Design of new protocol for secure communication of Messages

T.ChalamaReddy ,Dr.R.Seshadri

ABSTRACT-Security for computers and networks has increased in importance, as end users have become more aware of the value of the vast amounts of data being accumulated and the need to protect that data, as companies that do sensitive work, such as those with defense contracts, military activities, banking, are often heavily involved in data security. As the scope of the network is increased a lot, data security became a main network concept. Suppose sender wants to send a message to receiver securely, so that no eavesdropper can read the message. Authentication of messages and communication play a vital role in the present day business transactions. With help of various symmetric, asymmetric and hash algorithms, ourprotocol achieves three cryptographic primitives such as confidentiality, authentication and integrity for communication of messages. This protocol assumes that two communicating parties share a common session key and secrete value. Sender computes the hash value over the concatenation of message and secretes value and appends it to message,andthen result is compressed. The compressed message is encrypted by using conventional encryption algorithm (AES) with a session key. To protect the session key and secrete value, sender encrypts combined session key and secrete value using public key encryption algorithm(ECC) with the recipient's public key and the result is appended to compressed message, and then transmitted to receiver. Later the intended receiver applies the reverse process to obtain the original message, and verifies authentication and integrity of message. This protocol also provides better security than PGP protocol used in email security.

Keywords:-Cryptography, Encryption, Decryption, session key, compression, decompression, Digital signatures, Digital certificates, fingerprint.

---

1. Introduction

Secure communications for preventing the unauthorized interception of sensitive information data is a legitimate need of not only Institutions in the military and government, but also the business sector and private individuals. The increasing reliance on the Internet, e-mail and on-line business brings an increase in the potential for fraud, misuse and theft when conducting business electronically. Digital signatures and digital certificates help to reduce those threats. Ordinary e-mail can easily be forged and, under the right conditions, an e-mail message can be intercepted and read by others. It is also not uncommon for the sender to mistype an e-mail address and send private correspondence to the wrong person. Ordinary e-mail is not a safe and secure communication medium but it can be made more secure with the use of digital signatures. When people engage in e-Business over the World Wide Web, the customer needs some assurance that the Web site they are accessing is actually the Web site for the business they are transacting business with. It is not very difficult to highjack, misdirect or spoof a Web site and mislead customers into transacting business with a bogus web site. If the legitimate business has installed a valid and current Digital Certificate [1], issued by a trusted third party, the customer has strong assurance that they are using the correct Web site. Digital Certificates can also be used to provide confidentiality of the transaction by encrypting the data that is sent and received. If the customer has their own digital certificate, the business has assurance that the customer is who they claim to be. Data privacy [2], authentication [6], digital signature [4], and file security [10] are the various elements that need to be examined for protecting data in computer and communication systems for unauthorized disclosure and modification. If a non-inter acceptable means for data storage and transmission were available, then all messages and data in the communications as well as in the data storage unit could obviously be secured. One such possible system is cryptographic cipher system which can conceal the contents of every message by transforming it before transmission or storage.

There are several situations where the information should be kept confidential, and where an opponent can intercept vital information by monitoring the communications network. In such situations, necessary steps should be taken to conceal and protect the information contents. The role of cryptographer will be recognized and appreciated if adequate measures are taken:

i) To protect valuable data in computer systems for processing and storing of data

ii) To prevent the unauthorized extraction or deletion of information from messages transmitted over the open channel; and

iii) To prevent the unauthorized injection or addition of false data into the open channel.

There is a strong need for the general tools of utility, which can convert a plain text-file into a cipher-text file and vice-versa, for every user who intend to transfer/ receive text/data on the network.

Digital Signatures

When someone signs a document by hand, they are indicating that they are either the author or that they approve of the document. What we would like to achieve is for someone to make the same assertion about a string of bytes stored in a computer. Any scheme that allows this is called a digital signature.

