KERBEROS

Prof. Saroj Singh*

Abstract

Security is architecture and not an appliance. Before describing what basically koreros is one need to know the security threats that are related to the network. In Greek methodology, Kerberos was Greek Got 'Hades', watchody that generated the gates of the underworld Kerberos is network authentication protocol that provides strong authentication for client/server applications. Kerberos uses secrete key cryptography and require a third party. Kerberos is the best choice for most Microsoft office Share Point Server (MOSS) 2007 implementation in an intranet.

Keywords: Keywords: Authentication; cryptography; client/server; Hades; susceptible;

* **Dept. Computer Science & Engineering, Delhi Engineering College Ladiyapur, Faridabad, India**

I. INTRODAUCTION

The three security threats due to which Kerberos came into existence are:

a) Application sending password in an encrypted format is susceptible to threats.

b) Client applications or server applications relay that user is not faking with its identity.

c) Some network uses firewalls and the main disadvantage with firewalls is that firewall assumes that the attacker is outside the network. Most of the really damaging attacks are performed by the insider only.

Definition: Kerberos is network authentication protocol that provides strong authentication for client/server applications. Kerberos uses secrete key cryptography and require a third party.

Kerberos works for both password-based and smart card enabled authentication.

II. HISTORY

In Greek mythology, Kerberos was the Greek Got 'Hades', watchody that generated the gates of the underworld.

Kerberos was the best choice for most Microsoft office [1] Share Point Server (MOSS) 2007 implementation in an internet.

History: Kerberos was developed at MIT [2] in early 1980's. There was computing shift from mainframes to workstations. It uses the concept of network credentials.

A. Characteristics:

a) Provides strong cryptography so that the client and server can prove their identity across an insecure network connection.

b) After identification one can assure privacy and integrity of data transmission.

c) It is aimed at client/server model.

d) It provides mutual authentication.

e) It uses port 88by default.

B. Requirements:

a) It can integrate with the existing technology.

b) Single sign in for users.

c) It separate within distributed systems which are based on an open internet.

d) Mutual authentication must take place before any communication process.

e) Password should never be exposed during authentication.

f) Central administration of authentication should be kept secret.

g) It should make use of cryptographic measures.

h) It must support arbitrary distribution of services.

i) Do not trust any party until authentications done.

j) Operates in a hostile environment.

III. COMPONENTS

Kerberos uses the Symmetric Neeldham-Schroeder protocol [3]. It uses the third party called key distribution consists of two parts:

a) Authentication Sever

b) Ticket granting server

A. *Role of KDC [4]:*

a) Maintenance of database containing secret keys.

b) Generates a session key which is used by communication parties to encrypt transmission.

IV. KERBEROS TICKETS

These are short lived assertions of authority and the security of the protocols is based upon it.

A. *Working:*

The networking of Kerberos can be explained in the following steps:

a) Client authentication itself to the authenticating server.

b) Authenticating server forwards the username to the key distribution center.

c) Key distribution center [5] issues a tickets granting ticket (TGT). TGT is time stamped and is encrypted using the password.

d) The encrypted output is returned to the user.

e) If it is successful the user can now access the desktop.

B. ***Components of TGT***

a) Client ID

b) Client network

c) Ticket validity period

d) Client /TGS session key

C. ***Component of authenticator***

a) Client ID

b) Timestamp

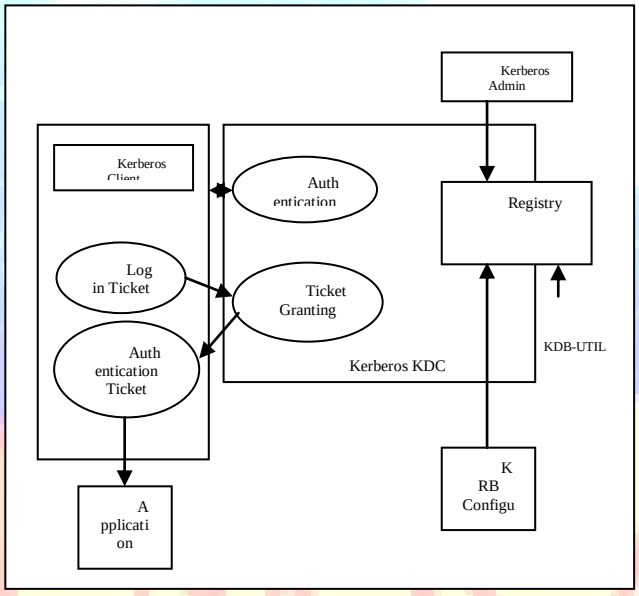

Figure 1: Kerberos Ticket

D. ***Components of client – server ticket***

a) Client ID

b) Client network address

c) Valid period

d) Client – server session key

E. ***User client based login***

a) User enters username and password on the client machine.

b) Client performs a one way function on the entered password. Thus this becomes secret key of client/user

V. CLIENT AUTHENTICATION

a) Client sends the message of the user ID to the authenticating server.

b) Authenticating server [6] generates secretes key by performing hashing on the password of the user. This password is found in the database.

