowledge-Based Authentication (KBA)
- **Something you have:**
  One-time password tokens
  Digital certificates
  Grid cards
- **Something you are:**
  Biometrics
- **Something known about you:**
  Risk-based authentication
  Device ID

Mostly two-factor authentication solutions combine "something you know" and "something you have". This includes the use of an additional device which demands for administration from the service provider and extra care from the user or client.

The following part of this paper will be arranged as below. In section 2, the paper introduces some related work. In section 3, the proposed work and overview of entire system is described. Section 4 gives the experimental setup followed by results and discussion in section 5. Finally conclusion is given in section 6.

2. RELATED WORK

In [5] the author describes the various ways of using mobile phone as an authentication token towards service providers on the Internet. Several different authentication solutions using the mobile phone as authentication token are given, where the end result differ in complexity, strength and user-friendliness. It also provides the evaluation of the different solutions, and attacks are discussed.

The [6] focused on various digital identification schemes and motivation to integrate mobile phone as token. To establish standard for mobile token, it gives the review of current schemes and explores the security architecture for strong authentication with mobile token. To generate dynamic password for token authentication Password algorithm is developed. It also explore various authentication mechanisms to implement mobile token on different prospective. Also it describes the various test cases and evolutionary result of various attacks on suggested schemes.

In [7] the author describes four promising methods for achieving strong authentication with mobile devices. The methods are SMS-OTP, Mobile certificate, NFC and On-board Credentials. The approaches of the methods differ greatly from each other; nevertheless all of those can be used for achieving the goal of usable strong mobile authentication. Methods are compared to each other from both service providers and users point of view.

3. PROPOSED WORK

The Proposed System will allow a particular user to be authenticated only when a miss-call from a predefined number is obtained. We have used two mobile phones, out of which one will be java enabled phone connected to the computer where we are going to authenticate our application and other for providing a missed call. User won't be authenticated if call from some other number is provided. Here we connect our mobile phone to a computer where the application is running via Bluetooth. The application is created such that it runs at start-up after the OS is loaded. The application may be of different types, we are only providing a very secure login to that particular application. The number which we have already predefined act as a mobile password acts as additional password here.

As soon as the application starts it locks the screen and asks the user to enter the static Username and Password. After entering the static username and password the user have to give a miss call from the predefined number to the mobile which is connected to the machine. This number is then transferred to machine via Bluetooth from the call log information to a text file at some particular location in machine. This number along with the static username and password is checked from the database. The entire details are then verified and accordingly the user is authenticated.

The proposed system can be categorized as Client side application coding algorithm and mobile application coding algorithm.

A. Mobile Application Algorithm

1. Start
2. Include Bluetooth APIs and Micro edition APIs.
3. To start connection, create Unique ID for Serial port profile.
4. Move into discovery mode by which connection established.
5. Start search for Serial Port Profile service.
6. Retrieve Miscall no. using call log
7. Transfer the log into text file which will be sent to Server via Bluetooth.
8. Open the Bluetooth Stream to transfer data in bytes to server.
9. Once data transferred, flush the Output Stream.
10. Close the connection.
11. Stop

B. Server Application Algorithm

1. Start
2. Include Bluetooth APIs and Micro edition APIs.
3. To start connection, create Unique ID for Serial port profile.
4. Move into discovery mode by which connection established.
5. Start search for Serial Port Profile service.

6. Retrieve miscall log and hold it temporarily.
7. Read data byte by byte through Stream.
8. Close the connection.
9. Stop.

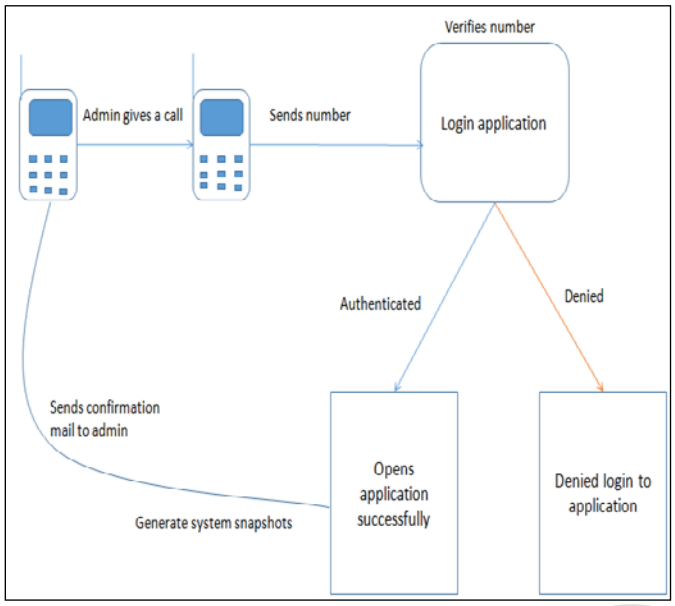

Fig 1. Proposed System Architecture

Steps involved in the entire process

Step 1:- Start the application on the computer

When user opens the application he is asked to enter details like static username and password.

