NEW AAA KERBEROS MODEL FOR HETROGENEOUS SYSTEMS

Manju Verma
Computer Science & Engineering
Graphic Era University
Dehradun,
Uttarakhand , India

Aditya Harbola
Computer Science & Engineering
Graphic Era University
Dehradun,
Uttarakhand , India

Dibyahash Bordoloi
Computer Science & Engineering
Graphic Era University
Dehradun,
Uttarakhand , India

Umesh Tiwari
Computer Application
Graphic Era University
Dehradun,
Uttarakhand , India

Deepti Negi
Computer Application
Graphic Era University
Dehradun,
Uttarakhand , India

Abstract – Distributed systems could be more secured with a distributed trust model based on Kerberos. The limitation of existing kerberos protocol is that it can only be used as an authentication service. However for many distributed services the authenticated subscribers must be verified for access authorization and for cost recovery, billing and resource planning purpose. Traditional Kerberos authentication schemes do not meet distributed system requirements of authorization, failsafe operation, accounting of service usage and resilience to loss of connectivity. This paper presents a new AAA Kerberos model for heterogeneous systems which can meet the requirements of authentication, authorization and accounting.

Keywords –Kerberos, Authentication, authorization, accounting, AAA protocol, heterogeneous systems

1. INTRODUCTION

A distributed network is full of challenges and meeting these challenges in a simplified and scalable manner lies at the heart of AAA protocols. AAA essentially defines a framework for coordinating the challenges across multiple network technologies and platforms.

Authentication involves validating the end user's identity prior to permitting them network access. This process keys on the notion that the end-user possesses a unique piece of information, a username/password combination, a secret key, or perhaps biometric data (fingerprints) that serves as unambiguous identification credentials. Authorization defines what rights and services the end user is allowed once network access is granted. This might include providing an IP address, invoking a filter to determine which application or protocols are supported, and so on. Authentication and authorization are usually performed together in an AAA-managed environment. Accounting provides the methodology for collecting information about the end user's resource consumption, which can then be processed for billing, auditing, and capacity planning purposes.

An AAA framework consists of a database of user profiles and configuration data communicates with AAA clients residing on network components. The AAA server compares the user supplied authentication data with the user-associated data stored in its database, and if the credentials match, the user is granted network access. A non match results in an authentication failure and a denial of network access. One of the requirements of AAA framework is a good price-to-performance ratio offering high-volume disk storage and optimized database administration. A single AAA server can act as a centralized administrative control point for multiple AAA clients contained within different vendor sourced NAS and network components. Thus, AAA functions can be added to the server, and incrementally to the client, without disrupting existing network functions. There is no need to incur the operational burden of placing AAA information on the NAS itself. The AAA Working Group within the IETF is also currently developing a set of requirements to support AAA across dial, roaming, and mobile IP environments [1].

2. EXISTING AAA TECHNOLOGIES

The best-known and most widely deployed AAA protocol is RADIUS-a clever acronym for the rather ordinary sounding Remote Access Dial-In User Service. It was developed in the mid-1990s by Livingston enterprise to provide authentication and authorization services to their NAS devices. RADIUS used UDP. RADIUS provide

1: client-server based operations
2: Network security
3: Flexible Authentication
4: Attribute pairs

Another protocol that provides AAA services is the TACACS+ (Terminal Access Controller Access Control System) protocol. Originally described in RFC 1492, it has been reengineered over the years by Cisco and is supported on many terminal servers, routers, and NAS devices found in enterprise networks today. TACACS+ provides many of the same AAA services as RADIUS. The primary differences are in

1: Transport: Uses TCP

Proc. of the Intl. Conf. on Advances in Electronics, Electrical and Computer Science Engineering — EEC 2012
Edited by Dr. R. K. Singh.

ISBN: 978-981-07-2950-9

2: Packet encryption
3: Authentication and Authorization

RADIUS and TACACS+ continue to enjoy widespread support among ISP and enterprise network managers. Both protocols, however, were originally engineered for small network devices supporting just a few end users requiring simple server-based authentication. The inherent problem of RADIUS is that it is not much scalable.

Another AAA protocol is Diameter, a lightweight, peer-based AAA protocol designed to offer a scalable foundation for introducing new policy and AAA services over existing (PPP) and emerging (roaming, mobile IP) network technologies. It employs many of the same mechanisms as RADIUS, including UDP transport, encoded attributed value pairs, and proxy server support. Diameter supports a much larger attribute-value length and incorporates a reliable, window-based transport that permits a sender (Diameter server) to transmit as many messages as the receiver (NAS) can handle.

