AUTHENTICATION, AUTHORIZATION AND ACCOUNTING PROVIDED BY DIAMETER PROTOCOL

Mitko Bogdanoski, Pero Latkoski, Tomislav Shuminoski, Aleksandar Risteski

Faculty of Electrical Engineering – Skopje, Karpoš II bb, 1000 Skopje, Macedonia,
mitko.bogdanoski@gmail.com, {pero, tomish, acerist}@feit.ukim.edu.mk

Abstract – The architecture and protocols for authentication, authorization, and accounting (AAA) are one of the most important design considerations in the next generation wireless networks. Many advances have been made to exploit the benefits of the current systems based on the protocol Remote Authentication Dial In User Service (RADIUS) protocol, and its evolution into the more secure, robust, and scalable Diameter protocol. Diameter is the protocol of choice for the IP multimedia subsystem (IMS) architecture, the core technology for the next generation networks. It is envisioned that Diameter will be widely used in various wired and wireless systems to facilitate robust and seamless AAA. In this paper, we provide an overview of the Diameter protocol, and short summary of the current and future trends related to the Diameter-based AAA systems.

***Keywords* – AAA, RADIUS, Diameter, EAP, Mobile IP**

1. INTRODUCTION

Diameter protocol [1], is one of the latest protocols and unknown to many security professionals, but is silently spreading and will soon be known as much as the RADIUS and TACACS+. Diameter protocol has been developed to build upon the functionality of RADIUS and overcome many of its limitations. The creators of this protocol decided to call it Diameter as a play on the term RADIUS—as in *the diameter is twice the radius*.

Diameter is another AAA protocol that provides the same type of functionality as RADIUS and TACACS+, but also provides more flexibility and capabilities to meet the new demands of today’s complex and diverse networks. At one time, all remote communications took place over PPP and SLIP connections and users authenticate themselves through PAP or CHAP. Those were simpler, happier times when our parents had to walk uphill both ways to school wearing no shoes. As with life, technology has become much more complicated and there are more devices and protocols to choose from than ever before. Today, we want our wireless devices and smart phones to be able to authenticate themselves to our networks and we use roaming protocols, Mobile IP, Ethernet over PPP, Voice over IP (VoIP), and other more sophisticated and advanced stuffs that the traditional AAA protocols cannot keep up with.

2. DIAMETER BASE PROTOCOL OVERVIEW

As network architectures evolved, together with the tremendous growth in the wireless data infrastructures, secure inter-domain communication among various AAA servers to exchange subscribers’ credentials, profiles, and accounting information became an absolute necessity. Despite its tremendous success, RADIUS inherent security vulnerabilities, its questionable transport reliability, and its limited redundancy support were the primary reasons for the introduction of the Diameter protocol [1] as a substitute protocol. Diameter was carefully designed to address security and reliability while thoroughly exploiting the benefits of RADIUS. Thus, secure transmission mechanisms using a choice of IPsec or transport layer security (TLS) protocols were integrated into Diameter, while reliable transport was enhanced by designing Diameter to run over either stream control transmission protocol (SCTP) or transmission control protocol (TCP) supported by standardized failover and failback (recovery) mechanisms.

