Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

End to End Multi Client Encrypted Windows Chat System

Karan A[#1], Krithika B[#2], Saurabh M[#3], Srishti B[#4],
[#]School of Computer Engineering,
Vellore Institute of Technology, Vellore, India

Dr. Manikandan K[*5]
[*]Associate Professor,
School of Computer Engineering,
Vellore Institute of Technology, Vellore, India

***Abstract*— In today's world, chat applications have become a very important and useful resource for everyone. To make our conversation more secure, we need some security protocols. For this purpose, an encryption algorithm in a Windows based chat application is required which makes the use of TCP/IP. A group chat system is being made in which RSA encryption is used for security purpose so that only two ends user can read their shared message no other third person can read our messages. Since the threats to privacy of user data is constantly increasing day by day, the current project can serve as an effective means of communication whenever the situation requires to transfer confidential data. In the chat system more than one person can chat by running client-side code in their system, all clients should be connected in same network, which can be local or wide area network.**

***Keywords*— RSA, TCP/IP, Sockets, Public/Private Keys, Cryptosystem**

I. INTRODUCTION

A chat board like service for Windows environment which supports various users on same network. All the messages exchanged are one to one encrypted by the help of "RSA algorithm". The RSA algorithm generates unique public and private keys for every group connected to server, so that the chat messages are completely secure.

For Message Transfer, a Windows based Winsock API, which is specific to the OS is used. Server can be setup on LAN, MAN or WAN like the Internet. IPv4 addressing is used in the project. The number of users and groups connected can be varied dynamically.
For encryption of messages, RSA algorithm is implemented so that all connection lines are secured from eavesdropping. There are unique public keys and unique private for each user group connected to the central server. The server is specifically configured to handle only encrypted data.

II. LITERATURE REVIEW

The basic RSA cryptosystem has 2 distinct quantities p and q. n is chosen as p times q, which is usually the key length. λ(n) is computed as lcm(λ(p),λ(q)) →lcm(p-1,q-1). λ(n) is known as Euler's totient function [1]. This value is kept private. An integer e is selected such that e and λ(n) are co-prime. The key exponent d is chosen as associate degree whole number which is smaller than λ(n) and comparatively prime to λ(n), calculated as $d = e^{-1} \bmod \lambda(n)$ [1]. There are 2 processes within the RSA cryptosystem, one is encryption/decryption and also the different is signing/signature-verification method. Before the message is encrypted or signed, it's split into many blocks with a similar word length within the case. However, the message m is assumed to possess smaller word length than the modulus n. Throughout the encryption/decryption method, the general public key e is employed to inscribe the message m and also the secret key is employed to recover the message m from the encrypted data c as within the signing/signature-verification method, the key d is employed to get the signature s from the message m by exploitation , and also the public key e is employed to verify the signature s by checking whether or not equals the message m.[2] The checking procedure is denoted as signature-verification method.

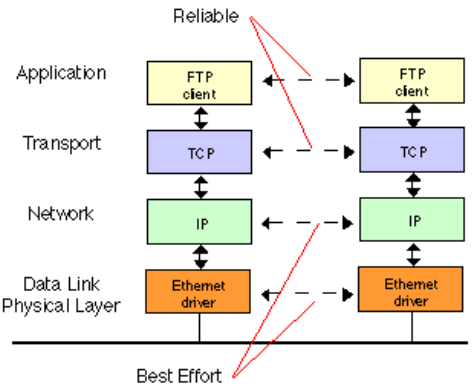

Figure 1: TCP facilitating data transfer over a network using Ethernet

III. EXISTING WORK

1. [3] "A STUDY OF INTERNET INSTANT MESSAGING AND CHAT PROTOCOLS"

It provides a study about the implementation of various popular internet messaging-based chat applications and ongoing efforts to standardize the chat protocols. This provided us with the knowledge of implementing the chat system over a TCP connection.

2. [4] "PEER-TO-PEER COMMUNICATION ACROSS NETWORK ADDRESS TRANSLATORS"

This work addresses connection parameters when connecting to a peer to peer-based system, which provided us insights about why we have chosen central server-based architecture.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

IV. PROPOSED ARCHITECTURE

The software implemented through this project aims to provide completely encrypted communication services to groups of users connected to a central server by the means of TCP. This project is coded in C++.
The 3 main components of the project are as follows-

- Establishing connection using sockets
- Making a client-server interface
- Encrypting the messages (RSA)

Each of the 3 components were implemented separately. This provides us with the flexibility of managing the program parts individually if something is wrong. The final program is implemented by merging all the components to function as one.

