THINK INDIA JOURNAL ISSN: 0971-1260

Vol-22-Issue-16-August-2019

Optimization of Kerberos

Puneet Kumar
(puneetlpu1@gmail.com)
Assistant Professor, School of Computer Science & Engineering
Lovely Professional University, Jalandhar Punjab

Sudha Shanker Prasad
(sudha.21826@lpu.co.in)
Assistant Professor, School of Computer Science & Engineering
Lovely Professional University, Jalandhar Punjab

Abstract

Kerberos is a third party trusted protocol used for authentication which is based on the symmetric key cryptography which means server and client will share only one key for encryption as well as for decryption. Now this paper analyses how Kerberos actually works and provide some idea how to improve the performance of this authentication protocol by removing some steps from it. In this paper the solution has been given to interact minimally with the client and provide the same security and trust in the authentication.

Keywords: Authentication, Cryptography, Decryption, Encryption, Session Key.

1. Introduction

Kerberos is the third party authentication protocol which means that for the authentication purpose server and client has to rely on someone else which will authenticate both the server and client. Kerberos authentication is based on symmetric key cryptography which means that the client-side and server-side will share a common key for encrypt and decrypt in server & client side. In this Client proves it by encrypting the message with the key and the server again decrypt the same message with a same key. After this, Server again encrypts the message and sends it to the client again.

Kerberos authentication depends on the central server which is called KDC which provides all the keys. KDC stands for key distribution center. KDC issues the ticket granting to the client which want to access a resource from the server. Kerberos authentication is used in various places but the biggest achievement of the Kerberos

authentication is that it is used as default authentication in Windows XP and Windows 2000. The only limitation in the Kerberos is the scalability as it is very important in this modern era where everything is expanded day by day along with the usage of internet. However, Kerberos can achieve the Scalability with the help of public key cryptography.

2. Working of Kerberos

The Kerberos authentication is done in three major steps: -

- Initial Ticket Granting Ticket is acquired by the Client.
- Client uses the acquired Ticket granting ticket to get the ticket to access the resources from the server.
- The client uses the ticket to access the resources from the server.

2.1.1 Initial Ticket Granting Ticket (TGT) is acquired by the Client:

To get the TGT client has to go from several steps which are as below.

- First user access the client system using the username and the password.
- After login, password in encrypted by the user.
- Asserting further, Client request the credentials for the TGT through a KDC message along with authentication message and user's encrypted password. Authentication message includes client name, network address and timestamp.
- Encrypted password is compared with master copy through authentication server in KDC so that client can be verified after the password matches. KDC also compares the timestamp and it should be within 5 minutes of its own time.
- If each thing matches, then KDC generates credentials that is requested for ticket granting ticket service for creating the login session key and encrypt it with user's key.
- KDC also defines another credential which contains login session key and encrypts it with its master key.
- Moving further, KDC sends both these credentials to the client where client decrypts the logon session key with its encrypted password and stores the logon session key along with TGT in its ticket cache.

2.1.2 Client uses the acquired Ticket granting ticket to get the ticket to access the resources from the server

- In this step client demands the ticket from the KDC to access the resources from the server, for this client present its TGT, name of the resource and message for authentication which is already encrypted by the client with the help of the login session key.
- The KDC decrypts the TGT using its master key and extracts the login session key. This Session key is then used by the KDC to decrypts the message from the user. User is verified, if matches.
- After this KDC creates the service session key for the client so that it can be presented by the client to the server whenever client requests the resource from the server. This service session key is encrypted with the logon session key of client. KDC Also encrypts this session key service with master key of the server. This all is done by ticker granting service in KDC.
- After this, KDC send both the credentials to the Client which decrypts the service session key with the help of the logon session key and stored the Service session key along with tickets in its cache.