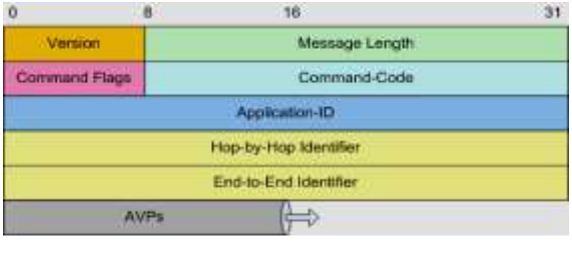


Fig. 1 - Diameter base protocol

Diameter RFC reused many of the RADIUS message codes and attributes and extended them. Fig. 1 shows Diameter's header format. The framed fields in Fig. 1 are those carried over from RADIUS. In contrast to RADIUS, note the introduction of the Version, Command Flags, Application ID, Hop-By-Hop ID, and End-to-End ID fields in Diameter. Furthermore, the increase in size of the message length field (from 2 octets in RADIUS to 3 in Diameter) can be noted. Also, the authenticator field is no longer present as security is guaranteed by the integrated IPsec and TLS protocols. Command codes in Diameter start from 257 to maintain compatibility with RADIUS. Unlike in RADIUS, the requests and answers have the same command codes in Diameter, for example, the accounting request (ACR) and answer (ACA) commands have the command-code of 271. Diameter, based on one of the command flags, can recognize message types (e.g., whether it is ACA or ACR). Other flag, for example, instructs nodes whether a message must be processed locally and should not be forwarded. There is a flag which along with the result-code AVP is used to indicate errors (and possibly redirection as we will see later). Finally, one of the flags is used to indicate a possible duplication in case of retransmissions after a failover.

3. DIAMETER BASE PROTOCOL APPLICATION

Diameter base specification only describes the support for accounting, while other protocols and services that use Diameter or Diameter servers are considered as applications for Diameter and are described in separate application-specific documents.

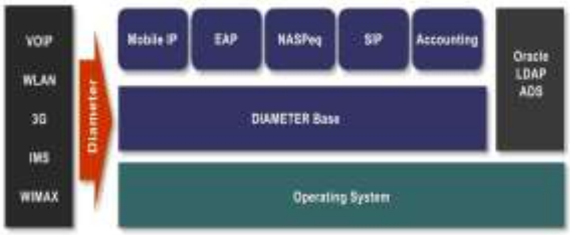


Fig. 2 – Diameter base protocol application

It can safely be assumed that not every Diameter node deployed in a Diameter infrastructure will support all the Diameter applications out there. Therefore, when two Diameter nodes intend to interact with each other on behalf of a Diameter application, each node needs to make sure that the other actually does support the said application. A Diameter feature called capability negotiation provides this assurance. To facilitate the capability negotiation, each Diameter application is assigned a standard unique application identifier by IANA, so that by passing the supported application IDs to the other party, each party can indicate what applications it supports. Since support for the Diameter base protocol is mandatory for all Diameter nodes, the Diameter base does not require its own application ID. Fig 2 shows some of the applications of the diameter base protocol defined in [1].

In the following we provide a brief overview of some of these applications.

3.1. Diameter Mobile IP application

Mobile IP is a technology that allows a user to move from one network to another and still use the same IP address. It is an improvement upon the IP protocol because it allows a user to have a *home IP address,* associated with his home network, and a *care-of address.* The care-of address changes as he moves from one network to the other. All traffic that is addressed to his home IP address is forwarded to his care-of address. Up until the conception of Diameter, IETF has had individual working groups who defined how Voice over IP (VoIP), Fax over IP (FoIP), Mobile IP, and remote authentication protocols work. Defining and implementing them individually in any network can easily result in too much confusion and interoperability. It requires customers to roll out and configure several different policy servers and increases the cost with each new added service. Diameter provides a base protocol, which defines header formats, security options, commands, and AVPs. This base protocol allows for extensions to tie in other services, such as VoIP, FoIP, Mobile IP, wireless, and cell phone authentication. So Diameter can be used as an AAA protocol for all of these different scenarios. As an analogy, consider a case in which ten people all need to get to the same hospital, which is where they all work. They all have different jobs (doctor, lab technician, nurse, janitor, and so on), but they all need to end up at the same location. So, they can either all take their own cars and their own routes to the hospital, which takes up more hospital parking space and requires the gate guard to authenticate each and every car, or they can take a bus. The bus is the common element (base protocol) to get the individuals (different services) to the same location (networked environment). Diameter provides the common AAA and security framework that different services can work within.

3.1.1. Mobile IPv4

The Mobile IPv4 application [2] allows mobile nodes to receive service from foreign service providers. The application allows the Diameter server to authenticate, authorize and collect accounting information for its clients. The Mobile IPv4 application cannot be used with the Mobile IPv6 protocol. More about Mobile IPv4 can be found in RFC 3344.