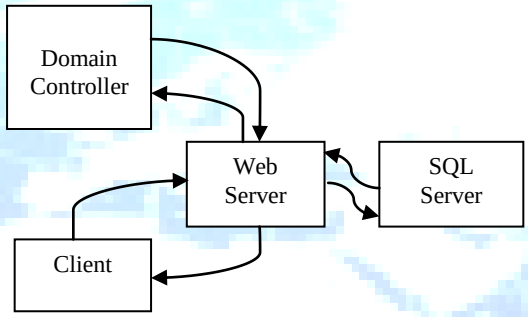

Figure 2: Client Authentication

c) Authenticating server [7] then performs the following functions:

- Authenticating server checks whether the client is in the database or not
- If the client is present in the database, then the following messages are sent back to the client
- Message A: client /TGT session key is encrypted using the secret key the client/user.
- Message B: TGT is encrypted using the secret key of TGS.

d) When the client receives messages A and B, it tries to decrypt the message A with the secret key generated from the password that was encrypted by the user.

e) If the user entered password does not matches the password in the AS database then the client's will be usable to decrypt the message A.

f) But when the two password matches, client decrypt the message A to obtain the client TGs session key.

g) Session key is then used for communicating with the TGS.

VI. CLIENT SERVICE AUTHENTICATION [8]

a) Client sends messages C and D to TGS while requesting services from it.

- Message C: it consists of two parts: TGT from message B and ID of the requested service.
- Message D: Authenticator which so encrypted using client /TGS session key.

b) Now TGS retrieve messages B from c and decrypt the message Busing TGS secret key. Thus client /TGS session key is obtained. TGS uses this session key to decrypt message D.

c) Message E and F are then sent to the client.

- Message E: client to server ticket which is encrypted using the service secret key.
- Message F: client/server session key which is encrypted with the client/TGS session key.

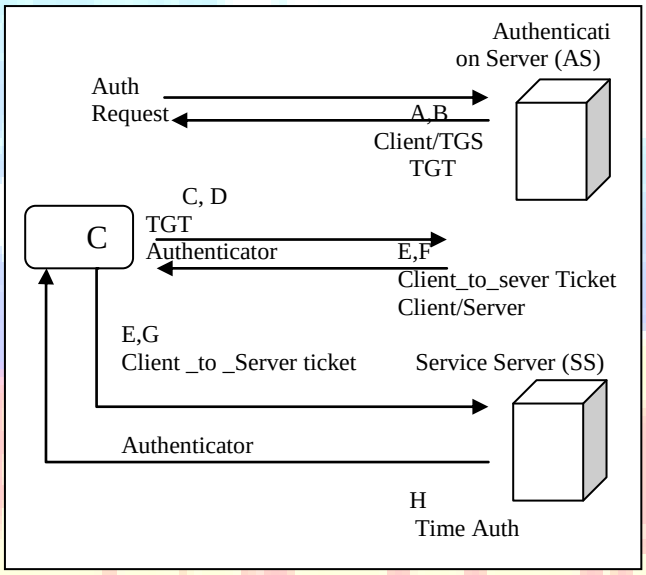

Figure 3: Client Service Authorization

VII. CLIENT SERVICE REQUEST

a) Since message E and F are received from TGS, the client has enough information to authenticate itself to the service server. Now the following messages are sent by the client to the service server.

- Message E: client to server ticket which is encrypted using the service secret key.
- Message F: A new authenticator.

b) The service server now decrypts the ticket using its own secret key to obtain the client / server session key.

c) This session key is now used by the service server to decrypt the authenticator [9]

d) Now the following messages are sent by client to confirm its identity.

- Message H: timestamp that was found in client's authentication plus 1 and encrypted using the client/ server session key.

e) Client now decrypts the confirmation using the client /server session key and checks that the timestamp is correctly updated or not.

f) If the timestamp is correctly updated, client can trust the server and start issuing service requests to the server and the server provides the request service to the client.