Digital Signatures can be used to provide authentication, non-repudiation, and information integrity. A digital signature is created using two distinct functions. A one-way hash function is used to establish information integrity while a cryptographic system (using the private key of a private-public key pair) is used algorithm that generates a large number representing the message, called the "hash total" or "message digest"[1]. The hash total is like a finger print of the message, and if there is even one small change in the message, like a deleted comma, the hash total for the changed message will be different from the original one. The original message itself cannot be retrieved from the hash total and the likelihood of two different messages having the same hash total is extremely small. Thus, the entire message is reduced to a number, which is easy to compute using a hash function. The sender encrypts the hash total using his or private key to produce the digital signature. The signature is attached to the message itself before transmitting it over a network.

The digital signature provides the recipient with mechanisms to authenticate the sender of the message and to ensure that the transmitted document has not been modified along the way. It also provides the recipient with a record that the message was sent. However, the recipient can deny ever receiving the message; hence the sender also needs a proof of the transaction. A digitally signed acknowledgement from the recipient is one possibility. Another solution would be to have a system similar to an Electronic Data Interchange (EDI) Value Added Network (VAN) where a trusted third party [5] (the VAN vendor) keeps a log of the transactions between the concerned parties.

Digital Certificates

Concern about the actual identity of the message sender identity may still exist. The entire recipient knows is that the sender is in possession of the unique private key that was used to encrypt[10] the message that the recipient successfully decrypted[10] with the corresponding public key. The actual identity of the sender may not be known. The role of a digital certificate is to provide this link between the public key of a unique private-public key pair and the actual identity of a group or individual. It is the combination of the digital signature and digital certificate that fully provides authentication, integrity, and non-repudiation of the sender in a transaction.

