DESIGN METHODOLOGY FOR IP SECURED TUNEL BASED EMBEDDED PLATFORM FOR AAA SERVER

M. Rajendra Prasad[1] J. Sarat Chandra [2] D. Krishna Reddy [3]

[1]Department of ECE, Vidya Jyothi Institute of Technology, Hyderabad, India

[2]Department of CSE, Vidya Jyothi Institute of Technology, Hyderabad, India

[3]Department of ECE, Chaitanya Bharathi Institute of Technology, Hyderabad, India

ABSTRACT

Authentication, Authorization, and Accounting (AAA) Server application provides users AAA services for network devices and mobile software applications. In authentication process if a user is requesting services with IP security highly customized hardware platform server with IP security protocol is required to handle validity of user for the network services. Development and testing of IPSec platform is a great challenge and this platform provides various IP security services for traffic at IP layer in both IPv4 and IPv6.It also provides encryption and decryptions of the payload of IP packets between communicating servers. Authentication process is accomplished via the presentation of an identity and credentials. This paper describes the methodology to develop and evaluate the embedded IP security platform for AAA server for IP sec network users. IPSec network users need to authenticate themselves to the AAA server application when they want to communicate with it. AAA Server application uses RADIUS/DIAMETER protocol and Extensible Authentication Protocol (EAP) to provide user AAA services. Finally results shows embedded IP security platform for AAA server is developed and tested successfully for IPSec network users.

KEYWORDS

IPSec, AAA Server application, Embedded System, Extensible Authentication Protocol(EAP) ,IPv4 network, IPv6 network, embedded linux.

1. INTRODUCTION

In mobile communication domain IPSec is one of the most secured commercially available standard protocols developed for transporting data. With IPSec technology, customers now can build Virtual Private Networks (VPNs) over the Internet with the security of encryption protection against wire tapping or intruding on the private communication [4]. In this project IPSec is using ESP (Encapsulating Security Payload) protocol to provide traffic security of blade cluster in AAA Server application. IPSec involves many advanced component technologies and different encryption methods. IPSec's operation mechanism can be described into four main stages based on the traffic between peer and Home Agent (HA) when the IPSec security policy is configured in the IPSec peers which initiates and starts the Internet Key Exchange (IKE) protocol process [6].

IKE phase 1 stage: In this stage IKE protocol authenticates IPSec peers and negotiates IKE Security Association (SA). An SA is defined as a logical connection between two devices to transfer the data. It provides data protection for unidirectional traffic by the defined IPSec

DOI : 10.5121/ijmnct.2013.3605

protocols. With the help of predetermined mechanism such as pre shared keys and digital certificates the two parties are authenticated each other.

IKE phase 2 stage: IKE negotiates and configures IPSec SA parameters and also sets up the matching IPSec SAs with the peers. The two parties negotiate the authentication algorithms and encryption techniques which are used in the IPSec SAs. To derive the IPSec SAs the master key is essential and it is used to deploy. Once the SA keys are exchanged and created then the IPSec SAs are ready to protect user data between the two VPN gateways in IKE phase 2 stages [6].
Data transfer stage: Based upon the IPSec parameters and keys stored in the SA database data is transferred between IPSec peers.

IPSec tunnel termination stage: Through deletion or by timing out IPSec SAs are terminated. The type of traffic is measured as part of formulating a security policy for use of a VPN. This policy is implemented while configuring the interface for each particular IPSec peer. For Instance, In Cisco routers and PIX Firewalls access lists are used to determine the traffic for encryption mechanism. As per the cryptography policy access lists are assigned and this policy permit statement indicates the specific or selected traffic should be encrypted and denies statements direct that the selected traffic should be sent unencrypted. When interesting traffic is generated, the client initializes the next step is in the process by negotiating an IKE phase 1 exchange.

IKE phase 1 stage

The fundamental purpose of IKE phase 1 stage is to authenticate the IPSec peers and to set up a secure channel between the peers to enable IKE exchanges.

The following functions are performed IKE phase 1:

- IPSec peers are authenticated and protected with their identities.
- To protect the IKE exchange, this phase negotiates a matching IKE SA policy between peers.
- This phase performs an authenticated Diffie-Hellman exchange with the end result of having matching shared secret keys.
- Its sets up a secure tunnel which negotiates IKE phase 2 parameters.
- Basically IKE phase 1 occurs in two modes

    1. **Main mode**
    2. **Aggressive mode.**

1. **Main mode:** This mode has three two-way exchanges from the initiator to the receiver.

