International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 7
July 2017

Secure SMS: Advanced Version of Cyber SMS

Sabeela K S, Neelesh Gupta, Abhishek Agwekar
Truba institute of Engg.&
InformationTechnology,karond, gandhinagar
bypassroad Bhopal

Abstract—Nowadays, short message service (SMS) is being used in many 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. In this paper, presented an efficient and secure technique called secure SMS. The working of the protocol is presented by considering the asymmetric key cryptography . The analysis of the proposed technique 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

Keywords -- — Authentication, security, SMS, symmetric key, cipher SMS, cryptography.

I. INTRODUCTION

Short Message Service (SMS) has become one of the fastest and strong communication channels to transmit the information across the worldwide. On December 3, 2013, SMS service has completed its 21 years as on December 3, 1992, the world's first SMS was sent by Neil Papworth from the UK through the Vodafone network . The SMS are used in many real world applications as a communication medium such as in Transportation Information System, MobileDeck ,SMSAssassin, SMS-based web search such as SMSFind, and so on. Sometimes, we 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 variousmobile 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 messages are transmitted as plaintext between mobile user (MS) and the SMS center (SMSC), using wireless network. SMS contents are stored in the systems of network operators and can be read by their personnel.

Organization

This paper has organized into VI sections. Section II presents literature review of the work done related to SMSsecurity. In section III, a new protocol is proposed which provides end-to-end secure transmission of SMS in cellularnetworks. Section IV illustrates the analysis of proposedprotocol. Section V, discusses suitable symmetric algorithmforsecure SMS protocol. Finally, section VI summarizes conclusion of the work.

II. LITERATURE SURVEY

Various cipher algorithms are implemented with the proposed authentication protocol.The cipher algorithms should be stored onto the SIM (part of MS) 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.And it does not provide channel security

Easy SMS that has end-end secure communication through SMS between end users. The working of the protocol is presented by considering two different scenarios. Authors claim that secure SMS is the first protocol completely based on the symmetric key cryptography and retain original architecture of core cellular network. Protocol reduces of the bandwidth consumption and reduces of message exchanged time during the authentication process in comparison to SMSSec and PK-SIM protocols respectively a Protocol for End-to-End Secure Transmission of SMS.Brief SMS flow is given for the Existing system.

In this paper presented SMS-based system for providing transit information based solely on existing cellular and GPS networks. The aim is to permit the development of information services that do not rely on a central authority or complex web hosting. We developed and applied our system to the network of privately-run marshrutka buses in Bishkek, Kyrgyzstan. However, our goal is to more broadly address issues of ad-hoc shared transportation systems in the developing world. A custom designed GPS-GSM unit is placed on a vehicle, and users can query our server over SMS with their own non-GPS enabled cell phones.Report the accuracy of our location naming approach and estimates of bus arrival times. In addition, we summarize interviews with bus drivers and bus riders relating their views of the system and outline directions for future work. This system is a grass roots solution to the persistent lack of transport information in developing countries. Above paper are most of uses for experiences with a Transportation Information System that Uses Only GPS and SMS.

A case study of a quiz game designed to be used using SMS technology; the study consists of monitoring the game adaption to the Mobile Deck concept. In the Mobile Deck concept, the SMSs are received and sent through an appropriate graphical user interface. System efficiency and game Improvement will be analyzed and discussed in this paper, in order to infer that the use of this proposed model is beneficial to the ecosystem of games based on SMS. The integration of the cited game to Mobile Deck concept was proved a success, providing a new way of playing games via SMS.In this paper Improving Games by SMS through the MobileDeck Concept without any data loss with secure concept. The application server (ASE) enables the external applications using the CIMD2 protocol to connect to the SMS Center kernel. The ASE communicates with the client applications using the CIMD2 the CIMD2 protocol allows each client to send and retrieve short messages and status reports in a flexible way by transferring data to and from the SMS Center.

III. SECURITY GOALS & PROPOSED SOLUTION

This section focuses on the attack model, system and communication model, basic assumption and detail description of proposed protocol.Represents definition of various symbols used in the paper with their sizes, while lists various functions used in the paper with their definitions.

