CIPHER SMS PROTOCOL FOR END-TO-END SECURE TRANSMISSION OF SMS

MADDIREDDY TEJA SREESAI

Department of Computer Science and Technology, Gitam School of Technology,
Gitam University, Hyderabad, Telangana, India[1]
E-mail:tejasreesai813@gmailcom

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, 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. In this paper, we propose an efficient and secure protocol called Cipher 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 Cipher SMS protocol generates minimum communication and computation overheads as compared with existing Easy SMS, SMSSec and PK-SIM protocols. On an average, the Cipher SMS protocol reduces 51% and 31% of the bandwidth consumption and reduces 62% and 45% of message exchanged during the authentication process in comparison to existing protocols. Authors claim that Cipher SMS is the first protocol completely based on the cryptographic algorithms and retain original architecture of cellular network.

Index Terms— Authentication, over-the-air, security, SMS, symmetric key, cipher SMS, cryptography.

I. INTRODUCTION

Nowadays 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 Pap worth 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, Mobile Deck, SMSAssassin, SMS-based web search such as SMS Find, Monitoring Community

A. Research Problem

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 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 between end-users. SMS usage is threatened with security concerns, such as SMS disclosure, man-in-the-middle attack, replay attack and impersonation attack. 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.

B. Key Contribution

The above requirements can be accomplished by proposing a protocol called Cipher SMS which provides end-to-end security during the transmission of SMS over the network. The Cipher SMS protocol prevents the SMS information from various attacks including SMS disclosure, over the air (OTA) modification, replay attack, man-in-the-middle attack, and impersonation attack. This Cipher SMS sends lesser number of transmitted bits, generates less computation overhead, and reduces bandwidth consumption and message exchanged.

C. Organization

This paper has organized into VI sections. Section II presents literature review of the work done related to SMS security. In section III, a new protocol is proposed which provides end-to-end secure transmission of SMS in cellular networks. Section IV illustrates the analysis of proposed protocol. Section V, discusses suitable symmetric architecture for Cipher SMS protocol. Section VI summarizes

conclusion of the work.

II. RELATED WORK

Previously, various authors have proposed different techniques to provide security to the transmitted messages. An implementation of a public key cryptosystem for SMS in a mobile phone network has been presented but, the security analysis of the protocol has not discussed. A secure SMS is considered to provide mobile commerce services and is based on public key infrastructure. A framework Secure Extensible and
Efficient SMS (SEESMS) is presented, which allows two peers to exchange encrypted communication between peers by using public key cryptography. Another new application layer framework called SSMS is introduced to efficiently embed the desired security attributes in SMS to be used as a secure bearer for m-payment systems and solution is based on the elliptic curve-based public key that uses public keys for the secret key establishment. An efficient framework for automated acquisition and storage of medical data using the SMS based infrastructure is presented and the results conclude that the proposed SMS based framework provides a low-bandwidth, reliable, efficient and cost effective solution for medical data acquisition. It generate shared key for each session but also generate huge overheads and not suitable for the real world applications.
In all, it is not clear whether the proposed approaches are able to prevent SMS against various attacks. All the above mentioned approaches/ protocols/ frameworks generate a large overhead as they propose an additional framework for the security of SMS. Due to physical limitations of the mobile phones, it is recommended to develop a protocol which would make minimum use of computing resources and would provide better security. However, implementation of framework always increases the overall overhead which is not much suitable for the resource constraints devices such as mobile phones. Thus, in this paper we compared our proposed protocol with the existing Easy Sms, SMSSec and PK-SIM protocols.
The reason for chosen these protocols for comparison is that these are the only existing protocols which do not propose to change the existing architecture of cellular networks. We wanted to compare our proposed protocol with some existing protocols devoted to provide end-to-end SMS security with symmetric key cryptography, but there is no such protocol exists. Both protocols are having two phases similar to the proposed protocol and are based on symmetric as well as asymmetric key cryptography while the proposed protocol is completely based on symmetric key cryptography and hashing algorithm
The SMSSec protocol can be used to secure an SMS communication sent by Java‘s Wireless Messaging API while the PK-SIM protocol proposes a standard SIM card with additional PKI functionality. Both protocols are based on client-server paradigm, i.e., one side is mobile user and the other side is authentication server but they do not present any scenario where an SMS is sent from one mobile user to another mobile user.
EasySMS with two different scenarios which provide end-to-end secure transmission of information in the cellular networks. First scenario is both MS belong to the same AS, in other words share the same Home Location Register (HLR) while the second scenario is where both MS belong to different AS, in other word both are in different HLR. There are two main entities in the EasySMS protocol. First is the Authentication Server (AS), works as Authentication Centre (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.
Once both MS have a shared secret symmetric key, they can exchange the message information in a secure manner using a suitable and strong cryptographic algorithm like AES/MAES .A session is generated which provides the secure communication between both MS for a specified time period ExpT. In this time period the same DK1 key is used to provide ciphering between MS1 and MS2but after the ExpT time the session gets expire and MS1 needs to send a fresh request to MS2 with a new request number ReqNo. Within the ExpT, the following steps are used for the communication between both MS: (1) The MS1 sends the IDMS1 and a timestamp (say Ti) to the MS2 encrypted with symmetric key of MS1 i.e., DK1. (2) MS2 decrypts the message using the same DK1 key and checks the validity of IDMS1. Then MS2 replies the same received Ti encrypted with DK1 as an acknowledgement to MS1. (3) Secure SMS communication between both MS takes place.

