SOP3: Service Oriented Privacy Preservation Protocol for Mobile Networks

[1]Rinkal Ambasana, [2]Nilesh Padhariya, [3]Srikanth Venkatesh
[1,3]Dept. of IT, PIET, Gujarat, India
[2]Dept. of Computer Science, AITS, Gujarat, India

Abstract
Mobility is a key to personal freedom. Thus, the emergence of privacy has gained considerable importance in mobile networking. Privacy is to be considered as a state of limited access to an entity. Privacy is required in mobile networks for on-demand services in the various forms such as content privacy, identity privacy, location privacy, authentication etc. The main concern about privacy in different services have arisen due to mobile constraints and its wide-spread explorations. We have proposed the service-oriented privacy preservation protocol (SOP3) for different services in mobile networks using encryption-based privacy-preservation techniques and attempt to identify the directions for future research.

Keywords
Service-Oriented Architecture, Privacy Preservation, Authentication

I. Introduction

Mobile Network provides the facilities operated by a carrier for the purpose of performing various public mobile telecommunications services. In revolution, third generation onwards, mobile networks offer any service anywhere at any time. Mobile networks have far more vulnerabilities than the traditional wired networks, in which security is hard to achieve in the mobile network than in the wired network. In this, the network privacy is the main requirement for confident of their usages. Here, privacy means right of the personal to be protected against intrusion into his personal life by physical means or by information publishing. Some challenges in mobile networks are the open, nondeterministic nature of web and, secure information flow of many web-based transactions that involve the transfer of personal information. HTTP provides the ability to cover data leakage through secured network connections for webmail, instant messaging, blog posts, or updates to social networking sites.

In a similar vein, the preservation of data is equally important in the mobile networks. Here, preservation means the activity of protecting something from loss or threat. In the mobile network preservation means the process of protecting the data against unauthorized access due to open-access environment.

Additionally, protocol refers to the recognized code of procedure or behaviour in any group, organization or situation. The data loss in mobile network requires the privacy. Various free online services have become ineradicable parts of Internet world. There are many online services like web search (Google search engine), web-based email (Hotmail, Gmail), Social network (Face book, Whatsapp), video sharing (YouTube) and many more which require user's privacy to be preserved on the go. Such services are become common on mobile devices in current time and hence the preservation protocol need to be imposed to provide data privacy at user's end for flawless migrations across the different mobile-based services. In this paper, we have proposed the service-oriented privacy preservation protocol named as SOP3 to perform restricted and wise information access by mobile services, while protecting user's data at its best.

In recent days, cryptography is no longer restricted to secure sensitive services information but recognized as one of the key components of the safekeeping strategy of any organization. For privacy issues, various encryption algorithms based on symmetric-key or asymmetric-key are used.

We consider the approach of providing privacy to the user's data by means of encrypting the information on mobile. For providing unique encryption on each device, we consider a unique and unambiguous key, so called IMEI number of a mobile device. IMEI (Internet Mobile-station Equipment Identity) is a unique number used by a GSM network to identify the validity of a device in the mobile network. It is 56 bits (14 decimal digits) long. Few mobile applications such as whatsapp (http://www.whatsapp.com) uses the IMEI as a password on a mobile device.

This proposal discusses the research carried out in the partial fulfilment of master degree of Information Technology. The rest of the paper has been discussed as follows. We have presented the detailed related work in Section 2. While, In Section 3, we explain the architecture of SOP3. The privacy preservation protocol has been defines and explained in detail in Section 4. Finally, we have concluded in Section 5 along with the future directions towards extension of SOP3.

II. Related Work

In this section, we review the previous works related to privacy preservation approaches in wired and wireless networks. Notably, a variety of approaches to protect privacy for different service in mobile network have been proposed.

A. Privacy

Nowadays mobile devices have become very powerful and ubiquitous. Users of mobile networks may require privacy to avert an attacker from their private information, such as where they are, where they work, whom they communicate with and what they discuss [1].

