Diameter-Based Protocol in the IP Multimedia Subsystem

Vinay Kumar.S.B, Manjula N Harihar

Abstract— The Diameter protocol was initially developed by the Internet Engineering Task Force (IETF) as an Authentication, Authorization, and Accounting (AAA) framework intended for applications such as remote network access and IP mobility. Diameter was further embraced by the Third Generation Partnership Project (3GPP) as the key protocol for AAA and mobility management in 3G networks. The paper discusses the use of Diameter in the scope of the IP Multimedia Subsystem (IMS) as specified by 3GPP. This paper presents a solution for the problem of how to provide authentication, authorization and accounting (AAA) for multi-domain interacting services by referring open diameter. We have studied the case of 'FoneFreez', a service that provides interaction between different basic services, like telephony and television. The involvement of several parties like television provider, telephony provider etc., secure interaction between multiple domains must be assured. A part of this security issue can be resolved using AAA. In this paper the AAA protocol Diameter is used for that purpose, which is the successor of the RADIUS protocol. The authors have taken a look at open diameter can be used for AAA in multi-domain service interaction.

Keywords: Diameter protocol, IP Multimedia Subsystem, AAA, CSCF, HSS, SIP

I. INTRODUCTION

Evolution of the 3rd generation network architecture is driven, among other factors, by the requirement to provide a rather fast, flexible and cost-efficient way of introducing new services for operators, as well as third-party service and content providers. The IP Multimedia Subsystem (IMS), as specified by the 3rd Generation Partnership project (3GPP), represents the key element for supporting ubiquitous service access to multimedia Internet services, with adequate support for Quality of Service as well as advanced, service-differentiated charging [1]. Initially specified by 3GPP/3GPP2, the IMS standards are now being adopted by other standards bodies including ETSI/TISPAN. For the purposes of Authentication, Authorization, and Accounting (AAA) and mobility management in 3G networks, 3GPP has adopted the Diameter protocol [2], developed by the Internet Engineering Task Force (IETF). This paper discusses the use of Diameter within the scope of the IMS.

Diameter is a very flexible protocol. The adoption by 3GPP boosted the number of network products that implement Diameter. Diameter is mainly used for end-user

authentication, authorization and accounting, and is specifically designed for roaming situations.

II. ROLE OF DIAMETER IN IMS

The IMS is based on a horizontally layered architecture, consisting of three layers, namely, Service Layer, Control Layer, and Connectivity Layer. Service Layer comprises application and content servers to execute value-added services for the user. Control layer comprises network control servers for managing call or session set-up, modification and release. The most important of these is the Call Session Control Function (CSCF). Connectivity Layer comprises of routers and switches, for both the backbone and the access network

A. IMS functions

Voice over Internet Protocol (Voice over IP, VoIP) is one of a family of Internet technologies, communication protocols, and transmission technologies for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. To transmit over the internet we have a architectural framework called IP Multimedia Subsystem (IMS).

A simplified IMS architecture is shown in Fig.1 As mentioned earlier, one of the key functions in the control layer is the CSCF. The HSS serves as the main data storage for user related information, such as IMS user profiles (including location), security and registration information, access parameters, and application server profiles.

The CSCF serves three different purposes, as the Proxy CSCF (P-CSCF), the Interrogating CSCF (I-CSCF) and the Serving CSCF (S-CSCF). The P-CSCF is a Session Initiation Protocol (SIP) proxy that acts as the first contact point between the IMS terminal and the IMS network. It is assigned to an IMS terminal during IMS registration. The I-CSCF is also a SIP proxy, usually located in the home network, at the edge of the administrative domain. Main functions of the I-CSCF are to contact HSS in order to obtain the name of the S-CSCF that is serving the user, and to assign the S-CSCF to the user based on received information received from the HSS.

The S-CSCF is the central node of the signaling plane, the "brain" of the IMS. The S-CSCF is located in the home network and it uses the Diameter-based Cx and Dx interfaces (reference points) towards the HSS to download and upload the user profiles.

Manuscript received December 17, 2011.

Vinay Kumar.S.B, Department of Electronics and Communication, School of Engineering and Technology, Jain University, Bangalore, India, (e-mail: vinayvinaysb@gmail.com)

Manjula. N. Harihar, Department of Electronics and Communication, School of Engineering and Technology, Jain University, Bangalore, India, (e-mail: manjulaharihar@gmail.com).

