International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Email:editorijoer@gmail.com http://www.ijoer.in

Vol.4., Issue.3., 2016
(May-June)

RESEARCH ARTICLE

ISSN: 2321-7758

SECURE END TO END MESSAGE PROTOCOL

V.ANITHA MOSES[1] , M.DIVYA BHARATHI[2]
[1]Associate Professor, [2]PG Student
Department of MCA
Panimalar Engineering College

ABSTRACT

The short message service (SMS) is organism in a lot of daily life applications, including healthcare monitoring, mobile banking, mobile commerce, and so on. But when we send an SMS from one mobile phone to another, the information contained in the SMS transmit as plain text. Sometimes this information may be confidential like account numbers, passwords, license numbers, and so on, and it is a major drawback to send such information through SMS while the traditional SMS service does not provide encryption to the information before its transmission. Proposition an efficient and secure protocol called Easy SMS, which provides end-to-end secure communication through SMS between end users. The working of the protocol is presented by considering two different scenarios. The analysis of the proposed protocol shows that this protocol is able to prevent various attacks, including SMS disclosure, over the air modification, replay attack, man-in-the middle attack, and impersonation attack. The Easy SMS protocol generates minimum communication and computation overheads as compared with existing protocols. Maintain that Easy SMS is the first protocol completely based on the symmetric key cryptography and retain original architecture of cellular network.

INTRODUCTION

The secure end to end messaging protocol is a protocol that keeps the messages in a secured manner. The messages cannot be viewed as the normal message till we enter the key. The key will only be known by the users who are authenticated. The unauthenticated users can only be able to view the encrypted form of the message. This helps us to create and send the confidential messages to others. Because it need a key to view the normal form of the message only the sender and receiver can able to create and view the message. If any other user is trying to view the message it will only be in the encrypted form. To prevent the messages from various attacks like SMS disclosure, over the air modification, replay attack, man-in-the middle attack, and impersonation attack.

Related Works

Community health workers (CHWs) have been shown to be an effective and powerful intervention for improving community health. Routine visits, for example, can lower maternal and neonatal mortality rates. Despite these benefits, many challenges, including supervision and support, make CHW programs difficult to maintain. An increasing number of mHealth projects are providing CHWs with mobile phones to support their work, which opens up opportunities for real-time supervision of the program.

Potential transportation users also need information about its availability. In the developed world, users can often access information about bus and train schedules easily via printed schedules or web pages maintained by centrally-funded transportation authorities. In many cases, users can view real time updates on the current location and expected arrival time of their bus or train via web, phone, or SMS/text message. These solutions rely upon central infrastructure to provide the servers needed to collect data and answer queries.

The Short Message Service (SMS) is one of its superior and well-tried services with a global availability in the GSM networks. The main contribution of this paper is to introduce a new secure application layer protocol, called SSMS, to efficiently embed the desired security attributes in the SMS messages to be used as a secure bearer in the m-payment systems. SSMS efficiently provides confidentiality, integrity, authentication and non-repudiation for the SMS messages.

The transformation of telecommunications networks from homogeneous closed systems providing only voice services to Internet connected open networks that provide voice and data services presents significant security challenges. For example, recent research illustrated that a carefully crafted DoS attack via text messaging could incapacitate all voice communications in a metropolitan area with little more than a cable modem. This attack highlights a growing threat to these systems; namely, cellular networks are increasingly exposed to adversaries both in and outside the network combination of modeling and simulation to demonstrate the feasibility of targeted text messaging attacks. Under realistic network conditions, we show that adversaries can achieve blocking rates of more than 70% with only limited resources.

Existing System

There are some more issues related to the open functionality of SMS which can incapacitate all voice communications in a metropolitan area, and SMS-based mobile botnet as Android botnet. SMS messages are transmitted as plaintext between mobile user (MS) and the SMS centre (SMSC), using wireless network. SMS contents are stored in the systems of network operators and can be read by their personnel.