- First exchange: It uses algorithms and hashes to secure the IKE communications and these are agreed based on matching IKE SAs in each peer.
- Second exchange: Shared secrete keys material is generated by Diffie-Hellman exchange and random numbers are sent to other end party. Their identity is proved by signed and returned values.
- Third exchange: It verifies the other side's identity parameters. The identity value is the IPSec peer's IP address which is in encrypted form.
- The main objective and the main mode outcome is matching IKE SAs between peers to provide a protected pipe for subsequent protected ISAKMP exchanges between the IKE peers. The IKE SA which specifies the values for the IKE exchange i.e the method of

authentication, the encryption and hash algorithms, the Diffie-Hellman group are used. The IKE SA in each peer is bi-directional.

2. Aggressive Mode

In aggressive mode very few exchanges are made with fewer packets. In the first exchange, everything is crushed into the proposed IKE SA values i.e. the Diffie-Hellman public key which is a nonce that the other party signs and identifies the packet which is also used to verify identity via a third party [16].

In order to complete the exchange the receiver sends everything back that is required and only thing left out is for the initiator to confirm the exchange. One of the drawbacks of using the aggressive mode is that both sides have exchanged information before there is a secured channel. Hence it is possible to "sniff" the wire and identify who has formed the new SA. In addition, an aggressive mode is faster than the main mode.

Stage 2—IKE Phase 2:

The main objective of IKE phase 2 is to negotiate IPSec SAs to sets up IPSec tunnel [11].
The following functions are performed IKE phase 2

- It negotiates IPSec SA parameters protected by an existing IKE SA.
- IPSec security associations are established.
- Renegotiates IPSec SAs to ensure security periodically.
- An additional Diffie-Hellman exchange performed optionally.
- IKE phase 2 defines by only one mode called quick mode.

It occurs after IKE has established the secure tunnel in phase 1. It also negotiates a shared IPSec policy and produces shared secret keying material which is used for the IPSec security algorithms, and establishes IPSec SAs. New shared secret key material are generated by nonces and it prevents replay attacks from generating bogus SAs.It is also used to renegotiates a new IPSec SA when the IPSec SA lifetime expires [4] ,[6], [7] , [8].

Stage 3—IPSec Encrypted Tunnel:

After IKE phase 2 is complete and quick mode has established IPSec SAs, information is exchanged via an IPSec tunnel. Packets are encrypted and decrypted using the encryption specified in the IPSec SA. This IPSec encrypted tunnel can be seen in stage 4

Stage 4 —Tunnel Termination

The termination of IPSec SAs are through deletion or by timing out and an SA can time outs when a specified number of seconds have elapsed or when a specified number of bytes have passed through the tunnel. As soon as SAs are terminated the keys are also discarded and subsequent IPSec SAs are required for a flow. At this time IKE performs a new phase 2 if it is essential for a new phase 1 negotiation. After a successful negotiation result, the new SAs contain new keys. New SAs can be secured and rooted before the existing SAs expire such that there is no interruption for continuous flow.

2. RELATED WORK

Recently, several works of researchers have been focusing on security of embedded telecom applications platforms. Lu & Lockwood proposed an IPSec implementation on Xilinx Virtex-II Pro FPGA1on a reconfigurable network device to secure the control and configuration channel [1]. M.Rajendra Prasad described methodology to develop the embedded platform with IP version 6 networking supportive feature [2]. ZHOU Qingguo describes the procedure to port embedded linux to the XUP Virtex-II Pro development system and using serials of development tool kits and provides an advanced hardware platform that consists of a high performance Virtex serials platform FPGA [3]. M. Rajendra Prasad presented the procedure for transplanting linux kernel on PowerPC based custom board which is considered as an embedded system targeted for IPBTS application software [5]. This paper proposes the system level methodology to develop and evaluate the embedded IP secured platform for AAA server application for IP secured network users.

3. SYSTEM LEVEL DESIGN METHODOLOGY

In this design methodology we are describing detailed procedure to develop the IP secured platform for AAA server application to support and operate in the CSN (Connectivity Service Network) of WiMAX networks. AAA Server uses RADIUS/DIAMETER protocol and Extensible Authentication Protocol (EAP) to provide user authentication, authorization, and accounting services to network devices and software applications. In this IP secured based platform messages are exchanged during the network access phase between mobile nodes and network equipments working as network access controllers – such as access points, access routers or AAA Server.