3.1.1.1. Interaction diagram

In the application presented in Fig.3, the Foreign Agent (FA) or Home Agent (HA) acts as the Diameter client, because the mobile nodes interact over IPv4 with the FA. The basic functionality of Mobile IPv4 is that the HA intercepts packets that are directed to the home address of the mobile user and encapsulates them. It sends the packets over the network through a tunnel to the FA to which the mobile node is connected.

The interaction between the devices is shown below.

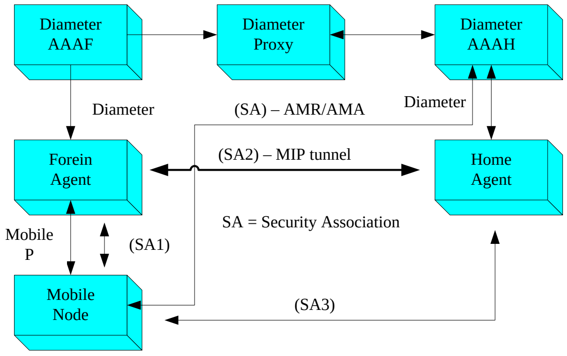


Fig. 3 - Diameter Mobile IPv4 interaction [2]

3.1.2. Mobile IPv6

The Diameter extension for Mobile IPv6 allows a Mobile IPv6 node to access a network of a service provider after the AAA procedures based on the Diameter protocol [1] [3] is completed.

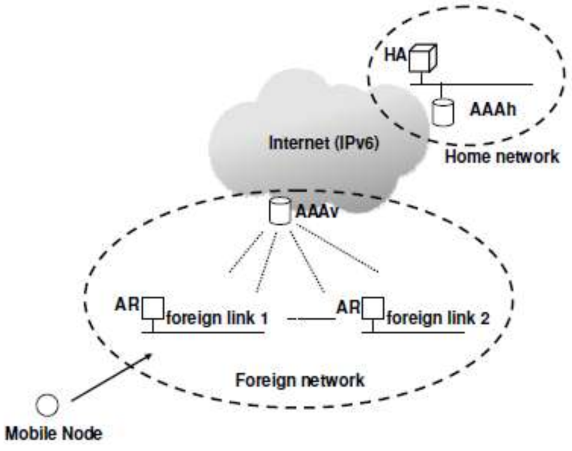


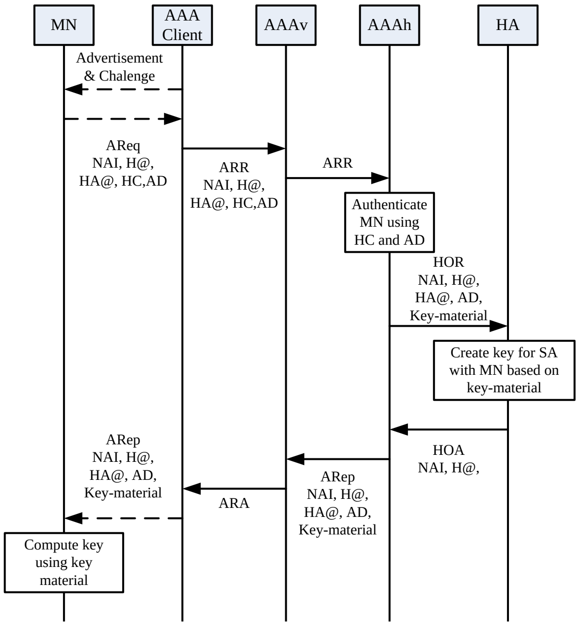
Fig. 4 – Mobile IPv6 AAA Architecture

This protocol assumes a network architecture for AAA services, as illustrated in Fig. 4. The AAAv is an AAA server in the foreign network, while the AAAh is an AAA server in the home network of the mobile node (MN). The AAA client operates in an entity in a foreign network. Hereafter, we assume that the AAA client is located at each access router (AR). The AAA client performs three tasks: (a) allowing the MN to be authenticated, (b) generating accounting data for the MN's network usage, and (c) authorizing the MN to use network resources.

