Highly Efficient Kerberos Style Authentication and Authorization for Cloud Computing

Sulochana.V†, Parimelazhagan.R††

†Research Scholar, Karpagam University, Coimbatore, India
††Department of Science and Humanities, Karpagam College of Engineering, Coimbatore, India

Summary
This article presents kerberos system which achieves security goals for cloud user like authentication, integrity, confidentiality and provides distributed authentication services across the insecure network. This kerberos style authentication is based on the secret key technology which keeps online password attackers away and it is implemented by using Windows Active Server.

General Terms:
Mathematics Subject Classification (2000), 68-04
Key words:
Security, Kerberos, Cloud Computing, Authentication, Authorization

1. Introduction

Cloud computing is an emerging, on-demand and internet based technology used by global customers to improve their business performance. Cloud is highly scalable, flexible and platform independable which has security loopholes like attacks, data loss, other authentication and security issues. Bo Wang [1] stated that to utilize cloud services by authorized user and to secure cloud data, it is necessary to use secure authentication system. This technology consists of dedicated user stations and distributed servers and provide services to multiple users and require the ability to accurately identify the cloud user. The authentication service can be achieved by using Kerberos which requires cloud user to prove identity for each service invoked, servers proves their identity to cloud users. Kerberos provide reliable authentication over open and insecure networks where communication between the hosts belonging to it may be intercepted.

Gagan Dua[2] presents an improved method which prevents replay attacks and password attacks by using Triple Password Scheme. Three password are stored on Authentication Server. Authentication server sends two passwords to Ticket Granting Server (one of the Application Server) by encrypting with the secret key shared between Authentication Server and Ticket Granting Server. Similarly ticket granting server sends one password to application server by encrypting with the secret key shared between TGS and application server. Meanwhile service granting ticket is transferred to users by encrypting it with the password that TGS has just received from AS which help to prevent replay attack.

Trapti Ozha[8] designed authentication protocol based on secret key encryption technology, uses data encryption algorithm for encryption to extend the security for system. Ved.M.Kshirsagar [9] proposed a scheme which achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the third party auditor- a privacy preserving manner. Pathan Mohd Shafi [3] designed a system which combines text based password authentication with cued click point and Kerberos authentication protocol. In this system, password consists of sequence of images in which user select one click point per image and select a sound signature. The sound signature is validated for accessing the system. Sulochana.V[5] proposed sequence level to access the cloud services. The sequence level authentication generates password at five levels and then concatenates into one single password.

Shubha Bharill[4] designed an authentication model for cloud based on Kerberos protocol using threshold cryptography to provide more security and to increase the availability of key. This model filters unauthorized access and reduce the burden of computation and memory usage of cloud provider against authentication checks for each client. Sulochana.V[6] also presented location based authentication where cloud user chooses a location as password and its longitude and latitude is extracted by GPS device and it is validated by local server and the cloud user get authenticated and start accessing the cloud services. Sulochana.V[7] developed A puzzle based authentication scheme in which cloud user registers and solves the puzzle, puzzle solving time and sequence of image block is stored and validated by local server and cloud user get authenticated and start accessing the cloud services. The proposed Kerberos style authentication works on the basis of ticket to allow nodes communicating over a non secure network to prove their identity to one another in a secure manner.

Manuscript received February 5, 2015
Manuscript revised February 20, 2015

2. Kerberos Style of Authentication and Authorization

2.1 Mathematical Model

Let A1 be the set of cloud user in the system

A1 = {CU, Auth_Srvr, Ti_Gr_Srvr, CS}

CU→Cloud User,
Auth_Srvr→Authentication Server,
Ti_Gr_Srvr→ Ticket Granting Server
CS→ Cloud Server on which User want to access the cloud services

Let A2 be the set of objects in the system

A2={ID_{CU}, $ID_{Ti\_Gr\_Srvr}$, T_S, K_{CU}, K_{CS}, Lifetime, AD_{CU}, $Ticket_{Ti\_Gr\_Srvr}$, $Ticket_{CS}$}

ID_{CU}→ID of Cloud User,
$ID_{Ti\_Gr\_Srvr}$→ID of Ticket Granting Server
K_{CU}→Key of Cloud User
K_{CS}→Key of Cloud Server
AD_{CU}→ Network Address of Cloud User

$Ticket_{Ti\_Gr\_Srvr}$= $E(K_{Ti\_Gr\_Srvr}$ [$K_{Ti\_Gr\_Srvr}$ || ID_{CU} || AD_{CU} || $ID_{Ti\_Gr\_Srvr}$ || TS_2 || lifetime])
$Ticket_{CS}$ = E(K_{CS} [$K_{CU,CS}$ || ID_{CU} || AD_{CU} || ID_{CS} || TS_4 || lifetime])
Authenticator = $E(K_{CU,Ti\_Gr\_Srvr}$ [ID_{CU} || AD_{CU} || TS])