2.1.3 The client uses the ticket to access the resources from the server

This is the final step in the Kerberos authentication and it involves the following steps:

- The Client in this step sends the session ticket along with the authentication message and encrypts it with service session key.
- The service session of the server is decrypted using its master key and with the help of this session key of service decrypts the message sent by the user, after decrypting the authentication message get session ticket for server and timestamp is being compared with on the time of request in respect of client with its own time to make sure it is within 5 minutes or not.
- Timestamp from the session ticket with session key of service is encrypted by server and sends it to the client.
- The client then decrypts the message and compares it with its original timestamp. If it matches, then user gets authenticated and gets the access on the requested service of the server.

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

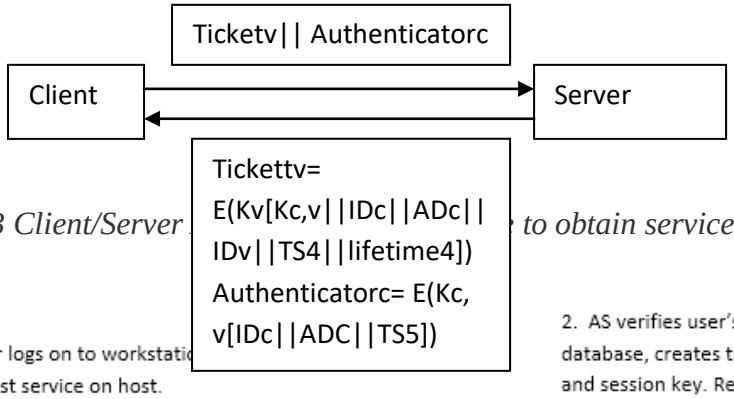

Fig.3 Client/Server ... to obtain service

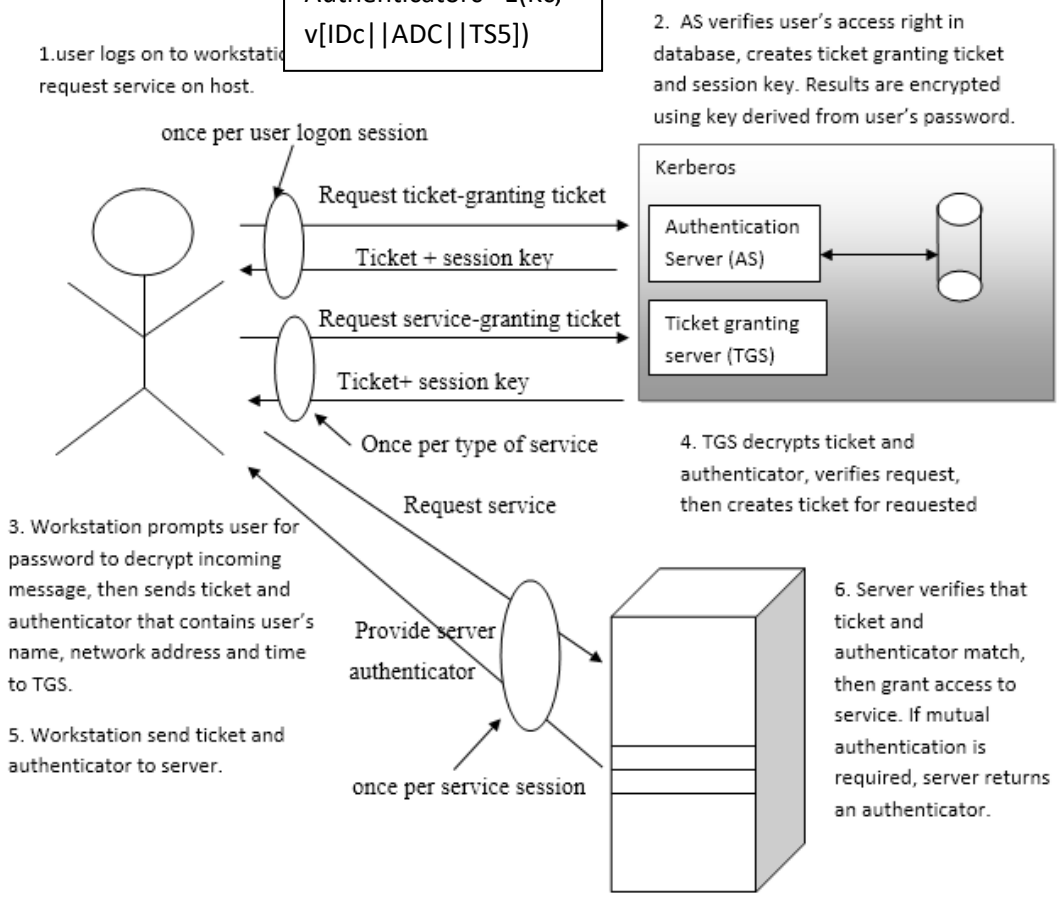

Fig. 4 Overall Working of the Kerberos Authentication

3. Limitations of Kerberos

Kerberos is not an effective technique when we talk about password guessing attacks; if the user chooses a password which is poor, and then an attacker can guess that password easily and impersonate the user. Moreover, Kerberos required a trusted and secured path between the paths where passwords are entered. If the user enters a password from the path which is already being modified by the attacker with the help

of Trojan horse or the initial path is being monitored by the attacker where the user will enter his password, then the attacker can get the enough information to impersonate the user. However, these limitations can be improved by using the Kerberos with other systems.

4. Proposed system for Kerberos Authentication

The Kerberos authentication scheme can add the option to ask the user to authenticate for the personal system or the public system. If the user select the personal system then the session key and service session key will be generated first time only when the user logs in from his personal system , rest of the time the Kerberos authentication will ask only for user password and if the authentication is correct then the user can access the resources of the server without exchanging the session key and the service session key by doing this a lot of time will be saved while if the system is public then each time the same process will be done as the Kerberos does normally.

Then second thing which can be done in Kerberos authentication is that when the user enters its user name and password the client goes to authentication server and when the password matches it creates the session key and send the message back to user which is encrypted by user password and the user then decrypts the message and gets the session key and ask for the TGS and encrypt that message with the session key and now TGS decrypts that message and generate service session key. Now these steps can be reduced by deleting the step in which the authentication server sends the message back to client and client sends the message to TGS. The new step will be the user will send his username and password the client will send it to authentication server here the authentication server will check the client password and see whether the user is verified and generate a session key. Now this session key will be encrypted with user password now authentication server will send this message to the TGS along with session key where the TGS will generate the service session key and encrypt it with session key and send this whole message to client where client will first decrypt the session key and after this use this session key to decrypt the service session key.

