Secure Message Recovery and Batch Verification using Digital Signature

By Makkar, Sarika & Thakral, Silvi
Manav Institute of Technology and Management, India

Abstract: This paper about the study of Secure message Recovery and batch verification using Digital Signature. Security is increased in batch verification through triple DES algorithm. Encryption is used for the Security in which the plaintext is transforming into the cipher text. A digital signature scheme involves two phases, the signature generation phase which is performed at the sender side and the signature verification phase that is performed by the receiver of that message. In computer to computer communication, the computer at sender’s end usually transforms a plaintext into cipher text using encryption. When the message is recovered at the Receiver Side than the original text is converted in to the encrypted text. That encrypted text is secure for the authenticated person. After recover the message if authentic person wants to get the original text then he/she enter the key and take the plaintext.

Keywords: digital signature, forgeries, encryption, triple des algorithm.

GJCST-F Classification: D.4.6, D.4.4, H.3.7

Strictly as per the compliance and regulations of:

© 2014. Makkar, Sarika & Thakral, Silvi. This is a research/review paper, distributed under the terms of the Creative Commons Attribution-Noncommercial 3.0 Unported License (http://creativecommons.org/licenses/by-nc/3.0/), permitting all non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Secure Message Recovery and Batch Verification using Digital Signature

Makkar, Sarika & Thakral, Silvi

Abstract - This paper about the study of Secure message Recovery and batch verification using Digital Signature. Security is increased in batch verification through triple DES algorithm. Encryption is used for the Security in which the plaintext is transforming into the cipher text. A digital signature scheme involves two phases, the signature generation phase which is performed at the sender side and the signature verification phase that is performed by the receiver of that message. In computer to computer communication, the computer at sender's end usually transforms a plaintext into cipher text using encryption. When the message is recovered at the Receiver Side than the original text is converted in to the encrypted text. That encrypted text is secure for the authenticated person. After recover the message if authentic person wants to get the original text then he/she enter the key and take the plaintext.

Keywords: digital signature, forgeries, encryption, triple des algorithm.

I. Introduction

Digital signature is an authentication process that is used to prove the identity of source and integrity of message. A digital signature scheme involves two phases, the signature generation phase which is performed at the sender side and the signature verification phase that is performed by the receiver of that message. In this pair of key is used private key and public key. Private key is Secret and public key known all the users.

Digital signature provides the following security services:

a) Message integrity

It guards against the inappropriate information modification or damage. Message integrity ensures the information nonrepudiation and authenticity. By using this, users are able to ensure that the message has not been altered during transmission. A loss of message integrity means that there is insertion, deletion or modification in message or replay of the message.

b) Authentication

This property defines being real and being able to be trusted and verifiable. The functionality of the authentication service is to guarantee the recipient that message is from the source that it state to be. Two aspects are involved: first at the connection initiation time, the entities are authentic that is each entity is the entity which it state to be. Second the process of authentication must assure that the connection is not interfere by the third party in such a way that a third party can impersonate one of the two legal parties for unauthorized transmission or reception of messages.

c) Nonrepudiation

It prevents from denying transmission of a message by either sender or receiver. Thus if the message is sent then the receiver can validate that the claimed sender has sent the message. This is called origin nonrepudiation. Similarly, when a message is received the source can validate that the claimed receiver has in fact receive the message.

Thus digital signature must have to posses the following properties:

1. The digital signature must validate the sender and date and time of the digital signature.
2. Digital signature must authenticate the content of message at the time of digital signature.
3. In case of any dispute, digital signature must be verifiable by third party to resolve it.

II. Digital Signature Requirements

The points described below states the requirement of the digital signature:

1. Digital signature (a bit pattern) must depend upon the message that is to be signed by the sender.
2. It must make use of some information related to sender that is unique to it to prevent against denial and forgeries.
3. Digital signature must be comparatively easy to compute on message.

It must be comparatively easy to recognize and validate digital signature.

