ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

An Overview of Real Time Secure SMS Transmission

Shital D.Rautkar[1], Dr. Prakash S. Prasad[2]

P.G. Student, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, India [1]

Associate Professor and Head of Dept., of Computer Technology, Priyadarshini College of Engineering, Nagpur, India[2]

Abstract: There are so much daily routine application where the SMS is being used including medical purpose, banking purpose and any other mobile purpose. Forwarding an SMS is one of the cheapest, fastest and simple method. When we delegates message from one cell phone to another cell phone, the data contained in the message transmit as a vanilla text (unencrypted text). Consistently this data contained in the message may be arcane (private) like bank account number, identification key, and license number and so on, and it is an extreme trouble to transfer such data through message until the traditional message courtesy dose not supply (give) encryption to the data contained in the SMS before its transmission.

Keywords: Vanilla Text, Arcane, Elliptic Curve cryptography, symmetric encryption, Asymmetric encryption, Public key cryptography.

I. INTRODUCTION

The SMS courtesy has become one of the breakneck and strongest communication channel to convey the information all over the world. The SMS courtesy will be completing 22 years on December 3 2014 .The world aboriginal (first) SMS was delegated by Neil papworth from united kingdom from Vodafone network. The GSM and SMS standard were primarily developed by ETSI. ETSI stands for European telecommunication standard institute [1] .Message are delegated as a vanilla text between the MS and SMS centre using wireless network. The SMS information is already gathered (saved) in the system of the network operator and this data can be easily perceive by their personnel. Because of this problem encryption is important for every SMS which is being delegate through the network operator. . Sometimes we transfer the private information like password, banking details to our family member, colleagues and service provider through a SMS.But traditional message courtesy does not give encryption to the data contained in the SMS before its transmission.

II. RELATED WORK

Until now, distinct authors have proposed various techniques to give security to the delegated messages. An implementation of public key cryptosystem for SMS in mobile phone network has been presented in java based public key infrastructure for SMS messaging. A secure SMS is considered to provide mobile commerce services presented in paper a high security framework for SMS and is based on public key cryptography [2].

An author design an application for secure extensible and efficient SMS transmission .This application is allow exchanging the message between two pears by using public key cryptography [3].

Next application design by the new author called the SSMS. This new application design for achieves the better security than the previous one. This application is used for payment system. For generate the key in this application used the elliptic curve cryptography. This application provides the low bandwidth and cost effective solution [4].

Another application is also based on the payment system. This application is based on the high security foundation. This application generates the shared key for each period and transfer the secure information between two peers [5].

Next application is design for the public health care. This application is based on the java public key cryptography. This application stored all the medical data of each person and secure message transfer from one mobile phone to another [6]

III.OVERVIEW OF SMS SECURITY ALGORITHM

A. *Data Encryption Standard Algorithm(DES)*

Data Encryption Standard (DES) is most widely used encryption technique which is developed in 1997. It is the most important encryption scheme used to encrypt and decrypt the data.DES algorithm does not provide the strong security, because the many attacks is bombarded on the DES. The Data Encryption Standard consists of the larger key than the other algorithm and the data are encrypted in block [7].

The Data encryption standard provides an authentication courtesy to all the users. In DES algorithm consist of the keys to provide integrity and the authentication. The DES algorithm involves the personal identity verification code to verify the identity of the users. Author implemented an application which is used to secure the data which are transfer from the one user to another user [8].

Author develops an application to delegates the encrypted form of payment from one mobile to another mobile using the symmetric and asymmetric key cryptography. In the symmetric cryptography use the same key on sending and receiving end and in the asymmetric key cryptography use the different key on both ends [9].

The Data encryption standard consists of one more type i.e. Triple DES.The 3DES is the session key which is used for the encryption. The 3DES session key is used to

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

encrypt the data when SMS is transfer between customer obile and the bank mobile. Many attacks are bombarded on the triple DES [10].

