ISSN:0975-9646

An Extension To Securedsms: A Protocol For Sms Security

Deepthi Sucheendran, Anju S, Arun. R

Final Year Mtech (Cyber Security)
Department of Computer Science and Engineering
SNGCE, Kerala, India

***Abstract*— Short Message Service (SMS) is widely being used in many applications. But the traditional SMS service was found to be vulnerable to various attacks like SMS disclosure, over the air modification, impersonation attack and replay attack. It is mainly because SMS contents was transmitted as plain text. SMS is also used for communication in military purpose. In this paper, we propose a secure application called 'Secret SMS' which can be used in military organizations. It is completely based on SecuredSMS protocol. This application acts as an efficient way for secure communication between warfighters and command center and also between military officials. The contents of SMS messages are protected from various attacks and also ensure timely delivery of messages to the intended recipients. Here along with the message the location of the sender is picked from google maps and is encrypted and send to the receiver. This is a great advantage in for military officials in identifying the location of various officers.**

Keywords- Cryptography, Military, Security, SMS, symmetric key.

I. INTRODUCTION

Short Message Service enables its users to send and receive messages via a network. It is actually a store and forward mechanism. Short Message Service has now become one of the strongest and fastest communication tool nowadays. There are several factors which are responsible for the ever growing use of SMS. Most important factors are ubiquity, reliability and end-to-end communication. It is cheap, fast and simple to send a SMS. Due to the widespread use of SMS messages, many researchers are interested to explore new fields of its application. Some popular banks are now using SMS as a means of communication with their customers. Some other areas where SMS are used for communication are Transportation Information System [2], SMSAssassin [3], SMS-based web search such as SMSFind [4], private health facilities using SMS [5] and many more.

Like other organizations, military organizations have also relied on SMS for communication. Even though due to development in technology there are several other ways for secure exchange of information between military units, the use of short messages are still found to be increasing. It is used as means of communication between warfighters and command center or between military officials.

Due to the tremendous increase in the usage of SMS for transmission of information, it has become necessary to protect the contents of SMS from eavesdropping and modification. But the traditional SMS service does not provide any means of security to the SMS content. It is mainly because SMS are transmitted as plain text between the Mobile Station (MS) and the Base Transceiver Station (BTS) which makes it vulnerable to several attacks like SMS disclosure [6], man-in-the middle attack [7], replay attack [8] and impersonation attack [9]. As SMS messages are stored unencrypted at the mobile operators, it is very easy for the mobile operator personnel to view the messages.

The above attacks can be efficiently prevented using SecuredSMS[1] protocol. So using this protocol an application called 'Secret SMS' in developed here which can be used for secure communication in military organizations.

A. Organization

This paper has been organized into IV sections. Literature review of previous works which had provided security to SMS are explained in Section II. Section III explains about the features and working of 'Secret SMS' application. Section IV summarizes the work.

II. RELATED WORKS

Previously various authors have proposed several cryptographic methods in order to provide security to the SMS contents. But it was found that these encryption techniques was not able to perform their activity in a complete manner because it affects the performance of mobile devices [10]. A secure application layer protocol called SSMS [11] was designed to be used in m-payment systems. Elliptic curve cryptography was used here for the secret key establishment. But SSMS generate huge overhead. A Secure Extensible and Efficient SMS (SEESMS) was developed in [12] which was used to exchange secure messages in the peer-to-peer network. But the drawback with SEESMS was that it was not suitable for resource constraint devices like mobile phones. Another method was proposed in [13] where the plain text was first converted into cipher text and then digitally sign the cipher text with public key signature. But there was some security issues related to this method. Another protocol SMSSec [14] was designed to provide end-to-end secure transmission of SMS. It uses asymmetric cryptography in the first handshake and symmetric cryptography in the second handshake. PK-SIM card introduced in [15] was designed as an ordinary SIM card which provides additional PKI functionality. It has got a tamper resistant

storage and works like an ordinary SIM card. Another secure and optimal protocol called SecureSMS [16] was found to generate less communication and computation overhead. In terms of bandwidth utilization this protocol was better than PK-SIM and SMSSec protocols.

