

Strong Authentication with Mobile Phone as Security Token (Miss-Call)

Saud I.Khan¹ Pranit R.Gharat² Swapnil J.Barge³ Prathamesh S.Kale⁴

^{1,2,3,4}Department of Information Technology

^{1,2,3,4}Padmabhushan Vasantdada Patil Pratishthan's College Of Engineering, Sion,Mumbai-400 022

Abstract— Today security concerns are on the rise in all areas industries such as banks, governmental applications, healthcare industry, military organization, educational institutions etc, with one common weak link being “passwords”. Several proper strategies for using passwords have been proposed. Some of which are very difficult to use and others might not meet the company's security concerns. The usage of passwords for authentication is no longer sufficient and stronger authentication schemes are necessary. Two factor authentication uses elements or devices such as tokens and ATM cards. We have proposed to resolve the password problem, which could be inconvenient for the user and costly for the service providers to combat otherwise. To avoid the usage of additional device, the mobile phone is adopted as security token. In this paper several different authentication solutions using the mobile as authentication token are discussed, where these solutions vary in complexity, strength, security and user friendliness. One of the authentication schemes (OTP solution) is implemented to verify their usability. Hence, a classification and evaluation of the different solutions is provided according to defined criteria.

Key words: Two-factor authentication, Security token, UPIF, IMSI, IMEI, one time password (OTP)

I. INTRODUCTION

With the increase in popularity of the Internet the number of frauds and abuses is literally exploding. Most serious is the theft of identity which causes grave damages both for the victim and also his entourage such as employee, banks, hobby clubs, etc. The protection of digital identities is getting more and more crucial. The usage of passwords for authentication is no longer sufficient and stronger authentication schemes are necessary. Strong authentication solutions require often two identification factors i.e., in addition to the first factor "something you know" represented by passwords it is introduced a second factor "something you have" materialized by a security token. The introduction of the additional device could be costly for the service providers in terms of deployment and administration at the same time as it could be inconvenient for mobile users. Furthermore, there is very little re-use or sharing such that the same security token can be used for several systems. To remedy the situation, here we have Proposed a authentication solution to avoid usage of extra device by re-using existing devices, namely the mobile phone or the SIM cards. This paper starts with a clarification of the notion of authentication in section II. The architecture of the two factor authentication solutions using mobile phone is given and the different authentication solutions are successively described in the sections III. The design implementation for the authentication system is provided in the sections IV and V along with the evaluation schemes.

II. AUTHENTICATION

Authentication is the assurance that the communicating entity claims to be genuine. According to Fermi Lab [1], authentication is a form of computer security in which the identities of networked users, clients and servers are verified without transmitting passwords over the network. The four levels of authentication [2] defined by NIST as follows:

- 1) Little or no confidence in the asserted identity's validity. There is no need for identity proofing on this level, on this level it is sufficient with a simple password challenge response protocol.
- 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]". At this level there is need for a proof of possession and a minimum of two authentication factors.
- 4) Very high confidence in the asserted identity's validity. "Level 4 is intended to provide the highest practical remote network authentication assurance [3]". At this level there is need for proof of possession through a cryptographic protocol. It is not specified which authentication level can be considered as strong but level 3 with multi-factor authentication is definitely considered as a strong authentication. It is also clear that strong authentication does not have to be multi-factor. According to strong authentication can start with two-factor authentication which combines of the following authentication options [4]:
 - Something you know, e.g. Passwords.
 - Something you have, e.g. One-time password tokens and Digital certificates.
 - Something you are, e.g. Biometrics.

Most of two-factor authentication solutions combine "something you know" and "something you have". They require the usage of an additional device, which demands administration from the service provider and extra care from the user. Multi-channel communication is another way to further improve the security of an authentication scheme.

III. THE DIFFERENT MOBILE PHONE AUTHENTICATION SOLUTIONS

To authenticate users through a mobile phone requires certain components to be placed. Figure 1 shows the required components and the general architecture [6] needed for the solutions described in this paper to work.



Fig. 1: A general architecture of mobile authentication

The user must access to a computer connected to the internet and be in possession of a mobile phone with a working SIM card. If the computer and mobile phone are equipped with Bluetooth, higher usability can be obtained. Through the Internet browser on the computer the user can access web services provided by service providers. The service provider (SP) is connected to an Authentication Server (AS) that will handle the authentication on behalf of the SP. The AS is connected to the GSM network which enables it to communicate with the user's mobile phone and the operator's Authentication Center (AUC). The AS is composed of two parts, an authenticator and an AAA server. The authenticator communicates with the client and relays messages to the AAA server which handles the authentication. When designing an authentication scheme which uses two separate devices that communicate over two different networks it is very important to ensure that it is the same user that controls both devices. This is done by ensuring that there is a "closed loop" going through all the components involved in the authentication as illustrated in Figure 1. The loop starts in the device requesting the service, the user's computer, goes through the network with SP and AS and then via mobile phone and back to the initial device, either by user interaction or Bluetooth.