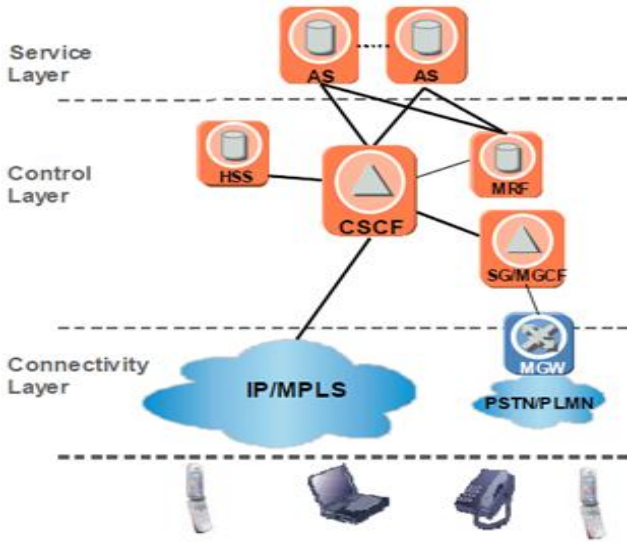

Fig. 1. The IMS architecture

B. The Cx reference point

As per IMS technical specifications [4,5], the Cx reference point is located between the S-CSCF/I-CSCF and the HSS, as shown in Fig.2 The Subscription Location Function (SLF) is required in a network in which there is more than one HSS; it provides the mapping between a particular user address and its corresponding HSS. As already noted, the protocol used at the Cx reference point is Diameter [3].

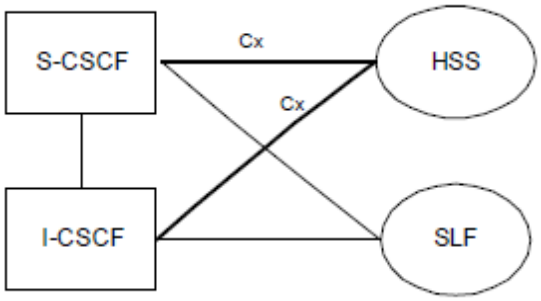

Fig. 2. The Cx interface

Procedures in the Cx reference point may be grouped
into three areas:

1. Location management procedures
2. User-data handling procedures
3. Authentication procedures

Each group of procedures is briefly described next.

Location management procedures

In location management procedures, the User-Authorization-Request (UAR) command is sent to the HSS whenever the I-CSCF receives a SIP REGISTER request from the P-CSCF. The UAR command contains private and public user identity, visited network identifier, routing information, and type of authorization. In response to the UAR command, the HSS responds with the User-Authorization-Answer (UAA) command. The UAA command contains the name of the S-CSCF assigned to the user. After authorization, the I-CSCF finds an S-CSCF that will serve the user, and it forwards the SIP REGISTER request to the S-CSCF. Once the S-CSCF receives the SIP REGISTER request, it uses the Server-Assignment-Request (SAR) command to communicate with the HSS, and it informs the HSS which S-CSCF will be serving the user. The HSS responds with the Server-Assignment-Answer (SAA) command, which contains the user profile and charging information. Later, when the HSS wants to initiate de-registration it uses the Registration-Termination-Request (RTR) command, stating the reason for de-registration. The RTR command is acknowledged by a Registration-Termination-Answer (RTA) command. If an I-CSCF receives any SIP method other than REGISTER, a procedure for finding S-CSCF uses the Location-Info-Request (LIR) command containing public user identity and routing information. The HSS responds to LIR with Location-Info-Answer (LIA) command, containing the name of the S CSCF.

User-data handling procedures

During the registration process, user and service-related data are downloaded from the HSS to the S-CSCF via the Cx reference point by using SAR and SAA commands. It is possible, however, for this data to be changed later, during the time while the S-CSCF is still serving the user. To update the data in the S-CSCF, the HSS sends a Push-Profile-Request (PPR) command with private user identity, routing information, and user data. The response to the PPR command is Push-Profile-Answer (PPA) command.

Authentication procedures

In the IMS, authentication relies on a pre-configured shared secret and a sequence number stored within the IP Multimedia Services Identity Module (ISIM) in the User Equipment (UE) as well as in the HSS in the network. To authenticate the user, the S-CSCF sends a Multimedia-Auth-Request (MAR) command to the HSS. MAR contains the private and the public user identities, S-CSCF name, routing information, number of authentication items, and authentication data. The HSS responds to the MAR command with the Multimedia-Auth-Answer (MAA).

C. *Overview of AAA Protocol*

AAA stands for Authentication, Authorization and Accounting. This section looks into the meaning of AAA, and the models used for authentication, authorization and accounting.

Authentication is the verification of the identity of the entity. An entity can be a user or the device a user has, like a computer or the SIM of his mobile phone. With authentication one can prove that it is really the person or device or it claims to be. This prevents from impersonations from other parties. Authentication consists of three sorts: user authentication, message authentication and device authentication.