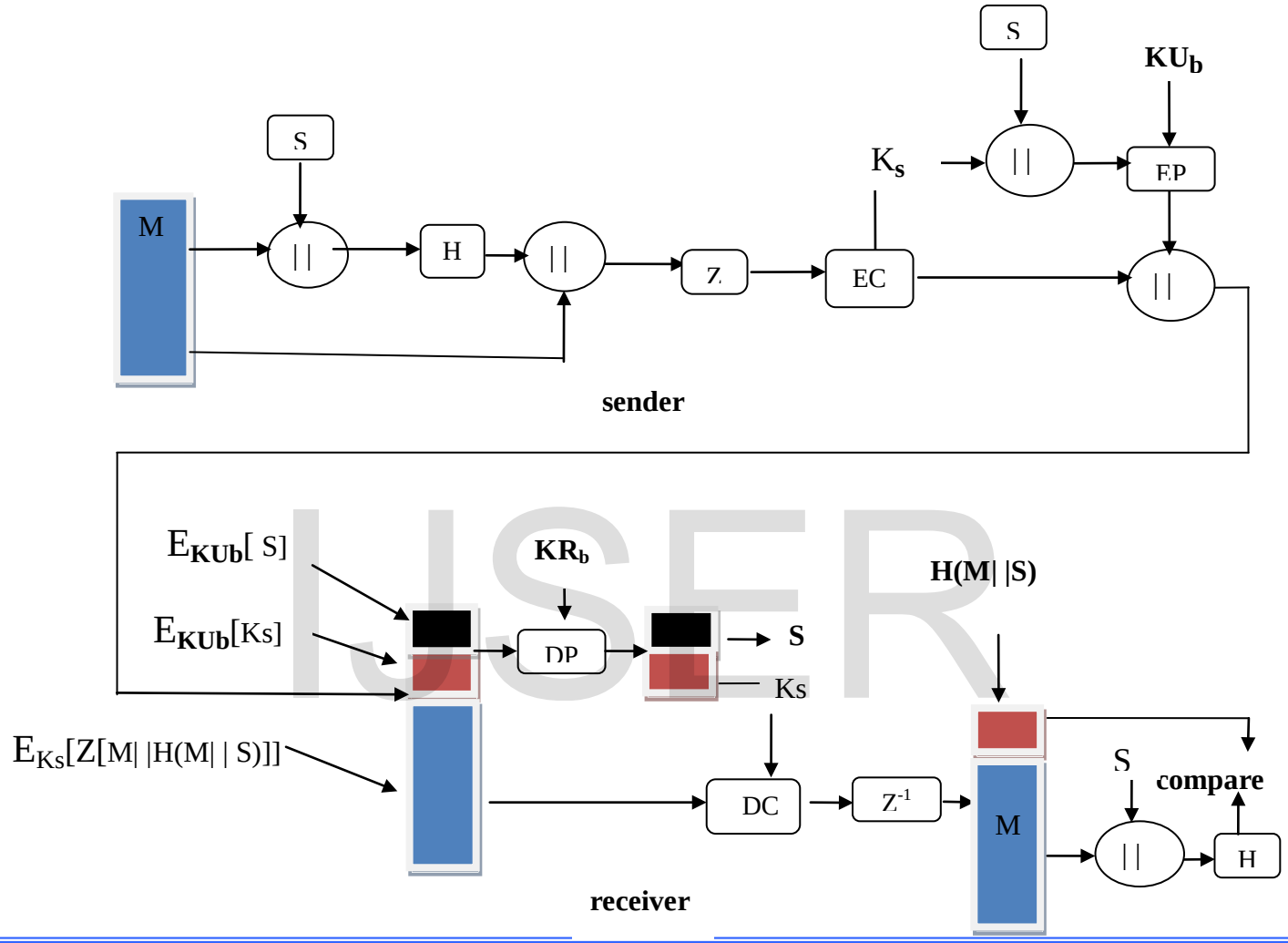
2. Proposed model

It is desired to communicate data with greater security. At present, various types of cryptographic algorithms provide high security to information on controlled networks. These algorithms are required to provide data security and user's authenticity. This new security protocol has been designed for better security using a combination of both symmetric and asymmetric cryptographic techniques, and secretes value and session key, and compression techniques.

Session key:- When two end systems (hosts, terminals, etc) wish to communicate, they establish a logical connection(e.g, virtual circuit). For the duration of that logical connection, all user data are encrypted with a one-time session key. After communication is terminated, the session key is destroyed.

Compression; this protocol compresses the message after applying the signature but before encryption. It has benefit of saving space both for message transmission and for file storage. It also provides greater security to the message.

In the following diagram, **M** denotes the message, **KR** and **KU** are private key and public key of the sender and receiver, and **K**s and S are 128 bit random numbers(11) used as the session key and secrete value , while **EP**, **DP** denotes public key encryption, decryption respectively. **EC** denotes conventional encryption, while **DC** denotes conventional decryption. The hash function is denoted by **H** and the compression using zip is denoted by **Z**, with || indicates concatenation. The proposed model is shown in the Fig1, the working of which is explained below.



The sender generates a message and a random 128-bit number to be used as a session key for this message only. This technique uses a hash function (MD5) but no encryption for message authentication. This assumes that two communicating parties share a common secrete value S. The sender computes the hash value over the concatenation of M and S and appends the resulting hash value to M. Because receiver receives S, he can recompute the hash value to verify. So authentication and data integrity is added to this approach. As default, this technique compresses the message after computing the hash value over the concatenation of M and S, and included with message, M but before encryption. Then the compressed message is encrypted by using conventional encryption AES with a session key Ks. So Confidentiality can be added to this approach because of session Ks, only known by sender and receiver. If no other party knows the key and can recover the plaintext of message from its cipher text of message.

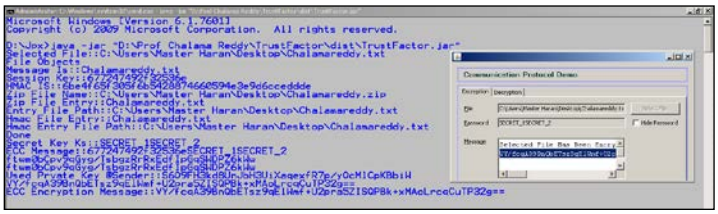


Figure 2: Data Encrpytion Process.

Figure 2 Shows the Encryption Implementation, using JDK 1.6, We have selected a Text File and encrypted it with the above

explained mechanism. The Encrypted Text file will be saved in a different format with .enc extension, so that the receiver will decrypt it.