Unluckily, users are often unaware that they are making their private information available to a company. Once a user uploads their facts, who owns it? What does the service do with that information? What steps does the service obtain to ensure the confidentiality and accessibility of the data? [6].

Millions of users have joined social networking sites, adding profiles that make public personal information. From that situation question arise that is it possible to join a network of millions of people and be able to belief all of them? This does not seem practical. Since people are obviously joining networks, what role does trust play in the use of social networking sites? [10].

Use of mobile device and mobile network causes risk to privacy preservation. Privacy can imply many things depend on the context of the condition [1]. Privacy can be divided with different concepts: information privacy, bodily privacy, privacy of communications, and territorial privacy. Todd P. Glidden defines four privacy requirements as: content privacy, identity privacy, location privacy, and authentication. He applies the virtualization

technique for content privacy protection.

In mobile sensing network for problem of privacy preserving Ling Hu and Cyrus Shahabi [8] have define HP3 (Hot-Potato Privacy-Protection) Algorithm in which data is first sent to one of the friend of the user and then that friend will choose another friend to send the data to the subsequently hop. They propose a key to user privacy preserving crisis in a participatory sensing network.

Users of mobile networks may require privacy so as to prevent an attacker from learning information of individual.

Services requires privacy in mobile network

Demonstrable Privacy is not only for users of service, but it also good for service itself. If a service never stores users' information unencrypted, then that service is indemnified from attacks on their own infrastructure [6]. There are many services in mobile network which requires privacy at data transfer within the network. Online social networks have become necessary part of internet access for these years. These networks help user to share information with their friends. Even users assign the social network provider with such personal information as sexual preferences, phone numbers, opinionated and religious views, occupation, photographs and identities of friends.

C. Existing Protocol

The privacy preserving prediction based routing protocol in which it forwards messages by comparing information about community of nodes instead of individual nodes [3]. Another Secure and Privacy-Preserving Authentication Protocol propose a new protocol for node authentication, message confidentiality and an anonymization scheme for privacy protection of users in WMNs (Wireless mesh networks) [4]. By combining Shamir secret sharing scheme and homomorphism encryption, Zheng Qiang [5], have proposed the first protocol for privacy-preserving set pattern matching in the cryptographic model; it is provably secure against a semi-honest adversary under the decisional Diffie-Hellman assumption.

D. Encryption Techniques

The encryption techniques can be classified in two classes:

Traditional encryption techniques are pen-and-paper based techniques developed in a time when computers did not survive, some of these techniques have been altered into computer-based algorithms [10].

For the sake of information, we have provided the timeline of the era of encryption in Table 1.

Table 1: Timeline for Encryption Methods

2003	Use of quantum encryption
2000	AES
1993	Blowfish
1991	Quantum encryption system
1984	Quantum encryption protocol
1978	RSA
1977	DES
1976	Public key encryption
1970	Lucifer algorithm

III. Architecture

This section discusses the design of our novel protocol towards privacy presentation. The main objective of this research is to develop and propose a new scheme, an authentication mechanism for SOP3.

In mobile network, node sends data only to one of its directly connected node. That node may transmit the data to another connected node and so on. In wireless mobile network end to end routing path cannot be assumed to exit between source node and destination node.

We propose the architecture for the privacy preservation in mobile network. Figs. 1, 2, 3 and 4 show privacy requirements for different services, which are video sharing, call service, web-based services and social networking.