B. *Advanced Encryption Standard Algorithm(AES)*
Advanced Encryption Standard is based on the symmetric encryption technique. Advanced Encryption Standard provides a better security than the triple DES and the strength of the security is much better than the other. The key size of the AES is small as compared to the other scheme.AES consist of the byte substitution and the shift rows and these form the round transformation. Many attacks are bombarded on the algorithm and they can break the algorithm [11].
Author develops an SMS security application to provide the authentication and the integrity to the content of message. Advanced Encryption Standard consists of the HMAC which is used to provide an authentication to the mobile users. In this application SMS is send from one mobile to another mobile with high speed and the efficiency is also very high. The new protocol is used in this application [12].
Using Advanced Encryption Standard algorithm an author develop an application to secure the data between two communicating users. The AES algorithm consists of the Diffie Hellman algorithm. In this application an author used the Diffie Hellman algorithm to exchange the key between two users. Diffie Hellman algorithm is the most effective algorithm than the other algorithm [13].

C. *Rivest Shamir Adleman Algorithm (RSA)*
Rivest Shamir Adleman Algorithm is one of the most challenging algorithm. This algorithm is develop by the Ron Rivest, Adi Shamir, and Len Adleman IN 1997.The RSA algorithm is one of the most widely used algorithm and the implementation of this algorithm is very simple as compared to the another algorithm. It consists of the encryption and decryption to encrypt and decrypt the data. The key size of the RSA algorithm is larger than the Elliptic Curve Cryptography. The RSA algorithm consists of the prime number and the product of the prime number forms the encryption key. This encryption is used to secure the data in the system [14].
In RSA algorithm consist of many operations. One of the most important operations is the modular exponentiation. By using this operation we can encrypt and decrypt the message. Many attacks are bombarded on the RSA algorithm and these attacks are hold successful against the RSA algorithm. The RSA algorithm having the block cipher scheme [15].
RSA algorithm is used to encrypt and decrypt the data on both side i.e. sending and receiving ends. In this Algorithm plaintext is encrypted in the block.RSA algorithm consist an integer and the binary values. This integer and binary value is explained in [16].
In the RSA algorithm message is encrypted using the asymmetric encryption cipher. Author develop an application using asymmetric encryption cipher.RSA algorithm consist of the large exponent and the efficiency is also large [17].
A secure extensible and efficient SMS application is develop using the RSA algorithm. Using this application two users can transfer the encrypted message to each other. All the procedure takes some time to exchange the message between two users. We can achieve the better performance by adding some random delay to the algorithm [18].

D .*Elliptic Curve Cryptography*
Elliptic curve cryptography is one of the most important cryptography and is more secure than the other cryptography. Elliptic curve cryptography consists of the mathematical bore. Elliptic curve cryptography consists of various operations. One of the most important operations is the addition operation .In the elliptic curve cryptography multiple addition is the identical part of cryptography. The key size in Elliptic curve cryptography is 256 bits.
Elliptic key cryptography contains the various techniques, the most important and high speed technique is the pollard rho technique. The elliptic curve cryptography contains the smaller key as compared to the other cryptography and this is the advantages of the Elliptic Curve Cryptography
Author has proposed an evaluation technique on the basis of the encryption and decryption. In this system author explain a whole encryption technique. Firstly the message is in the plaintext form and this message is encrypted using any key and then send the message and lastly the receiver decrypt the message using any key. Either the key is symmetric key or asymmetric key [19].

IV. SMS SECURITY THREATS

Message Disclosure: In the SMS service message is transmitted as an unencrypted text. Message could be intercepted during transmission.SMS is first stored as an unencrypted text in the SMSC and then delivered to the destination receiver. This message could be viewed by the users in the SMSC.AES encryption approach secure the transmitted SMS from Message Disclosure attack.

Replay Attack: The attacker can misuse the already transmitted message between the user and network. The exclusive timestamp values can secure the message from the Replay Attack.

Man-in-the-middle Attack: When the user does not authenticate network then the attacker can use a different BTS with the same mobile network Id and then man-in-the-middle attack is perform. This attack can be prevented by the AES algorithm.

Denial of Service: Denial of Service attack is performing when sending repeatedly messages to the destination mobile phone.

SMS Viruses: There have been no reports of viruses with message when the message is transfer from one mobile device to another but mobile devices are getting more powerful and programmable. The SMS viruses being spread through the message [20].

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 1, *January 2015*

V. CONCLUSION

Secured Messenger application is successfully designed in order to provide end to end secure communication through SMS between mobile users. The analysis of the proposed system shows that this system is able to prevent various attacks. The transmission of symmetric key to the mobile users is efficiently managed by the proposed system. This system utilizes bandwidth efficiently. . This system contains a high security authentication mechanism, which confirms true identities can generate the 128 bit session key. And it also ensures message integrity and confidentiality.