A. SMS Authentication with Session-ID Check;

This solution exploits that a user with a valid mobile subscription is already authenticated through the GSM system. Session IDs are used to ensure that it is the same user that controls both the computer and the mobile phone. When the user accesses a service provider a unique session ID is created and sent both to the user's computer and to the mobile phone. The session ID is sent over the Internet to the computer and shown in the web browser and sent to the phone by SMS. Then the user can confirm that the session IDs match and send a confirmation by SMS to the service provider. When receiving the confirmation from the user the AS knows that the user is in possession of the phone and the authentication is successful. The comparison of the session ID can be made by the user or automatically by software if the phone is connected to the computer by Bluetooth.

B. User Verification of Session ID:

The user accesses the service provider through the Internet browser and chooses to be authenticated by his mobile phone. The user identifies him with his mobile phone number and the request is redirected to the authentication

server. The authentication server then creates a unique session ID and sends this to the user by SMS and over the Internet to the computer. The user checks that the session ID in the SMS is the same as the one shown in the browser. If this is the case the user replies by sending an SMS back to the AS confirming that the session IDs match. When receiving the confirmation the authentication server redirects the browser back to the service provider and the user is given access to the service. The message exchange is shown in Figure 2.

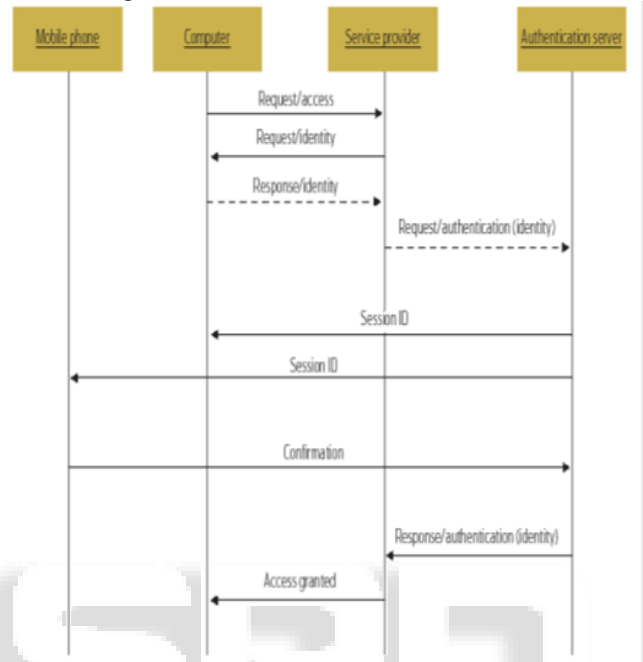


Fig. 2: Session ID check

C. Automatic Check of Session ID:

To make it even easier for the user the session ID can be checked automatically. This can be done by pairing the mobile phone and the computer by Bluetooth.

D. One-Time-Password:

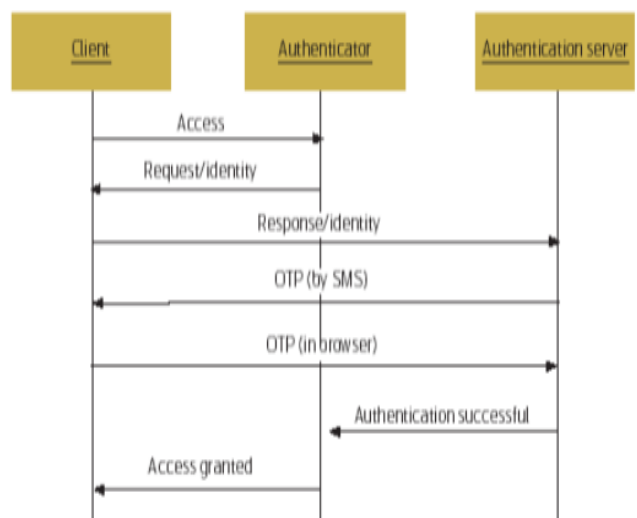


Fig. 3: OTP Check

One-Time Password is one of the simplest and most popular forms of two-factor authentication today. This solution builds on the same principle as the session ID check, that a user with a working phone is already authenticated through

the GSM network. The difference is that the check is done by the server and therefore relieves the user from this burden. The user starts the authentication procedure by entering his username. The session is redirected to the AS which creates an OTP based on the user's identity by a cryptographic hash function. The OTP is then sent to the user by SMS. When receiving the SMS the user types the OTP in the browser. The AS verifies that the OTP is correct and redirects the browser back to the service provider and the user is logged in. Figure 3 shows the message exchange of this solution.

In this paper, we proposed a design implementation of TP[5].

IV. DESIGN IMPLEMENTATION

The proposed system is secure and consists of three parts:

- (1) Software installed on the client's mobile phone,
- (2) Server software, and
- (3) A GSM modem connected to the server.

A. Proposed System:

The Proposed System will allow a particular user to be authenticated only when a miss-call from a predefined number is obtained. User won't be authenticated if call from some other number is provided.

1) **Application for login**

Username:

Password:

2) Password

PC will scan this text box for the entry of predefined mobile number.