III. Encryption and Decryption

Encryption is used for the Security in which the plaintext is transforming into the cipher text. In computer to computer communication, the computer at sender’s end usually transforms a plaintext into cipher text using encryption. The encrypted cipher text message is sent to the receiver over a network then the receiver takes encrypted message and performs the reverse of encryption. I.e. performs the decryption process obtain the plaintext.
a) Plaintext and cipher text

Any communication in the language that we speak that is the human language, takes the form of plain text or clear text. That is, a message in plaintext can be understood by anybody knowing the language as long as the message is not codified in any manner. Plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets access to the message. When a plaintext message is codified using any suitable IV.

IV. DIGITAL SIGNATURE MODES

There are two modes of operation, Appendix Mode and Recovery Mode.

a) Appendix mode

In appendix mode, the creator of the message attaches a code with the message that acts as a signature. Typically, the signature is produced by taking the hash of the message and encrypts it with the private key of the sender. This signature guarantees the integrity of the message and claimed identity of source.

In the figure 3 first a hash code generation algorithm has been applied on the message and then it is encrypted with the private key of the sender. The generated code then appends to the message and transmitted to receiver via network. Receiver verifies the signature using three items, the public key of sender, the packet and the signature. The receiver first cuts off the message from the digital signature. It first computes the hash of the message and decrypts the received signature with the public key of the sender. If both values are equal then the message will be considered as authentic otherwise it has been modified during transmission.

b) Recovery mode

In message recovery mode the signed message is implanted in the digital signature and it can be recovered from it. The well-known digital signature scheme with message recovery is the RSA digital signature scheme which is based upon solving the factor of large prime numbers. Later Nyberg and Rueppel also proposed the digital signature scheme with message recovery based upon the discrete logarithm. Some of these schemes have the capability of privacy of signed message and thus only the legal receiver can recover the message and verify its authenticity. However, the scheme only allows a signer to sign each message independently.

As shown in the figure 4, the receiver requires only two parameters to verify the digital signature of the message, the public key of sender and the digital signature. The receiver first recovers the message from the received signature and then performs computation for digital signature verification.

V. OBJECTIVE

1. An unauthorized person cannot get the original text.
2. If any person tries to get the plaintext than he/she get the encrypted form text.
3. If the authenticated person knows the key than get the plaintext.
4. It must detect integrity violation. An attacker must not be able to replace false packets for legitimate ones i.e. multiple packets should not be modified.
5. It must detect integrity violation. An attacker must not be able to replace false packets for legitimate ones i.e. multiple packets should not be modified.

VI. PROPOSED METHODOLOGY

a) Triple DES Algorithm

Triple DES Algorithm is same as the DES with two 56-bit key is applied. Given a plaintext message first key is used to DES encrypt the message. The second key is used to decrypt the encrypted message. The twice scrambled message is encrypted again with the first key to yield the final ciphertext. It uses three 56 bits DES keys giving a total key length of 168 bits. The block size is 64 bits and the key sizes are 168, 112, or 56 bits with respect to keying option 1, 2, or 3. The input key sizes are 3 64-bit keys, which are shortened to 56 bits because of the internal key scheduler.

The block of data is encrypted 3 times with each of the keys according to the keying options:

Keying Option 1: All of the keys are independent
Keying Option 2: K1 and K2 are independent and K3 = K1
Keying Option 3: All keys are identical K1 = K2 = K3

Triple DES Algorithm has following steps:

Step1: Encrypt the data using DES with the first 56 bit key.
Step2: Decrypt the data using Second 56 bit key.
Step3: Encrypt the data using DES third key 56 bit.
Secure Message Recovery and Batch Verification Using Digital Signature

Figure 2: TDES Encryption Decryption Process

i. Advantages
1. TDES Algorithm not Easy to break.
2. It is more Secure rather than DES.

ii. Disadvantage
1. This algorithm take 3 times more than DES.

Figure 3: Appendix Mode Digital Signature

VII. Conclusion
In This Present Work We Increase The Security Of Batch Verification. After Rec-Overy The Message Is Not In The Original Form. No One Can Get The Plaintext Whether He/She Not Enter The Key. If Any Unauthentic Person Tries To See The Plaintext He/She Only Gets The Encrypted Text.

References Références Referencias