III. SECURITY GOALS & PROPOSED SOLUTION

A. Security Goals

This section focuses on the attack model, System and communication model, basic assumption and detail description establishes an independent 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, 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 pretend like a legitimate MS and asks 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. Proposed Protocol: CIPHER SMS

In this section, we propose a new protocol named Cipher SMS. The Cipher-SMS protocol achieved by using cryptographic algorithms of AES and MD5. Cipher-SMS is the first protocol completely based on the symmetric key cryptography of AES and hash cryptography of MD5 for cellular network.

I) The Advanced Encryption Standard or AES

It is a symmetric block cipher implemented in software and hardware throughout the world to encrypt sensitive data.

AES is more secure than its predecessors -- DES and 3DES -- as the algorithm is stronger and uses longer key lengths. It also enables faster encryption than DES and 3DES, making it ideal for software applications, firmware and hardware that require either low-latency or high throughput, such as firewalls and routers. It is used in many protocols such as SSL/TLS and can be found in most modern applications and devices that need encryption functionality.

AES comprises three block ciphers, AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. (Rijndael was designed to handle additional block sizes and key lengths, but the functionality was not adopted in AES.) Symmetric or secret-key ciphers use the same key for encrypting and decrypting, so both the sender and the receiver must know and use the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

II) Message-Digest Algorithm or MD5

MD5 is an algorithm that is used to verify data integrity through the creation of a 128-bit message digest from data input (which may be a message of any length) that is claimed to be as unique to that specific data as a fingerprint is to the specific individual.

Message digests (also called hashes) are commonly 128 bits to 160 bits in length and provide a digital identifier for each digital file or document. Message digest functions are mathematical functions that process information to produce a different message digest for each unique document.

A MD5 hash is nothing but a 32 digit hexadecimal number which can be something as follows:

e4d909c290d0fb1ca068ffaddf22cbd0.

This hash is unique for every file irrespective of its size and type.

III) System Model :

The Authentication Server (AS), works as Authentication Center (AuC) and is used for encrypting and decrypting the message. The mobile users should register with AS to connect to the cipher SMS protocol He may get an ID from the AS. The following steps to be followed in order to exchange secure SMS between users.

(1) Mobile user send plain text SMS to AS
(2) AS encrypts the plain SMS into cipher SMS using AES symmetric key cryptography algorithms.
(3) The secret key used for encryption is again encrypted using MD5 hash function and converted into 128 bit hash value
(4) The resultant hash value and cipher SMS vas sent to the Destination user with his ID in the message
(5) Now MS2 provide its ID to the AS for authentication.
(6) If the received Id and ID in message are equal AS asks the receiver MS to provide the decryption key
(7) AS applies hash function on received key and compares the generated hash value and received hash value
(8) If they are equal the message was decrypted with the key and sent to the receiver MS

IV. ANALYSIS OF PROPOSED PROTOCOL

This section analyzes proposed protocol in various aspects such as mutual authentication, prevention from various threats and attacks, key management, and computation & communication overheads.

