ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

Secure Message Transmission with Low Computation

Dr.K.Venu Gopala Rao, Dr.P.Ramkumar

Abstract – Confuse the attacker of a network by obfuscating message content is a technique for data hiding. It involves concealing the secret text inside the cheating text. If the cheating text is intercepted with security algorithms, the secret text may still be undetected. Here, this technique provides following service for the Message Transmission system, which are Confidentiality, Authentication and Integrity. This study focuses on reducing the complexity and simplifies the security of Message transmission systems and this technique we called as "CheatSec". We can use any article on the internet as a cheating text. The sender only needs to transmit the encrypted Uniform Resource Locator (URL) of cheating text, and then the receiver can follow the URL and download the cheating text. This avoids transmitting large amounts of cheating text, which is a major drawback of traditional confused document encrypting schemes. In this paper, we are focusing the different categories of security attack, existing widely used mitigation strategies, difficulty over present strategies and proposed a new approach which can improve existing Message Transmission Security Systems and provides the Confidentiality, Authentication and Integrity by reducing their transmission overhead, and thus makes it suitable for wireless environment with low data rate.

Key Words **– CheatSec, Cheating Text, Obfuscation, URLs, Confidentiality, Authentication, Integrity.**

I. INTRODUCTION

Security is an essential part of any Message Transmission Systems, especially valuable data like holding bank account, personal transaction and et. al. The threats from unauthorized party is growing rapidly and also increasing in technical sophistication, thereby requiring a depth of defense to safeguard Message Transmission system, against the risks they present with the attacks they deliver. Unauthorized parties are becoming increasingly flexible in their functionality, simultaneously sharing resources across many criminal operations security on the Internet is, by its very nature, highly interdependent. Because of the advances in attacker's technology, a single attacker can relatively easily employ many distributed systems to launch devastating attacks against a single victim communication. The security attack (any action that compromises the security of information owned by the organization) there are several types of security attacks on Different Layers in OSI i.e. [5, 6, 7]. They are categorized as two types

1). Passive attacks
2). Active attacks

Passive attack - A passive attack on a cryptosystem is one in which the cryptanalyst cannot interact with any of the parties involved, attempting to break the system solely based on observed data (i.e. the cipher text). This can also include known plaintext attacks where both the plaintext and its corresponding cipher text are known. They are two type of passive attacks i.e.,

1). Traffic Analysis.
2). Release of message contents

Traffic analysis: In it all incoming and outgoing traffic of network is analyzed but not altered.

Release of Message contents: we send confidential email to our friend, we desires to only she/he access it. Otherwise our content of message released against our wises.

Active attacks – An active attacks on a cryptosystem in one in which the cryptanalyst directly interact with any of the parties involved or done some modification of the data stream in the network or the creation of false stream. These attacks can be subdivided into four categories i.e.,

1. Masquerade
2. Modification of message or Modification
3. Interruption
4. Fabrication attack

Masquerade: It takes place one entity pretends to be a different entity. For example, following attack can takes place by doing Masquerade i.e.,

a. Impersonation
b. Replay attack
c. Session Hijacking
d. Man in the middle attack

Modification: It is simply means that some of a legitimate message is altered, or that message are delayed or reordered, to produce an unauthorized effect.

a. Spoofing
b. Man in the middle attack

Interruption: Prevent or inhibits the normal use or management of system.

a. Denial of Service
b. Replay attack
c. Ping to death attack
d. SQL injection attack
e. Buffer over flow attack

Fabrication attack: Fabrication attack is also called as tampering attack, in this attack malicious node do not interrupt or modify any routing table thus the attacker fabricates its own packets and transmit it on the network to create a chaos to bring down the network. Fabrication attacks can also be launched from the internal misbehaving nodes like route salvaging attacks. To secure Message Transmission from the such attacks, we need to establish secure transmission layer with following services, such as Confidentiality, Signing and Integrity. To provide above services we need to implement following Security Mechanisms, that are Encryption,

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

Hash Functions or Message Digest, Signing [1, 2, 3, 4]. This paper organizes as follow section 2, preventing security attacks give service and mechanisms to mitigate the above said attacks. Section 3, Compares the computational efficiency of different encipher techniques. Section 4, illustrate the need of CheatSec, functional algorithm, and architecture of CheatSec.Finally, section 5, concludes the CheatSec.

II. PREVENT SECURITY ATTACKS

A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms. A mechanism, that is designed to detect, prevent or recover from a security attack. Following tables (1 &2) show the relationship among security mechanisms, services and security attacks. In table (2) security mechanisms message encryption is widely used security scenario in security services. This Message Encryption is two types

1. Symmetric Key Encryption
2. Asymmetric Key Encryption

Symmetric key algorithms are a class of algorithms for cryptography that uses the same cryptographic keys for both encryption of plaintext and decryption of cipher text. The keys should be identical. The keys, in practice, represent a shared secret among two or more parties that maintains a private information link. This requirement that both parties have access to the secret key is one of the main drawback of symmetric key encryption, in comparison to public-key encryption or Asymmetric Key Encryption. Public-key or Asymmetric Key cryptography refers to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cyphertext. Neither key will does both functions. One of these key is published or public and the other is kept private. If the encryption key is the one published then the system enables private communication from the public to the decrypting key's owner.

