ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

A Survey on Various Approaches for Secure SMS Communication

Rasmita Sahu [1], Upendra Chaurasiya [2]

P.G. Student, Department of Computer Engineering, RSR-RCET, Bhilai, Chhattisgarh, India[1]

Assistant Professor, Department of Computer Engineering, RSR-RCET, Bhilai, Chhattisgarh, India[2]

ABSTRACT: Short Message Services (SMS) is the most popular, easy and cheapest means of textual communication, but due to tremendous growth of media and communication technology, now it is a real challenge to widely share/send information through the insecure network/media ensuring that, the receiver will get the authentic information. Nowadays, short message service (SMS) is being used in many daily life applications such as healthcare monitoring, mobile banking, mobile commerce, and so on. We may send confidential information like passwords, account numbers, license numbers etc through SMS. This important information in SMS may be hacked by the hackers if we do not provide any security mechanism to the SMS content. Security is very much essential in case of transmitting the information through the network and this can be achieved by using cryptography, encoding and decoding mechanisms. In this paper various approaches to provide security to SMS is discussed.

KEYWORDS: Text Short Message Service (SMS), Cryptography, Attacks, Honey Encryption

I. INTRODUCTION

Short message service (SMS)[1] referred to as "Text Messaging" is a service for sending short messages from mobile devices, including smart phones, cellular phones and PDAs to another. Now a Days SMS is considered as a fastest, cheapest and strong communication medium of transferring the information worldwide. SMS is being used in many data centric applications including railways enquiry, mobile banking, news alert and health care etc.[1][3].

Security Problem in SMS Communication:

User sends confidential information like banking details, password, private identities, pass code etc. through SMS. But the traditional SMS service does not provide security to the important information in the messages. So the channel is not secure to transfer confidential information in network. SMS are sending from base station to the Short Message Service Centre (SMSC) in the form of plain text and check the recipient in home location register (HLR) or visitor location register (VLR). Generally the SMSC stores-and-forwards messages between the SME (Short Message Entity) and the MS (Mobile Station). The stored message content at Short Message Service Centre (SMSC) can be easily read by network operator or network provider Staff. They can be easily modifying the content of SMS. So privacy will not be maintained [1].

Most users do not realize how easy to hack the SMS message. A hacker can easily hack the SMS Center and read the message contents. We need to provide security to the SMS like Confidentiality, Integrity and Availability. Confidentiality is the most common aspect of information security. In confidentiality it prevents the unauthorized user to access the private information. The encryption techniques[6] are used to provide confidentiality to the message. In integrity it is preventing anybody other that authorized parties from modifying the computer system assets like writing, changing status and deleting and creating files. The methods of attacking integrity we found replay, reordering and modification of messages [2].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

II.SECURITY APPROACHES

In transmission of messages from sender to receiver, message travels through network. So attackers can easily attack the network and listen the messages. As SMS Messages are transmitted in plain text, they can be easily read by the eavesdropper and steal the information. Apart from user data, private information passed through the messages such as login id, password etc. So security must be needed to protect this important information from unauthorised user access. The security may be provided to the SMS by using the technique cryptography [9].

Cryptography:

Cryptography is the science and art of converting the original message into an unreadable format to make them secure in network and again retransforming that unreadable format into its original format at receiver end. Cryptography mainly uses two processes known as Encryption and Decryption. Encryption is happens at sender side and decryption is happen at receiver side. That means plaintext is encrypted into cipher text at sender side and the cipher text is decrypted into usable plaintext at receiver end[6].

Fig. 1 Process of Cryptography

Encryption: The process of converting plain text or original data into an unreadable format (cipher text) is known as Encryption. For this, it uses keys and mathematical operations with the original data.
Decryption: The process of converting the cipher text, which is generated after the process of encryption, is known as decryption.
There are two main category of cryptography:

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography

Symmetric Key Cryptography:

In this system, a single key is used for encryption as well as decryption process. For this system, secret key must be present towards all the parties involved in the communication. If attacker gets the key, then he/she will be able to decrypt and read the messages. Secret key encryption system is of two types: Stream and Block Cipher. Example of Stream Cipher is RC4 cipher. Examples of Block Cipher are DES,3DES, AES and Blow Fish. Block ciphers are usually used for huge amount of data. This cipher works on Fixed Length data or Blocks of data [6].