Three Stages of Problem Solving

a) Authentication service exchange to obtain Ticket Granting Ticket ($Ticket_{Ti\_Gr\_Srvr}$)

Step1: CU→Auth_Srvr ID_{CU}||$ID_{Ti\_Gr\_Srvr}$||TS_1

Step2: Auth_Srvr→CU $E(K_{CU}[K_{CU,Ti\_Gr\_Srvr}$ || $ID_{Ti\_Gr\_Srvr}$ || TS_2 || lifetime || $Ticket_{Ti\_Gr\_Srvr}$])

Cloud User request Auth_Srvr for ticket to access Ti_Gr_Srvr. Auth_Srvr checks Cloud user authenticity and sends $Ticket_{Ti\_Gr\_Srvr}$ to cloud user.

b) Ticket granting service exchange to obtain server granting ticket ($Tickets_{cs}$)

Step3: CU→Ti_Gr_Srvr
ID_{cs} || $Ticket_{Ti\_Gr\_Srvr}$ || $Authenticator_{CU}$

Step4: Ti_Gr_Srvr→CU $E(Kcu,_{Ti\_Gr\_Srvr}$ [$K_{CU,CS}$ || ID_{CS} || TS_4 || $Ticket_{CS}$])
Cloud user sends the ID and $Ticket_{Ti\_Gr\_Srvr}$ to Ti_Gr_Srvr to authenticate itself. Ti_Gr_Srvr replies with a $Ticket_{cs}$(Ticket to Cloud Server)

c) Cloud user|Cloud server authentication exchange to obtain service

Step5: CU→CS $Ticket_{CS}$ || Authenticator

Step6:CS→CU E ($K_{CU,CS}$ [TS_{5+1}]) for mutual authentication. Cloud User sends $Ticket_{CS}$ to Cloud server to authenticate and access service.

2.2 Conventions

In this paper we use new terms which are elaborated as follows
Key Distribution Center: KDC is the heart of Kerberos realm, handles the distribution of keys and tickets. It provides Kerberos authentication services by issuing encrypted tickets which require secret keys to decode.
Session Key: Temporary private keys generated Kerberos which is known to cloud user to encrypt the communication between cloud user and cloud server.
Authentication Server (AS): An authentication service to know the password of cloud user and stores in centralized database, shares a unique secret key with TGS and Cloud Server.
Ticket Granting Server (TGS): This server issues service tickets to cloud user upon request.
Ticket Granting Ticket (TGT): The ticket issued by Authentication Server, TGT is encrypted in cloud user password which is known only by the user and KDC.

2.3 Working Model

This kerberos style provide strong authentication for client/server applications by using secret key cryptography and verify the identities of network server on an open network without relying on authentication by host operating system, physical security of the host on the network.When cloud user wants to access a service from cloud server which requires Kerberos ticket, server grant access to subscribed service to cloud user based on the ticket. In the first phase cloud user logs on to a workstation, cloud process running in the workstation issues a message to AS. Authentication Server validates username, password and issues TGT, session key to the cloud user which can be used to communicate with the server. TGT and session key are encrypted using key generated from the cloud user password. Cloud user decrypts the message and gets TGT used for communication with the TGS.
In the second phase cloud user presents TGT to the TGS along with an authenticator. Authenticator includes ID of the cloud user and timestamp. TGT is encrypted with a secret key that is shared by AS and TGS. TGS can decrypt the message and gets the session key which decrypts the authenticator that is received from the cloud user. TGS checks the sender details by validating TGT with the details in the Authenticator and incoming packet network address. If details are validated, TGS issues a Service Granting Ticket to the cloud user and encrypted using the secret key shared between TGS and Cloud Server. TGS

generates a session key shared between the cloud user and cloud server for secure communication, sends the session key to the cloud server by encrypting with the ticket. The TGS sends session key to cloud user by encrypting the message with the session key shared between the cloud user and TGS. In the third phase, cloud user presents ticket to the cloud server along with authenticator. The cloud user encrypts the message by using session key that is sent by TGS. Cloud server uses session key to encrypt the message from the cloud user. If credentials of the cloud user are correct, the cloud server will issue a response to the cloud user in case if a mutual authentication is required.