REFERENCES

[1] Neetesh Saxena and Naerendra S. Chaudhari ,"Easy SMS:A protocol for End to end secure transmission of SMS" IEEE transactions on information forensics and security, July 2014.
[2] S.wu and C.Tan, "A high security framework for SMS,"in proc.2nd Int.conf.BMEI,2009.
[3] A. De Santis, A.castiglione, G.Cattaneo,M.Cembalo,F.Petagna, and U.F.Petrillo, "An extensible framework for efficient secure SMS", in Int.conf.CISIS,2010.
[4] M.Torani and A.Shrazi, "SSMS- A secure SMS messaging protocol For the m-payment system",in IEEE ISCC,July 2008.
[5] H.Rongu,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.4,2009.
[6] P.Mondal,P.Desai,S.K.Ghosh and J.Mukherjee, "An efficient SMS based framework for public health surveillance", in IEEE PHT,Jan 2013.
[7] D.Linonek and M.drahasky, "SMS encryption for mobile communication",International conf. On security Technology,Hainan Island, 2008.
[8] H.Zhao and S.Muftic, "Design and implementation of a mobile transaction client system:secure UICC mobile wallet,International Journal for information security research vol.1 2011.
[9] H.Harb,h.Farahat and M.Ezz, "secure SMS pay :secure SMS mobile payment model,proc 2nd .International conference,2008
[10] D.Ojha ,R.Singh,A.Sharma,A.Mishra and S.Garg, "An ennovative approach to Enhance the security of data encryption scheme",International Journal of computer Theory and engineering 2010.
[11] N.F standard,Announcing the advanced encrypted Standard (AES) federal information processing standard publication,vol.197,2001.
[12] Jhonny Li-Chang Lo,Judith Bishop, and J.H.P Eloff, "SMSSec:an end to end protocol for secure SMS,"comput.security,vol.27,2008.
[13] A. Singh,S.Maheshwari,S.Verma and R. Dekar, "Peer to Peer Secure Communication in Mobile Environment:A Novel Approach",International Journal of Computer Application Vol 52,2012.
[14]S.Sharma, J.S.Yadav, and P.Sharma, "Modified RSA public key cryptosystem using short range natural number algorithm",international Journal,vol.2,2012.
[15] Farrukh Saleem, Muhammad Sharif,Aman Ullah Khan, "An Efficient And Secure Method for Public Key Cryptosystems", National onference on Information Technology: Present Practices and Challenges, New Delhi, India,Aug 31,2007.
[16] M.Hassinen, "Java based public key infrastructure for SMS Messaging", Proc. 2nd International Conference on Information and Communication Technologies, 2006.
[17] D.Lisonek and M.Drahansky, "SMS encryption for mobile communication", Proc.International Conference on Security Technology, 2008.
[18] A. De Santis.A. Castiglione, G.Cattaneo,M.Cembalo,F.Petagna, and U.F.Petrillo, " An extensible framework for efficient secure SMS", Proc. International Conference on Complex Intelligent and Software Intensive System,2010.
[19] M.Agoyi and D.Seral, "SMS security: an asymmetric encryption Approach",Proc.6th International Conference on Wireles and Mobile Communication,2010.
[20] Prof. Rashmi Rmesh Chavan and Prof. Manoj Sabness, "Secured mobile messaging",in International conference On computing,2012.
[21] J .P.Albuja and E.V.Carrera, "Trusted SMS communication on mobile evices",11th Brazillian workshop on Real Time and Embeded system, pernambuco,Brazil,2009.

BIOGRAPHIES

Shital D. Rautkar received undergraduate degree in electronics engineering in 2013. She has presented a paper in national conference. She is currently student of M.E. in wireless communication and Computing Branch at Priyadarshini College Of Engineering Nagpur.

Dr. Prakash S. Prasad obtained Ph.D. degree in Computer Science & Engineering. He has published more than 16 papers in National and International Conferences. He is Member of IEEE, ISTE and IACSIT. He has completed his bachelor's degree in 1997 and Masters Degree in 2007.
He is currently working as Associate Professor at Priyadarshini college of Engineering Nagpur and Head of the Department of Computer Technology. He is having 16 Years of teaching experience and his interests include network security, Operating System and System Software.