Step 2:- The user whose mobile number is set as password gives a call to the connected mobile.

Step 3:- This log information (recent call record) will be transferred to the machine via Bluetooth.

Step 4:- This number is stored in a text file at some particular location of computer and is verified from the database along with the textual password to check the necessary authentication.

Step5:- If the entered details and the mobile number is same as that of stored in database, the user is authenticated or else user is denied for authentication.

Step 6:- Once the user is authenticated the snapshots of every activity performed by user is captured for a certain interval of time. These snapshots are then sent to user mobile for security purpose.

4. EXPERIMENTAL SETUP

To test the capability of this proposed system, we have used Java enabled mobile phone which will receive the miss call as an additional level of authentication apart from username and password.

Second, dummy application created in Jframe and connected to backend MySql database to store the credentials (username, password and secret key i.e. mobile no.)

Apart from this we have the application coding for retrieving the miss call from log file and a J2ME coding from which java archive file (jar) file created is transferred to Java enabled mobile phone.

5. RESULTS AND DISCUSSION

Following snapshots are showing the experimental execution of the proposed solution.

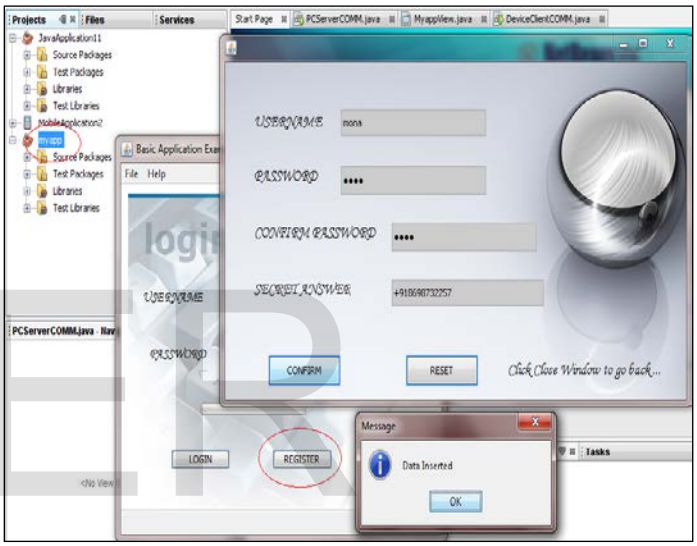

Fig 2. A dummy application for experimental purpose

Before login user needs to register by providing necessary credentials i.e. username, password & a secret key, which is our mobile number in this case that forms the 3rd level of authentication as shown in figure 2.

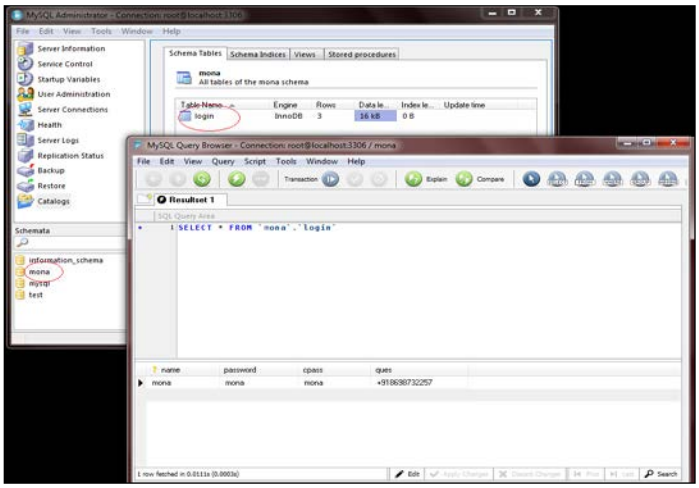

Fig 3.MySql database table

After clicking on confirm, the values are stored inside the table for validation as shown in figure 3

.

Fig 4. Java enabled mobile phones

We make the necessary setup required for establishing Bluetooth connectivity between the mobile device and computer where the application needs to be authenticated. Figure 4 shows the java enabled mobile phone that is used to connect to the machine via Bluetooth.