Table 1: AAA protocol comparison with existing Kerberos protocol

	RADIUS	**TACACS+**	**KERBEROS**
Packet Delivery	UDP	TCP	TCP/UDP ports 88, 543, 749, and TCP ports754, 2105,4444
Packet Encryption	RADIUS encrypts only the password in the access-request packet from the client to the server.	TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header.	Kerberos supports username/password encryption
AAA Support	Yes	Yes	NA
Multiprotocol Support	None.	AppleTalk, NetBIO S, and Internet Packet Exchange (IPX).	Telnet, TCP/UDP
Router management	RADIUS does not allow users to control which commands can be executed on a router.	TACACS+ allows network Administrato r's control over which commands can be executed on a router.	Kerberos + allows network Administrator's control over which commands can be executed on a router.

3. KERBEROS

Kerberos is a trusted third-party authentication application layer service (Layer 7 of the OSI model), relying heavily on an authentication technique involving shared secrets. The basic concept is quite simple: If a secret is known by only two people, then either person can verify the identity of the other by confirming that the other person knows the secret. Kerberos is a secret-key network authentication protocol, developed at the Massachusetts Institute of Technology (MIT), that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. In the Kerberos protocol, this trusted third party is called the key distribution center (KDC).

The most important part of Kerberos is the key distribution centre, which called KDC for short. It provides two services, one is AS (Authentication service), and the other is TGS (Ticket granting service). The operation flowchart of the protocol is demonstrated in Fig.1. Kerberos protocol is now widely used in the distributed network applications [6]. Independent development platform, high speed communication of authentication, mutual authentication between entities and transferable relation-ship of trust, and a relatively strong compatibility with heterogeneous domains which may adopt various trust polices, are all the predominance of the Kerberos.

However, many security flaws appear during its usage in that the protocol heavily relied on certain aspects when it was designed and the limitation is quite striking. From the point of view of the network attack [3, 4, 5], some serious problems demanding more attention are as followed:

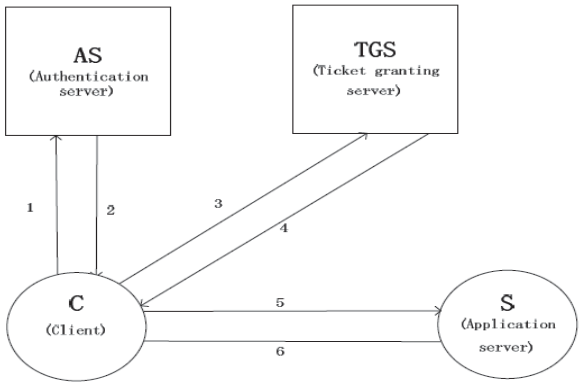

Figure 1. Model of Kerberos protocol

A: Password guessing attack: Kerberos is not effective against password guessing attacks; if a user chooses a poor password, then an attacker guessing that password can impersonate the user.

B: The security of the application system: At the present time, the worst network attack comes from vicious software. Kerberos authentication protocol depends on the absolute reliability of the software based on the protocol. An attacker may design software to replace the primary Kerberos application, which can execute the Kerberos protocol and record the username and password.

C: The problem of timestamp: Kerberos uses timestamp in order to prevent playback attack. But during the lifetime of the ticket, playback attack may still take effect. For example, in a certain Kerberos trust domain, all the clocks of the equipments keep synchronous. The period of validity for the message is 5 minutes, if the message arrives during the period, it is regarded as fresh.

D: Secure storage for session key: In Kerberos system, each user shares a session key with the server. KDC of the Kerberos system must provide a service to store a huge number of session keys. It is arduous to manage or update the keys and information related. Special measures must be taken to protect the KDC.

E: No support for authorization and accounting: In Kerberos system user authentication is necessary, but user authorization mechanisms are implemented using other ways than Kerberos. Network service accounting cannot be possible using Kerberos.

4. A NEW AAA KERBEROS MODEL FOR HETROGENEOUS SYSTEMS

The existing kerberos protocol provides network authentication. According to the problems and limitation of kerberos protocol discussed above, this paper presents a new model for authentication, authorization [7,8] and accounting between trust domains. It is based on Kerberos. The new AAA kerberos model is shown in fig 2.