A. Attack Model

An attack model describes different scenarios for the possibilities of various attacks where a malicious MS can access the authentic information, or misguide the legitimate MS. Since, 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. The attacker establishes an independent connection with both the victim’s MS. It performs eavesdropping on the active connection, modifies and intercepts the messages. However, the intruder must intercept the transmitted message between two victim MS and inject false information, which is straightforward in the circumstances where communication is done in an unencrypted or weak encryption network. But all is possible when an attacker gets the secret key or some information based on which he/she could guess the secret key. Normally, this attack executes during the key exchange phase of the protocol and tries to capture the session key. It may happen that the intruder could impersonate the MS or the AS, if the proper integrity is not maintained over the network. The intruder can pretend like a legitimate MS and ask to the AS for valid authentication tokens in order to make the AS believe that originate from the authentic MS. Similarly, he/she can also show him(her)self like a valid AS and ask legitimate MS to send the information in order to make the target MS believe that originate from a genuine AS.

B. System and Communication Model

In order to overcome the above stated attacks, various cipher algorithms are implemented with the proposed authentication protocol. We recommend that the cipher algorithms should be stored onto the SIM (part of MS) 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. Authors propose toinclude one more service as 'Secure Message' in the menu of mobile software developed by various mobile companies as shown in 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 secureSMS is executed which makes available the symmetric shared key between both MS and then ciphering of message takes place using a symmetric key algorithm.

C. Proposed Protocol: secureSMS

In this section, we propose a new protocol named secure SMS which provide end-to-end secure transmission of information in the cellular networks.In this paper add the channel security . In channel the plain text encrypted and in receiver side automatic message deletion also take place. This protocol produces lesser communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged ratio during authentication.Fig.5.1shows the block diagram

a.Registration phase

- User sending a registration request to DB
- Validate user profile and request the registration phase is complete
- If it fails it send a failure acknowledgement
- It it success it send success registration ID to user
- Then the channel encrypt the plain text

b.message transfer phase

- Sender encrypt the data by using sender registration ID
- Mobile user send plain text SMS to AS as encrypts the plain SMS into cipher SMS using AES symmetric key cryptography algorithms
- Decrypt cypher text using sender registration ID
- Encrypt and generate cypher format SMS
- The secret key used for encryption is again encrypted using MD5 random ID
- Compare hashes
- It it success decrypt message and encrypt with receiver registration ID
- AS applies hash function on received key and compares the generated hash value and received hash value
- If they are equal the message was decrypted with the key and sent to the receiver MS
- The receiver decrypt the data by using receiver registration ID

IV. ANALYSIS OF PROPOSED PROTOCOL

This section analyzes proposed protocol in various aspectssuch as mutual authentication, prevention from various threatsand attacks, key management, and computation & communicationoverheads

SMS Disclosure:

In the secure SMS protocol, a cryptographicencryption algorithm AES/MAES is maintained toprovide end-to-end confidentiality to the transmitted SMS inthe network. Thus, encryption approach prevents the transmittedSMS from SMS disclosure.

Replay Attack:

The proposed protocol is free from thisattack because it sends one timestamp (like T1, T2, T3, T4and T5) with each message during the communication over thenetwork. These unique timestamp values prevent the systemfrom the replay attack. This attack can be detected if laterprevious information is used or modified.

Man in the middle attack:

In this protocol,a symmetric algorithm AES/MAES is used for encrypting/decrypting end-to-end communication between the MS andthe AS in both scenarios. The message is end-to-end securelyencrypted/decrypted with DK1 key for every subsequentauthentication and since attacker does not have sufficient informationto generate DK1, thus it prevents the communicationfrom MITM attack over the network.

OTA Modification in SMS Transmission:

The proposedprotocol provides end-to-end security to the SMS from thesender to the receiver including OTA interface with an additionalstrong encryption algorithm AES/MAES. The protocoldoes not depend upon the cryptographic security of encryptionalgorithm (such as A5/1, A5/2) exists between MS and BTSin traditional cellular networks. This protocol provides endto-end security to end users. It protects the message contentbeing access by mobile operators as well as from attackerspresent in the transmitted medium.

