The scheme of personal privacy protection based on data separation in Mobile identity authentication

Fang Zheng¹, Pingzhen Li² and Jianqin Wei*¹

¹,²,³ Department of Information, Shanxi University of Finance & Economic, Taiyuan, Shanxi, 030006, China

*Corresponding author’s e-mail: alice20110324@126.com

Abstract: To avoid privacy leaked in mobile identity authentication by telephone number, this paper proposes a scheme of data separation that separates telephone number from server of service provider and stores it on trusted third-party server. In the process, we put forward some ideas to solve the problems brought by this scheme, which includes a table introduced to associate real identity and network one, a way of access authorization. Finally, we analyze the performance of the scheme and discuss the time efficiency by experiment.

1. Introduction

With the smart phone widely accepted, many mobile apps are developed such as hotel reservation, train and flight reservation, online reading, the reservation of the online hospital registration etc. Almost every service is related with telephone number. As one of user identities, telephone number is widely used for identity authentication when users log in, register, retrieve password, locate in mobile apps, compared to traditional complex registration process, which is greatly convenient to users by sending message authentication code. But at the same time many personal privacy problems arise [2].

One kind of attack to personalized privacy is privacy leaked by untrusted service providers which may collect [4] user information or publish [3] or sell [5] them without data desensitization. The second attack is inference attack by machine learning [6].

The contributions of this paper are as follows:

First: This paper introduces TTPS (Trusted Third Party Server) and the technique of data separation, which is to separate telephone number from SSP (Server of Service Provider) and store it on TTPS to protect privacy and avoid untrusted service providers to leak it;

Second: This paper proposes a method that binds telephone number with pseudonym together in a table on TTPS as a link between real information and network one. Whenever users want to log in, register or find password by telephone number or by pseudonym, TTPS and SSP can identify them as the same user, which doesn’t influence recommendation by pseudonym;

Finally: this paper proposes a way of access authorization. For being TTPS introduced, in this framework, it is TTPS that communicates with SMS Platform, not SSP, but the service of SMS Platform is purchased by SSP not by TTPS. This paper proposes a way of granting SSP access to SMS Platform to TTPS.

The rest of this paper is organized as follows: section 2 is related work; section 3 describes some concepts and application scenarios before introducing TTPS. Section 4 details in our approach. Section 5 analyses performance from security. Section 6 discusses the time efficiency by experiment. Section 7 concludes our scheme and looks forward to the future work.
2. RELATED WORK

[7] proposes a model named k-anonymity for protecting privacy, which introduces third party anonymizer to make k-anonymity algorithm. [1] describes personalized k-anonymity model, architecture and algorithms for protecting location privacy. [8] introduces trusted third party server to protect data or communicate safely. [9] presents a technique of anatomy which is releasing quasi-identifier and sensitive information in two separate tables to protect privacy. This paper borrows the technique of trusted third-party server and the technique of anatomy to preserve privacy. But trusted third-party server in literature [7] [10] knows all activity information of the user and when it is compromised, the user’s all information will be leaked.

3. APPLICATION SCENARIOS

There are two ways for identity authentication when users log in, register or locate, etc. One way is by pseudonym and the other is by telephone number. This paper is only to discuss the second. Figure 1 shows the scenario and the work process is as follows:

1) User fills in the telephone number in mobile client app and submits it to SSP for SMVC (Short Message Verification Code);
2) SSP generates SMVC and returns it to user in the form of short message through SMS Platform.

![Figure 1. The process of short message validation](image1)

4. OUR WORK

4.1 The introduction of TTPS

To avoid privacy information leaked, this paper introduces TTPS to store the telephone number which is separated out from SSP. The architecture graph is shown in Figure 2. Except the telephone number, pseudonym and RSSN (Random Session Serial Number) are together saved on TTPS in the form of a table, which we call it link_info. The definition of link_info table is as follows: link_info (id, TelNum, userId, RSSN, stamptime).

On the definition above, id is a sequence number, TelNum represents telephone number, userId is a pseudonym, RSSN is a unique random serial number to denote this session and stamptime is timestamp.

4.2 The work process of the scheme

The work process of Figure 2 is as follows:

![Figure 2. The process of message validation after TTPS introduced](image2)
From step ① to step ②, TTPS gets the telephone number from request packet of mobile client apps and queries the value of userId in the link_info table stored on itself by telephone number. If it is not the first time to visit SSP, there is a record about the telephone number, userId in the table. If it is the first visit, there is not the historical record about the telephone number in the table. So the query result is null. In this situation TTPS will assign null to userId. After that, TTPS will make a RSSN randomly, inserts a new record {id, TelNum, userId, RSSN, stamptime} into the link_info table. Then TTPS will reconstruct a new packet of request, made of {userId ||RSSN|| stamptime}, in which telephone number has been filtered out, and then send it to SSP. Table 1 shows the data in the link_info table in this process.

Table 1. The data structure and values of link_info table

| id  | TelNum       | userId | RSSN  |
|-----|--------------|--------|-------|
| 1   | 13228394032  | alice222 | 1231212 |
| 2   | 15638298493  | _top23_ | 1029384 |
| 3   | 18627453940  | Null   | 15895248 |

Table 2. The data structure and values of user_info table

| id  | userId | password |
|-----|--------|----------|
| 1   | alice222 | ***      |
| 2   | _top23_ | ***      |
| 3   | sysu234 | ***      |

In this table userId is not null in record 1, 2, indicating that it is not the first visit to SSP, while null in record 3, meaning that it is the first visit to SSP.