AAA Kerberos model combines the authentication, authorization and accounting to form a new Kerberos protocol. The model is divided into two phases, service and accounting. In service phase the user is authenticated first by the existing kerberos protocol and then the services according to the authorization are provided to the user. The prime difference in this model and the original Kerberos is that user is authenticated and then it can use as many services, provided

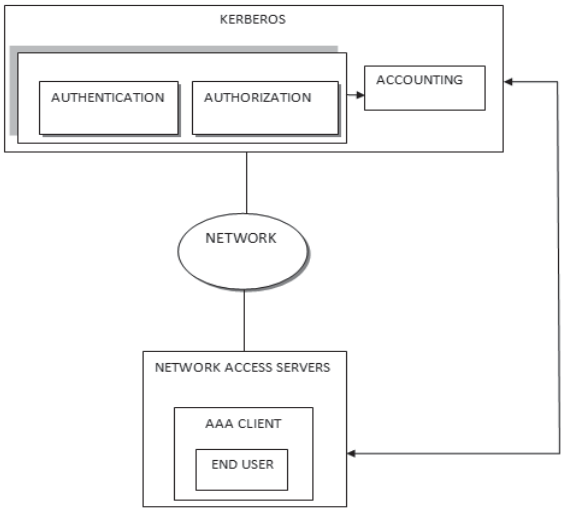

Figure 2: A new AAA Kerberos Model

The user is authorized for each service. As soon as the user completes the service uses, the cost accounting can be done. The main advantage of this model is that Kerberos can be used for many services as per the authentication and authorization.

5. MODEL FLOW WORK

The AAA kerberos model work flow is divided in to two phases. In the first phase the authentication and authorization are done based upon kerberos protocol database. In second phase the service accounting is done.

A. *Phase 1(Authentication)*

The authentication process based on existing kerberos, demonstrated in figure 3 works as follows.

Step 1: U→S: User sends a request to the AS (Authentication server) for establishing session with TGS. The message is encrypted with PKAS (public key of authentication server) by the user. The message also contains the user`s digital CertU(certificate), which is issued by CA1.

Step 2: AS→U: When AS decrypt the request, he gets the CertU and verifies the user`s identity. If AS can make sure the request sender is unquestionable the one asserted, AS generates the session key KU, TGS which will be used for the communication of the user and TGS.

Step 3: U→TGS: User uses his private key SKU to decrypt the response, and then he will get a session key KU, TGS and a cipher text TU, TGS. Second, user sends a request to the TGS in order to get the permission for visiting the server S. The request contains the name of the server, the session key KU, TGS shared between the user and the TGS, and the ticket TU, TGS which encrypted with KA, TGS by AS. User can not modify the ticket in private.

Step 4: TGS→U: When the request arrives, TGS uses its private key SKTGS to decrypt the request and get the session key KU, TGS and the cipher text of ticket TU, TGS. Then, TGS decrypts the cipher text and gets the ticket. If the ticket is authenticates issues the ticket TU, S and the session key KU, S which is shared by the user and the server.

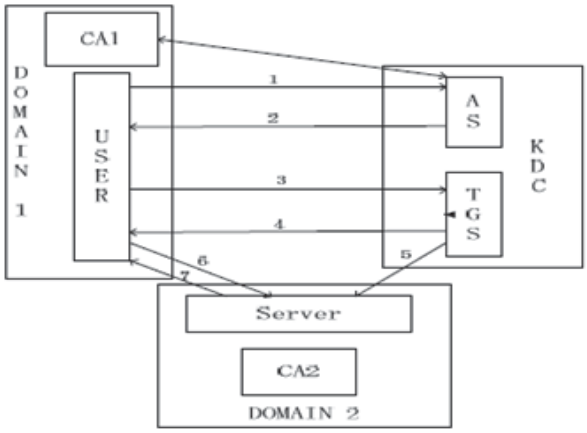

Figure 3: Phase 1 based on PKI and Kerberos

B. *Phase 2(Authorization)*

In this model we use kerberos server tables for authorization. There are 4 tables, subject table, object table, priority table and the authorization table. Subject table is classified in name of subject, TGT, IP address, role of subject, and pointer reference. Object table is classified in service name, service type, accessibility, and pointer reference. The priority table classified in type of authorization, priority variable and the time stamp of the subject. Now the authorization table has the references of subject and object table.