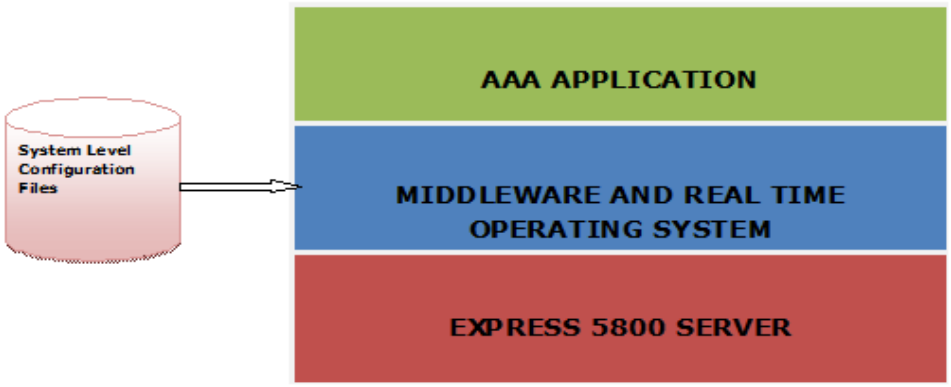

Figure 1. AAA Server Architecture.

The system level design architecture diagram of AAA server is depicted in the figure 1 and configured with secured system files. The Express 5800 Server is a reliable and supports essential networking features for wireless applications. The customized hardware is well suiting for AAA application. AAA application uses middleware components and RTOS (RT-linux) APIs to serve Session management services, operation management services LAN Redundancy Control services, database management services and log management services [15]. In this proposed design methodology RT linux is used as Real time operating system and transplanted on Express server as shown in the figure 1 [9] [10] .The detailed procedure to port linux kernel on Express server is discussed in [5].To enable IPSEC on the server following steps should be followed:

- RTOS kernel is configured with enabling options:
  - PF_Key Sockets
  - IP: ESP Transformation
  - IP: IPComp Transformations
- Enable the cryptographic options from the list given below:
  - DES
  - Diffie-Hellman
  - MD5 (HMAC Varient)
  - SHA (HMAC Varient)

In IP security process the configuration of RTOS and method of transplanting of RTOS is shown in the figure 2.

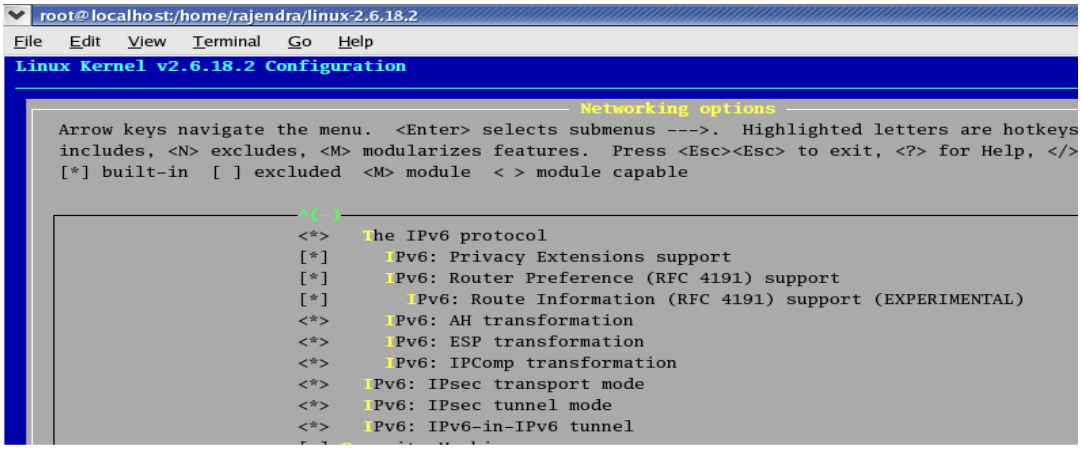

Figure 2. Linux kernel configuration for IPSec

After configuration and changes in the RTOS code RT linux is booted on Express Server 5800. The mode of IPSEC operation IP packet contains message header and payload. Communications has been started before AAA services start, so entire IP packet need not to encrypt and/or authenticate. Only Payload should be encrypted and/or authenticated while data transfer occurs. IPSEC uses Transport Mode to encrypt the packets which include only payload encryption and/or authentication for AAA server.

