A Study on Cooperation between Kerberos system and Credit-Control Server

Bae-young Choi*, Hyung-Jin LIm Tai-Myoung Chung****
*bychoi@imtl.skku.ac.kr
**hjlim@imtl.skku.ac.kr
**tmchung@ece.skku.ac.kr

Abstract. –. Kerberos is system that offer authorization in internet and authentication service. Can speak that put each server between client and user in distributed environment and is security system of symmetry height encryption base that offer authentication base mutually. Kerberos authentication is based entirely on the knowledge of passwords that are stored on the Kerberos Server. A user proves her identity to the Kerberos Server by demonstrating Knowledge of the key. The fact that the Kerberos Server has access to the user's decrypted password is a rwsult of the fact that Kerberos does not use public key cryptogrphy. It is a serious disadvantage of the Kerbercs System.. The Server must be physically secure to prevent an attacker from stealing the Kerberos Server and learning all of the user passwords. Kerberos was designend so that the server can be stateless. The Kerberos Server simply answers requests from users and issues tickets..
This study focused on designing a SIP procy for interworking with AAA server with respect to user authentication and Kerberos System. Kerberos is security system of encryption base that offer certification function mutually between client application element and server application element in distributed network environment. Kerberos provides service necessary to control whether is going to approve also so that certain client may access to certain server. This paper does Credit-Control Server's function in AAA system of Diameter base so that can include Accounting information that is connected to Rating inside certification information message in Rating process with Kerberos system.

Keywords: SIP,AAA(Authentication,Authorization Accounting),Kerberos System.Diameter protocol,Credit-Control Server,one-way fuction. Ticket Granting Server.

1 Introduction

1.1 Kerberos Characteristic

Kerberos authentication is based entirely on the knowledge of passwords that are stored on the kerberos Server.Unlike UNIX passwords, which are encrypted with a one-way algorithm that canmot be reversed, Kerberos passwords are stored on the server ercrypted with a conventiojnal encryption algorithm . In this case, DES –so that they can be decrypted by the server when needed. A user proves her identity to the Kerberos Server by demonstration knowledge of the key.

The fact that the Kerberos Server has access to the user's devrypted password is a result of the fact that kerberos does not use public key cryptography. It is a serious disadvantage of the Kerberos system. It means that the Kerberos Server must be both physically secure.
Kerberos was designed so that the server can be stateless. The Kerberos Server simply answers requests from users and issues tickets. This design makes it relatively simple to create replicated,secondary servers that can handle authentication requests when the primary server is down or otherwise unavailable.
keberos is certification system developed to protect integrity and confidentiality of authentication information about user in network environment between Client and Server. That is, if client has own authentication information and send message that request service to server who offer service, requested server passes through process that invest authority that can be serviced to client.
As deciding to refer and also argue about Credit-Control of 2 chapter's 1 Diameter based relationship whole action process and characteristic about contents that detail about Kerberos relationship general characteristic and action process in 2 chapter's 1 do to describe about Credit-Control's process in 3 of 2 chapter, and describe about gear with Credit-Control Server of Diameter base in Kerberos system in Chapter 3.

2 . Main text

2.1 Kerberos' abstract

Kerberos provides a mutual authentication between client and server and between servers before a network connetcion is opened.
Do as can give network access competence to stable user in network environment and approach to server who only specific user who is given Ticket provides service. Is designed to do function that make server who permit so that may ease user approach that is quoted therefore and take charge central authentication although do not need authoritativeness of all workstations trust.

2.2 Kerberoses' authenticaion element

Element that compose authentication information in Kerberos' system is as following.
Have authentication server (Authentication Server:AS) to give competence about service, client passes through negotiation process for AS and authentication for confirmation of information and authentication information confirmation identity at early authentication process. AS offers one authentication price that is not revealed to user to client. This authentication information is offered by TGT (Ticket Granting Ticket). Also, (Ticket Granting Server:TGS) that is Kerberos' component does access request in other service from TGS with TGT that is authentication information that client is given from AS beforehand, have function that pass through process that get Service Granting Ticket at service process that request this access.
If Kerberos client module in user's Work station requires password and user inputs password, it can do with the most important urea that confirm whether is a person who transmit user's ID, server's ID, password by AS and connection is admitted to number, server AS that AS confirms user's password.

2.3 Kerberoses' authentication process

It must secure impossible must and high authenticity, and select discrete server structure that Kerberos' authentication process gets information that important thing need because attacker disguises by right user at general authentication process of Kerberos authentication system that priority user is serviced. To do not realize that complicated authentication process happens to users, must do and must support large scale client and server

2.3.1 1 step process

User passes through process that log in to client. Pass through process that is this log and process that request service to server again. Client passes through process that send message that require connection about SGT (Service Granting Server) grant server that is TGS (Ticket Granting Server) by Authentication server (AS : Authentication Server). Include time stamp that mark user's ID and ID about service, validity time about service in message that is passed at this process.