Authorization is the determination whether the requesting entity is allowed access to a particular resource. Authorization is the process of determining if the user has the right to access the network or use services, like the print server from that network. Furthermore, authorization is needed for resource reservation and quality of service support.

Accounting. is the collecting of information about resource usage for the purpose of capacity planning, auditing, billing or cost allocation. For example, records are kept about the duration a user surfs the Internet.

Re-Authentication is the renewal of the authentication by the client upon request of the server. When a session lifetime has expired, or when an error has occurred in the path, re-authentication can be necessary to ensure trust.

D. Diameter Protocol

Diameter is an authentication, authorization and accounting (AAA) protocol developed by the Internet Engineering Task Force (IETF). It is based on an earlier IETF's AAA protocol called RADIUS (Remote Authentication Dial-In User Service), widely used for dial-up PPP (Point-to-Point Protocol) and terminal server access. Extending the functionality of RADIUS, Diameter is designed to provide AAA services for a range of access technologies, including wireless and Mobile IP. The Diameter specifications consist of the Diameter Base Protocol [2], Transport Profile, and applications such as Mobile IPv4, network access server, credit-control, and Extensible Authentication Protocol (EAP). The Diameter Base protocol is utilized for negotiating capabilities, delivering Diameter data units, handling errors, and providing for extensibility. On the other hand, the Diameter application defines application-specific functions and data units.

Diameter is an application layer protocol. Transport protocols to carry Diameter messages include Transmission Control Protocol (TCP) and Stream Control Transmission Protocol (SCTP). For securing the connection, Internet Protocol Security (IPSec) and Transport Layer Security (TLS) are applied. Diameter is a peer-to-peer protocol, meaning that any Diameter *node* may initiate a request. The three types of nodes are *clients*, *servers*, and *agents*. Clients are generally the edge devices of a network which perform access control. A the Diameter agent provides relay, proxy, redirect, and translation services, while Diameter server handles the AAA requests for a particular domain, or realm. Message routing is based on the network access identifier of a particular user. It is observed from literature review for data structure that in each Diameter node there is a peer table, which contains a list of known peers and their corresponding properties. Each peer table entry is associated with an identity and can be either statically or dynamically assigned. It includes a relative priority setting, which specifies the role of the peer as primary, secondary, or alternative. The status of the peer relates to a specific configuration of the finite state machine of the peer connection, called the Diameter Peer State Machine. As a part of message-routing process, Diameter realm-routing table references the Diameter peer entries.

All realm-based routing lookups are performed against a realm-routing table. The realm-routing table lists the supported realms, with each route entry containing certain routing information. Each route entry is either statically or dynamically discovered. Dynamic entries are associated with an expiry time. The route entry is associated with an application identifier, which enables route entries to have a different destination depending on the Diameter application.

A Diameter message consists of a Diameter header, followed by a certain number of Diameter attribute-value pairs (AVPs). The Diameter header is composed of fields denoting Command Flags, Command Code, and Application ID. The Command Code denotes the command associated with the message, while the Application ID identifies the application to which the message is applicable. AVPs define the method of encapsulating information relevant to the Diameter message.

III. DIAMETER PROTOCOL IMPLEMENTATIONS

A. Connections vs. Sessions

A connection is a transport level connection between two peers, used to send and receive Diameter messages. A session is a logical concept at the application layer, and is shared between an access device and a server, and is identified via the Session-Id AVP.

In this paper we are attempted to implement the client and server interaction using Diameter based protocol in the IMS is shown in Fig.3, peer connection A is established between the Client and its local Relay. Peer connection B is established between the Relay and the Server. User session X spans from the client via the Relay to the Server. Each "user" of a service causes an authorization request to be sent, with a unique session identifier. Once the message is accepted by the server, both the client and the server are aware of the session. It is important to note that there is no relationship between a connection and a session. The Diameter messages for multiple sessions are all multiplexed through a single connection[2].

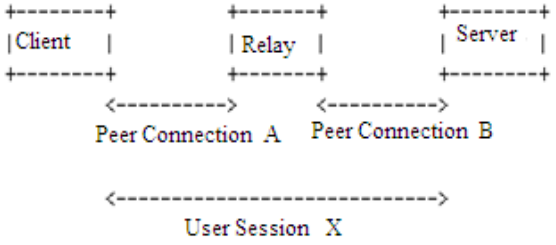

Fig. 3. Diameter connections and sessions

As shown it contains several client/server examples, which we used to examine Diameter mechanisms. As a starting point in our development we used the example presenting an authorization application. In terms of specifications, we followed the specifications of the Diameter protocol [2, 6] and Cx interface [4, 5] provided by 3GPP.