Services Provided by IPSEC

IPSEC provides IP security services for Traffic at IP layer. These security services are **Encryption**, IPSEC uses ESP protocol to encrypt the IP packet and **Payload Compression** IPSEC uses IP Payload Compression (IPcomp) to provide compression before a packet is encrypted.

Steps to enable IPSEC

Following are the important steps to enable IPSEC:

- Install IPSEC tool.
- Create a file ipsec.conf with read-write permission to root. This file contains the key for encoding policies between the sender and receiver. These keys can be generated manually by using the following command.
  dd if=/dev/random count=24 bs=1 | xxd –ps
- To enable IPSEC following command is used:

"setkey –f <path of ipsec.conf>"

- To test whether IPSEC is enabled or not, following command is used: "tcpdump -i eth0"

The AAA Server provides its services for authentication and authorization to RADIUS module on receipt of authentication request (ACCESS REQUEST). To provide the services for the authentication AAA handler uses the services of EAP module for both initial authentication and re authentication. Upon receiving an Access-Request as part of network entry, where the username is a pseudo-identity, the HAAA will check Pseudo-ID mapping table to ensure that the pseudo-identity is not in use by an authenticated MS in the realm. If the pseudo-identity is used by another MS, then the HAAA will fail the EAP Authentication by sending an ACCESS REJECT containing an EAP-failure indication as described in the flow and The detailed flow of processing of requests from users with security and authentication flow with security is shown in the figure 3 and figure 4.

