International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 7 ǁ 2021 ǁ PP. 51-54

Securing Client-Server communication by Encryption using Kerberos Authentication System

Pushkar Bhadle [1], Prof. B.B. Gite [2]
Computer science engineering.
Sinhgad academy of engineering, Kondhwa, Pune, India.

Abstract: *Kerberos authentication system is a system which allows to communicate securely between computers, it prevents the stealing of information which is sent across network. Kerberos authentication system is well suited for authenticating users over distributed network which is widely in used. It encrypts the information with help of keys no other third person can decrypt it or decode it. Kerberos never shares a password across network while communicating. Kerberos ensures that third person can not tap the lines or listen all information which is shared across network. So, I am using kerberos authentication protocol to securely communicate between client and server.*
Keywords: *Kerberos; Authentication; Public-Private Key Encryption; Decryption*

Date of Submission: 06-07-2021 Date of acceptance: 19-07-2021

I. INTRODUCTION

From old mythology Kerberos got its name. In Greek mythology there is word Cerberous which means it is a three headed beast just like a dog which is guarding something which needs to be secured. In late 1980's at MIT the design of Kerberos was stated with project name Athena. Kerberos is authentication mechanism for distributed network. Kerberos authenticate the client and server before communicating. This makes sure that the client which is communicating is authenticated client and the server which is communicating is authenticated server. First public version of kerberos was kerberos version 4. In 1995 actual version 5 was release, after there were many reviews were given for version 4. Kerberos specifications are defined in internet RFC 1510 [4]. Initially kerberos was only design for UNIX system. But after a wide public review and it is uses is available for all major operating systems. There are many commercial versions are developed later which can be use for different purposes and that are freely available in MIT [6]. Kerberos is designed keeping in mind that there are three threat exists when client and server wants to communicate in distributed network which can be located anywhere.

- Third person may get access of workstation and can communicate to clients on be half of original workstation.
- Third person may get access of other user network and change his details and can send communicate to server on behalf of original user
- Replay attack - Third person may keep watch on information which is exchanging over network and after some time he can use that information to access the server.

In all three cases given above, third person my get an access to data which is not authorize for him. So, there was a need to develop the authentication protocol in world. Hence, MIT came up with a centralized server which can authenticates users as well as servers which are communicating over network. Symmetric encryption is used by Kerberos authentication protocol, but we will try to use public key encryption.

II. LITERATURE SURVEY

Turkan Ahmed Khaleel (2020), In his paper entitled by "Review of Network Authentication Based on Kerberos Protocol" stated Securing user information and server resources is crucial in authentication especially with distributed systems architectures and networks. Attackers can keep watch on user-server traffic and grab the needful information from rightful owner. Hence need of strong authentication method is required, and Kerberos authentication system is well suited for authenticating users in such challenges [8].

Jabbar Al-Gburi (2017), In his paper entitled "Protect Data from Attacking by Authenticate Clients Using Kerberos Protocol" stated that Every system needs a security protocol that can helps them to protect their data from attacker from losing information as well as to prove their identity. Kerberos allows the clients to

prove its identity to an application server. This paper explains how kerberos based on secret key encryption and extend the security for the system. It also states that how was the system before kerberos authentication protocol [9].

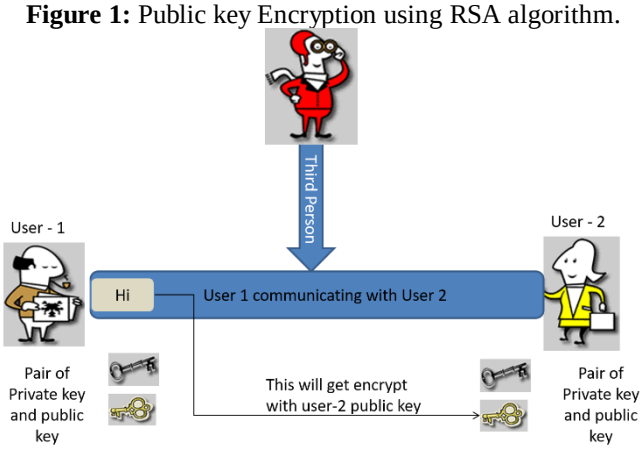
Yun-yun Du, Hong-yun Ning, Ping Yang, Yan-xia Cui (2014), In their paper entitled by "Improvement of Kerberos Protocol Based on Dynamic Password and "One-time Public Key" stated that kerberos is widely used network security protocol and they tried to improve kerberos protocol by focusing on new dynamic password and one public key. Public key encryption is slower that one key encryption which can improve the efficiency and optimize an algorithm [10].

III. PROPOSED METHODOLOGY

In proposed methodology we will use the public key encryption. By using the public key encryption, resolves the distribution of key. Mainly kerberos uses a symmetric cryptography, where clients' needs to share the key before commutating with server. In public key cryptography client's private key is not get shared over the network. Client can share his public key before initiating the communication. With help of this data or message gets encrypted. This method is used in email communication which is known as Pretty Good Privacy (PGP). Main advantage of kerberos authentication system is that there is no need to store any key and no need of sharing those keys before initiating a communication. To get a ticket from ticket granting server client only needs to give is public key. The KDS then uses this public key to encrypt this ticket and session key [7]. Everybody can easily create his own pair of public key and private key pair. Public key which is used to share with everyone and the private key which they can only keep with themselves. To have valid public keys there is a need of authorisation. Hence additional infrastructure is required to sign those keys. The keys which are signed are only considered as authorised keys. A trusted Certification Authority (CA) is used to sign the public key. All public keys need to be signed by this CA. Client can share his keys which are signed by authorised CA. When client gives his public key authentication service checks whether this key has a valid signature which was given by trusted authority. After verifying a valid sign authentication server give the session keys to clients for communication. When client receives it, He then decrypts it with the help of his private key, which is a pair of his public key which was initially shared. Following like this, A communication is handled in kerberos with help of public key cryptography. This algorithm is known as RSA algorithm.