In this model after successful authentication user enter its TGT generated by TGS and role of the user, role is

define in role based access control as, For instance, a system administrator may create an access role for managers only. So a user would need to be assigned the role of a manager to use those resources. When role is verified then condition checked whether the user is administrator or other user. If the user is administrator then he directly allowed all access then he go to the authorization table, where the reference of object table is stored, and use the service. If user is not a administrator then server check whether he is a new user or old if he is a new user then he register to the priority table where initial priority is 0 which is the highest priority. If he is not a first time user then he checks his priority from priority table. If his priority is high, means his priority variable is less, he go to the authorization table , where the reference of the object table is stored, and checks whether the service he wants is accessible or not if the service is accessible the he uses the service and goes back when he comes back after using the service his priority variable is increased by 1. If the service is not accessible then server prompts access denied to the user. If user is first time user then his priority is high and he directly check whether the service is accessible or not and use it.

Step 5: TGS→S: While TGS sends the session key to the user, TGS also sends the server a message of notification which contains the name of the user, a message digest of the ticket TU, S the hash algorithm, the session key KU, S and the authorization details of the user AUTH, U. TGS maintains a authorization table of the users.

Step 6: U→S：As the user want to access the server the server the server reference the authorization details AUTH, U. If the user is authorized, the user accesses the resource server as soon as he gets the ticket. Before establishing the secure communication between them, user has to send a message encrypted with KU, S. The message contains the ticket TU, S, the user`s name U, user`s certificate CertU and a random number R1.

We categorize the authorization in 2 category one is permissive and the other is prohibitive. Subjects authorized permissive authorization are allowed to access the corresponding object, while the ones authorized prohibitive authorization are prohibited. So if the subject has low priority server checks whether the subject is permissive authorized or the prohibitive. If the subject is permissive authorized then server prompts access denied otherwise prompts access allowed and goes to the authorization table where the reference of the object table is stored through which the service is used and then the priority variable is increased by 1. The flow of AAA kerberos authorization is shown in figure 4.

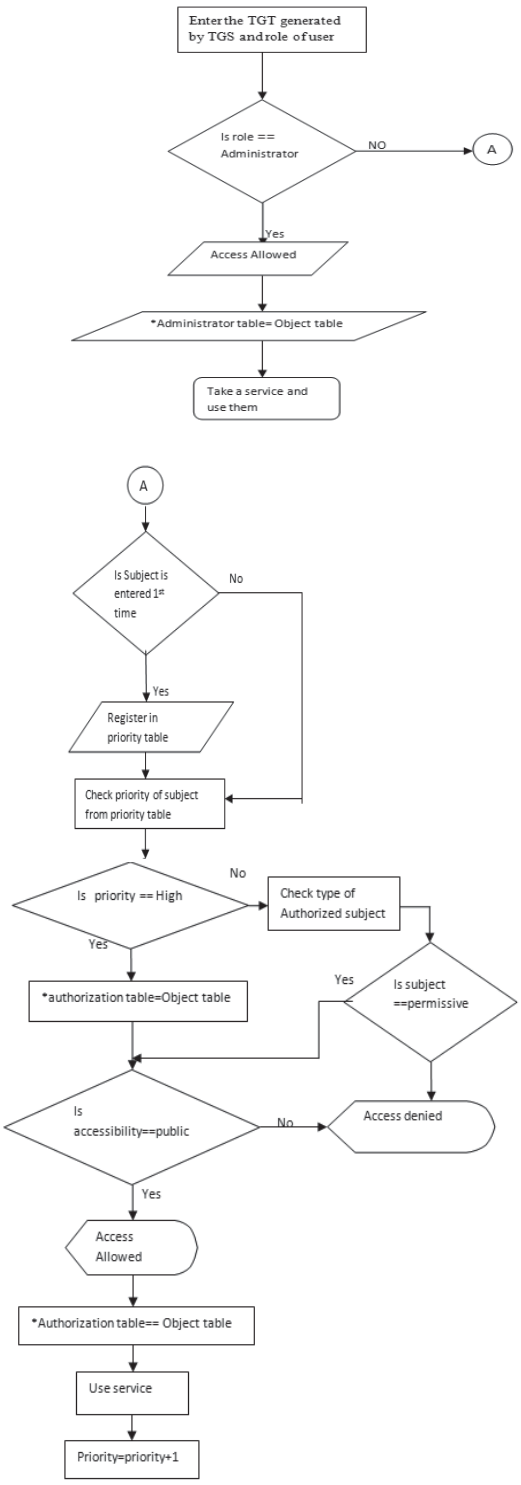

Figure 4: AAA Kerberos authorization process

C. Phase 3(Accounting)

Upon successful authentication and authorization, service server will send a ticket to the accounting server. The ticket contains the details of user name, session details. In accounting phase the user service usage accounting is done and can be verified with the user databases and service providers. The ticket contains the user information and access rights. The ticket has a limited validity period; otherwise accounting server can become a potential security concern. The accounting process demonstrated in figure 5 works as follows

Step 7: S→A The service server send a ticket to the accounting server containing user name U, session details SD.
Step 8: A→U The accounting server sends the accounting details AC to the user U.