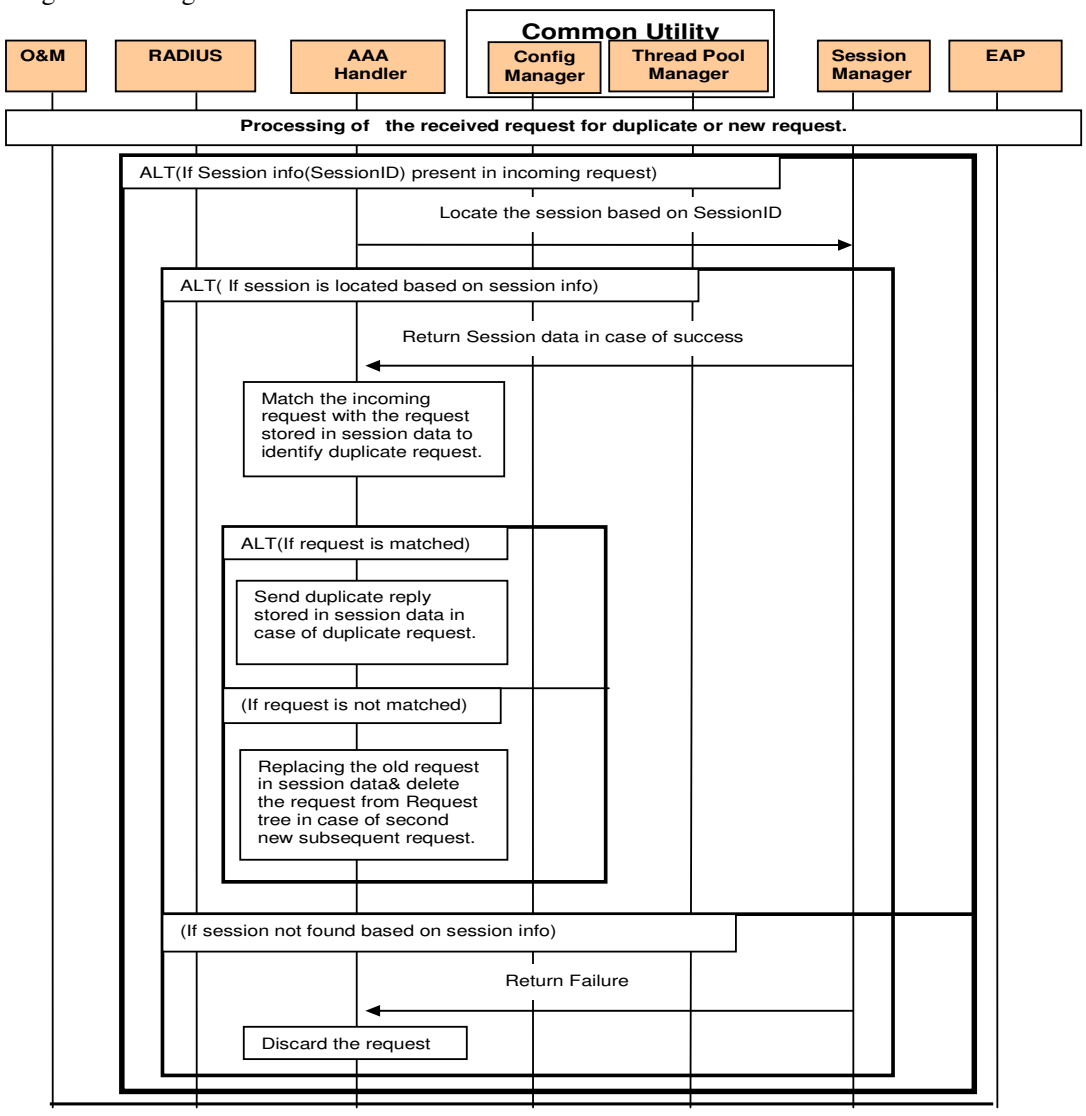

Figure 3. Authentication request processing flow from NAS

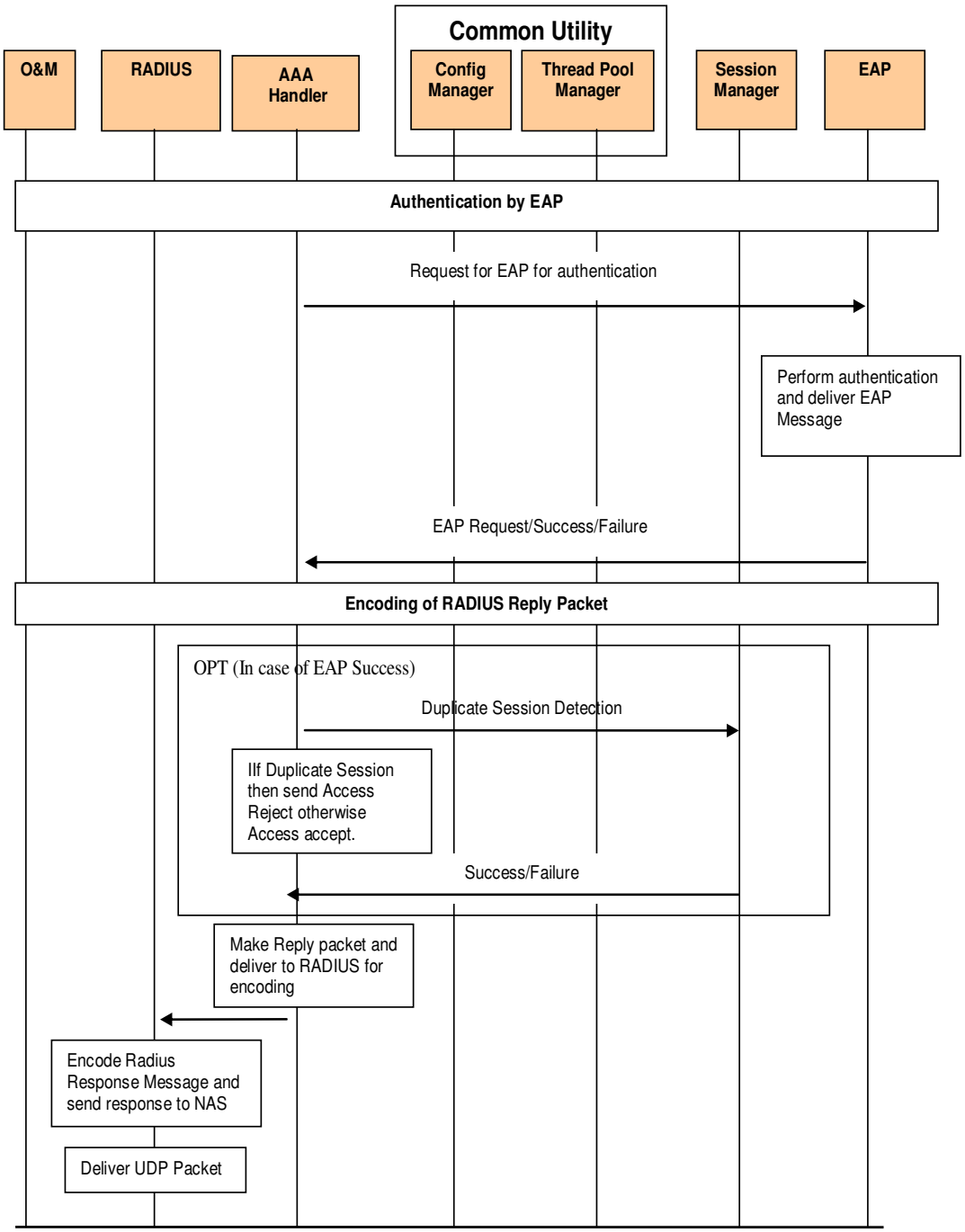

Figure 4. Authentication request processing by EAP.