III. EFFICIENCY OVER MESSAGE ENCRYPTION SCHEMA

Presently, the most widely used Public key or Asymmetric key cryptography for message encryption algorithms are RSA and followed by ECC. RSA is an innovative cryptographic technique, which was discovered in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman [8]. RSA, it is based on the large integer factoring problem. Nevertheless, some timing attacks succeed to be applied against to RSA. The key size must be expanded to ensure the security. Consequently, the system is extraordinarily time consuming. In the precondition of achieving the same security level, short key is more popular, especially in resource constrained environments such as smart phone and ipads, where processing speed is very less even for high end devices show in table (3). Because of this reason RSA large integer factorial is not compatible for Mobile Commerce. "Mobile Commerce is any transaction, involving the transfer of ownership or rights to use goods and services, which stated and/or completed by using mobile access to computer-mediated networks with the help of an electronic device". To resolve this problem, ECC is an innovative cryptographic technique, which was discovered in 1985 by V.S.Miller [12] as an alternative scheme for public key cryptography. In table(4) is based on, a comparative test of certificate against RSA and ECC is discussed, which is based on the PC of Intel Pentium Dual E2180 2GHz's CPU, 1GB's RAM, and MS Windows XP sp2. According to FIPS 104-2 [9], the key length of RSA and ECC having equivalent security level. ECC, its security depends on the intractability of ECDLP (Elliptic Curve Discrete Logarithm Problem). In fact, ECC is no longer new, and has withstood much of cryptanalysis and a long series of attacks. With respect to all this issues, we are proposing new security mechanism such as *CheatSec* algorithm. This algorithm is based on any message encryption scheme using a concept called Cheating Text is proposed. The original message is embedded in a meaningful text called Cheating Text.

IV. ALGORITHM AND ARCHITECTURE CHEATSEC

Message encryption schemes presently being used require that the total message is encrypted with max key size or large integer factorization. It leads to increase in the computational cost of message. Some researchers are working on cheating text message encryption [10, 11] based on cheat text and URL. In this paper we proposed an encryption scheme *CheatSec* based on cheating text, URL and digital signature. It comprises complete security pack with less computation, reduces network bandwidth by send URL instead of cheating text completely and increases number of computations with small key length of RSA.

Algorithm:

Step 1 : Read the Real Message text or file.
Step 2 : Select the cheating text URL that embedded Real Message (URL content should be static).
Step 3 : Calculate Character Position Table (CPT) from CPT table construct Real Index File (RIF) table.
Step 4 : In sender side, calculate Hash value to the Real Message using MD5 or SHA or any hash function algorithms.
Step 5 : In sender side, encrypt the Message consists of RIF, Cheating Text URL and Hash value using RSA.
Step 6 : In sender side, use RSA algorithm for Signing the text.
Step 7 : After signing the message sender send the Message consists of encrypted RIF, URL

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

of Cheating Text and Hash value to the receiver.

Step 8 : In Receiver side, verify the Sign of Sender, if it is Authenticated Goto STEP 9. Otherwise Goto STEP 12.

Step 9 : In Receiver Side, Decrypt the Message and separate the RIF, URL of Cheating Text and Hash value.

Step 10 : Find the Real Message from the URL and calculate Hash value for Real Message. Then verify calculate Hash value with senders hash value, if both are same Step 11 otherwise step 12.

Step 11 : Receiver has to send positive acknowledgement to the Sender state that communication is successful.

Step 12 : Receiver has to send negative acknowledgement to the Sender state that communication is intercepted by the third party.

Architecture:

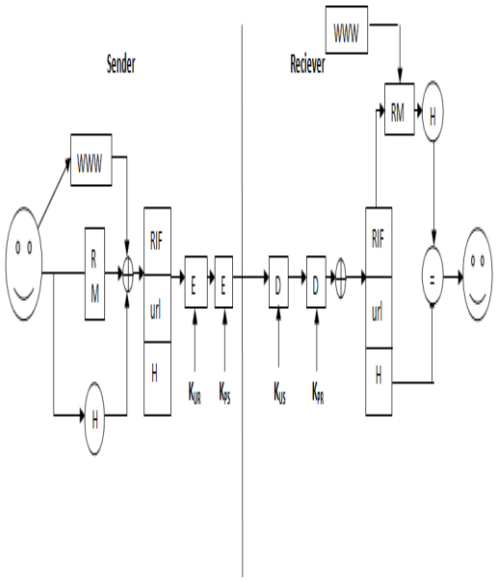

Fig 1. Architecture of CheatSec

V. CONCLUSION

A message encryption scheme based on cheating text and URL is proposed. The scheme is cost effective because only an index table called RIF file is hashed and sent to the receiver along with the cheating text URL in which the original message is embedded. The original message can be retrieved from the RIF file table and the cheating text URL. Here message authentication also possible of the message using RSA signature and encryption.