ISSN: 0971-1260

Vol-22-Issue-16-August-2019

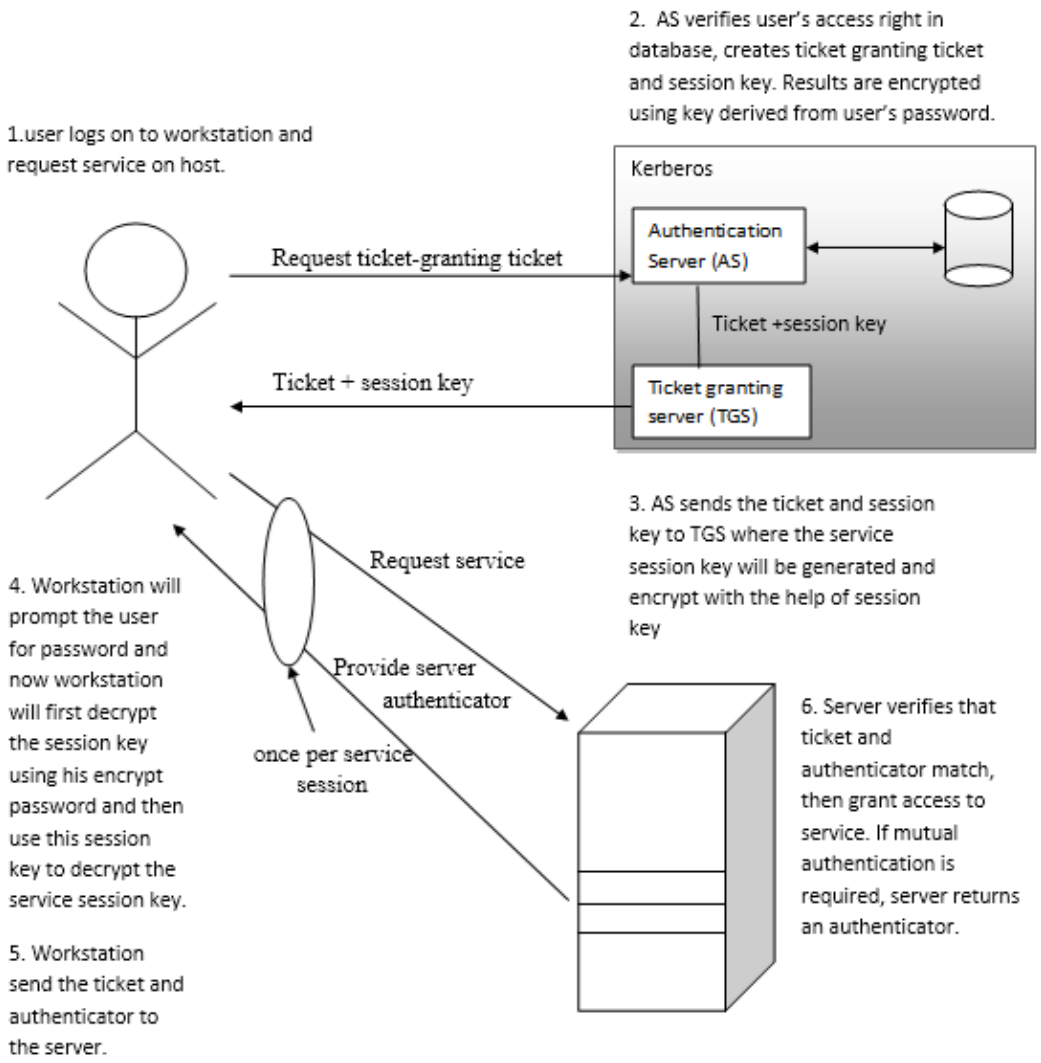

Fig. 5 Proposed System for Kerberos Authentication

5. Conclusion and Future Work

Proposed system require less number of steps to communicate with server with the KDC and it leads to time efficient system without missing any security constraint. If the system is personal system, then in our system improvement is done by reducing the number of steps before communication for getting session key from KDC and if the system is public nothing is changed from previous system.

In future it can be improved for the public system as well as more steps can be reduced from the proposed system which enhance the efficiency of Kerebros without affecting its security policies.

References

[1] Kristin Lauter: The Advantages of Elliptic Curve Cryptography for wireless Security, Microsoft corporation, IEEE Wireless Communications • February 2004.

[2] R. Sakai, K. Ohgishi, and M. Kasahara. Cryptosystems Based on Pairins, The 2000 Symposium on Cryptography and Information Security, 2000.

[3]www.giac.org/cissp-papers/47.pdf

[4]www.kerberos.org/software/adminkerberos.pdf

[5]technet.microsoft.com/en-us/library/cc780469(v=ws.10).aspx

[6]http://searchsecurity.techtarget.com/definition/Kerberos.

[7] J.Kohl and C.Neuman, "RFC 1510: The Kerberos Network Authentication Service (V5)," Sep.1993.

[8] H.-Y. Chien and J.-K. Jan, "A hybrid authentication protocol for large Mobile network," The Journal of Systems and Software, vol. 67, no. 2, pp. 123–130, Aug. 2003.

[9] G. Bella and E. Riccobene, "Formal analysis of the Kerberos authentication system," Journal of Universal Computer Science, vol. 3, no. 12, pp. 1337–1381, Dec. 1997.

[10] A. Scedrov, F. Butler, A. D. Jaggard, and C. Walstad, "Formal analysis of Kerberos 5," Theoretical Computer Science, vol. 36, no. 1–2, pp. 57–87, Nov. 2006.