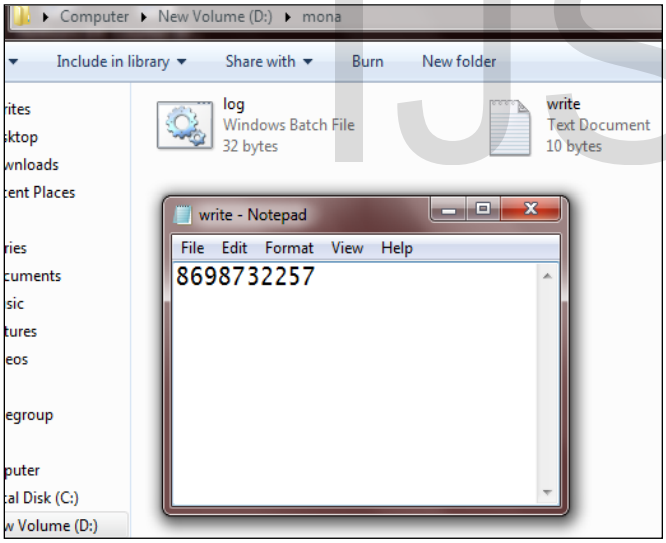

Fig 5. Directory containing a log file & text file

After debugging the application, when we provide miss call from registered number, a write.txt file is being created temporarily containing the mobile number required for 3rd level authentication as shown in figure 5.

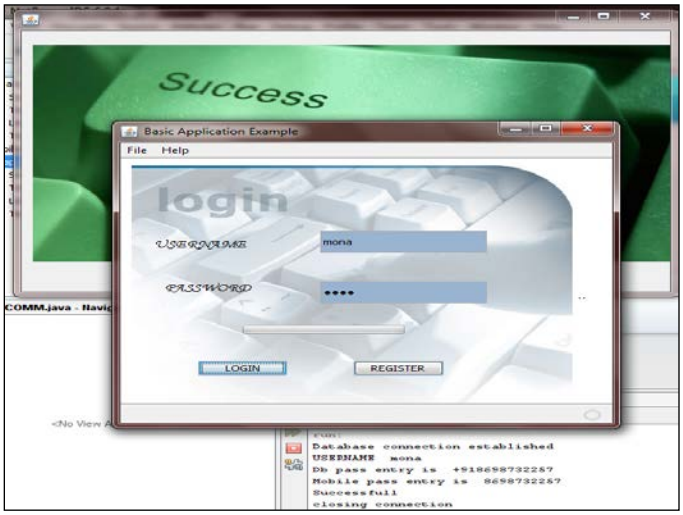

Fig 6. Application login screen

Once database registration, Bluetooth connectivity & miss call is provided, the application can now be logged in for validation of all the credentials i.e. username, password & secret key. Figure 6 shows the application login screen.

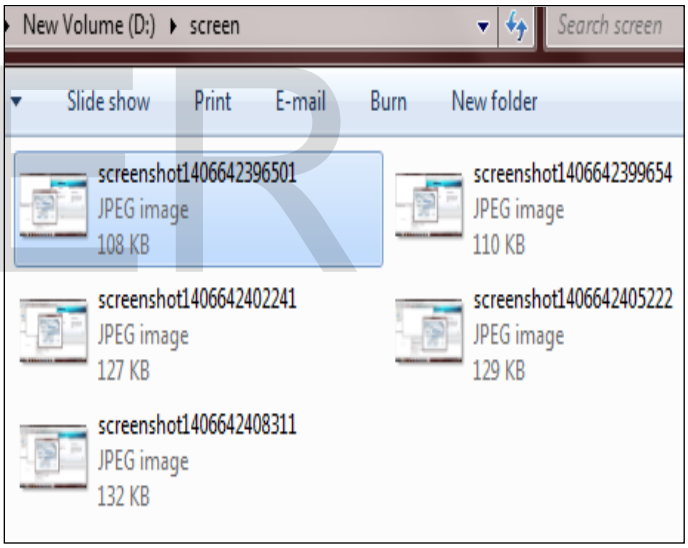

Fig 7. Directory capturing the screenshots

Once the application is authenticated, it also captures the screenshots and stores it at the specified location as shown in figure 7. Also because of the log file as shown in fig 5, write.txt file automatically get deleted for security reasons. Based on the execution of the above setup following points can be delineated.

The main feature of the application developed here is, it is not vulnerable to attacks. If the user makes an entry of wrong password or secret key it shows Unsuccessful & unable to login. Till now the work done was based on SMS, OTP which are strong but might be vulnerable to many of the attacks.