To protect the session key and secrete key, sender encrypts them with ECC using the recipient's public key KUb, and included with message, and the result is then transmitted to receiver. When the receiver receives the message, he first decrypts the session key and secretes value using his private key, KRb to recover session key and secrete key. He then uses the session key to decrypt the rest of compressed message. Then he decompresses the rest of compressed message. The receiver uses received secrete value S, and computes the new hash value over the concatenation of M and S, and then compares it with the received hash value. If the two match, the message is accepted as authentic. The process of Decryption implementation is showed in Figure 3.

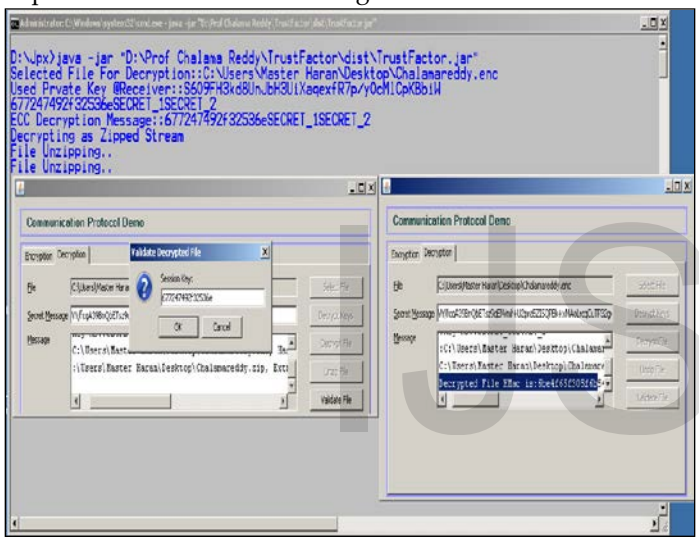


Figure 2: Data Decryption Process and Validating Received Data.

3. Application to fingerprints

Consider a Bio-metric (fingerprint) authentication system. Finger prints of human beings are unique in nature, the captured fingerprints are inconsistent. Since finger prints are often inconsistent, we can't make difference between a tampered one and the inconsistent one. So finger prints must be transmitted securely over the network. Our model is used to transmit the finger print over the network securely. The sender generates a random 128-bit number to be used as a session key for this message only.

This technique assumes that two communicating parties share a common session key Ks and secrete value S. The sender computes the hash value over the concatenation of fingerprint message M and S, and included with the message M, and then compressed. The compressed message is encrypted by using conventional encryption AES with a session key Ks. So Confidentiality can be added to this approach. To protect the session key and secrete value, the session key and secrete value is encrypted using ECC with the recipients' public key and included with the finger print message and the result is then transmitted to receiver.

Later the intended receiver applies the reverse process to obtain the original finger print message and verify finger print message authentication. When the receiver receives the message, he first decrypts the encrypted session key and secretes value using ECC with his private key KR_b to recover session key and secrete value. He then uses the session key to decrypt the rest of the compressed fingerprint message. After decompression the rest of message, receiver recovers fingerprint message M. Then receiver computes the new hash value over the concatenation of M and S, and the result is compared with the received hash value. If the two match, the fingerprint message is accepted as authentic

4. Comparative Analysis:

This section delineates some of the comparison between the existing technique and our technique. The Table.1 shows the comparison of the existing technique and our proposed technique.

	Existing Technique [4]	Our Technique
The Purpose of this technique	This is used to exchange messages and session key between sender and receiver.	This is used to exchange messages ,and session key and secrete value between sender and receiver.
Security services provided	• Message and message digest is encrypted with conventional encryption algorithm ; if it is assured that only sender and receiver share the encryption key, then authenticity and	Message and message digest over concatenation of message and secrete value is encrypted with conventional encryption algorithm ; if it is assured that only sender and receiver share the encryption key, and then authenticity and confidentiality is assured. In addition to providing authentication and