3. RESULTS AND DISCUSSIONS

Initially we have installed/configured/tested and communicated successfully Linux Open swan U2.3.1/K2.6.11-1.1369_FC4.We created the IPSec connection between two hosts and exchanged messages and ESP packets output. We also tested by ping one of the hosts in the tunnel from the other one as shown in the figure 5 and figure 6.

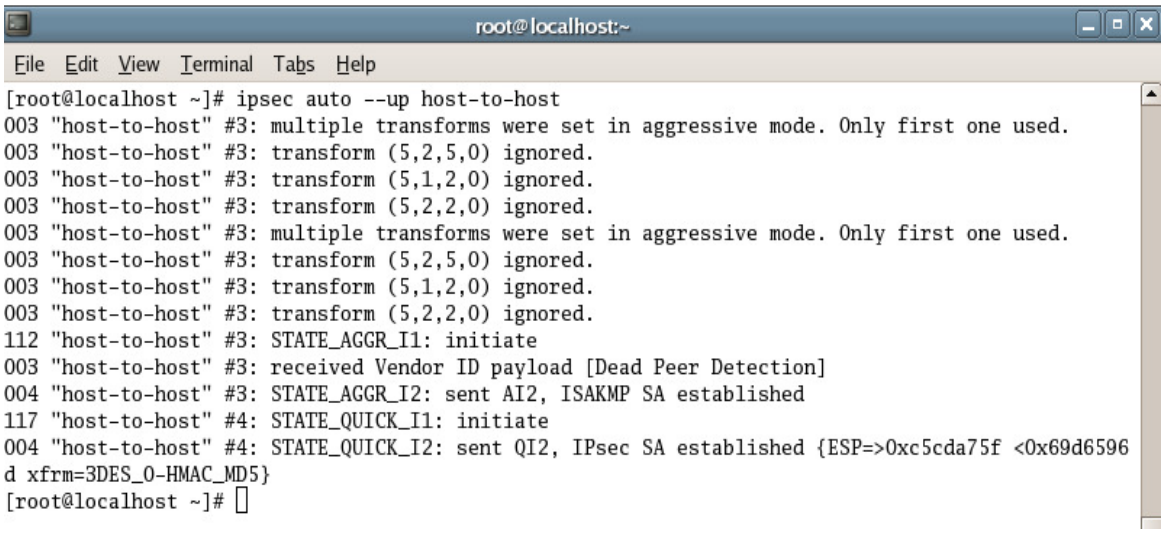

Figure 5. IPSec Configuration

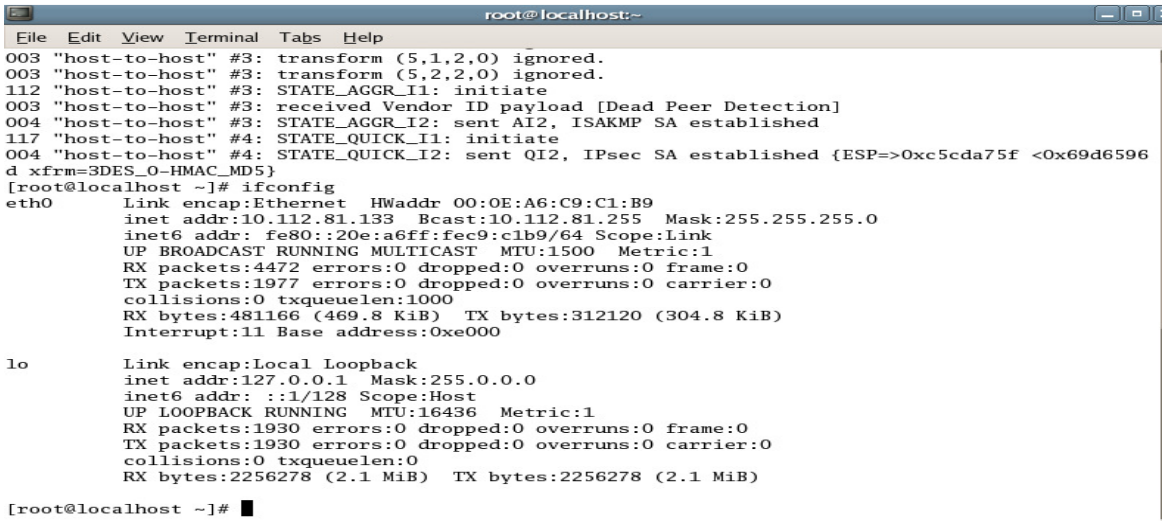

Figure 6. IPSec Configuration

Later one of our host system is replaced with the customized Express Server 5800 and tested IKE authentication between a product (DUT) and Open swan running Express server. Log file of client and server are shown in the figure 7 and figure 8. Log files for Main mode and Aggressive mode for Phase1 scenario are also shown in these figures. Finally the proposed

methodology is developed and evaluated successfully for an embedded IP security platform for AAA server for IP sec network users [12], [13].

003 "router-to-linux" #1: multiple transforms were set in aggressive mode. Only first one used.
003 "router-to-linux" #1: transform (5,2,5,0) ignored.
003 "router-to-linux" #1: transform (5,1,2,0) ignored.
003 "router-to-linux" #1: transform (5,2,2,0) ignored.
003 "router-to-linux" #1: multiple transforms were set in aggressive mode. Only first one used.
003 "router-to-linux" #1: transform (5,2,5,0) ignored.
003 "router-to-linux" #1: transform (5,1,2,0) ignored.
003 "router-to-linux" #1: transform (5,2,2,0) ignored.
112 "router-to-linux" #1: STATE_AGGR_I1: initiate
004 "router-to-linux" #1: STATE_AGGR_I2: sent AI2, ISAKMP SA established
117 "router-to-linux" #2: STATE_QUICK_I1: initiate

Figure 7. Test log file in agreesive mode

104 "router-to-linux" #1: STATE_MAIN_I1: initiate
106 "router-to-linux" #1: STATE_MAIN_I2: sent MI2, expecting MR2
108 "router-to-linux" #1: STATE_MAIN_I3: sent MI3, expecting MR3
004 "router-to-linux" #1: STATE_MAIN_I4: ISAKMP SA established
117 "router-to-linux" #2: STATE_QUICK_I1: initiate

Figure 8. Test log file in main mode

TEST SPECIFCATION	
Protocol	IKE
Test Case Group	Main Mode