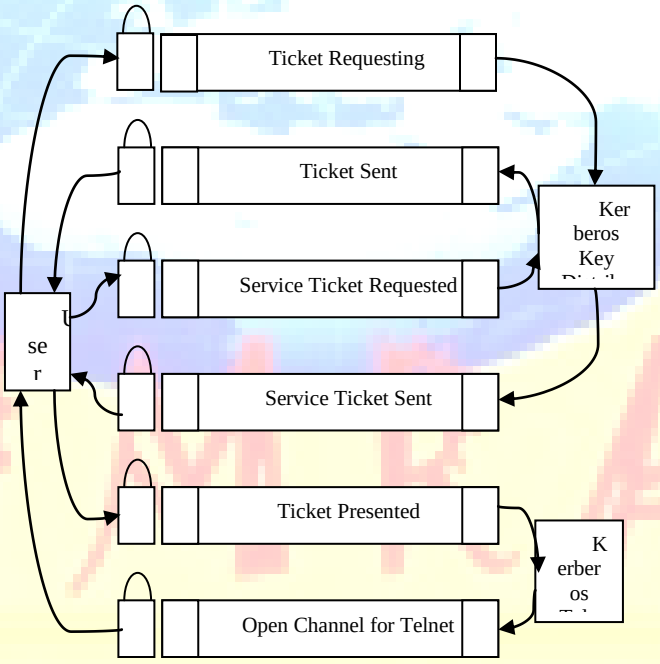

Figure 4: Client Service Request

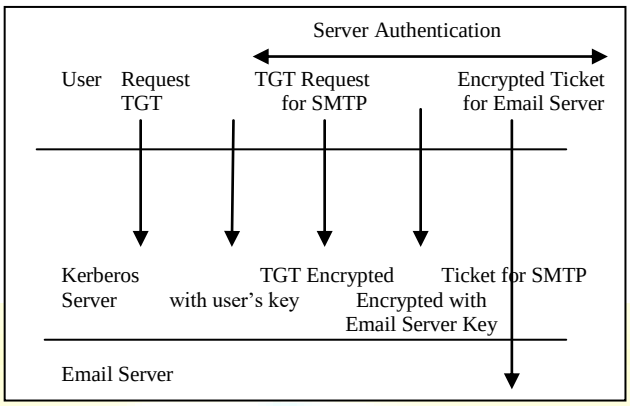

Figure 5: Email Server

VIII. ADVANTAGES

a) It is protected against reply attacks.

b) Ease and quality of organization.

c) Interoperability

d) Cost effective

e) It provides choice of authentication mechanisms [10].

f) User's password is never sent across network neither in encrypted or plaintext format. Thus contents of the conversion over an insecure network can never be deduced.

g) Client and server mutually authenticate. Thus both the system is certain that they are communicating with their authentic counterpart.

h) Authentications are reusable and durable.

i) User needs to authenticate with the Kerberos system only once.

j) It is based on open standards and implementations are available free of charge to the internet.

IX. DISADVANTAGES

a) Strict time requirements: Clocks of the hosts must be synchronized within configuration limits.

b) Server must be available all the time. When the Kerberos server is down then no one can log into the server.

c) Kerberos system may fell prey to the ticket stealing and replay attacks. Security of multiuser Kerberos systems is a limiting factor of Kerberos authentication.

d) Since it is manual authentication model the client and server machines must be designed with Kerberos authentication in mind.

e) Vulnerable to brute force attack against KDC.

X. APPLICATIONS OF KERBEROS

a) Network files access.

b) Email

c) rlogin

d) Printing.

XI. AKNOWLEGEMENT

Nobody can do anything without the grace of God. I first thank to "Lord Krishna" and "OMKAR" who blessed me to achieve my ambition by writing this research paper named "Kerberos". I am thankful to almighty God for blessing me with the strength to face any situation with courage and patience. I extended my thanks to my dear husband who encourage me finish the task successfully on time. I also thanks to my parents for their inspiration and blessings.

I also thank to my children and my in-laws who supported me for accomplishing my goal.

I would also like to thank my friends and my colleague who supported me in each step. I would like to thank my publishers who gave me the golden opportunity to write this research paper.

XII. REFERENCES

1. Resource KIT Team, "Microsoft Kerberos (Windows)" MSDN Library.
2. "Kerberose Overview: An Authentication service for open network systems" Cisco Systems date 19 January 2006.
3. "How Kerberos Authentication Works", Learn Networking .com, 28 Jan 2008. Retrieved 15 Aug 2012.
4. RFC 5021 "Exteded Kerberose" Version 5 Key Distribution Center (KDC) Exchanges Over TCP.
5. RFC 1510 "The Kerberos Network Authentication Service", V5, obsolete

6. RFC 6251 “Using Kerberos”, Version 5 over the Transport Layer Secuirty (TLS) Protocol.
7. B. Clifford Neuman and Theodore Ts’o , “Kerberos: An Authentication service for Computer networks” IEEE Communication 32(9): 33-8 doi: 10.1109/35.312841, Sept.1994.
8. RFC 4120 “The Kerberos Network Authentication Service”, Current.
9. RFC 6448 The Unencrypted form of Kerberos 5 KRB-CRED Message.
10. RFC 1964 “The Kerberos” Version 5 GSS-API Mechanism.