The modification of the client and the server classes provided the Cx interface specific Diameter messages UAR, MAR, and SAR, and building the client and server applications to use the functionality of those classes. The client and the server code have rather similar structures, up to the point of Diameter session management. we needed to implement the UAR, MAR, and SAR commands, which, according to the Cx specification, are sent from the client (CSCF) towards the server (HSS)[3].

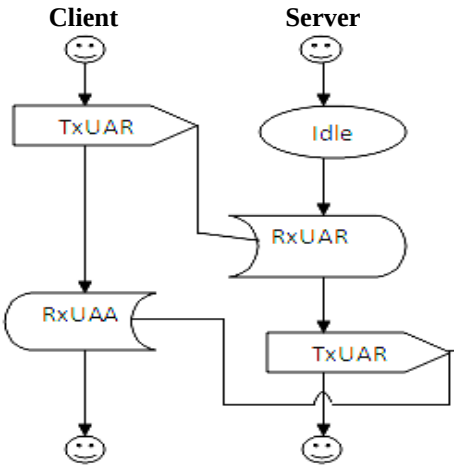

Fig. 4. Exchange of Cx specific Diameter messages

Fig.4 contains both the server and the client classes to enable a Cx node to operate in a peer-to-peer network. In our application, we have attempted to implement the functionality of the Cx interface as if the CSCF acted as a client and the HSS acted as a server. Fig.4 shows the exchange of messages in our attempted implementation. It may be noted that each message transmission method (i.e. TxUAR) on the client side has its corresponding counterpart on the receiving, server side (i.e. RxUAR)[7]. The notation used here is Tx for transmission and Rx for receiving. Messages are distinguished by their message code, embedded in the message header. The client composes a message with the specific code, and sends it across to the server, which then recognizes the message code and initiates the appropriate receiving method. Each message type carries some specific information, being coded as AVPs. Thus, it was necessary to implement the method for composing and resolving the message for all types of messages. This included definition of message parts, initialization of message fields, and finally, construction of message body.

IV. CONCLUSION

In this paper, we have concentrated on developing AAA service model based on Diameter. With the emergence of new wireless access technologies and new applications envisioned in new generation networks, the need for AAA becomes more pressing. The AAA solution adopted by the 3GPP and 3GPP2 for use in the IMS is based on the Diameter protocol. In this paper, we have studied the Diameter protocol and its application in the IMS Cx interface.

Therefore that the Diameter protocol can be reused in its existing form to provide AAA for multi-domain interacting services. We found that authentication between different parties is better done with the Kerberos protocol. Furthermore the provisioning of quality of service by Diameter for multi-domain interacting services should be explored.

REFERENCES

1. G. Camarillo, M. A. García-Martín, *The 3G IP Multimedia Subsystem: Merging the Internet and the Cellular Worlds*, John Wiley and Sons, Ltd., England, UK, 2004.
2. P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko, *Diameter Base Protocol*, IETF RFC 3588, September 2003.
3. http://www.fer.unizg.hr/images/50010415/Mipro_2006.pdf.
4. *IP Multimedia (IM) Subsystem Cx and Dx interfaces; Signaling flows and message contents*, The 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; TS 29.228, 2005.
5. *Cx and Dx interfaces based on the Diameter protocol; Protocol details*, The 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; TS 29.229, 2005.
6. J. Loughney, *Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5*, IETF RFC 3589, September 2003.
7. Open Diameter Website, http://www.opendiameter.org/

AUTHORS PROFILE

Vinay Kumar S.B, is a student in the Department of Electronics and Communication Engineering, School of Engineering, Jain University, Bangalore. He obtained his Bachelor degree in Electronics and Communication Engineering from Coorg Institute of Technology, ponnampet in 2009 and He is pursuing M.tech(SP and VLSI) in Electronics and Communication Engineering, Jain University, Bangalore. My research interest includes VLSI, DSP, and Embedded Systems.

Dedications: This paper is dedicated to all my peers/mentors for their inspirational support and guidance to understand - Diameter protocol. I would also wish to extend my gratitude and thanks to Vishwamanava PU College, Mandya and SBMJCE, Bangalore.

Manjula. N. Harihar, is a Assistant Professor in the Department of Electronics and Communication Engineering, School of Engineering, Jain University, Bangalore. She obtained her Bachelor degree in Electronics and Communication Engineering from S.T.J Institute of Technology, Ranebennur and Master degree in Communication Systems from P.D.A College of Engineering, Gulbarga, Karnataka, India. She is pursuing Ph.D in Electronics and Communication Engineering, Jain University, Bangalore. Her research interest includes Image Processing, VLSI, Neural Networks and Wireless Communication.