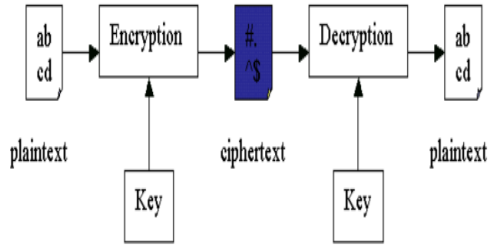

Figure 2. Flow diagram of the encryption-decryption process.

V. IMPLEMENTATION

1. USING WINSOCK FOR SOCKET PROGRAMMING IN C++

- The windows API to socket programming is called Winsock.
- Sockets are the fundamental "things" behind any kind of network communications done by computer.
- For example, when we type www.google.com in our web browser, it opens a socket and connects to google.com to fetch the page and show it to us.

WINSOCK ALGORITHM FOR SERVER

- Creating a socket for the server.
- Binding a socket.
- Listening on a socket.
- Accepting a connection
- Receiving and sending data on the server.
- Disconnecting the server.

WINSOCK ALGORITHM FOR CLIENT

- Creating a socket for the client.
- Connecting to a socket.
- Sending and receiving data on the client.
- Disconnecting the client.

2. ENCRYPTION WITH RSA ALGORITHM

The RSA Algorithm has four steps:

- Key Generation
- Key distribution
- Encryption
- Decryption

RSA is known as an asymmetric cryptography algorithm. The algorithm being asymmetric means is works on two different keys: A Public key and a Private Key. As their names suggest the public key can be given to everyone and the private kept is kept private and is not made public.
For example:

- The Client (for a web browser) sends in public key to the server and requests to fetch some data.
- The server encrypts the data using client's public key and sends the data which is encrypted by it.
- The encrypted data which is sent by the server the client fetches it and decrypts it. Since this algorithm being asymmetric nobody except the web browser can decrypt the data, even if a 3rd party application has the public key of browser it cannot decrypt the data. The basic idea of RSA Algorithm is the fact that it becomes very difficult to factorize a large enough integer. It has a public key, which consists of two numbers in which the one number is multiplication of other two very large prime numbers. The private key for the algorithm is also derived from the same two large prime numbers from which the public key is formed.

Thus, the strength of this algorithm depends on the key size and. If we double or triple the key size, the strength of this algorithm will increase exponentially and it becomes incredibly harder to decrypt it. RSA keys can be typically 1024 or even 2048 bits long, but one report suggests 1024bit keys could be broken in the near future. But till date it is still an infeasible task.

VI. ADVANTAGES

a. The server encrypts the data using client's public key and sends the data which is encrypted by it.
b. Easier to implement than ECC.
c. Easier to understand.
d. Signing and decryption are similar, encryption and verification are similar.
e. Widely deployed, better industry support.

VII. DISADVANTAGES

a. Very slow key generation.
b. Slow signing and decryption, which are slightly tricky to implement securely.
c. Two-part key is vulnerable to GCD attack if poorly implemented.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 03, March-2018

VIII. CONCLUSION

This review paper focuses on secure communication between groups of people on a network using TCP/IP and uses RSA algorithm for encryption of messages.

In today's world, the need of secure channels for communication is increasing, and thus this project establishes one of the most secure and reliable communication system among a group of users. The application is easy to use and works reliably on a local connection or a wide area connection. It is especially useful in situations where data privacy is of prime importance, and conventional means of communication are not a viable choice.

This also provides secure and uninterrupted communication channel in a world where the need for security is constantly increasing.

REFERENCES

[1] Gary Kessler (2018). RSA Public Key Cryptography. [Online].Available: https://www.garykessler.net/library/crypto.html

[2] Claude E. Shannon, "Communication Theory of Secrecy Systems", Bell System Technical Journal, vol. 28, pp. 656-715,1949.

[3] R.B., Jennings, E.M., Nahum, D.P., Olshefski, D., Saha, S., Zon-Yin, C., Waters. (2006). A Study of Internet messaging and chat protocols. *IEEE Network, 20(4), 16-21*.

[4] P.,Srisuresh, B.,Ford (1999). Peer-to-Peer Communication Across Network Address Translators. [Online].Available: https://pdos.csail.mit.edu/papers/p2pnat.pdf