Diffie and Hellman has done a research on cryptography and challenges the cryptographist to do new research on crypto graphical algorithm that can match up the public key system. Various algorithm is proposed with public key encryption. Some of them have given a great result. Around 1977, Ron Rivest, Adi Shamir, and Len Adleman are the guys who tried to solve the challenges and got successful in it. Hence this is known as Rivest-Shamir-Adleman (RSA). This protocol was widely used and accepted. The plain text and cipher text values lies in between 0 and n-1 where n is integer for RSA protocol. Where the general size of n is 1024 bits, or 309 decimal digits. It means that n value will be less than 21024.

Figure 1: Public key Encryption using RSA algorithm.



Algorithm Description

RSA uses an exponential with expression. Here the data which needs to encrypted is encrypted in blocks, where block size is in binary value and always less than some x value which we can consider as n. Each block size value should always be equal to log2 (n) + 1 or less than log2 (n) + 1; For consideration, we can say

that block size is i bits, where $2^i\ n \leq 2^{i+1}$. For some of plain text block M and block of cipher text C, Encryption and decryption are of following form [3].

$$C = M^e \bmod n$$
$$M = C^d \bmod n = 1M^{ed} \bmod n = M^{ed} \bmod n$$

Value of n must be available to both client and server side. Value if e is available to client while value of d is available to server. Hence, public key of $PU = \{e, n\}$ and a private key of $PR = \{d, n\}$ are with public key algorithm. There are some preconditions which must be met for this public key algorithm:

1. It should be possible to get values of n, d, e such that $M^{ed} \bmod n = M$ for all values of $M < n$. [5]

2. It should be easy while calculating
$M^e \bmod n$ and $C^d \bmod n$ for all values of $M < n$. [5]

3. It should be impossible to get d given e and n. [5]

Firstly, we can focus on the first requirement where we must find out the relationship of the from -
$M^{ed} \bmod n = M$

The previous relation controls if d and e, are multiplicative inverses modulo $\varphi(n)$, where $\varphi(n)$ is the Euler totient function $\varphi(pq) = (p - 1)(q - 1)$. Were,
$ed \bmod \varphi(n) = 1$
is a relationship between d and e.
Considering above we can say that mod f(n) is multiplicative inverse

IV. RESULT AND ANALYSIS

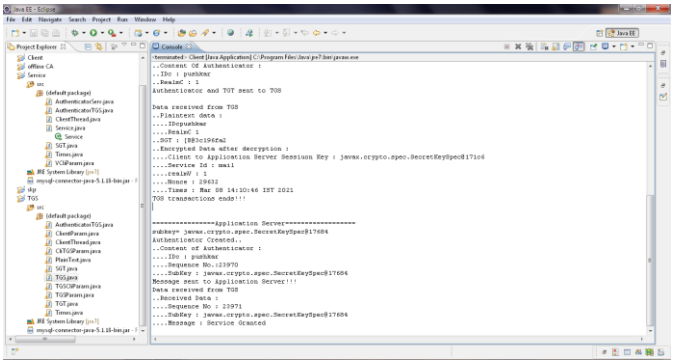


Figure 2: Output result of sending message.

This shows that without sharing secret keys client and server can communicate with each other.

V. CONCLUSION

Kerberos allows us to securely communicate between client and server. Kerberos is authenticating client and server is biggest main advantage of it. Kerberos ensure that passwords are never to be sent across the network while communicating. Adding public key in kerberos authentication level ups the authentication and security level of the system. Using kerberos we can secure the communication between client and server. In addition to this kerberos is completely based on open internet standards which makes it to use widely across many big and small-scale companies.

REFERENCES

[1]. M. A.-s. R. Sufyan T. Faraj Al-Janabi, "Public-Key Cryptography Enabled Kerberos Authentication," in 2011 Developments in E-systems Engineering, Dubai, United Arab Emirates, 2011.
[2]. D. A. M. Alan H. Harbitter, "Performance of Public-Key-Enabled Kerberos Authentication in Large Networks," in IEEE, 2001.
[3]. T. Y. S. H. K. R. C. Neuman, "The Kerberos Network Authentication Service (V5)," Internet Society (ISOC), 2005.
[4]. C. N. J. Kohl, "The Kerberos Network Authentication Service (V5)," Internet Society (ISOC), 1993.
[5]. L. a. B. T. Zhu, "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)," 2006.
[6]. [Online]. Available: www.mit.edu/kerberos.
[7]. L. L. P. a. K. J. Zhu, Kerberos Cryptosystem Negotiation Extension, 2006.
[8]. T. A. Khaleel, "Review of Network Authentication Based on Kerberos Protocol," Journal of Basic Education college, vol. 16, pp. 1141-1150, 2020.

[9]. J. Al-Gburi, "Protect Data from Attacking by Authenticate Clients Using Kerberos Protocol," International Journal of Scientific Research in Science, Engineering and Technology, vol. 3, no. 6, pp. 687-689, 2017.
[10]. H.-y. N. P. Y. Y.-x. C. Yun-yun Du, "Improvement of Kerberos Protocol Based on Dynamic Password and "One-time Public Key"," in IEEE 10th International Conference on Natural Computation, 2014.