Test item	Verify DUT acts as Initiator and Responder for Phase 1 Main Mode.
Objective	DUT should receive the ISAKMP-SA Establish message for Phase 1 main mode from remote machine.
Test Procedure	
1. Basic environment set up is done. **2. On DUT side conf file configure for main mode.** **3. Apply conf file on DUT side.** **4. Run the deamon for IPSEC at client side.**	
Test Results Details: DUT should receive the ISAKMP-SA Establish message for Phase 1 main mode.	

Figure 9. Test specification of DUT

5. CONCLUSION

Network security is the most vital mechanism in information security because it is responsible for securing all data/information communicated through networked devices. To serve Authentication, Authorization and Accounting (AAA) mechanisms security based platform is essential. This paper describes the methodology to develop and evaluate the embedded IP security platform for AAA server for IP sec network users. IPSec network users need to authenticate themselves to the AAA server application when they want to communicate with it. In this methodology detailed procedure is discussed for Main mode and Aggressive mode for Phase1 scenario of IPSec. This methodology is tested successfully for embedded IP security platform for AAA server for IP sec network users.

ACKNOWLEDGEMENTS

We would like to thank Correspondent and Director of Vidya Jyothi Institute of Technology, Hyderabad for their encouragement to publish this paper.

REFERENCES

[1] Lu, J,Lockwood, J, "IPSec Implementation on Xilinx Virtex-II Pro FPGA and Its Application",Parallel and Distributed Processing Symposium & 19th IEEE International Proceedings, pp. 158b, 2005

[2] **M. Rajendra Prasad** , **D.Krishna Reddy**, "Development of Mobile IPv6 Protocol Based Platform for AAA Server", Pearl Jubilee International Conference on Navigation and Communication, Technically Co-sponsored by IEEE Hyderabad Section, Dec 2012.

[3] ZHOU Qingguo, YAO Qi, LI Chanjuan & Hu Bin "Port Embedded Linux to XUP Virtex-II Pro Development Board", IT in Medicine & Education, IEEE International Symposium,(ITIME), Vol. 1, pp 165 – 169, 2009.

