OSAP: Online Smartphone's User Authentication Protocol

Rabia Riaz[†], Sanam Shahla Rizvi[††], Erum Mushtaq[†††], Sana Shokat[††††]

[†,†††,††††]Department of CS & IT, University of Azad Jammu and Kashmir, Muzaffarabad, 42714, Pakistan
[††]Department of Computer Sciences, Preston University, 15, Banglore Town, Shahrah-e-Faisal, Karachi, 75350, Pakistan

Summary
Internet services have become an essential part of our daily activities. Due to rapid technical progress mobile web browsing has become a reality now. User authentication is a vital component in most systems that need to assure security of services and data. A weak authentication mechanism enables hackers to steal user information or bypass authentication. In some services, such as online banking, strong authentication is needed to protect the service provider as well as the users of the services.
In this research paper, a user authentication scheme for mobile devices has been proposed for Smartphone applications. The results clearly indicate that the proposed authentication scheme provide protection from attacks such as man-in-the-middle attack, shoulder surfing attack, dictionary attack, spoofing and manipulation. It also overcomes the drawbacks of internet banking authentication system and WhatsApp such as PIN eavesdropping and time synchronization. Also it authenticates the users as well as devices. It is efficient in time and user friendly.

Key words:
IMEI, OTP, Smart Phones, Steganography, Authentication.

1. Introduction

With the growth in popularity of the internet, online frauds and abuses are increasing at an exponential pace. Most serious among these is the theft of identity that causes immense damage both for the victim and its associates such as employees, banks, health providers, etc. Mobile devices are often used by an on-the-go user, in public places, in short sessions, and using less robust user interfaces. Authentication tasks in this environment become more intrusive, less intuitive, and more frequent than in traditional computing environment. Due to the sensitive nature of information they carry [1], they are susceptible to various kind of attacks.

Authentication can be broadly categorized into three basic types. The most commonly used is authentications based on something that one knows, generally a password. The second type is authentications based on something that one has, such as a smart card. Third type is based on something that a person is, an immutable personal characteristic for example finger print. Strong authentication solutions need at least two identification factors for example something you know a password and secondly something you have is security token [2].

Use of extra device for authentication could be expensive for the service provider; as it can be difficult to deploy and manage and at the same time it could be problematic for mobile users [3].To remedy the situation, an authentication solutions has been proposed that avoid introducing extra device by re-using existing devices, such as the mobile phone or the international mobile equipment identification (IMEI). The IMEI is a 15-digit number that is used to recognize the device on mobile networks. There is a regulatory requirement for each mobile device to have a unique identifier and the IMEI number is used for that purpose.
In present study a user authentication scheme for mobile devices has been designed to improve security flaws of existing schemes. The proposed authentication scheme can be helpful in improving overall system performance.

2. Literature Review

To authenticate the user in WhatsApp, verification SMS containing a 3-digit PIN is sent to the phone by server. The user then copies that code into the WhatsApp application's GUI. It founds that the phone number verification process of WhatsApp can very easily be intercepted and hijacked [4]. It is possible for an attacker to take control of any WhatsApp account; this can be achieved by entering victim's phone number during the "verification phase" and then intercepting the communication between the phone and the server to eavesdrop the PIN. Although this communication is SSL-protected; but the attacker has to capture only the connection between the phone and sever of WhatsApp. When attacker has entered the PIN into his device the victim's WhatsApp account is linked to the attacker's phone. In this way attacker can send and receive messages from the victim's account. It also unlinks victim's phone so that it cannot receive messages from the victims account and Man-in-the-Middle attack (MITMA) occurs in this situation [4].

Authentication security is very essential in internet banking. The mobile phone is used here to generate a token for authentication. Token number is generated by

Manuscript received March 5, 2017
Manuscript revised March 20, 2017

applying the SHA algorithm and XOR operation. The user contact number, IMEI number, PIN number and international mobile subscriber identity (IMSI) number were incorporated to produce token number. A six digit token number is generated. The token number is then sent to the user mobile. To do the banking operation, token number is then used. New token number is generated for every time period. After three attempts, if user fails to provide correct PIN then account gets blocked and cannot be accessible by user [5].

A new authentication method called Σ-hash was proposed that combines an efficient steganographic algorithm and hashing. The Σ-hash scheme involves three steps: hashing, embedding and Σ -Hashing. In this method, hash function (H) of original message (M) is calculated (e.g., see Eq. 1). This value is then embedded into the original message by steganographic algorithm and it becomes stego object MS (e.g., see Eq. 2). Again hash function is applied to this stego object, result is HS. The final hash function that will be used is produced by XORing H and HS (e.g., see Eq. 3). To verify the validity of original message inverse steganographic function is performed at receiver side [6].

$$fh(M) = H \quad (1)$$

$$F_s(M, H, H) = M_S \quad (2)$$

$$\sum\text{-}Hash = H \; XOR \; H_S \quad (3)$$

3. Proposed OSAP Algorithm

The online Smartphone's user authentication protocol (OSAP) consists of two modules. Client side where client provides data and confirms back to server. Server side where server is responsible for PIN generation, PIN encryption and authentication of user.