From step ③ to step ⑤, after receiving the request from TTPS, SSP will get the values of userId and RSSN, make a SMVC, reconstruct a packet which is made up of {SMVC||userId||RSSN} and send it to TTPS.

During this process, if the value of userId from TTPS is null, which means it is the first time for the user to visit SSP, the scenario of which is analogous to registration, SSP will make a system userId for the user, adds it in the table, which we give a name user_info, which records information of all users having visited the server. The definition of user_info is as follows:user_info(id, userId, password).

In this definition there are two kinds of sources about the value of userId. One source is registered by user with pseudonym, the value of which is given by user itself and the other is assigned by SSP, the value of which is a system Id, when user visits SSP firstly by phone number. Table2 shows the content of user_info. In this table, the value of userId in Row1, 2 is given by user itself and that in Row 3 is assigned by system.

4.3 SSP grants access to SMS Platform to TTPS

In the fourth step in Figure 2, TTPS sends {SMVC||TelNum} to SMS Platform. But SMS Platform does not recognize TTPS. It is SSP not TTPS that purchases the service from SMS Platform. How to let SMS Platform provide service for TTPS? SSP needs to authorize its access to SMS Platform to TTPS. This paper proposes a suitable way to solve it, the process of which is as follows:

SSP signs SMVC as M with its private key and transfers M and its identifier: ID_SSP, which has been registered in SMS Platform, to TTPS:

\[
M \leftarrow \text{Sig}_{\text{privkey}}(\text{SMVC});
\]

• TTPS forwards it with the time stamp to SMS Platform;
• SMS Platform will make verification. It decrypts M as u with the public key of SSP, then compares u with SMVC and judges the result if it is equal. If the result is true and time is not outdated, then access is allowed, otherwise it is rejected.

5. Security analysis

5.1 Preserve privacy data not to be leaked by the untrusted service providers
In this paper, TTPS is introduced and privacy data: telephone number, separated from SSP is stored on TTPS, which protects privacy and makes it impossible for the untrusted service providersto sell or publish data without desensitization.

5.2 TTPS will not leak the users’ detailed activities provided by SSP
TTPS takes effect only when identity authentication happens and after authentication is finished, the mobile client will directly communicate with SSP without going through TTPS. Therefore, TTPS doesn’t know the user’s detailed activity information, such as flight ticket booking, doctor’s appointment, etc. except telephone number and pseudonym. So, even TTPS is compromised, for password cannot be gained, the attacker could not log in SSP and get the activities of the users.

6. EXPERIMENT
The experimental environment is Intel® Core™ i5-825U CPU @ 1.60GHz and 8.00GB RAM. We develop a TTPS program and simulate to accept the request from client mobile and SSP and initiate 20 threads in a thread pool of MySQL database. We collect time that is consumed on each process of request and respond, when n takes a different value. For each n, we issue 10 requests, and get 10 time values. In figure 3, x-axis represents the number of request, and y-axis represents request to respond time, with millisecond as its unit. Every curve represents a different n. In figure 3, from small to big, the value of n respectively is 10,000, 50,000, 100,000, 500,000.

![Figure 3. The graph of the number of request and request and response time when n takes different value](image)

Figure 3. The graph of the number of request and request and response time when n takes different value

![Figure 4. the average request and response time varies with n](image)

Figure 4. the average request and response time varies with n

Figure 4 is the graph of average request and response time varying with the value of n. From the graph we can know the average time is roughly 8s when n is equal to 500,000. So in formula (4), the value of T2-T1 is about 8s. That is, after TTPS introduced, the total time is 8s longer than the original time. In general, the valid time is set 60 seconds in short message verification. So generally, more than 8 seconds will not affect the normal operation of the system too much. Therefore we consider this scheme to be feasible from time aspect.

7. Conclusion
In this paper we proposes a scheme of privacy protection in mobile identity authentication, which prevents information leak brought by a series of attacks because of telephone number leaked, and put forward many ideas to solve the problems met in this scheme. From performance analysis and experiment, it proves that this scheme is feasible.
Acknowledgment
This work is partly supported by the youth fund of Shanxi University of Finance & Economics under grant no. QN2015014, Shanxi soft science research project under grant no. 2018041039-2 and Teaching reform project of Shanxi university of finance and economics under grant no. 2018226.

REFERENCES
[1] Gedik B, Liu L. Protecting Location Privacy with Personalized k-Anonymity: Architecture and Algorithms[J]. IEEE Transactions on Mobile Computing, 2008, 7(1):1-18.
[2] George T. Duncan, Thomas B. Jabine, and Virginia A. de Wolf, editors. Private Lives and Public Policies.National Academy Press, 1993.
[3] Samarati P. Protecting respondents identities in microdata release[J]. IEEE Transactions on Knowledge & Data Engineering, 2001, 13(6):1010-1027.
[4] Sarigol E, Garcia D, Schweitzer F. Online privacy as a collective phenomenon[C]// ACM Conference on Online Social Networks. ACM, 2014:95-106.
[5] BJullieny. Privacy and protection. http://www.cresse.info.
[6] Zheng Y, Jia L, Cao H. Multi-Objective Gene Expression Programming for Clustering[J]. Information Technology & Control, 2012, 41(3):283-294.
[7] LATANYA SWEENEY. k-ANONYMITY: A MODEL FOR PROTECTING PRIVACY[J]. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 2002, 10(05):557-570.
[8] Dan A, Iyengar A K, Kumar M. System and method for providing trusted services via trusted server agents: US, US 6823456 B1[P]. 2004.
[9] Xiao X, Tao Y. Anatomy: simple and effective privacy preservation[C]// International Conference on Very Large Data Bases. VLDB Endowment, 2006:139-150.