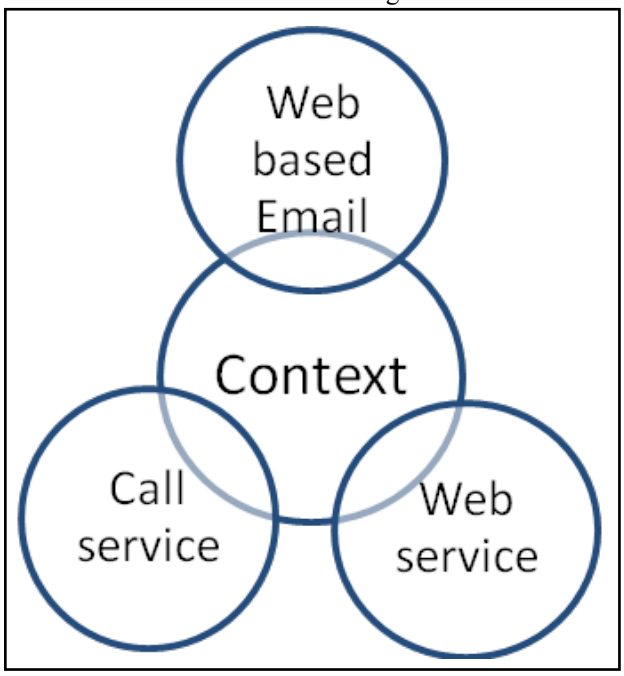

Fig. 1: Service Requires Context Privacy

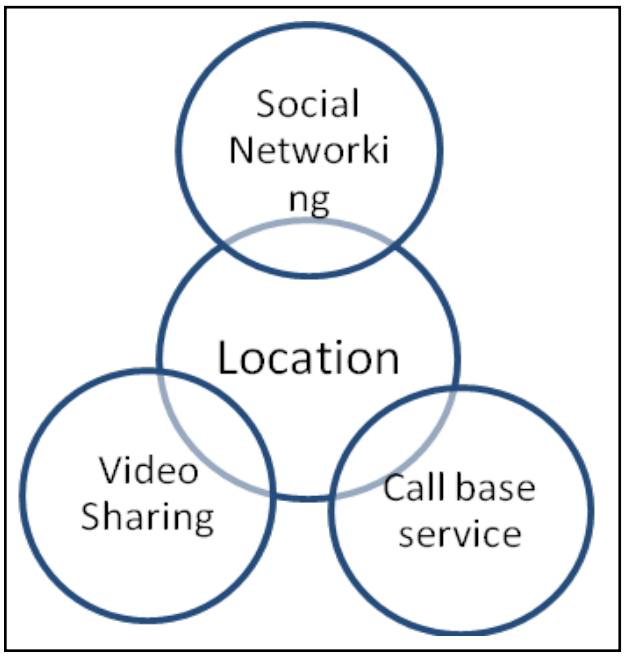

Fig. 2: Service Requires Location Privacy

In social networking the authentication is required to check information in the exhibit appear on the website, whether the posting can be adequately shown to have arisen from the source.

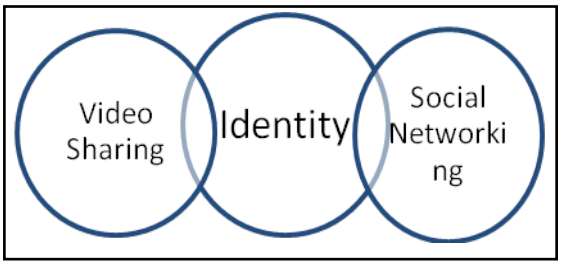

Fig. 3: Service Requires Identity Privacy

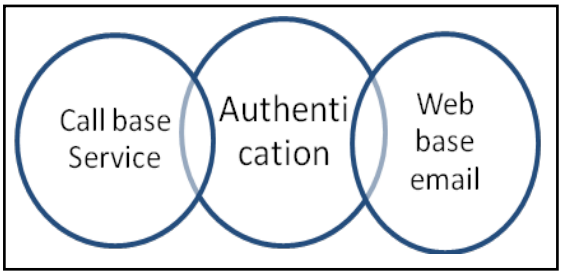

Fig. 4: Service Requires Authentication Privacy

After considering the scenario shown in Table 1 for privacy requirements we design the protocol for mobile node in the network, in which they pass the information through different nodes.