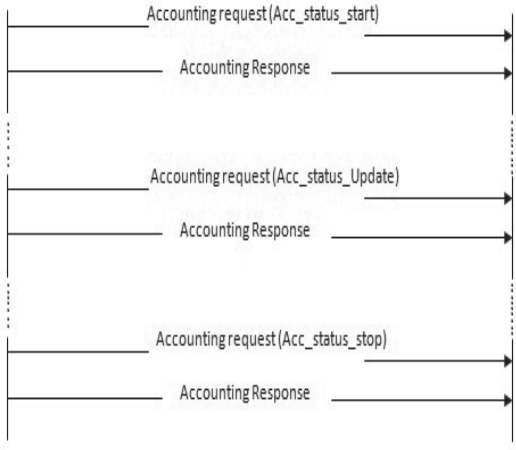

Figure 5: AAA Kerberos accounting process

6. MODEL ANALYSIS

Reliance relationship between heterogeneous domains can be established by adopting this model, providing high expandability and capability of mutual communication. The demand of interlinking different domains without any modification to the security policy or the architecture of the domain could be met. The model uses Kerberos protocol for the authentication and authorization between domains, greatly cutting down time waste and resource waste on building and verifying the certificate path, which is a disadvantage of the old PKI model. The trust between domains is built on the validity of the ticket, which is issued by the KDC of the Kerberos system. The format and content of the ticket is much more fixed than the certificate based on X.509. In this way, valid certificate regarded as invalid due to its different format will be avoided during the process of authentication. The Kerberos server is only responsible for setting up cross-domain communication and granting tickets, while any addition or reduction to the number of the users or authentication registration falls to the CA's obligation. Users in different domains follow the different security policies based on PKI.

7. CONCLUSION AND FUTURE WORK

In this paper, a new representative protocol of authentication, authorization and accounting is analyzed and a new high-compatible model is proposed. This model helps to realize the aim of interlinking heterogeneous domains supported by AAA technique and security policy. However a security policy or trust model, no matter how ideal it is theoretically, could not speak well for its feasibility. To imperfect this model, future studies will be focused into strengthening the ticket validity and enhancing mutual authentication and authorization efficiency according to the characteristics of the distributed network environment.

8. REFERENCES

[1] Internet Engineering Task Force (IETF) Authentication. Authorization. And Accounting (AAA) Working Group Charter; available at http://www.ietf.org/html.charters/aaa-charter.html
[2] Neuman C. RFC 1510, The Kerberos Network Authentication Service(V5) [S]. 1993.
[3] Bellovin S M, Merritt M. Limitation of the Kerberos authentication system [A].Proceedings of the Winter 1991 Usenix Conference [C]. 1991.
[4] Wen Tei-hua, Gu Shi-wen, An improved method of enhancing Kerberos protocol security, Journal of China Institute of Communication
[5] Bellovin S M, Merritt M. Limitation of the Kerberos authentication system [A].Proceedings of the Winter 1991 Usenix Conference [C]. 1991.
[6]. Neuman, C, et aI. The Kerberos Network Authentication Service (V5). s.l. :Network Working Group, July 2005. 4120.
[7]. Moustafa, H., Bourdon, G. and Gourhant, Y. Providing Authentication and Access Control in Vehicular Network Environment. Security and Privacy in Dynamic Environments. s.1. : Springer Boston,2006.
[8]S.P. Miller, B.C. Neuman, J.I. Schiller, and J.H. Saltzer,"Kerberos Authentication and Authorization System",Project Athena Technical Plan, Section E.2.1,27 October,1988.
[9] J.G. Steiner, B.C. Neuman, and J.I. Schiller, "Kerberos:An Authentication Service for Open Network Systems",Project Athena, March30,1988.
[10] Burr W E. Public Key Infrastructure (PKI) Technical Specifications: Part A-Technical Concept of Operations: [WORKING Draft] TWG-98- 59. Federal PKI Technical Working Group. Sep. 1998
[12] [X.509] CCITT Recommendation X.509, The Directory: Authentication Framework, 1997.
[13] Guan Zhen-sheng, Publication Key Infrastructure PKI and the applications. Beijing: Publishing House of Electronics Industry. 2008.1