In addition, the following assumptions are used by [3].

- An MN is identified by its network access identifier (NAI) [4], which is globally unique.
- An MN and its AAAh have a long-term key.
- Communication between the AAAv and AAAh is secure.

The basic information flow of the DIAMETER extension for Mobile IPv6 [3] is shown on Fig.5.



MN
AAA Client
AAAv
AAAh
HA
Advertisement & Chalenge
AReq NAI, H@, HA@, HC,AD
ARR NAI, H@, HA@, HC,AD
ARR
Authenticate MN using HC and AD
HOR NAI, H@, HA@, AD, Key-material
Create key for SA with MN based on key-material
ARep NAI, H@, HA@, AD, Key-material
HOA NAI, H@,
ARep NAI, H@, HA@, AD, Key-material
ARA
Compute key using key material

Notations:
NA: Network Access Identifier; H@: Home Address; HA@: Home Agent Address; HC: Host Challenge; AD: Authentication Data

Fig.5 – Information flow in AAA protocol for Mobile IPv6

3.2. Diameter NASREQ application

This application [5] is the direct replacement of the authentication part of RADIUS and offers secure authentication in the Network Access Sever (NAS) environment. In this application the interaction with RADIUS is taken into account.

The interactions between Diameter and RADIUS as described in [5] of this application are to be applied to all Diameter applications, so this RFC extends the Base protocol in this area.

3.2.1. Interaction diagram

In the interaction diagram of this application in Fig.6, the normal behavior of the NASREQ application is shown. First an *AA-Request* (AAR) is sent to the server and if allowed an *AA-Answer* (AAA) is sent back. The *Re-Authentication-Request* (RAR) can be used by the server to verify if the user is using the service. The NAS sends back a *Re-Authentication-Answer* (RAA), where after an AAR and AAA message should follow. The session can be terminated by the server or NAS. The server can send an Abort-Session-Request (ASR) or the NAS can send a Session-Termination-Request (STR).

The accounting is done by the *Accounting-Request* (ACR) and *Accounting-Answer* (ACA) messages. All these messages are described in the NASREQ specification.

The NASREQ application also suggests some basic guidelines to be used by a server that acts as a RADIUS–Diameter protocol gateway, i.e. a server that receives a RADIUS message that is to be translated and transmitted as a Diameter message, and vice versa.

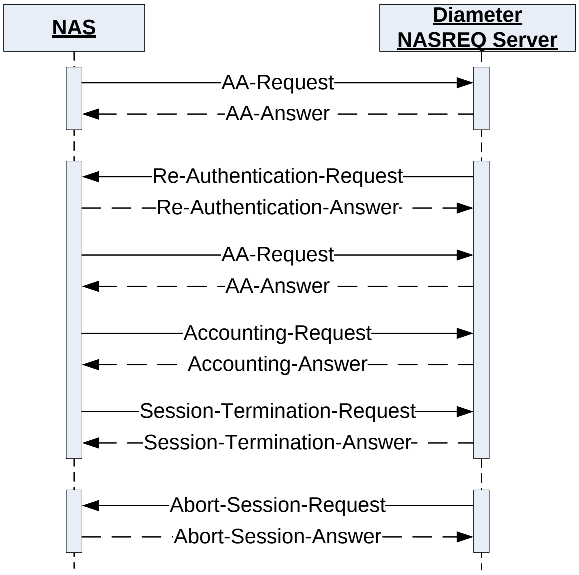


Fig. 6 - Interaction NASREQ

3.3. Diameter Credit control application

The Diameter Credit control application [6] provides real-time credit-control for different end-user services. The application is only concerned with credit authorization for prepaid subscribers. Some accounting features are already specified at the base protocol, but these are not sufficient for real-time accounting for prepaid subscribers.

Two types of events can be seen at the application: session based credit-control and one-time events. Price enquiry, user’s balance checks and refund of credit on the user’s account is usually done in one-time events.

