Volume 2, Issue 3, March 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A NEW A^3 KERBEROS MODEL

Aditya Harbola*
School of computing
Graphic Era University,
Dehradun, UK
adityaharbola@gmail.com

Deepti Negi
School of computing
Graphic Era University,
Dehradun, UK
deeptine@gmail.com

Deepak Harbola
Department of computer science
BCTKEC,
Dwarahat, UK
deepak.harbola@gmail.com

Abstract – ***An internet service provider (ISPs) offers easy access to the network to meet the ever growing demand for business. The authenticated subscribers must be verified for access authorization and for cost recovery, billing and resource planning purpose. For all business services coordination between the various administrative system's are required. This paper presents a new AAA Kerberos protocol for distributed systems. Traditional Kerberos authentication schemes do not meet distributed system requirements of authorization, failsafe operation, accounting of service usage and resilience to loss of connectivity. Our new AAA Kerberos protocol model meets the requirements of authentication, authorization and accounting.***

Keywords - Authentication, authorization, accounting, key management, control systems.

INTRODUCTION

A network is full of challenges and meeting these challenges in a simplified and scalable manner lies at the heart of authentication, authorization, and accounting. AAA essentially defines a framework for coordinating the challenges across multiple network technologies and platforms. An AAA framework consists of a database of user profiles and configuration data communicates with AAA clients residing on network components. 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. 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.

Authentication 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, the third 'A" 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.

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].

EXISTING TECHNOLOGES

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 Terminal Access Controller Access Control System protocol. Originally described in KFC 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

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.

KERBEROS

Kerberos [2] is a network authentication protocol. It was designed to provide strong authentication based on the reliable third-party authentication system for the project Athena. Now, it is available in many commercial products. Kerberos builds a safe bridge between client and server by providing central authentication service and symmetrical key system. In other words, an appointed server works for the user only when the central authentication server validates the service request and access right sued by the user. The most important part of Kerberos is the key distribution centre, which called KDC for short.

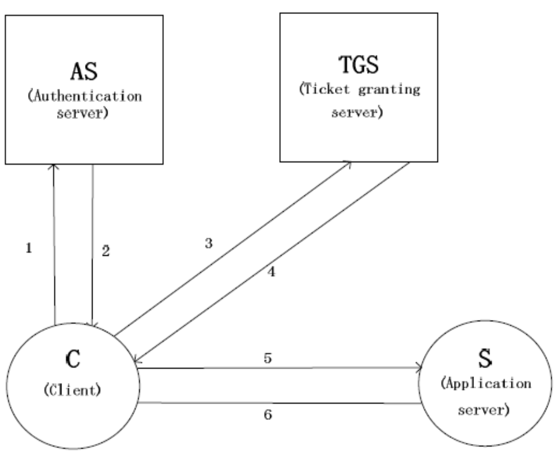

Figure 1. Model of Kerberos protocol

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:

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. Similarly, Kerberos requires a trusted path through which passwords are entered. If the user enters a password to a program that has already been modified by an attacker (e.g. a Trojan horse), or if the path between the user and the initial authentication program can be monitored, then an attacker may obtain sufficient information to 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. Generally speaking, the cipher application which has been installed on unsafe computers will more or less face the problem. Also, Kerberos must be integrated with other parts of the system. It does not protect all messages sent between two computers, and it only protects the messages from software that has been written or modified to use it. While it may be used to exchange encryption keys when establishing link encryption and network level security services, this would require changes to the network software of the hosts involved.

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. In fact, the attacker can easily fabricate a message according to the protocol format beforehand. Once he intercepts and captures the ticket from the user to server, the attacker could send the fake message within 5 minutes, server cannot easily find what exactly happened.

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. Naturally, the KDC becomes the targets of the attackers. Especially for the government or the military, it will be a disaster if the KDC has been destroyed which will result in failed communication among users of the domain. It is also quite demanding to store the system.

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.

So in Kerberos, the authentication and authorization protocol based on symmetric key algorithm is fitted with the environment which does not own a large number of registered users, but demands high efficiency.

A^3 KERBEROS

According to the problems discussed above, this paper develops a new model for authentication, authorization [7, 8] and accounting between trust domains. It is based on Kerberos. The new framework is shown in fig 2. A3 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 and then the services according to the authorization are served to the user. The prime difference in this phase with respect to the original Kerberos is that the user authorization is done for services.

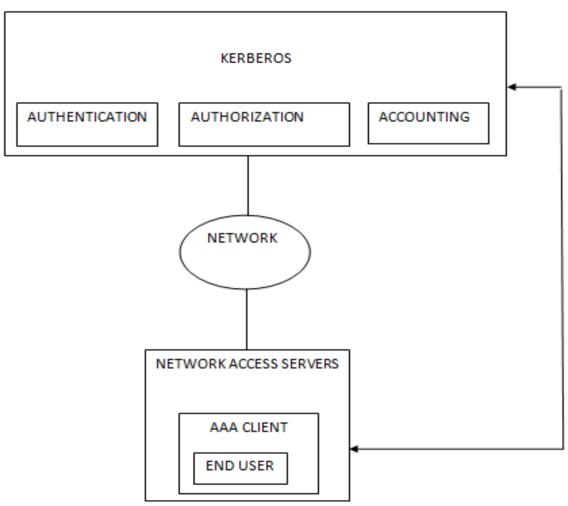

Figure 2: A new A^3 Kerberos Model

Once a user is authenticated it can use as many services, provided he is authorized. The main advantage of this model is that Kerberos can be used for many services as per the authentication and authorization.

A: Phase 1:

1: Establish a Security Association

A security association is an agreement of security parameters and the creation of a secure communication channel to perform the subsequent phases. After the completion of this phase, the AAA Service authentication and authorization are complete. The Ticket Granting Ticket (TGT) and the session key are the enabling components for the Remote Trust Cache to perform remote station local authentication and authorization.

2: Create new child Security Association

This optional phase allows the Client and server to create multiple child security associations as needed.

3: Client Service Authorization

Client service is authorized for the usage.

4: Client Service Request

At this phase, the client is requesting access to a service. For a device, the service is with the Key Manager. For an entity, the request will be for access to a device.

5: Terminate Associations

For key security, all participants should eliminate established security associations after specified information or a determined period of time has passed. Each participant will cease to use keys in expired security associations.

B: Phase 2:

Upon successful authentication and authorization, the AAA Service will send a Kerberos-like ticket to the accounting server. 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.

CONCLUSION AND FUTURE WORK

In this paper, a new representative protocol of authentication, authorization and accounting are 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.

REFERENCES

[1] Internet Engineering Task Force (IETF)Authentication. Authorization. And Accounting (AAA) Working Group Charter; available at http://www.ictf.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.