1) SMS Disclosure: In the Cipher SMS protocol, a cryptographic encryption algorithm AES/MAES is maintained to provide end-to-end confidentiality to the transmitted SMS in the network. Thus, encryption approach prevents the transmitted SMS from SMS disclosure.

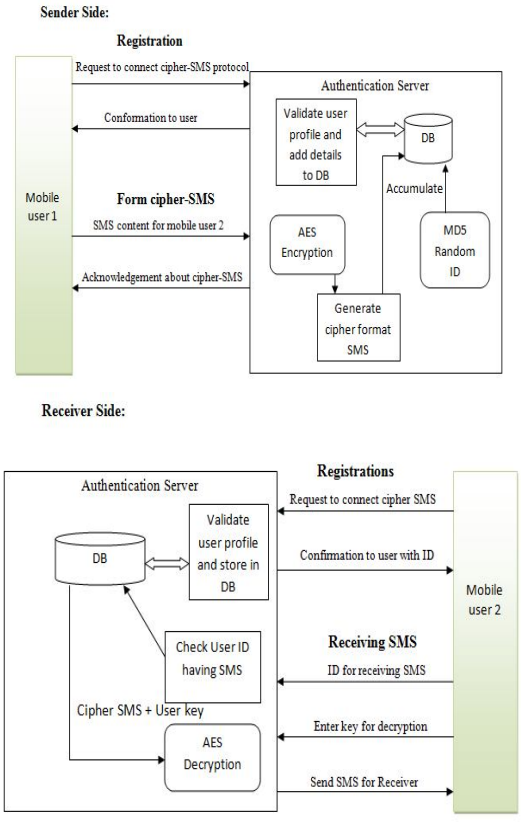
2) Replay Attack: The proposed protocol is free from this attack because it sends one timestamp with each message during the communication over

the network. These unique timestamp values prevent the system from the replay attack. This attack can be detected if later previous information is used or modified.

3) 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 and the AS in both scenarios. The message is end-to-end securely encrypted/decrypted with symmetric key for every subsequent authentication and since attacker does not have sufficient information to generate key as it was encrypted using hash function of MD5, thus it prevents the communication from MITM attack over the network.

4) OTA Modification in SMS Transmission: The EasySMS protocol provides end-to-end security to the SMS from the sender to the receiver including OTA interface with an additional strong encryption algorithm AES/MAES. The protocol does not depend upon the cryptographic security of encryption algorithm (such as A5/1, A5/2) exists between MS and BTS in traditional cellular networks. This protocol provides endto- end security to end users. It protects the message content being access by mobile operators as well as from attackers present in the transmitted medium.

V. SYSTEM ARCHITECTURE AND TABLES



Symbol	Definition	Bits
MS	Mobile Station referring user	–
AS	Authentication Server referring AuC	–
CA/RA	Certification/Registration Authority	–
IDMS	International Mobile Subscriber Identity of MS	128
Qi/Qn	New Session Identifier	28
Rc/Nc/Ns/Na	Random Number	128
Pf	Private Port Number	16
ReqNo	Request Number	8
SK/SK_MS	Symmetric key shared b/w MS and AS	128
DK1	Delegation key	256
MAC/H	Message Authentication Code/Hash	64
Ti	Timestamp	64
CertSAG	Certificate of Security Access Gateway	40
SK_AS-CA	Symmetric key shared b/w AS and CA/RA	128
SK_AS1-AS2	Symmetric key shared b/w AS1 and AS2	128
SQ/Seq	Sequence Number	28
PK/PK_PK-SIM	Public key of Server	128
UAKey	Primary key	128
Expiry/ExpT	Expiry Time	64

Table represents definition of various used in the paper with their sizes.

CONCLUSION

Cipher SMS 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.

REFERENCES

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

[2] 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.

[3] D. Risi and M. Teófilo, ―Mobile Deck: Turning SMS into a rich user experience,‖ in *Proc. 6th MobiSys*, no. 33, 2009.

[4] K. Yadav, ―SMSAssassin: Crowdsourcing driven mobile-based system for 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. 383398.

[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, ―Application layer security mechanism for M2M communication over SMS,‖ in *Proc. 20th TELFOR*, 2012, pp. 5–8.

★★★