ISSN: 2321-7782 (Online)
Volume 2, Issue 2, February 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

KERBEROS: An Authentication Protocol

Sanket Bhat[1]
Padmabhooshan Vasantdada Patil Institute Of Technology
Pune – India

Saumitra Damle[2]
Padmabhooshan Vasantdada Patil Institute Of Technology
Pune – India

Priyanka Chaudhari[3]
Padmabhooshan Vasantdada Patil Institute Of Technology
Pune – India

Abhijeet Saraogi[4]
Padmabhooshan Vasantdada Patil Institute Of Technology
Pune – India

Abstract: ***In an open network computing environment, a work station cannot be trusted to identify its users correctly to network services. Kerberos provides an alternative approach whereby a trusted third-party authentication service is used to verify user's identities. This document gives an overview of the kerberos authentication protocol frameworkThe document describes the protocols used by clients, servers and Kerberos to achieve authentication. It also describes the management and replication of database required. Kerberos is a computer network authentication protocol, which allows nodes communicating over a non-secure network to provide their identity to one another in a secure manner. It provides mutual authentication – both the user and the server verify each other's identity.***

Keywords: Client, Server, Ticket, Kerberos.

I. INTRODUCTION

When the network connection (internet) came into picture then the password based authentication was invented. But this present authentication system is not good enough to ensure the users safety of personal data. The Password Based authentication can be easily known by the attacker to know the password. And also the user must always remember the password, and enter it every time he tries to login. The attacker can know the password by hit and trail method.

So, in all, the problems of network eavesdropping and internal security are not solved with password authentication.

Therefore the development of the Kerberos concept for the authentication of one workstation to another has recently been intensified.

Kerberos is an authentication system that uses symmetric key cryptography to protect sensitive information on an open network. It is a ticket based system in which Kerberos server issues a ticket encrypted with the user's password when the user logs in. The user decrypts the ticket and uses it to obtain tickets for other network services he or she wants to use.

II. LITERATURE REVIEW

Kerberos is the Protocol in which a client will authenticate to a server and receive a ticket from it. It consists of the three parties. Those are the client, the server and the key distribution server. Whereas the key distribution Centre consists of authentication server and ticket granting server. A file is sent from the client to the authentication server with certain username and password. Then the authentication server checks with the database to find the username stored in the kerberos' database. If the match is found then the ticket granting server replies with the secret key to the client. It is based on the trusted third party protocol and symmetric cryptography protocols. It shares different secret key with different entity on the network. The proof of identity equals to the knowledge of that secret key. 1. Client is requesting for a Ticket Granting Ticket and waiting for the response. 2. A Ticket Granting Ticket is been confirmed and issued to the client. 3. Client is again requesting for a server ticket to which the Ticket Granting Server will confirm it to the client. 4. A TGS i.e. Ticket Granting Server or server ticket is been

issued in order to communicate among the client and server. 5. Client will send a request regarding for the service to the server and waits for the response. Kerberos mainly uses two types of keys for generating tickets and authenticators. If a client wants to communicate with the server then it sends a name to the TGS and waits for the response. Kerberos authentication server looks up in the database whether the received client information is stored or not, and thenit issues a session key which is been used between both which is known as the Ticket Granting Ticket (TGT). Then encryption of the session key with the client's secret key is done by Kerberos. A TGT is created in order to authenticate with the TGS and can encrypt the TGS's secret key and both of these encrypted messages are send back to the client by the authentication server. The session key is been retrieved after the client decrypting the first message and one way hash method is to be used for it. If any of the conditions are not been satisfied with the exchanging of the keys then the authentication process is n77ot be in further process and leads to the deny of the access. TGT and session key are been saved by the client and the password is been erased by the one way hash. Checking of the time stamps [6] and all other assumes over the machines have the synchronized clocks at least to within several minutes.

III. PROPOSE SYSTEM

A. *Purpose*

The main objective in the proposed technique is to have the highest impact, and acceptance among average applications. Hence, a kerberos frame work which can be easily integrated into any client server application is being proposed. For wider acceptance the simple and user friendly user interface is being made.

The proposed technique will work with any average application using encrypted ticket based communication without compromising on security.