There are two different credit authorization models: authorization with money reservation and credit authorization with direct debiting. The money reservation model is session based and works as follows: the server rates the request from the client and reserves a suitable amount of money from the user’s account. Resources corresponding to the amount are returned to the user. When the user runs out of resources or ends the service, the client reports back to the server how much is used. The server returns money when resources where left over or can make a new reservation.

The money reservation model is session based. A credit-control session always consists of first, possibly intermediate and final interrogations.

Credit authorization with direct debiting is a one-time event. The server directly deducts the right amount of money for the request from the user’s account.

Two messages are added by this Diameter application: *Credit-Control-Request* (CCR) and Credit-Control-Answer (CCA). Credit-control sub-sessions can be used for certain applications, for example when multiple services are embedded in one user session.

3.4. Diameter 802.1X / EAP Application

Extensible Authentication protocol (EAP) is an arbitrary authentication mechanism that is used to authenticate a remote connection. As an extension of the Point to Point Protocol (PPP) it views many forms of network connections (i.e.: wired ports, Virtual Private Network (VPN), wireless connections) that are not immediately seen as such as remote connections. EAP is negotiated at the connection phase with the exact method negotiated between the authenticator and the client [7].

The IEEE 802.1x authentication system is a means for authenticating and controlling user access to a protected network, as well as dynamically varying encryption keys. 802.1X works in conjunction with an extensible authentication protocol (EAP), and a Diameter authenticator [8], to both the wired and wireless LAN media [9]. It consists of three parts:

1. The Supplicant – the client wishing to join the network
2. An authentication server – an authentication system, in our case Diameter
3. An authentication device – an intermediary between the server and client, usually an access point

It supports multiple authentication methods including Kerberos, one-time passwords, certificates, and public key authentication. In wireless networks, the process involves a four way handshake as shown in Fig. 7. Client authentication with 802.1x works in the following manner:

1. The supplicant (Mobile Station) sends an authentication request to the authentication device.
2. The authentication device (Gateway) responds with a request to the supplicant to provide authentication and blocks all other traffic
3. The supplicant sends an its identity response to the authentication server
4. The authentication server receives and verifies the supplicants’ response. If successful an accept message is sent to the authenticating device, if unsuccessful a failure message is sent.

If the authentication server accepts the supplicant, then the authentication device will transition the client’s port to an authorized state, unblock traffic and forward additional traffic.

There are many different types of EAP, which can be used in conjunction with the 802.1x system. These include: protected EAP (PEAP), lightweight EAP (LEAP), EAP with transport layer security (EAP-

TLS), tunneled transport layer security (EAP-TTLS), and EAP message digest (EAP-MD-5) [11].

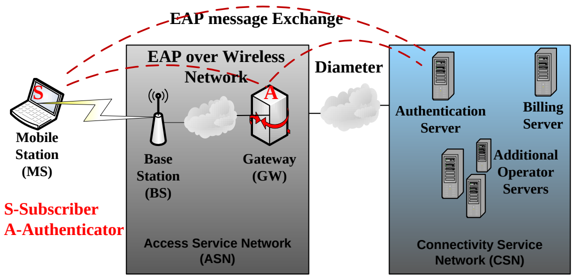


Fig. 7 - The four way handshake process used to authenticate clients in a wireless network using 802.1x [10]

3.5. Diameter SIP application

The Diameter SIP application [12] is designed to be used in conjunction with the SIP protocol [13]. It provides the functionality of authentication of the user of a SIP request and authorization of SIP resources. The SIP server and Diameter client are co-located in the same node. For this application no particular sequence of events between SIP and Diameter are required, nor a mapping of SIP procedures to Diameter SIP application procedures.

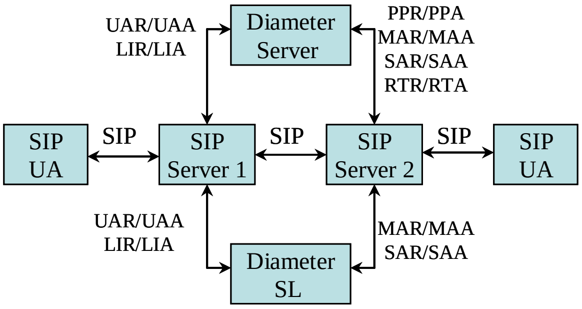


Fig. 8 - Diameter SIP application architecture [12].