2.3.2 2 step process

AS is send to client because pass through process that verify whether user's access competence which include to DB is valid and encrypt secret height (Kc) that is sharing with user in message. Encoded message includes TGT (Ticket Granting Ticket) and session key (Kc, tgs) in message. It means that it is section key that this message is used in message exchange between TGS with client that suffix mean here. TGT is user's ID and user's client's network address, also, include section key (Kc, tgs). TGT is including user ID and address of user client relationship network and include session key (Kc, tgs). TGT is encoded by secret key (Ktgs) that AS and TGS are sharing.

2.3.3 3 step process

With secret key that client passes through examination process about password to user, and gets from password above message process that do cipher processing flow . Client with ID of need service password process that send message including user authentication information that pass through done process to TGS flow. User authentication information that say here includes Timestamp that express validity time of authentication with user's ID and client's network address, session key Kc, tgs Ro is encoded. Unlike TGT that can reuse, this user authentication information has usable characteristic once only and can defend threat element that is peculated about attack from invader because validity time is short.

2.3.4 4 step process

TGS uses secret key (Ktgs) that share with AS, TGT cipher processes do with user ID included inside user authentication information because pass through process that know and use included session key Kc, tgs in TGT network address in TGT included information compare . If all agrees, TGS encrypts message by session key Kc, tgs and sends to client. Message includes SGT (Service Granting Ticket) and session key (Kc, s).SGT includes secret key (Kc, s) that TGS and server are sharing. SGT passes through process that encipher by secret key (Ks) that TGS and server are sharing, client can not read SGT's contents.

2.3.5 5 step process

Client uses session key Kc, tgs, message at the ciphers SGT and session Kc, s get and send message including encoded SGT and user authentication information in server.

2.3.6 6 step process

Server uses secret key that share with AS, SGT cipher process that is , and do cipher processing of user authentication information using included session key in SGT flow . After pass through such process, user ID and network address included inside user authentication information compare network address with included information in SGT with user ID in SGT. If all agrees, server can convince that a person who send SGT is SGT's actuality owner. Finally, though client and server share session key, this session key uses to use to encrypt message that

exchange between this two during session at authentication process that is continued or can be used exchanging new random session key. If authentication is required mutually, server authentication information that add 1 to timestamp that was included to user authentication information as authentication information about server and this value can convince to client that did not use before. Server authentication information, message is encoded by session key Kc, s and can convince to client. Server authentication information, message session key Kc, s Ro be encoded and pass through process that is sent to client.

2.3.7 7 step process

Client server authentication information using session key ciphered. Because pass through process that server authentication information is encoded by session key, service request and message exchange of service response form can consist between two while session ends mutually between authentication server. If need encryption of this messages, use because use session key Kc, s directly or create session key that do random for new encryption, is encoded by new random session key and is exchanged

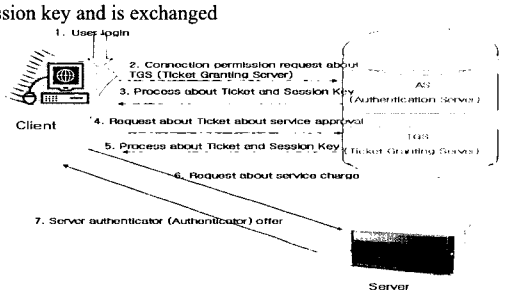

Figure 1.Kerberos System Authentication Process

2.4 Diameter Protocol abstract

Have user's authentication information at Protocol that do processing about accounting and by real time amount used of user's service putting server who decide use time of service through payment in advance or deferred payment to provide user's service the purpose be. Diameter Protocol that have basis structure that use SCTP achieves function that take charge administration service about Accounting as protocol that do Accounting also. Achieve function that offer negotiation and reporting of error, control of transmission protocol about last month of AVP (Attribute-Value Pair) and ability of node and watch function by additional service. Also, take charge Credit-Control process that do processing about Accounting through payment in advance and deferred payment. Purpose of this protocol gets user's Accounting information through user's authentication information by real time and Accounting processing, Client and Server of between doing processing about Accounting according to user's certification information putting one Server that achieve Credit-Control process that take charge accounting of payment in advance and deferred payment.

2.4.1 Protocol Model Architecture

Credit-Control process puts Credit-Control Server that take charge Accounting information, only user who have Accounting information for network resources to user to receive service that is approached in network environment giving competence via Authentication process to subject that use payment in advance subscribers that is service approaches under network environment and make service according to Accounting information usably. User who pass through this Credit-Control process connects to Server that give service to limited user that is payment in advance subscriber or deferred payment subscribers' service user because can do so that may can be serviced during competence Authentication period being given competence and offer environment that can use. It is request service to Server in End User grade; Server passes through process that verifies whether right user in Credit-Control Server is again. Competence that only user who receive authentication to user's information here requests service to AAA Server. Users send approached competence request message to pass through authentication process being given competence to Credit-Control Server. Users send approached competence request message to pass through authentication process being given competence to Credit-Control Server. Have information that need to information about user's information and user's Accounting to receive competence and include in request message. And information about user's certification information and Accounting which is given competence includes together in message that request service. If competence is given, again message about service request to AAA Server user via confirmation that is approval process that was given competence lastly service receive can . These process is thing which user to receive service in network makes user's approval can be serviced during valid period being given competence and does as can do function that can do fixed Accounting to user processing Accounting information.