B. *Architecture*

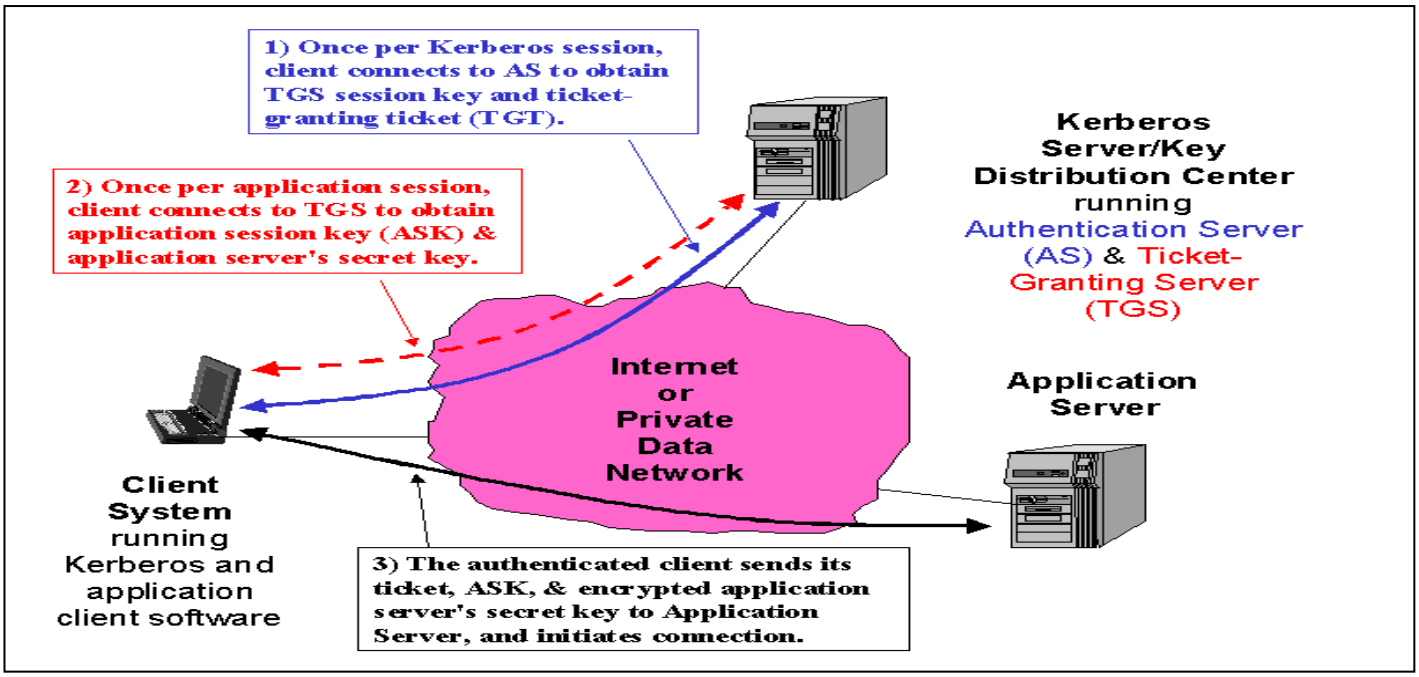

Fig. 1 Architecture of kerberos protocol

C. *Mathematical Model*

Problem statement: To build an application helps user to have secure authentication by using ticket based communication.

1. *Problem description*

Let S1 be the set of user/controller in our system.

S1= { C , AS , TGS , V}

C = Client

AS = Authentication Server

TGS = Ticket Granting Server

V = Server on which we want to access the service

Let S2 be the set of objects in our system.

S2 = { ID_c , ID_{TGS} , T_S , K_C , K_V , lifetime , AD_C , $Ticket_{TGS}$, $Ticket_V$ }

ID_C = ID of client

ID_{TGS} = ID of Ticket Granting Server

K_C = Key of client

K_V = Key of Server

AD = Address

$Ticket_{TGS} = E(K_{TGS}[K_{TGS} || ID_C || AD_C || ID_{TGS} || TS_2 || lifetime])$

$Ticket_V = E(K_V [K_{C.V} || ID_C || AD_C || ID_V || TS_4 || lifetime])$

$Authenticator = E(K_{C,TGS} [ID_C || AD_C || TS])$

Working:

There are three stages in our problem solving

A] Authentication service exchange to obtain Ticket Granting Ticket ($Ticket_{TGS}$)

1. C -> AS

   $ID_C || ID_{TGS} || TS_1$

2. AS -> C

$E(K_C[K_{C,TGS} || D_{TGS} || TS_2 || lifetime || Ticket_{TGS}])$

In the above stage client request As for Ticket(access) to TGS Server.

As checks client authenticity and sends $Ticket_{TGS}$ to Client.

B] Ticket granting service exchange to obtain server granting Ticket($Ticket_V$)

3. C -> TGS

   $ID_V || Ticket_{TGS} || Authenticator_C$

4. TGS -> C

   $E(K_{c,TGS} [K_{C,v} || ID_V || TS_4 || Ticket_V])$

In the above stage client sends the ID and $Ticket_{TGS}$ to TGS to authenticate itself.

The TGS replies with a $Ticket_V$ (Ticket to Server).