In Fig. 8 the architecture of the Diameter application for SIP can be seen. There is a single Diameter server that stores the user data. The Diameter SL is the Subscriber Locater, which has the responsibility to find the Diameter Server that contains the user-related data. For redundancy multiple Diameter servers can keep the data synchronized. Co-located with the SIP servers is a Diameter client which handles the Diameter messages for that server.

3.6. Diameter CMS Security Application

The Diameter protocol may employ either IPsec or TLS for hop-by-hop integrity and confidentiality between two Diameter peers. However, Diameter endpoints might communicate through relay and proxy agents, and in such environments, security may be compromised.

The Diameter CMS (Cryptographic Message Syntax) application [14] provides end-to-end authentication, integrity, confidentiality and non-repudiation at the AVP level. Individual AVPs may be digitally signed and/or encrypted. Diameter proxies can add, delete or modify unsecured AVPs in a message.

The Diameter CMS security application makes use of two main techniques: digital signatures and digital certificates. Digital signatures, along with digital certificates, provide authentication, integrity and non-repudiation. Encryption provides confidentiality. These techniques can be used simultaneously to provide the required security.

The Diameter CMS security application defines the Diameter messages and AVPs that are used to establish a security association between two Diameter nodes, and the AVPs used to subsequently carry secured data within Diameter messages.

3.7. Diameter QoS application

The Diameter Quality of service application provides AAA for quality of service reservations [15]. This means that a reservation request can be authenticated and authorized and that the resources consumed are accounted for.

A quality of service request must be made by protocols like the Resource Reservation Protocol (RSVP) [16]. The network element receiving this request then processes this request and has to perform three different actions: admission control, authorization and resource reservation. The admission control means determining if there are enough resources to fulfill the request. The authorization server is contacted to perform authorization of the request. Then the resources are reserved.

There are two different models: the three party model and the token-based three party model. In the three party model the visited network is compensated for the resources consumed by the user via the home network. In the token-based three party model a token is used when authorization takes place at the application level, then the server will send a token to the network element which authorizes the request from the user.

The messages added by this application are: QoS-Authorization-Request QAR), QoS-Authorization-Answer (QAA), QoS-Install-Request (QIR), QoS-Install-Answer (QIA).

The first two messages are used for client initiated authorizations requests to the server. The last two messages are used server-side initiated QoS parameter provisioning, which means that the server is able to update installed QoS parameters.

3.8. Diameter 3GPP applications

In IMS, several interfaces are specified that use the Diameter protocol [17]. The interfaces are defined as a Diameter application where the vendor is 3GPP. In the table below, the different interfaces are stated. Per interface the location (between functions) is given where it appears in IMS, what the general purpose of the interface is and in which document the interface is specified.

Interface name	Location	Purpose	Specified in document
Cx	CSCF-HSS	Authenticating and authorization	3GPP TS 29.228 and 29.229
Sh	AS-HSS	User profiles	3GPP TS 29.328 and 29.329
Re/Rf	OCRP-RF	Charging	3GPP TS 32.296
Wx	HSS–AAA Server	Charging WLAN	3GPP TS 29.234
Zn	BSF-NAF	Authentication	3GPP TS 29.109
Zh	BSF-HSS	Fetch Keying Material	3GPP TS 29.109
Gq	PDF-AF	Not in release 7	3GPP TS 29.209
Gmb	GGSN-BM-SC	Exchange MBMS service control information	3GPP TS 29.061
Gx	PCRF-PCEF	Flow Based charging GPRS	3GPP TS 29.210
Gx over Gy		Online charging GPRS	3GPP TS 29.210
MM10	MMS Relay-MSCF	MMS	3GPP TS 29.140
Rx	CRF-AF	Charging	3GPP TS 29.211
Pr	PNA-AAA Server	Presence I-WLAN	3GPP TS 29.234

Fig. 6 – 3GPP Interfaces

3.9. Future Diameter Application

Future applications can be added using the Diameter API specified for programming using C/C++. Sun Microsystems test implementation SunWaal follows the Diameter Application Programming Interface (API). There also exists another draft named Diameter C++ API, it is defined for use with C++. The open-diameter implementation is based upon the Diameter C++ API and is released under Lesser GNU Public License (LGPL), it is available through the open-diameter homepage.