Table 1: Scenario of Different Service in Mobile Networks

Service	Location	Identity	Context	Authentication
Social Networking	✓	✓		✓
Video Sharing	✓	✓		
Web based Email	✓		✓	✓
Call service			✓	✓
Web service			✓	✓

For the sake of understanding, consider an example as follows. Let's consider, x1, x2 and x3 are friends; x1 wants to send private message about third person say z1 to x2 but not to x3. Here they all are friends so message should be communicate privately between x1 and x2 in such a way that x3 can't interpret that message. For that, x1 sends message that contains only one portion of the information; name of that person (z1) in one session, then another part of message; the name of event related to z1 in second session, so that x3 cannot interpret that message as a whole. This can be demonstrated as shown in fig. 5.

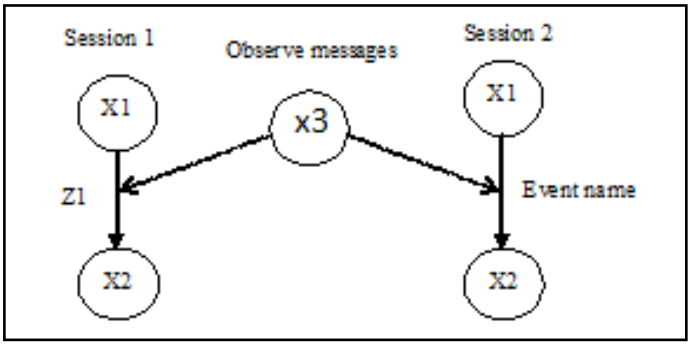

Fig. 5: Message Passing Between x1 and x2; x3 can't get the Message

For the above example, we use the IMEI number as encryption key for our encryption method to provide secure transmission of the information across the users in open-access network. Hence, to avoid unauthorized access to the information.

IV. Proposed Protocol

In this section we consider all the service as generalized form and take the above example for transaction in mobile network which requires privacy.

When two peers want to communicate the super peer is required for authentication of peer. So let we take x1, x2 are mobile peers in mobile network and s1 is the superior or super peer for the mobile network. Based on these considerations we have proposed the following protocol as SOP3.

Participants: x1, x2 and s1, where x1 and x2 are peers and s1 is a super peer

Input: (1) m, a message, (2) IMEI number, encryption key (3) psw, password required for authentication (4) ack, for acknowledgement (5) fin, finish statement

Output: Message m is delivered to the node x1! = x2, if psw(x1) = psw(x2)

Setup: Nodes in mobile network activated

1. x1 sends message m1 to s1
2. S1 checks for authenticate user
3. S1 sends message m1 to x2
4. If psw(x1) != psw(x2)
5. S1 send message m2 to x1 and x2 for wrong psw
6. else psw(x1) == psw(x2)
7. then x2 sends ack1 to s1
8. S1 sends message m1 to x1 with ack1 of x2
9. X1 find IMEI number
10. X1 send message m3 to x2 encrypted with IMEI of x1 $E(pr_{x1}\ m2)$
11. S1 send message m3 to x2
12. X2 decrypt message m3 with public key of x1 $D(pu_{x1}\ m2)$
13. X2 send ack2 to x1
14. Repeat step 10 to 13 for more messages
15. X1 send fin to x2
16. X2 send ack3 to x1
17. End.

In SOP3 protocol, the simple scenario for message transfer between two peers. The super peer in network handles the communication process between them. Every message passed between different nodes passed through s1, so for that peers on network should be authenticated for transmission process. In protocol s1 authenticate peers by password matching. If the password match then and then only transaction occurs otherwise not. The Sequence for the transaction flow of algorithm is shown by the sequence diagram as shown in fig. 5.

Here encryption technique is used for privacy issue. Asymmetric key encryption algorithm is used for this protocol in which he IMEI number of x1 is used as encryption key. The private key of x1 is passed to KDC (Key Distribution Center) to pass the key to x2. We have chosen IMEI number because this number is not known to other than mobile device holder. If the mobile device is hand-held PC such as tablets then MAC address is used instead of IMEI number.