OSAP uses user details like 11 digit contact number, 15 digits IMEI number and 4 digit Pass code to register the client at server. Contact number and Pass code are entered manually by the user but IMEI is auto-retrieved for the mobile device. PIN is generated at server side and least significant bit (LSB) technique of image steganography is then used to hide the PIN inside cover image.

Server saves the IMEI number and its associated PIN in its database and sends the image to user; user decrypts the image and retrieves PIN and IMEI number. To assure that legitimate user has intercepted the PIN and PIN is intercepted by same device that initiated the communication, user confirms the PIN back to server. When user presses confirm button IMEI is again auto-retrieved and XORed with PIN before being send. IMEI is never entered manually by the user during whole authentication process. Server receives this XORed value and recovers PIN by XORing this value with IMEI that it is stored in its database. Server then compared this PIN with the original PIN that it has generated and if both are same, user is successfully authenticated, else authentication is not granted. Table 1 shows the list of abbreviations used in Fig. 1 which describes the working of OSAP Algorithm.

Table 1: List of Abbreviations

Abbreviation	*Definition*
C_N	Contact Number
I_N	IMEI Number
P_C	Pass Code
C_{N5}	first five letters of C_N
I_{N7}	first 7 letters of I_N
P_{C3}	first 3 letters of P_C
I_U	Concatenation of C_N and P_C
A	XOR PIN with IMEI at user side
A'	XOR A with IMEI at server side
P	PIN

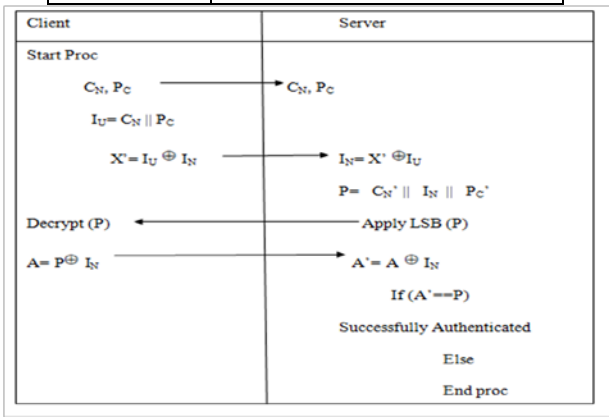

Fig. 1 OSAP Algorithm.

4. Security Analysis

4.1 Phishing Attacks

Phishing is a specific attack designed to steal user authentication details. If an attacker obtains the steganographic image he will have to XOR his IMEI with PIN for authentication. This XORed PIN is then sent to server for confirmation. Server authenticates the PIN by XORing this PIN with IMEI that it has saved earlier from original user. Since attacker IMEI will be different from original users, a different PIN will be generated. This will not match at server side thus attacker will not get authenticated.

4.2 Dictionary Attacks

It tries to guess its decryption key by assuming millions of possible options like a word in a dictionary. In our scheme

authentication PIN is not based on alphanumeric strings so dictionary attacks are fully evaded.

4.3 Brute Force and Cryptanalysis

The proposed scheme defends against Brute force attacks. In case if attacker was able to retrieve the cipher after a successful steganlaysis attack, still the attacker requires the user's device IMEI which is secure and only original user knows it. Authentication is done at server side so this second phase of authentication prevents from brute force attacks.

4.4 Shoulder Surfing

In shoulder surfing attack, attacker uses direct observation techniques, commonly this is used to get passwords, PIN, security codes, and similar data. In the proposed system, if the attacker sees the phone number and random code entered by user he cannot use it for registration purpose. PIN will be generated at server. Thus proposed system is resilient to shoulder surfing attacks.

4.5 Content Injection Attack

Content injection attack refers to an attack in which an attacker inserts malicious contents. In OSAP initially user has to enter data and sent to server. Server will generate the PIN and client will receive it and just confirms the PIN back to server, in this process no hacker can insert the data to PIN so chances of this attack are also eliminated by OSAP.

4.6 Guessing Attacks

Guessing attack is another eminent strategy used by the intruders. Even if the attacker tries to guess the password; the random number used in our proposed system makes our system resilient against guessing attacks since user has a chance to select a random number of his own choice. Even if the attacker tries on guessing the numbers it would be of no use since he can change random numbers for every login attempt. Hence the probability of successful guessing attacks is very low.