EasySMS [17] protocol provides an end-to-end secure communication through SMS. It protect the SMS contents from various attacks like over the air modification, replay attack, SMS disclosure, man-in-the-middle attack and impersonation attack. It is the first protocol which is completely based on symmetric key cryptography. The key idea of our previous protocol SecuredSMS was from EasySMS. In EasySMS the sender initially sends a request to the receiver and the receiver then sends the details of both the sender and receiver to the server. In this case if a malicious user acts like the receiver then he could mislead the communication between sender and server. To avoid this in SecuredSMS, the protocol was designed in such a way that both the sender and receiver directly communicates with the server. Also it protects the SMS contents from various attacks and generates minimum communication and computation overhead and utilizes the bandwidth efficiently.

III. 'SECRET SMS'

This section focuses on the proposed method and architecture of the SecuredSMS protocol. This application is mainly designed for military organizations.

A. The proposed method

We know that military officials deals with highly confidential information which requires high security. 'Secret SMS' can be used to protect communications from warfighters to the command center or between military officials. This application prevent the interception or modification of the information from interceptors and also deliver the contents to the intended recipients within the required time.

The working of 'Secret SMS' is completely based on the protocol SecuredSMS [1]. It has got a client-server architecture. The flow diagram of the protocol is shown in the Figure 1. Sender initially transmits a request to the Authentication Server (AS) when it wants to communicate with another user. AS then informs the other user about this. AS then sends the details of both sender and receiver to the Certification Authority (CA) for validation. After authentication of both sender and receiver a symmetric key is generated which will be valid only for a specified time. The sender then encrypts the message using this symmetric key within the expiry time and sends it to the receiver. The receiver then decrypts the message using the symmetric key. Here along with the message the location of the sender is picked from google maps and is encrypted and send to the receiver. Hence the receiver can easily find from where the sender is sending the message. So in addition to SMS security this application also provides an effective way for the military officials to understand the location of various officers. This helps them in their missions.

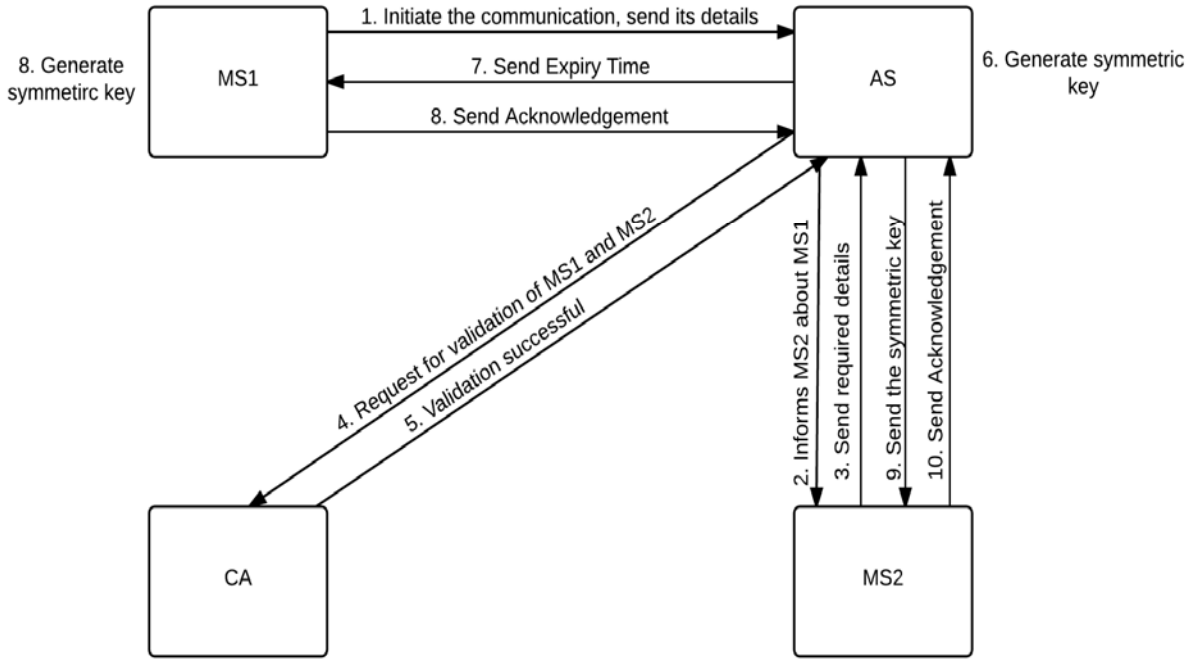

Fig 1 : Flow diagram of SecuredSMS

SecuredSMS protocol is free from various attacks such as Replay attack, Man-in-the-Middle attack, SMS Disclosure and Impersonation attack. AES encryption is used here. Due to the high security offered by this protocol, it is used to design the application 'Secret SMS'. Military organizations mainly focus on the confidentiality, integrity and also on timely delivery of messages to the intended recipients. This application provides this and hence it offers another option to the already existing communication options.