The application avoids the use of internet which prevents Sniffer attacks, also called as eavesdropping that generally occurs via internet. Here we made the use of mobile network as an additional factor of authentication. Hence it can tackle this attack. Also even if the attacker guesses username & password, it can overcome man-in-middle attack as we have an additional authentication factor i.e. missed call. Attacks like Data Modification can be avoided by securing our database as it is the main entry point for performing attack. The proposed solution has brought novelty in authentication by combining the static password with the missed call that leads to strong security.

6. CONCLUSION

Log-in applications till date requires user to enter the username and password in textual format. We have seen so many cases where the textual passwords are easily cracked and intruder breaks into the system's vital information section. As a result, private data becomes accessible and modification of these data causes great harm and financial losses to businesses.

Authentication scheme of the proposed application provides one additional level of protection in the form ofcomparing two types of passwords (textual as well as mobile number). Mobile phone ensures strong authentication as compare to other security tokens. Also it is least expensive authentication method and users don't need to remember complex passwords. This provides enhanced security to a machine and makes it difficult for the attacker to gain access to system's resources.

Thus the performance of the system can be enhanced by achieving the CIA (Confidentiality, Integrity and Availability) properties. The research work also enhances the image of the organization by securing user credentials more effectively.

ACKNOWLEDGENMENT

We would like to take this opportunity to thank all the researchers for their tremendous and valuable related work which help us to come out with this new solution. Our institute for their encouragement throughout the research work. We would also like to thank our family and friends.

REFERENCES

[1] S. Indu, T. N. Sathya& V. Saravana Kumar "A stand-alone and SMS-based approach for authentication using mobile phone," IEEE Transaction on Information Communication and Embedded Systems (ICICES), pp. 140-145, Feb 2013.

[2] National Institute of Standards and Technology (NIST), U.S. Department of Commerce: Electronic Authentication Guideline-Information Security, Special Publication 800-63-1, December 8, 2008.

[3] W. E. Burr, D. F. Dodson, W. T. Polk. Electronic Authentication Guideline. Technical Report 800-63, National Institute of Standards and Technology, 2008.<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>.

[4] T. VenkatNarayanaRao, K. Vedavathi, "Authentication Using Mobile Phone as a Security Token," IJCSET, vol 1, Issue 9, pp. 569-574, Oct 2011.

[5] Do van Thanh, IvarJorstad, Tore Jonvik& Do van Thuan, "Strong authentication with mobile phone as security token", IEEE Transaction on Mobile Adhoc and Sensor Systems, pp. 777-782, Oct 2009.

[6] Parekh Tanvi, GawshindeSonal& Sharma Mayank Kumar, "Token Based Authentication Using Mobile Phone", IEEE Transaction on Communication Systems and Network Technologies (CSNT), pp. 85-88, June 2011.

[7] PengKunyu, ZhengJiande& Yang Jing, "An identity authentication system based on mobile phone token", IEEE Transaction on Proceedings of IC-Network Infrastructure and Digital Content, pp.570-575, Nov. 2009.

[8] JanneKaavi, "Strong authentication with mobile phones", Seminar on Network Security, fall 2010.

[9] S. Uvaraj, S. Suresh, N. KannaiyaRaja, "Two Aspect Authentication System Using Secure Mobile Devices. International Journal of Wireless Communications and Mobile Computing. Vol. 1, No. 1, pp. 26-34, June 2013.

ABOUT THE AUTHORS

Ms. Monalisa P. Kini has received Bachelor's Degree in Information Technology from Mumbai University in 2012 and is currently pursuing Master's in Computer Engineering from Mumbai University. This is the first paper of his research work and area of interest includes computer security, Data Mining, Database Technologies.

Email: kinimonalisa@gmail.com

Ms. Kavita V. Sonawane has received M.E (Computer Engineering) degree from Mumbai University in 2008, currently Pursuing Ph.D. from Mukesh Patel School of Technology, Management and Engineering, SVKM's NMIMS University, Vile-Parle (w), Mumbai, INDIA. She has more than 12 years of experience in teaching. Currently working as a Assistant professor in Department of Computer Engineering at St. Francis Institute of Technology Mumbai. Her area of interest is Image Processing, Data structures and Computer Architecture. She has 28 papers in National/ International conferences / Journals to her credit. She is the member of ISTE.

Email: kavitavinaysonawane@gmail.com

Mr. Shamsuddin S. Khan is currently Assistant Professor at St. Francis Institute of Technology, Mumbai in Computer Engineering department. His areas of interests include artificial intelligence, neural network, database systems, data mining and distributed computing and have published several research papers.

Email: Shams21980@gmail.com