5. Results and Discussions

5.1 Comparison of OSAP and WhatsApp for authentication

Table 2 gives a comprehensive comparison of OSAP and WhatsApp authentication mechanism against message communication and security resilience for various attacks.

Table 2: Comparison of OSAP with WhatsApp

Observed Attributes	OSAP	WhatsApp
No of messages communicating	3	3
Encrypted passwords	LSB steganography	No
Man-in-the-middle attack	No	Yes
Spoofing/Manipulation	No	Yes
PIN entry by user	No	Yes

In WhatsApp user enters phone number after some time user receives SMS from server that contains 6 digits. User then enters this code into verification GUI and server authenticates the PIN. This PIN will change every time the user comes with different number or mobile device. The maximum time limit for reception of this SMS from server is 5 minutes.

In OSAP average time of authentication of any user is two minutes and fifty one seconds. So OSAP provides faster authentication and it is time efficient, see Fig. 2.

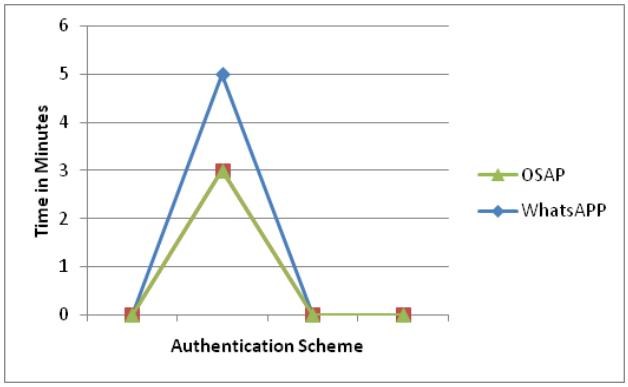

Fig. 2 Execution Time comparison of OSAP and WhatsApp.

5.2 Comparison of OSAP and Online Banking System

A secure communication in Smartphone's using two factor authentications [7] is purely internet banking user authentication scheme. It has client /server architecture. When user enters his username and password and press login button server receives request. One-time-password (OTP) algorithm runs and client submitted OTP matched with server side's OTP. If both are same next page is opened at website and server side pin is displayed to user. Then user compares his phone's pin and server's pin. In case both were same then he enters his real password for accessing account.

We compared authentication mechanism in internet banking with OSAP. Table 3 gives a comprehensive comparison of both schemes.

6 Experimental Results of OSAP

OSAP was executed on a Smartphone with Windows-8 operating system see Fig. 3 and Fig. 4 for client and server side respectively.

Execution results shown in Table 4 and Table 5 clearly indicate that OSAP authenticates the valid users. When the PIN is received unaltered from server by the client then the user was authenticated successfully. But if PIN is altered by some malicious intruder during transmission then even the valid user was not able to get authentication from the server. These results also indicted that OSAP was resilient to interception as well as man-in-the-middle attack. In Table 5, unsuccessful authentication of users is due to two reasons; if user received an incorrect PIN and if device is changed, i.e. IMEI is different, then user will not get authenticated.

Table 3: Two factor authentication comparison with OSAP.

Security Parameters	Two Factor Authentications	OSAP
Online registration	No	Yes
PIN eavesdropping	Possible	No
Two factor authentication	Yes	Yes
Two factor Authentication parameters	Password and PIN	PIN and device
OTP generation unit	Mobile phone	Server
Time synchronization required	Yes	No
Needs Extra devices	No	No
SMS –Cost overhead	No	Yes
SMS delivery delays	No	Possible
User entry of PIN	Yes	No

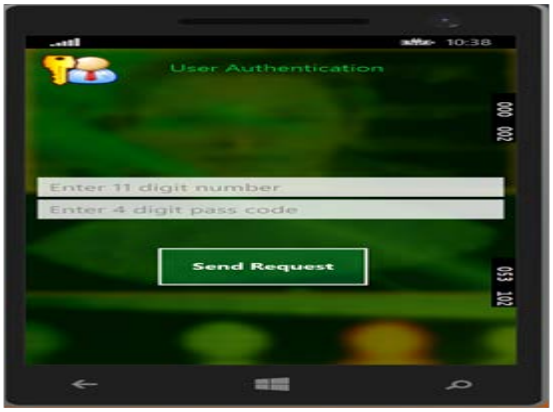

Fig. 3 Client side OSAP

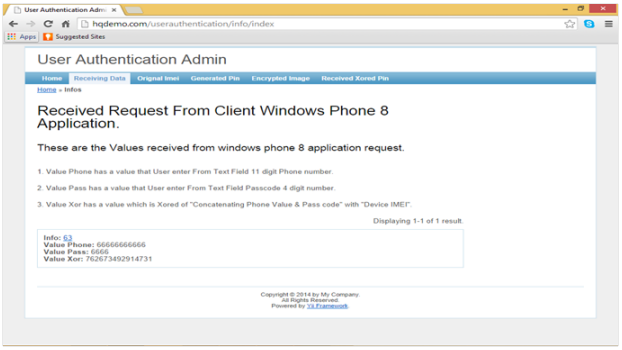

Fig. 4 Server side OSAP

7. Conclusion

We found that OSAP authenticates only legitimate users. It does not require extra devices and it is efficient in time. OSAP is a good choice for Smartphone applications that do not require a permanent username and password combination for user login. OSAP use image steganographic LSB for hiding the PIN, for future extension, audio or video Steganography can also be used instead. Many strong cryptographic mechanisms can be used for data security purpose as new Smartphone's are launched with enhanced processing capabilities.