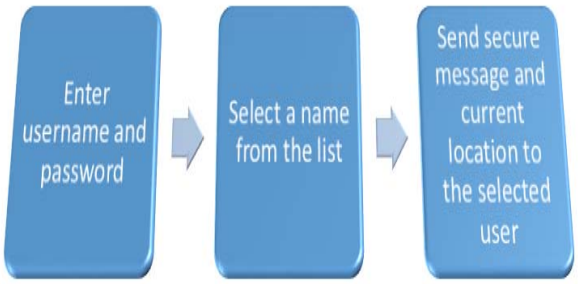

Fig 2 : Steps done by the Sender

Figure 2 shows various steps done by the sender in the 'Secret SMS' application. First sender opens the application and enters his username and password. After successful authentication a dialog box opens where he can see the list of other users. In this case names of all the military officials will be shown. Now the sender can choose to whom he wants to send the secure message. When he selects a name from the list, the SecuredSMS protocol begins to execute in the background. After clicking on the name, a new dialog box opens where he can type the message. When he press the send button the message is encrypted with the symmetric key generated and is securely transmitted to the receiver. Here along with the message the current location of the sender is picked using google maps and is encrypted and send. So in case of an emergency during their mission the receiver (here military official) can decrypt the message using the application and also he can know the exact location of the sender and if needed he can provide necessary help to the sender. Hence we can say that 'Secret SMS' application is an efficient method to protect the communication between warfighters and command center or between military officials.

IV. CONCLUSION

'Secret SMS' application was developed in such a way that it can be efficiently used for secure communication for military organizations. The working of this application is based on SecuredSMS protocol. This application protects the SMS contents from various attacks and also ensure timely delivery of messages to the intended recipients. It provide high security to exchanged messages because military organizations deals with highly confidential information. Location of the sender is picked from google maps and is encrypted and send together with the message.

REFERENCES

[1] Deepthi Sucheendran, "SecuredSMS: A Protocol For Sms Security",*Proceedings of the International Conference on Emerging Trends in Engineering and Management (ICETEM14)30 – 31*, December 2014.

[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.

[3] K. Yadav, "SMSAssassin:Crowdsourcing driven mobile-based system for SMS spam filtering," *in Proc. Workshop Hotmobile*, 2011, pp. 1–6.

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

[5] M. Densmore, "Experiences with bulk SMS for health financing in Uganda," *in Proc. ACM CHI*, 2012, pp. 383–398.

[6] 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.

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

[8] 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.

[9] S. Gupta, S. Sengupta, M. Bhattacharyya, S. Chatterjee, 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.

[10] A. Grillo, A. Lentini, G. Me, and G. F. Italiano, "Transaction oriented text messaging with Trusted-SMS," *Proc. Computer Security Applications Conference*, 2008, 485-494.

[11] 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.

[12] A.De Santis, A. Castiglione, G. Cattaneo, M. Cembalo, F. Petagna, and U. F. Petrillo, "An extensible framework for efficient secure SMS," *in Proc. Int. Conf. CISIS*, 2010, pp. 843–850.

[13] M. A. Hossain, S. Jahan, M. M. Hussain, M.R. Amin, and S.H. S Newaz, "A proposal for enhancing the security system of short message services in GSM", *2nd International Conference on Anti-counterfeiting, Security and Identification, ASID*, Guiyang, China, 2008@IEEE, pp. 235-240.

[14] Johnny Li -Chang Lo, Judith Bishop, J.H.P. Eloff, "SMSSec: An end-to-end protocol for secure SMS", 2008 *Elsevier*.

[15] H. Rongyu, Z. Guolei, C. Chaowen, X. Hui, Q. Xi, and Q. Zheng, "A PK-SIM card based end-to-end security framework for SMS,"*Comput. Standard Interf.*, vol. 31, no. 4, pp. 629–641, 2009.

[16] Neetesh Saxena, Narendra S. Chaudhari, "SecureSMS : A secure SMS protocol for VAS and other applications," *Journal of Systems and Software 90*, 138-150.

[17] Neetesh Saxena, and Narendra S. Chaudhari," EasySMS: A Protocol for End-to-End Secure Transmission of SMS," *IEEE Transactions On Information Forensics And Security*, Vol. 9, No. 7, July 2014.