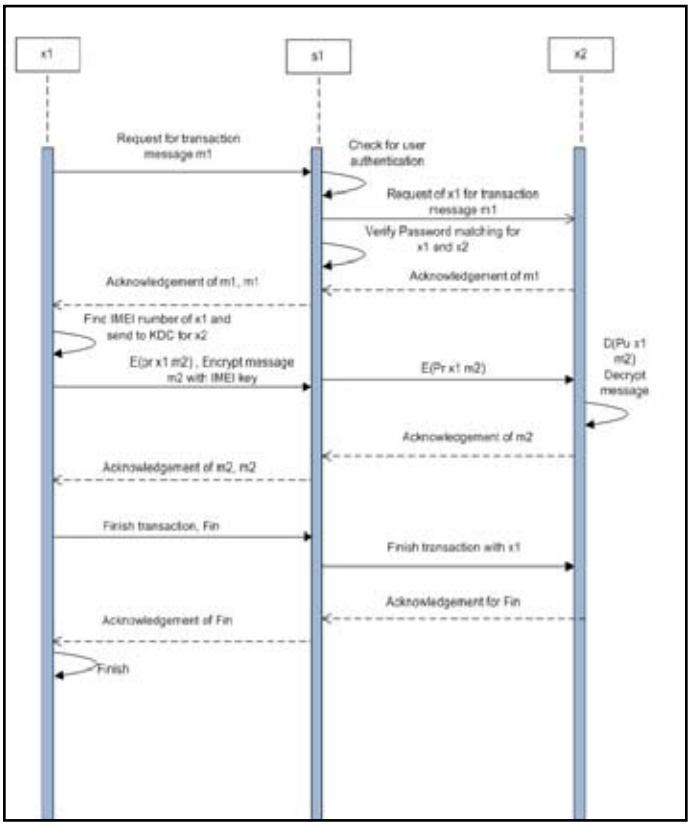

Fig. 5: Sequence Diagram for SOP3 Algorithm

V. Conclusion

Social networking sites are quite popular, and are beginning to attract the attention of academic researchers. In mobile network all service requires privacy at each level. In this paper we propose a protocol for privacy preservation for on-demand service in mobile network. The algorithm which uses encryption technique can be easily implemented in mobile environment.

Service oriented privacy is not only to prevent illegal access to user information, but also to ensure not abuse genuine access to user information. In future work we will study about more services and attacks in mobile network.

VI. Acknowledgment

My deepest gratitude goes first and foremost to my guides for their constant encouragement and guidance. They have walked me through all the stages of the writing of this research paper. Without their consistent and illuminating instructions, this research could not have reached to its present form.

I sincerely appreciate experts and professors for spending their valuable time to review this research work.

References

[1] Todd P. Glidden,"Privacy for mobile networks via network virtualization", OMB No. 0704-0188, March 2009

[2] WJ Buchanan, Z Kwecka, E Ekonomou,"A Privacy Preserving Method Using Privacy Enhancing Techniques for Location Based Services", Mobile Networks and Application, Springer, 2012.

[3] Hasan, Omar, et al.,"A Privacy Preserving Prediction-based Routing Protocol for Mobile Delay Tolerant Networks", 2012.

[4] Sen, Jaydip,"Secure and Privacy-Preserving Authentication Protocols for Wireless Mesh Networks", arXiv preprint arXiv:1209.1803 2012.

[5] Qiang, Zheng, et al.,"Protocol for Privacy-Preserving Set Pattern Matching", Multimedia Information Networking and Security, 2009. MINES'09. International Conference on. Vol. 1. IEEE, 2009.

[6] Baden, Randy, et al.,"A Case for Addressing Privacy Problems with Technical, not Legislative, Solutions".

[7] H. Van Kranenburg,"Privacy aspects in Internet and mobile services", November 28, 2000.

[8] Hu, Ling, Cyrus Shahabi,"Privacy assurance in mobile sensing networks: go beyond trusted servers", Pervasive Computing and Communications Workshops (PERCOM Workshops), 2010 8th IEEE International Conference on. IEEE, 2010.

[9] Morkel, T., J. H. P. Eloff.,"Encryption Techniques: A Timeline Approach", Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria 2.

[10] Dwyer, Catherine, Starr Roxanne Hiltz, Katia Passerini, "Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace", Proceedings of AMCIS. 2007.