References

[1] S.S. Rizvi, T.S. Chung. "VAQAR: Flash memory based long term in-network vital data sustainability and availability for data centric wireless sensor network applications." Proc. IEEE Youth Conf. Inf. Computing and Telecom., pp. 363-366, 2009.

[2] J. Kaavi. "Strong authentication with mobile phones," presented at Aalto University, T-110.5290 Seminar on Network Security, 2010.

[3] S. Acharya, A. Polawar, and P.Y.Pawar. "Two Factor Authentication Using Smartphone Generated One Time Password." IOSR Journal of Computer Engineering (IOSR-JCE), vol .2, pp. 85-90.2013.
[4] S. Schrittwieser, P. Fruhwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. Weippl. "Guess who's texting you? Evaluating the security of Smartphone Messaging applications." in Network and Distributed System Security Symposium, 2012.
[5] P.Y. Pawar, S. Acharya, A. Polawar, P. Baldawa, and S. Junghare. "Internet Banking Two Factor Authentication using Smartphone." International Journal of Scientific & Engineering Research, vol. 4, pp. 1-4.2012.
[6] G. Sumalatha, and P. Madhuravani." A Novel Steganographic Algorithm and Hashing to Improve Authentication using Mobile Phones." Special Issue of International Journal of Computer Science & Informatics **(**IJCSI), vol. 2, pp. 181-186.2012.
[7] Murali, S., B. Anitha. and A.Paul.. "A Secure Communication in Smartphones using two factor Authentication" International Journal of Research in Engineering and Technology, vol. 2, issues 2, pp.153-157. 2013.

Rabia Riaz working as assistant professor in university of Azad Jammu and Kashmir. She is currently chairperson of department of Software Engineering. She holds a PhD in electrical engineering from AJOU University, South Korea. Her research interests include, wireless network, sensor networks, data security, encryption and authentication mechanism.

Sanam Shahla Rizvi received the B.C.S. degree in Computer Science from Shah Abdul Latif University, Khairpur Pakistan, in 2003, and the M.C.S. degree in Computer Science from KASBIT University, Karachi Pakistan, in 2004, and M.S. degree in Computer Science from Mohammad Ali Jinnah University, Karachi Pakistan, in 2006, and Ph.D. degree in Information and Communication Engineering from Ajou University, Suwon, South Korea, in 2010. She is currently working as associate professor at Department of Computer Sciences at Preston University, Karachi, Pakistan. Her research interests include flash memory storages, data management, database systems, indexing structures, and wireless sensor networks.

Sana Shokat received her MS (Software Engineering) degree from Bahria University Islamabad. She is currently candidate of P.h.D degree at University of Azad Jammu & Kashmir, Muzaffarabad, Pakistan.

Table 4 Successful authentication of valid users

Contact number	*IMEI number*	*Pass code*	*PIN number*	*PIN sent by user*	*Result*
03449540840	*951342790070039*	*8907*	*034499513427890*	*034499513427890*	*Successful*
03469632872	*22889283906568*	*3456*	*034692288928345*	*034692288928345*	*Successful*
03215494206	*589624617732441*	*6780*	*032155896246678*	*032155896246678*	*Successful*
03469705846	*345937184720517*	*5420*	*034693459371542*	*034693459371542*	*Successful*
03345494206	*465810197313767*	*7865*	*033454658101786*	*033454658101786*	*Successful*

Table 5 Unsuccessful authentication of invalid users

Contact number	*IMEI number*	*Pass code*	*PIN number*	*PIN sent by user*	*Result*
03425724396	*61515574068383*	*9087*	*034256151557908*	*034256151559708*	*Unsuccessful*
03009540840	*879064532165432*	*6754*	*030098790645675*	*030498790456758*	*Unsuccessful*
03339632872	*908764567323909*	*5632*	*033399087645563*	*033399087044563*	*Unsuccessful*
03089705846	*215679087465432*	*8907*	*030892156790890*	*030892176795890*	*Unsuccessful*
03125724396	*890754321890654*	*4532*	*031258907543453*	*031258905549458*	*Unsuccessful*