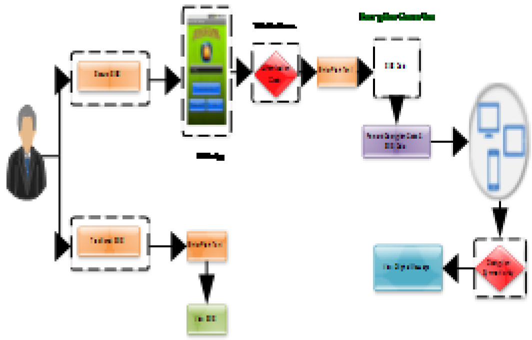
Occasionally send the confidential information like password, pass code, banking details and private identity to our friends, family members and service providers through an SMS. But the traditional SMS service offered by various mobile operators surprisingly does not provide information security of the message being sent over the network. In order to protect such confidential information, it is strongly required to provide end-to-end secure communication between end users. SMS usage is threatened with security concerns, such as SMS disclosure, Man-in-the-middle attack, Replay attack and Impersonation attack.

Drawbacks

The SMS is sent as plaintext, thus network operators can easily access the content of SMS during the transmission at SMSC. This leads to SMS disclosure attack. In traditional cellular network, the OTA interface between the MS and the Base Transceiver Station (BTS) is protected by a weak encryption algorithm (such as A5/1 or A5/2), thus an attacker can compromise these algorithms to capture the information contained in the SMS or can alter the SMS information. The attacker can also try to cryptanalyze the generated cryptographic keys used in the authentication protocol.

The attacker may fraudulently delay the conversation between both MS and can capture or reuse the authenticated information (during the protocol execution) contain in previous messages which results in the form of replay attack. Later, the attacker may send the captured information to the server or can modify the sequence of messages for getting the authentication token. An attacker can also perform a man-in-the-middle attack when an MS is connected to a BTS through wireless network and eavesdrops the session initiated by legitimate MS.

System Architecture



Proposed System

An assortment of cipher algorithms are implemented with the proposed authentication protocol. Recommend that the cipher algorithms should be stored onto the SIM as well as at AS. Since providing security needs to do some extra effort which is measured in terms of cost, thus providing or adding extra security means increasing more cost. Propose to include one more service as 'Secure Message' in the menu of mobile software developed by various mobile companies. Mobile operators can add some extra charges to send secure message by their customers over the networks. Whenever a user wants to send a secure message to other user, the proposed protocol namely EasySMS is executed which makes available the symmetric shared key between both MS and then ciphering of message takes place using a symmetric key algorithm.

A new protocol named EasySMS with two different scenarios which provide end-to-end secure transmission of information in the cellular networks. First where both MS belong to the same AS, in other words share the same Home Location Register (HLR) while the second where both MS belong to different AS, in other words both are in different HLR. There are two main entities in the EasySMS protocol. First is the Authentication Server (AS), works as Authentication Center (AuC) and stores all the symmetric keys shared between AS and the respective MS. In this paper, we refer AuC as the AS. Second entity is the Certified Authority/Registration Authority (CA/RA) which stores all the information related to the mobile subscribers.

Advantages

The proposed protocol shows that this protocol is able to prevent various attacks, including SMS disclosure, over the air modification, replay attack, man-in-the middle attack, and impersonation attack. The EasySMS protocol generates minimum communication and computation overheads as compared with existing protocols.

Conclusion

EasySMS protocol is successfully designed in order to provide end-to-end secure communication through SMS between mobile users. The analysis of the proposed protocol shows that the protocol is able to prevent various attacks. The transmission of symmetric key to the mobile users is efficiently managed by the protocol. This protocol produces lesser communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged ratio during authentication than SMSSec and PK-SIM protocols.

Reference

[1]. R. E. Anderson *et al.*, "Experiences with a transportation information system that uses only GPS and SMS," in *Proc. IEEE ICTD*, no. 4, Dec. 2010.

[2]. B. DeRenzi *et al.*, "Improving community health worker performance through automated SMS," in *Proc. 5th ICTD*, 2012, pp. 25–34.

[3]. M. Toorani and A. Shirazi, "SSMS—A secure SMS messaging protocol for the m-payment systems," in *Proc. IEEE ISCC*, Jul. 2008, pp. 700–705.

[4]. P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating attacks on open functionality in SMS-capable cellular networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 40–53, Feb. 2009.