- 3) Compare the password with password in database
- 4) If it matches user is authenticated else not authenticated.

B. Advantages of Proposed System:

- Least expensive authentication method to use.
- Enhance the image of the organization by securing user credentials more effectively.
- Users don't need to remember complex passwords.
- Can be used for login and transaction authentication.

V. EVALUATION

This section provides an evaluation of the different authentication solutions [6] using the mobile phone as authentication token. The evaluation is performed according to the following criteria:

- Strength & vulnerability
- Cost
- User friendliness.

The different authentication solutions can be subject to attacks in several areas, depending on the specific scheme:

- 1) On the mobile phone
- 2) Across the Bluetooth connection
- 3) On the computer
- 4) Across the Internet connection
- 5) Across the connection between service provider and authentication server
- 6) On and between GSM network components and connections.

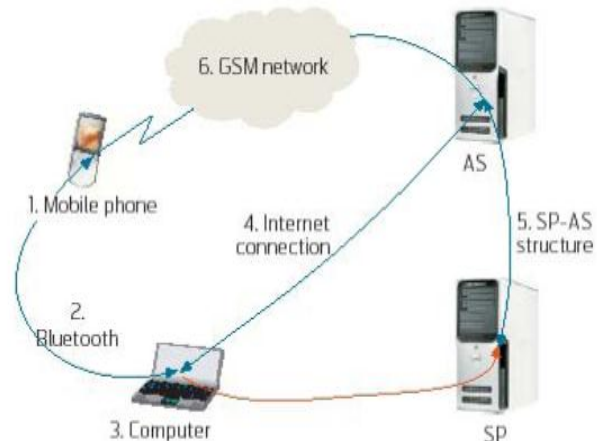


Fig. 4: Possible points of attacks

The above figure illustrates the possible points of attacks in the architecture.

VI. RESULT

Our successfully completed project has the ability to perform all the functions that were desired by us.

- User registers itself by choosing the desired sername and password(both textual and desired mobile-number).
- While performing the authentication, both the passwords are checked carefully.
- Miss-match of any one the passwords does not allow user to log in.

A. Snapshot:

1) Login Page:



Fig. 5: Login Page

2) Register Page:

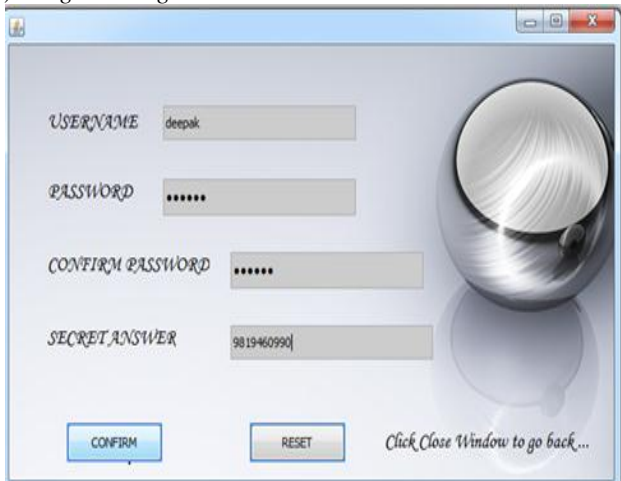


Fig. 6: Register Page

3) Failed Login Attempt:



Fig. 7: Failed Login Attempt

4) Successful Login:



Fig. 8: Successful login

VII. CONCLUSION

Thus through our project we have developed an application which provides two levels of security by considering not only the textual password but also a unique mobile number which the user chooses. At the time of login, user needs to receive a mis-call from the number which he/she defines in the database along with the textual password. Only if both the passwords match, user gets authenticated to the system. Since the application is a stand-alone application, it can be integrated with other authentication schemes to provide enhance security.

VIII. FUTURE SCOPE

Future Scope of this project can be to extend it to other mobile OS platforms like Android. Also we can combine the feature of miss-call with SMS to provide higher means of protection.

REFERENCES

- [1] Fermi National Accelerator Laboratory, Office of Science / U.S Department of Energy: Strong Authentication at Fermilab, Sept 2006
- [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] CA.Managing strong Authentication: A Guide to Creating an Effective Management System, 2007.
- [5] Fadi Aloul, Syed Zahidi and Wassim El-Hajj “Two factor authentication using mobile phones” in Pro 2009 IEEE/ACS International Conference on Computer Systems and Applications, ISBN: 978-1-4244-3807-5.
- [6] Do van Thanh; Jorstad, I Jonvik, T, Do van Thuan “Strong authentication with mobile phone as security token” in Pro Mobile Adhoc and Sensor Systems, 2009. MASS '09. IEEE 6th International Conference on.
- [7] SMSLib. Available at <http://smslib.org/>
- [8] Pernilla Stolpe Johansson “Economic aspects of web authentication”in Project Report for Information Security Course Linköping University, Sweden. In 2011.
- [9] Steffen Hallsteinsen,Ivar Jorstad, and Do Van Thanh “Using the mobile phone as a security token for unified authentication” in Pro Second International Conference on Systems and Networks Communications (ICSNC 2007).