	confidentiality is assured. In addition to providing authentication and confidentiality, a message digest also provides data integrity.	confidentiality, a message digest also provides data integrity
No-of-times encryption processes are required	• Three times • Two times it uses public key encryption process. • One time it uses private key encryption process.	• Two times. • One time it uses public key encryption process. • One time it uses private key encryption process.
Which conventional algorithm used	• IDEA	• AES: it is faster than IDEA
Which Public key encryption algorithm is used to encrypt session key.	• The session key is encrypted using RSA with the recipient's public key and included with the message. • RSA is used. Advantage of RSA: • Well established. • The RSA patents have expired in 2000	• The session key and secrete value is encrypted using ECC with the recipients' public key and included with the message. • ECC is used. Advantages of elliptic curve: • Shorter keys are as strong as long key for RSA • Low on CPU consumption. • Low on memory usage • Some elliptic curve patents are still alive.
Sender public Key exchange required	• Sender public key must be exchanged	• Not required
Which Hash algorithm is used for message authentication and data integrity.	• In this technique, SHA-1 is used. It is slower than MD5 because it takes 4 rounds for each 20 steps needed.	• In this technique, MD5 is used. It is faster than SHA-1 because it takes 4 rounds for each 16 steps needed.
performance	• It gives less performance than proposed technique.	• It gives greater performance than existing technique.
Data integrity	• For checking data integrity, sender public key is needed ,but no secrete value is needed.	• For checking data integrity, Secrete value is required but no sender public key is needed.

4. Conclusion

In this paper we proposed a model for secured transmission of inconsistent information like fingerprints. We discussed the problem of transmitting the fingerprints over the network. This model also solves the problem of sending the same message for a group of members (multiple recipients). In defense applications sending the

same message to all the troops is vital. For those applications this model achieves integrity and confidentiality, and authentication of messages that are transmitted over the network. It also provides better security than PGP protocol used in email security

5. References

1.GiuseppeAteniese "Verifiable Encryption of Digital Signatures and Applications", ACM Transactions on Information and System Security, Vol.7, No.1, February 2004,pp. 1-20.

2.CarlH.Meyer and Stephen M.Matyas, "Cryptography: A new Dimension in Computer Data Security", John Wilsey And Sons, Inc., USA, 1998.

3.National Bureau of Standards/NIST "NBS FIPS PUB 46, Data Encryption Standard", United States Department of commerce, January 1997.

4.Ron Rivest, Ali Shamir and LeornandAdleman "A Method for Obtaining Digital Signatures and public-Key Cryptosystems", communications of the ACM, v.21, n.2, February 1978.

5. Whitefield Diffie and Martin Hellman "New Directions in Cryptography", IEEE Transactions on Information Theory, v. IT-22, n.6, November 1976,.

6. William Stallings "Cryptography and Network Security: Principles and Practices" 3rd Edition, PHI Ltd , 2001.

7. Dan Boneh and Matthew Franklin "Efficient Generation of Shared RSA Keys", Journal of the ACM, v.48, n.4, July 2001,pp. 702-722.

8. Randall J.Atkinson, "Toward a More secure Internet", IEEE Computer, v30, n1, January 1997.

9. Jianying Zhou and Robert Deng "On the validity of Digital Signatures", ACM SIGCOMM Computer Communication Review.

10.Douglas R. Stinson, "Cryptography: Theory and Practice", CRC Press, Boca Raton.

11.T.chalamareddy Dr. R.seshadri "New Design of Crypto-Based Pseudo random number generator (CBPRNG) using BLOW FISH cipher" International Journal on Computer Science and Engineering (IJCSE) June 2013

Dr.R.Seshadri Working as Professor and Director, University Computer Centre,
Sri Venkateswara University, Tirupati.He completed his PhD in S.V.University in 1998 in the field of " Simulation Modeling & Compression of E.C.G. Data Signals (Data compression Techniques) Electronics & Communication Engg.". He has richest knowledge in Research field. He is guiding 10 Ph.D in Fulltime as well as Part time. He has vast experience in teaching of 26 years. He has attended several national and international conferences and published number of technical papers in different national and international Journals.

T.ChalamaReddy Working as Assoc Professor in Narayana Engineering College, Nellore . He completed his M.Tech in J.N.T.University in 2000 in the Specialization of "Software Engineering". His interested area is Networks Security and Cryptography .He has vast experience in teaching of 16 years. He published 3 national and 1 international conferences and 3 papers published in different international Journals.