- **RC4** (Rivest Cipher 4) is a stream cipher. It is very fast and easy to use and is widely used in TLS protocol and WEP protocol. It generates pseudorandom stream of bits or keystream using 256-bit state table. The plaintext or datastream is XOR with the keystream to generate ciphertext [6]. In the same way decryption is performed. Weakness of RC4 is when non-random keys are used or keys are related.
- **DES** is a type of block cipher. DES maintains confidentiality of information to a large extent. It is generally useful for authentication purpose. Weakness of DES is that it has Short Length Key. Keys of DES can be easily broken so it is unsecure.
- **AES** is a symmetric key algorithm. AES takes fixed block size of 128 bits and a key size of 128, 192, or 256 bits. It uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. AES is

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Stronger and faster than Triple-DES. It is highly secure and provides good speed. But AES requires more processing as compared to others. Configuration of AES is complex. [12]

- **Blow Fish** is also a type of block cipher. It is not patented by any authority or organization. That's why it is license free. It is energy efficient and has fast execution time. In case of blow fish, it is not sufficient for large documents. It has long initialization time period so it is time consuming.[6]

Asymmetric Key Cryptography:

Asymmetric key algorithms use pair of keys for encryption and decryption. The keys are: Private Key and Public Key. The encryption key is public, decryption key is private. Anyone can encrypt a message using public key but only the one who knows the corresponding private key can decrypt it. Asymmetric key cryptography or Public Key Encryption System uses a pair of keys. Both keys can decrypt the message encrypted by other. One of the keys must be kept secret. Communication is encrypted using public key and it can be decrypted using the private key with the receiver. So the communication is secure. It is infeasible to derive private key from public key because of algorithmic properties Example of Public Key Encryption System are Rivest Shamir Adleman (RSA), Elliptic Curve, Digital Signature Algorithm(DSA), Chor–Rivest, El Gamal, Blum Goldwasser, XTR, NTRU etc. Out of this RSA is one of the mostly used algorithms to encrypt the blocks of data. Algorithm uses Random key generation to generate two prime numbers. These prime numbers are multiplied to generate the key. It is affected by the impersonation. After encrypting the data, Size of data becomes very large.

III. ATTACKS ON SMS COMMUNICATION

The message travelling in the network is prone to various types of attacks. Attacks are of following type:

1. **Impersonation attack**- Impersonation attack is an active attack in which attacker acts as the character of authenticated user. Attacker can get the confidential information by various methods. Attackers rely on shoulder surfing to get the passwords by just reading a password that is typed or monitoring the activity using a camera. Dictionary attack also helps to get the password of the user. Some attackers torture or force the user to extract the password. Sometimes attacker attack on the computer and monitors the history and saved passwords to gain access to the user's account [1],[3].

2. **Man in middle attack-** In Man in middle attack[3], attacker intercepts a connection between client and server. It then retransmits those messages with his/her alternate own public key. Attacker acts as a proxy who is being able to intercept, add, delete or modify the messages. In this attack, Users, who are communicating feels that they are talking to each other but in the middle eavesdropper is intercepting their messages and may be modifying those or inserting new messages [1],[3].

3. **Side channel attack**-In Side channel attack the attacker analyses information obtained from the physical implementation of cryptosystem. For instance, timing data, power utilization, electromagnetic releases or even sound can give an additional wellspring of data, which can be misused to break the framework. Technical knowledge of the internal operation of system is necessary for side channel attack. Many Side channel attacks are view of factual techniques spearheaded by Paul Kocher[3], [7].

IV.HONEY ENCRYPTION

Honey Encryption[4] is a type of data **encryption** that "produces a cipher text, which, when decrypted with an incorrect key as guessed by the attacker, it will produce a valid -looking, meaning full fake plain text which is not the original. So the attacker gets confuse, by viewing the meaning full messages for every possible incorrect key used for decrypt the cipher text." Honey encryption provides security against the brute force attack.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

Today many working systems in world depend upon password-based encryption (PBE). These PBE encryption techniques users pick easy-to-remember and weak passwords to encrypt confidential information. Because of the hugely smaller space these secret keys are being generated from, systems that depend on this type of encryption are affected to brute-force guessing attacks. That means the password-based encryption (PBE) cannot prevent from brute force attack. Honey encryption [4] Search a new approach to providing security against brute force attacks.
Honey encryption aims to build a strategy where attackers gain no information about the message, even after trying every possible password to decrypt. When a cipher text is decoded with an invalid key, an obviously valid message is produced. In this way, the honey encryption system protects against brute force attack and low entropy passwords as well as low entropy message spaces.Honey encryption can be used in pin, CVV and credit card data encryption. When an attacker tries to decrypt the credit card data by entering the wrong key, then they will be conferred with a fake key that looks identical to the real one.

Operation of Honey Encryption Scheme:

In order to recover the drawback of the traditional password based encryption (PBE) with low-entropy passwords, Juels and Ristenpart introduced Honey Encryption (HE) [7]. The main idea is that encryption of plaintext M is randomized with a password kp, and decryption of cipher text results in plausible-looking plaintext M´ with wrong password kp'. They construct a distribution-transforming encoder (DTE) for encoding and decoding of message as bit string, denoted DTE = (encode, decode). In brief, overall process is HE[DTE,Sym.E]=(HEnc,HDec) where Sym.E means conventional symmetric encryption. The ciphertext is C = HEnc(kp;M) and decryption works M = HDec(kp;C) .