V. SYSTEM ARCHITECTURE AND TABLES

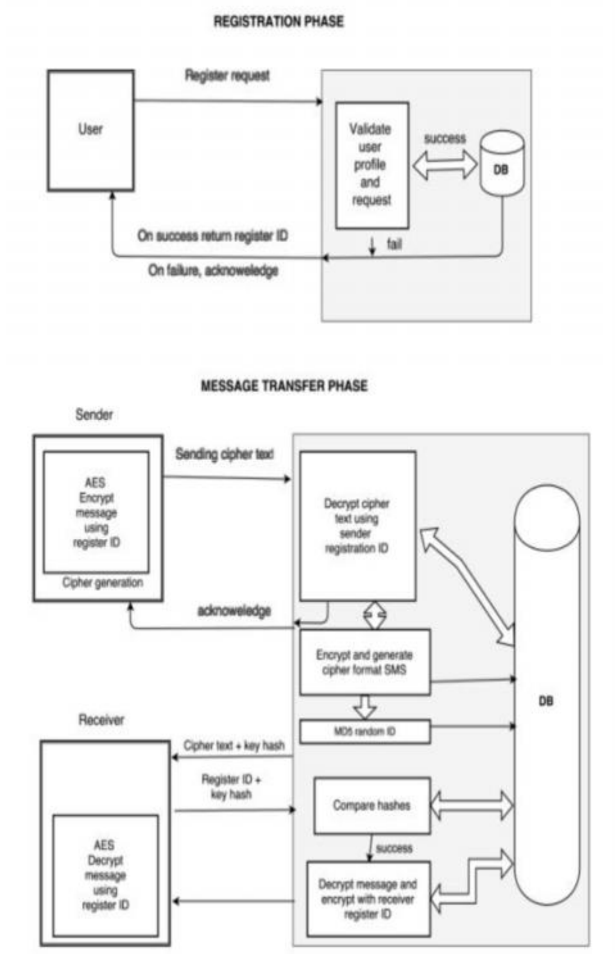
REGISTRATION PHASE
Register request
User
Validate user profile and request
success
DB
On success return register ID
fail
On failure, acknowledge
MESSAGE TRANSFER PHASE
Sender
Sending cipher text
AES Encrypt message using register ID
Cipher generation
acknowledge
Decrypt cipher text using sender registration ID
Encrypt and generate cipher format SMS
MD5 random ID
DB
Receiver
Cipher text + key hash
Register ID + key hash
Compare hashes
success
Decrypt message and encrypt with receiver register ID
AES Decrypt message using register ID

Fig 5.1 block diagram

VI .CONCLUSIONS AND FUTURE SCOPE

The SMS protocol can be successfully designed in order to provide end-to-end secure communication through SMS between mobile users at user end. The proposed protocol shows that the protocol is able to protect from 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.

REFERENCES

[1] Press Release. (2012, Dec. 3). Ericsson Celebrates 20 Years of SMS[Online]. Available: http://www.ericsson.com/ag/news/2012-12-03-smsen_3377875_c

[2] R. E. Anderson et al., “Experiences with a transportation informationsystem that uses only GPS and SMS,” in Proc. IEEE ICTD, no. 4, Dec.2010.

[3] D. Risi and M. Teófilo, “MobileDeck: Turning SMS into a rich user experience,” in Proc. 6th MobiSys, no. 33, 2009.

[4] K. Yadav, “SMSAssassin: Crowdsourcing driven mobile-based systemfor SMS spam filtering,” in Proc. Workshop Hotmobile, 2011, pp. 1–6.

[5] J. Chen, L. Subramanian, and E. Brewer, “SMS-based web search for low-end mobile devices,” in Proc. 16th MobiCom, 2010, pp. 125–135.

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

[7] M. Densmore, “Experiences with bulk SMS for health financing in Uganda,” in Proc. ACM CHI, 2012, pp. 383–398.

[8] J. Hellström and A. Karefelt, “Participation through mobile phones: A study of SMS use during the Ugandan general elections 2011,” in Proc. ICTD, 2012, pp. 249–258.

[9] I. Murynets and R. Jover, “Crime scene investigation: SMS spam data analysis,” in Proc. IMC, 2012, pp. 441–452.

[10] K. Park, G. I. Ma, J. H. Yi, Y. Cho, S. Cho, and S. Park, “Smartphone remote lock and wipe system with integrity checking of SMS notification,” in Proc. IEEE ICCE, Jan. 2011, pp. 263–264.

[11] A. Nehra, R. Meena, D. Sohu, and O. P. Rishi, “A robust approach to prevent software piracy,” in Proc. SCES, 2012, pp. 1–3.

[12] N. Gligoric, T. Dimcic, D. Drajic, S. Krco, and N. Chu, “Applicationlayer security mechanism for

M2M communication over SMS," in Proc. 20th TELFOR, 2012, pp. 5–8.

[13] S. Gupta, S. Sengupta, M. Bhattacharyya, S. Chattrejee, and B. S. Sharma, "Cellular phone based web authentication system using 3-D encryption technique under stochastic framework," in Proc. AH-ICI, 2009, pp. 1–5.

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

[15] Y. Zeng, K. Shin, and X. Hu, "Design of SMS commanded-andcontrolledand P2P-structured mobile botnets," in Proc. 5th WiSec, 2012,pp. 137–148.