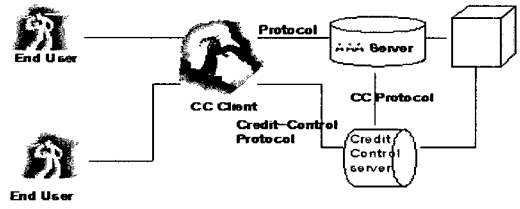

Figure 2 . Credit-Control Architecture

2.4.2 Credit-Control Process

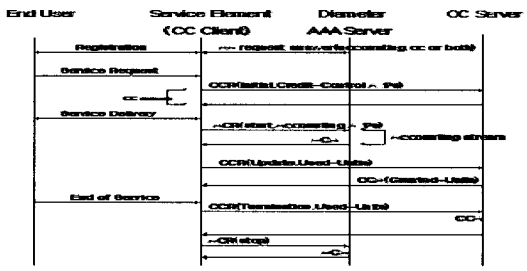

Figure 3 . Credit-Control Process

If user requests service in network, Service Element demands the user's request to server of user's Home domain. That is, that Credit-Control process of information that send request message

that is given competence about service to CC-Client and also come out here gets thin before expiration time is passed without being changed continuously keep. By next time, CC-Client Server does to give competence that can send message that can request that can be serviced at Credit-Control process if receive message that request competence to AAA Server. User who is given this competence sends request message about service to AAA Server and user who receive authentication competence at the same time includes authentication information in message is serviced, request service to AAA Server. So, user who is given competence at the same time takes charge function that keep as can approach and is serviced to AAA Server until competence expiration point of time to CC-Server.

3.1 A Cooperation Kerberos and Credit-Cotrol Server

Referred is Diameter protocol that handles Kerberos and AAA System. Make competence that user who is going to receive service in network putting Credit-Control Server that handle Accounting information about user's Authentication information or service use time or amount used by real time in Kerberos' Authentication system using Credit-Control process can approach to network can use service as that is Ticket's Authentication validity time during the time being given and processing about Accounting as utilization time of service. Embodiment of reliable Authentication system may be easy doing processing about Authentication information at the same time Authentication information about user in breakup network at the same time.

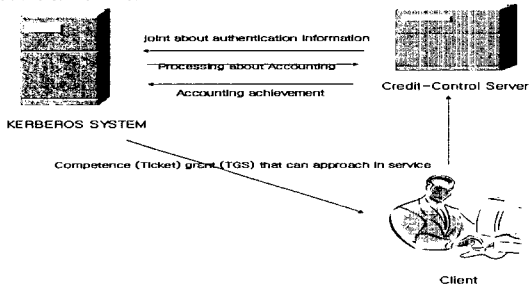

Figure.4 A Cooperation Kerberos and Credit-Cotrol Server

3.1.1 Credit-Control Cooperation Effect

Credit-Control Server that achieve process of Credit-Control in Diameter Protocol's base to do processing about Accounting in network that is opening traces Authentication server (AS) and TGS (Ticket-Granting-Server) of to do to do processing about Accounting putting between and finish grasping about Accounting information of service examining information that need in user's certification when approach of Credit-Control Server including user's certification information about payment in advance and deferred payment to security of certification information and play service as is available continuously by real time approving access about service the purpose be . Can provide service that user requires doing so continuously and secure safety of Attacker invasion or artificial service incapability element Accounting in network or Authentication information. That this result appears Accounting information or certification information protecting vulnerability of security doubly sharing information to Credit-Control Server that Kerberos' system is not possible can. There is advantage that verify whether user who approach via Credit-Control process because approaching to Credit-Control's server by real time as can handle processing for fare by defect of network or that is cut spontaneously at service utilization in user's situation which also assign area about Accounting about user before and use also being serviced directly is right user and production of correct service achievement expense eases via right Accounting process. This Paper is emphasis enemy in this treatise are thing to put Credit-Control server in Kerberos system and accomplish correct active Accounting information processing and authoritativeness of accounting information at the same time in user's network environment.

4. Conclusions

Handle Credit-Control Server about Accounting information according to amount used of service within Authentication information to user who have right authentication information worming for Accounting information processing in Kerberos' Authentication system now. Next research may have to put emphasis in authoritativeness security about correct Accounting information about Authentication server (AS) at this Authentication process and design of efficient security mechanism and service amount used in Credit-Control Server and get along with research

5. Acknowledgement

This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment)

6. References

[1] C.Rigney,S.Willens,A.Rubens,and .Simpson,"Remote Authentication Dial In User Service",RFC 2865,June 2000.

[2] J.Kohl,C. Neumsn,"The Kerberos Network Authentication Service(V5)",RFC1510,September 1993

[3] Pat R. Calhoun,Stephen Farrell, William Bulley"draft-ietf-aaa-diameter-초-sec-04.txt",IETF work in progress

[4] B.Aboba, J.Arkko, D.harrington. "introducation to Accoounting Management", RFC 2975, October 2000.

[5] Harri Hakala, Leena Mattila,"draft-ietf-aaa-diameter-cc-00.txt",IETF work in progress.