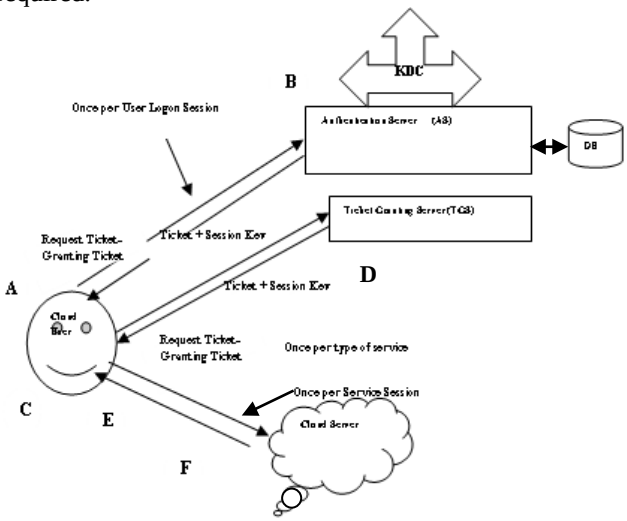

Fig 1. Working Model of the Kerberos Style Authentication

A→ Cloud User logs on to workstation and request service on host
B→ AS verifies user's access right in database, creates ticket-granting ticket and session key. Results are encrypted using key derived from cloud user's password
C→ Workstation prompts user for password and uses password to decrypt incoming message, then sends ticket and authenticator that contains cloud user's name, network address and time to TGS
D→TGS decrypts tickets and authenticator verifies request then creates tickets for requested server
E→ Workstation sends ticket and authenticator to server
F→ Cloud server verifies that ticket and authenticator match, then grants access to service. If mutual authentication is required, cloud server returns an authenticator

The Kerberos style authentication and authorization can be implemented by Windows Active Server. Kerberos system is based on the distribution of tickets. A ticket is an encrypted data generated by the Kerberos server and it is used by a service. It gives the right for the cloud user to access the service, assuming the service can decrypt the ticket. It contains ticket's expiry date field. KINIT command line utility on Linux Operating System is used to obtain granting ticket from Kerberos server. This Kerberos style authentication provides three level of security. The first level is provided by session key which is renewed every time by the cloud user who requires to access new service stored on cloud server. The second level of security provided by the cloud user password is stored in the database at TGS. The third level of security is provided by cloud user password which has already been forwarded to the cloud server.

Screenshot for getting Tickets:

```
[ediga@psrlxediga1 cshrc]$ kinit -c /tmp/del/s.tmp sulokerbuser@INFAKRB.INFAQA.COM
Password for sulokerbuser@INFAKRB.INFAQA.COM:
[ediga@psrlxediga1 cshrc]$ klist -c /tmp/del/s.tmp
Ticket cache: FILE:/tmp/del/s.tmp
Default principal: sulokerbuser@INFAKRB.INFAQA.COM

Valid starting     Expires           Service principal
07/15/14 16:41:55  07/16/14 02:41:58  krbtgt/INFAKRB.INFAQA.COM@INFAKRB.INFAQA.COM
       renew until 07/16/14 16:41:55
[ediga@psrlxediga1 cshrc]$
```

3. Conclusion

Kerberos is a powerful authentication system that is transparent to the cloud user except when entering initial password. The Kerberos system provides authentication and strong cryptography to secure information systems across an entire network or enterprise and a highly effective solution to network security problems.

References

[1] Bo Wang, HongYu Xing The Application of Cloud Computing in Education Informatization, International Conference on Computer Science and Service System (CSSS),2011.
[2] Gagan Dua,Nitin Gautam,Dharmendar Sharma,Ankit Arora,"Replay Attack Prevention in Kerberos Authentication Protocol Using Triple Password", International Journal of Computer Networks & Communication,Vol.5,No.2,pp.59-70,2013.
[3] Pathan Mohd. Shafi, Dr.Syed Adbul Sattar, Dr.P.Chenna Reddy,"Cued Click Point Image Based Kerberos Authentication Protocol", International Journal of Computer Engineering and Technology,Vol.4,No.3,pp.560-569,2013.
[4] Shubha Bharill, T.Hamsapriya, Praveen Lalwani,"A secure key for cloud using threshold cryptography in Kerberos", International Journal of Computer Applications,Vol.79,No.7,pp.35-41,2013.
[5] Sulochana.V, R.Parimelazhagan,"Implementing Graphical Password and Patternlock Security Using MVC into the Cloud Computing", International Journal of Computer Applications,Vol.79,No.8,pp.7-10,2013.
[6] Sulochana.V, R.Parimelazhagan,"Geographic Location Password Scheme: How can the Geographic Science Use and Help to Shape the Cloud Computing", Pensee Journal,Vol.75,No.11,pp.277-282,2013.
[7] Sulochanasrisriravishankar.V, R.Parimelazhagan,"A Puzzle Based Authentication Scheme for Cloud Computing",International Journal of Computer Trends and

Technology,Vol.6,No.4,pp.210-213,2013.
[8] Trapti Ozha,"Kerberos: An Authentication Protocol", International Journal of Computer Technology and Applications,Vol.4,No.2,pp.354-357,2013.
[9] Ved.M.Kshirsagar, Prof.V.S.Gulhane,"Result Paper on Public Auditing by Using Kerberos to Secure", International Journal of Computer Science and Information Technologies,Vol.5,No.3,pp 3312-3317,2014.