4. CONCLUSION

In this paper we presented and discussed Diameter protocol which is used to provide AAA services for a range of access technology, one of the most important design considerations in the next generation of telecommunication networks. It was given a short overview, and an extended elaboration why we are using Diameter in spite of RADIUS. We surveyed the details of the Diameter protocol and some of its applications.

The Diameter protocol uses a binary header format and is capable of transporting a range of data units called AVPs. The Diameter base protocol specifies the delivery mechanisms, capability negotiation, error handling and extensibility of the protocol, whereas individual Diameter applications specify service-specific functions and AVPs. We showed that the Diameter base protocol plays an increasingly important role in the three major network tiers, that is, access, distribution, and core. We concluded the paper with a short summary of the current and future trends related to the Diameter-based AAA systems.

5. REFERENCES

[1] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko: Diameter Base Protocol, IETF RFC 3588, September 2003

[2] P. Calhoun, T. Johansson, C. Perkins, T. Hiller, P. McCann: Diameter Mobile IPv4 Application, IETF RFC 4004, August 2005

[3] F. Le, B. Patil, C. Perkins, S. Faccin, “Diameter Mobile IPv6 Application,” Internet draft (work in progress), draft-ietf-dime-mip6-integrated-12.txt, 9 January 2009.

[4] B. Aboda and M. beadles, “The Network Access Identifier,” IETF RFC 2486, January 1999.

[5] P. Calhoun, G. Zorn, D. Spence, D. Mitton: Diameter Network Access Server Application, IETF RFC 4005, August 2005

[6] H. Hakala, L. Mattila, J-P. Koskinen, M. Stura, J. Loughney: Diameter Credit-Control Application, IETF RFC 4006, August 2005

[7] Microsoft: Implementing and Administering Security in a Microsoft Windows 2003 Network, 2006

[8] P. Eronen, T. Hiller, G. Zorn: Diameter Extensible Authentication Protocol (EAP) Application, IETF RFC 4072, August 2005

[9] J.Edney, W. A. Arbaugh (): Real 802.11 Security: Wi-Fi protected access and 802.11i, Addison Wesley Professional, 2004 (in Boston, USA)

[10] M. Bogdanoski, P. Latkoski, A. Risteski, B. Popovski, "IEEE 802.16 Security Issues: A Survey", 16th Telecommunications forum TELFOR 2008 , November 2008 (in Belgrade, Serbia)

[11] Intel: The Alphabet Soup of EAP types - MD5, LEAP, PEAP, FAST, TLS and TTLS, (2005), Retrieved September 15th 2008 from http://www.intel.com/support/wireless/wlan/sb/CS-008413.htm

[12] M. Garcia-Martin, M. Belinchon, M. Pallares-Lopez, C. Canales, K. Tammi: Diameter Session Initiation Protocol (SIP) Application, IETF RFC 4740, November 2006

[13] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler: SIP: Session Initiation Protocol, IETF RFC 3261, June 2002

[14] P. R. Calhoun, B. Storm, S. Farrell, W. Bulley: Diameter CMS Security Application, draft-ietf-aaa-diameter-cms-sec-04.txt, March 2002

[15] D. Sun, P. McCann, H. Tschofenig, T. Tsou, A. Doria, G. Zorn: Diameter Quality of Service Application, Internet Draft (work in progress), draft-ietf-dime-diameter-qos-08.txt, May 7, 2009

[16] S. Herzog: RSVP Extensions for Policy Control, IETF RFC 2750, January 2000

[17] J. Loughney: Diameter Command Codes for Third Generation Partnership Project (3GPP) Release 5, IETF RFC 3589, September 2003