C] Client|Server Authentication Exchange to obtain service

5. C -> V

$Ticket_V || Authenticator$

6. V -> C

E ($K_{C,V}$ [TS_{5+1}]) For mutual authentication

In the above stage client sends $Ticket_V$ to server to authenticate and access service.

Thus we see from above solution that in our problem solving there are no unknown stages or unpredictable branching.

Thus we can conclude that the problem is a P(Polynomial Time) Problem as it is deterministic in solving[1].

IV. FEASIBILITY STUDY

Feasibility study is performed to determine the possibility or probability of either improving the existing system or developing a completely new system. Following are the feasibilities, which are considered for the development of the application:

- Operational Feasibility: It means to estimate whether it is required to the train the user to handle the system. In this case there is only training of interaction with user interface. Since the users are computer literate it would not to be difficult to adapt to new system.
- Technical Feasibility: Technical feasibility is to estimate whether it is possible to develop the proposed system with the available hardware and software and network resources. Since all proposed hardware, software and network requirements are easily available; the development of the application is feasible.

We can prove that our system is P-Complete because in our system the most complex module is kerberos module but it is implemented in polynomial time. So our can be considered as P-Complete.

From above mathematical model we can see that in our problem solving there is no unknown stages or unpredictable branching.

Thus we can conclude that the problem is a P(Polynomial Time) Problem as it is deterministic in solving[1].

V. SYSTEM FEATURES

A. *Functional Requirements*

- **Client:** Client sends Client id and Server id over the network to Kerberos for authentication.
- **Remote Computer: -** The Remote Computer will consist of Web browser that will contain log-in interface.
- **Kerberos**: - Kerberos consist of AS and TGS.AS receives request from client, it verifies and sends TGS address back to client along with TGT specifications. TGS than receives request from client for server access .TGS verifies and sends back Session specifications to client and server.
- **Server**: -Server receives access to service from client along with Session specifications. Server verifies Session information and gives service to client

B. *Non-functional Requirements*

- Secure access of confidential data (user's details). SSL can be used.
- 24 X 7 availability.
- Better component design to get better performance at peak time.
- Flexible service based architecture will be highly desirable for future extension
- Ease of Use- Few clicks, intuitive, flexibility, performance and installing/download.

- Security- Privacy, Confidentiality, Integrity, Authentication, Verification/Non-repudiation.
- Technical Acceptability- Integration Effort, Interoperability, Scalability, Remote Access, Performance.

VI. FUTURE SCOPE

Security has been an issue since internet came into picture. kerberos was invented to come over the security issues. Current infrastructures offer a comfortable environment for secure communication over network, but the structure is not portable and scalable. for instance consider Windows OS, red hat, apple, sun etc. they have integrated kerberos into their operating system. In other words we can say that they have vendored their own version of kerberos. We are going to see Kerberos as a framework working for any application rather than being integrated with just one. This kerberos framework can be improved further to integrate into adhoc network.

The above proposed framework of kerberos is implemented considering the available technology infrastructure. The algorithms can be changed according to the network needs in the future. The framework is secure and scalable. Kerberos is currently available for the various operating systems, databases, and other vendored applications. kerberos will be seen to support mobile devices in future.

VII. CONCLUSION

In this paper we have proposed an authentication protocol framework, considering the security issues over the network during authentication process. The proposed protocol framework not only satisfies the need of authentication that is generally required in the protocol, it also provides the better security as the trusted third party is involved. the proposed framework is designed in a way so that it can be used with any application instead of integrating it with just one. Although the proposed technique has been optimized for the current AES algorithm, but it can be made enable to accept future improvements as the security algorithm advances, with minimum change in the protocol framework structure.

Acknowledgement

We are greatly indebted to our college Padmabhooshan Vasantdada Patil Institute Of Technology that has provided a healthy environment to drive us to do this project and thankful to our management for their guidance

References

1. William Stallings,-"Cryptography And Network Security ". Edition 5,year 2007
2. Fabrice Kah Giac-"Understanding Kerberos V5 Authentication Protocol Security Essentials Certification (Gsec)" - November 2003.
3. J Kohl, C Newman -"The Kerberos Network Authentication Service (V5) "– 1993.
4. Clifford Neuman And Theodore Ts'o "Kerberos: An Authentication Service For Computer Networks ". – 2001.
5. Http://Www.Kerberos.Isi.Edu/ - THE KERBEROS HOMEPAGE.
6. HP-KERBEROS white Paper.
7. Asad Amir Pirzada and Chris McDonald-"Kerberos Assisted Authentication in Mobile Ad-hoc Networks " The University of Western Australia 35 Stirling Highway, Crawley, W.A. 6009, Australia.
8. Kashif Bashir and Mohammad Khalid Khan-"Kerberos Authentication in Mobile Ad-hoc network to prevent Ticket replay attack."IACSIT International Journal of Engineering and Technology, Vol. 4, No. 3, June 2012.