[4] Chang-Soo Ha, Jong Hyoung Lee, Duck Soo Leem, Myoung-Soo Park, Byeong-Yoon Choi , "ASIC design of IPSec hardware accelerator for network security" , Advanced System Integrated Circuits, Proceedings of 2004 IEEE Asia-Pacific Conference , pp. 168-171,2004 .

[5] **Rajendra Prasad.M**, S. Ramasubba Reddy, V.Sridhar, "Framework to port linux kernel on powerpc based embedded system used for telecom application – ipbts", International Journal of Software Engineering & Applications (IJSEA), Vol. 2, No.4, pp127-139, 2011.

[6] Yi Xiaoqing, Wang Ming," Design of IKEv2 protocol based on the PKI/OCSP", International Conference on Computer Science and Information Processing (CSIP), 2012, pp 1357 – 1360, 2012.

[7] Jing Tao, Baosheng Wang "Towards Practical IPSec over Challenged Networks" , Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), pp 398 - 402 ,2011.

[8] Ferrante A, Piuri V, "High-level Architecture of an IPSec-dedicated System on Chip " , 3rd Euro NGI Conference on Next Generation Internet Networks,pp159 – 166, 2007.

[9] Song Kai, Yan Liping, "Improvement of Real-Time Performance of Linux 2.6 Kernel for Embedded Application", ifcsta, vol. 2, pp.71-74, 2009.

[10] Robert Love,"Linux Kernel Development", Pearson Education, USA, pp. 11-21, 2005.

[11] Treytl A, Hirschler B, Sauter T, "Secure tunneling of high-precision clock synchronization protocols and other time-stamped data ", 8th IEEE InternationalWorkshop on Factory Communication Systems (WFCS), Page(s):303–312,2010.

[12] Gunar Schirner, Gautam Sachdeva, Andreas Gerstlauer, Rainer D omer "EMBEDDED SOFTWARE DEVELOPMENT IN A SYSTEM-LEVEL DESIGN FLOW" International Federation for Information Processing (IFIP, a Springer series in computer science) Volume 231, Pages 289-298, 2007

[13] A. Rettberg, Zanella, M., Dömer, R., Gerstlauer, A., Rammig,F, " Embedded System Design: Topics, Techniques and Trends" IFIP Advances in Information and Communication Technology, 2007, Volume 231, Pages 289-298, 2007

[14] Ahmed MF, Gokhale SS;"Reliable Operating Systems: Overview and Techniques", IETE Tech Rev, 26:461-9, 2009.

[15] Musabekov S.B, Srinivasan, P.K., Durai, A.S. Ibroimov R.R, "Simulation analysis of abis interface over IP over DVB-S2-RCS in a GSM over satellite network", ICI 4th IEEE/IFIP International Conference BC Transactions on ECE, Vol. 10, No. 5, pp120-122, 2008

[16] Chu-Chuan Lee, Shao-Wei Chen, Pao-Chi Chang, "Active packetization and priority description for scalable video over IPv6 based wireless networks", Applications and the Internet Workshop, SAINT Workshop. pp179-183. 2004

Authors

M.Rajendra Prasad obtained his B.E and M.E Electronics and Communication Engineering from SK University and Osmania University, Hyderabad respectively. He has 17 years of experience in embedded and telecom research and development.He is persuing his research on system level design methodology for embedded systems for telecom applications from Osmania University, Hyderabad.He is currently working as a Associate Professor, **ECE Department,Vidya Jyothi Insitute of Technology, Hyderabad**. He authored 15 more research papers in various International Journals and presented papers in International Conferences. He is also a member of IEEE. His main research interests are embedded system design ,wireless protocols and RTOS.

Sarat Chandra . Jangam obtained his B.Tech in Computer Science & Engineering from Gudlavalleru Engineering College affiliated to JNTUH and obtained M.Tech in Computer Science & Eng ineering with Specialization Artificial Intelligence & Robotics from Andhra University.He is currently working as Assistant Professor,CSE Department, Vidya Jyothi Institute of Technology, Hyderabad.

D. Krishna Reddy was born in November 1966 at Gudipadu, Andhra Pradesh. He obtained his B.E. from Andhra University in 1990 with distinction and M.Eand Ph.D from Osmania University in 1995 and 2008 respectively. Presently he is working as Professor in CBIT, Hyderabad. He has 21 years of teaching experience. His present areas of interest includes 3G, data communications, LBS and GPS. He is MIEEE, Fellow of IETE, India and LM of ISTE and SEMCE.