REFERENCES

[1]. Choudhury, H, Roychoudhury, B, Saikia, D.K."End-to-End User Identity Confidentiality for UMTS networks", Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on Volume: 2, Page(s): 46 – 50.

[2]. Guilin Wang, "An Abuse-Free Fair Contract-Signing Protocol Based on the RSA Signature", Information Forensics and Security, IEEE Transactions on Volume: 5 , Issue:1,Page(s):158-168.

[3]. Sida Lin, Qi Xie, Zhejiang Natural Sci. Found. Comm., Hang Zhou "A Secure and Efficient Mutual Authentication Protocol Using Hash Function", Communications and Mobile Computing, 2009. CMC '09. WRI International Conference on 6-8 Jan. 2009.

[4]. Xiang Wu, Financial Bur. of Lishui, Lishui, "Data synchronization for integration systems based on message digest", Educational and Information Technology (ICEIT), 2010 International Conference on Issue Date : 17-19 Sept. 2010 Volume : 1.

[5]. William starlings "Introduction to Network security and cryptography" by Pearson education.

[6]. www.Wikipedia.org

[7]. Dr. 許 富 皓's " the attack and defense of computers".

[8]. Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM **21** (2): 120–126. doi:10.1145/359340.359342. http://theory.lcs.mit.edu/~rivest/rsapaper.pdf.

[9]. NIST, "Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program", April 13, 2010. Available at http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf.

[10]. Ch. Rupa and P. S Advani "Message Encryption Scheme using Cheating Text" Sixth International conference on Information Technology, IEEE @2009.

[11]. Chao-Wen Chan, Chin-Chen Chang, Zhi-Hui Wang "Cheating Resistance for Secret Sharing",

[12]. International Conference on Network Security, Wireless Communications and trusted computing.

[13]. V.S.Miller, Use of Elliptic Curves in Cryptography. Proc. CRYPTO'85, Springr-Verlag, New York, 1986, pp.417-426.

[14]. http://www.phonearena.com/

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 6, June 2012

Table 1. Relationship between Security Services and Security Attacks

Security Attacks / Security Services	Masquerade	Modification of message or Modification	Interruption	Fabrication attack
Data Authentication	Y	Y		Y
Confidentiality	Y			
Data Integrity		Y	Y	Y
Access Control	Y		Y	Y
Nonrepudation	Y			
Availability			Y	Y

Table 2. Relationship between Security Services and Security Mechanism

Security Mechanism → / Security Service ↓	Message Encryption	Digital Signature	Message Digest	Sequence No.
Data Authentication	Y	Y		
Confidentiality	Y			
Data integrity			Y	
Access Control	Y	Y		Y
Nonrepudation	Y	Y		Y
Availability	Y	Y	Y	Y

Table 3. Today's High End Mobiles Configuration [13]

Model	Processor	RAM	Platform
HTC ONE X	Quad core 1.5GHz	1GB	Android™ 4.0.3
HTC HD7	Single core 1GHz	512MB	Windows® Phone OS 7
Samsung Tab 2(10.1)	Dual core 1GHz	1GB	Android™ 4.0
Samsung Note 10.1	Dual core 1.4GHz	1GB	Android™ 4.0
iPhone 4S	Dual Core 0.8GHz	512MB	iOS
iPad 3	Dual core 1GHz	1GB	iOS
Motorala Driod XYBOARD 10.1	Dual core 1.2GHz	1GB	Android™ 3.2
Motorala RAZR MAXX	Dual core 1.2GHz	1GB	Android™ 2.3.6
LG LUCID	Dual core 1.2GHz	1GB	Android™ 2.3.6
LG OPTIMUS	Quard core 1.5GHz	1GB	Android™ 4.0
BlackBerry Curve 9220	Single core 1GHz	512MB	BlackBerry OS 7.1
BlackBerry Torch 9850	Dual core 1.2GHz	786MB	BlackBerry OS 7.1.7
Nokia Lumia 900	Single core 1.4GHz	512MB	Windows 7.5 Mango
Nokia 603	Single core 1GHz	512MB	Symbian Belle
Sony Xperia P	Dual core 1GHz	1GB	Android™ 2.3
Sony Tablet S	Dual core 1GHz	1GB	Android™ 4.0

Table 4. Key Length Of Equivalent Security Level (Bits)[9]

RSA	1024	2048	3072	7680	15360
ECC	160	224	256	384	512