V.LITERATURE REVIEW

Various author suggesting various technique to provide security to the SMS .For security and confidentiality to the SMS they provide different ideas on their papers .The Survey is base on which technique is used to provide security to the SMS.
In paper [1] author propose a secure protocol called User End secure SMS with, which provides end-to-end secure communication through SMS between end users. This protocol is able to prevent various attacks like man-in-the middle attack, SMS disclosure, replay attack, and impersonation attack.
In paper [2] author propose a framework for sending the SMS by encrypt it using 3D-AES Algorithm and a secret key, because 3-AES Algorithm is most secure and require less time for sending SMS.
In paper [3] author propose a secure protocol based on symmetric key cryptography called User End secure SMS along with integrity key check, which provides end-to-end communication through SMS between end users. The analysis of the proposed protocol shows that this protocol is able to restrict various attacks, including SMS disclosure, man-in-middle attack, over the air modification, replay attack, and impersonation attack.
In paper [4] author present Honey Encryption (HE) which is a new technique that provides resilience against brute force attacks by ensuring that messages decrypted with invalid keys produce a valid-looking fake message.
In paper [5] author propose a protocol EasySMS that improve the authentication technique. In this it provide a technique that authenticate the user and provide end to end security. This protocol prevent various attack like Man-in middle, SMS Spoofing, Replay attack, SMS disclosure etc. The protocol also reduces consumption of bandwidth during the authentication process in comparison to other protocol.
In paper [6] author study about symmetric algorithms like AES, DES, 3DES, BLOWFISH, RC4, RC6 etc. . In this survey she make the blowfish algorithm is more secure, as compare to other symmetric algorithms.
In paper [7] author explain about Honey Encryption technique in detail. They present the detail working of this algorithm with its benefit and application.
In paper [8] author propose a symmetric key-based solution for secure SMS messaging, that provides confidentiality, integrity and authentication. It combines AES and digital MD5 Algorithms.
In paper [9],[10] authors provide various cryptographic framework for secure SMS transfer through network securely to prevent the SMS content from various attacks.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 4, April 2017

In paper [11] the author present a secure model for SMS mobile banking services for mobile phone users. The solution provides end to end security to the message with authentication, integrity and confidentiality.
In paper [12] author provide an idea to encrypt the SMS using AES encryption algorithm which is based upon symmetric key approach before transfer. So the author develops an android based SMS application using AES to provide security to the SMS.

VI .CONCLUSION

In today's world use of SMS is growing and it is becoming an important way of communication. As the number of users using SMS are increasing, need for security of SMS also becomes an important issue. SMS is sent as a plain text into the network and it is vulnerable to third party attacks or brute force attacks. This paper discusses about various existing approaches which can be used to encrypt the SMS content and provide the security.

REFERENCES

[1] Amin Khan, Nikita Umare " A Survey on Enhancing the Security for End to End SMS in GSM or UMTS Networks", International Journal of Scientific Engineering and Applied Science , Volume-2, Issue-5, May 2016 ISSN: 2395-3470
[2] Varsha S. Bari1,Nileema R. Ghuge,Chaitali C. Wagh,Sayali R. Sonawane ,Mr.M.B. Gawali", SMS Encryption on Android Message Application", IJARIIE-ISSN (O)-2395-4396 Vol-2 Issue-2 2016
[3] SandeepKumar Laxman Sahu, Pragati Patil " A Survey on Secure SMS Transmission and authentication at user end", International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-4, June 2015 ISSN: 2395-3470
[4] Nahri Syeda Noorunnisa1, Dr. Khan Rahat Afreen "Review on Honey Encryption Technique" International Journal of Science and Research (IJSR) ISSN : 2319-7064, 2015-16
[5] Neetesh Saxena ,Narendra S. Chaudhary "EasySMS: A Protocol For End-to-End Secure Trans-mission Of SMS" IEEE Transactions On Information Forensics And Security, Vol. 9, No. 7,July 2014
[6] P. Princy "A Comparison Of Symmetric Key Algorithms DES, AES, BLOWFISH, RC4, RC6: A Survey" International Journal of Computer Science & Engineering Technology ISSN : 2229-3345 Vol. 6 No. 05 May 2015
[7] Ari Juels, Thomas Ristenpart "Honey Encryption:Security Beyond the Brute-Force Bound"
[8] Nimmya Unnikrishnan, Divya KV "End To End Secure Sms Communication: A Literature Survey" International Journal of Innovations & Advancement in Computer Science ISSN 2347 – 8616 Volume 4, Issue3 March 2015
[9] Abdullah Talha Kabakus & Resul Kara, Survey of Instant Messaging Applications Encryption Methods , European Journal of Science and Technology Vol. 2, No. 4, pp. 112-117, June 2015
[10] Nishika , Rahul Kumar Yadav "Cryptography on Android Message Applications – A Review" International Journal on Computer Science and Engineering ISSN : 0975-3397 Vol. 5 No. 05 May 2013
[11] Amol B. Jawanjal , R. B. Joshi2 "A Secure Protocol for SMS Mobile Banking" International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 2013
[12] Rohan Rayarikar , Sanket Upadhyay , Priyanka Pimpale " SMS Encryption using AES Algorithm on Android" International Journal of Computer Applications (0975 – 8887) Volume 50– No.19, July 2012