International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 1, Issue 2, February 2014)

Media Stream Encryption Device using VoIP and ARM 9 Microcontroller

Mr. Parmeshwar B. Khawal(1) Prof. S.B. Kalyankar(2)
(1)Electronics and Telecommunication Engineering, (2) Computer Science Engineering
D. I.. E. M. S. Aurangabad, Maharashtra, India, D. I. E. M. S. Aurangabad, Maharashtra, India.

Abstract- The VoIP is the advance method as compare to PSTN System. Voice over IP (VoIP) software used to conduct telephone like voice conversations across Internet Protocol (IP) based networks. VoIP services convert the voice into a digital signal that travels over the Internet. VoIP can allow a call directly from a computer, a special VoIP phone, or a traditional phone connected to a special adapter. In addition, wireless "hot spots" in locations such as airports, parks, and cafes allow you to connect to the Internet and may enable you to use VoIP service wirelessly. System has been implemented in a wide variety of structures with multiple protocols, codes, software and hardware based distributions. VoIP is very suitable communication for the network, it has also the cost saving and much more advantages compare to the PSTN network. Quality of service also achieve in the VoIP system. This paper analyzes the VoIP Media stream Encryption, and also performance of VoIP system.

***Index terms* - VoIP, QOS, MSED, PSTN, PBX, LOS**

I. INTRODUCTION

The VoIP Service is very suitable for the communication system, we can made free calls from that VoIP service. In hole word we can communicate from one point to the another point when the MSED using VoIP is connected to the both the ends. [1] Depending upon the network traffic, channel capacity, compression technique the QOS decide. Now days If the devices want to communicate through voice, we require PSTN.[2] By using PSTN no free calls possible and installation of PSTN PBX requires extra wiring, expensive proprietary hardware. That's why MSED using VoIP plays very important role in the communication through voice. This paper is very important to those who are design low cost feature which is based on embedded platform for VoIP media using ARM 32-Bit Microcontroller. Now days Linux operating system is very friendly OS, LOP is used in VoIP.

II. KEY VOIP FEATRUES

The common parameters used in VoIP service are delay, jitter and packet lost. Although the thresholds of those parameters could be subjective, their characteristics are well defined. The QoS parameters and the throughput on VoIP networks have a closed relationship with the used codec. The required bandwidth is selecting according to the parameters and the desired service.

III. OBJECTIVE OF PAPER

The main aim of the paper is to design "design of a voip media stream encryption device". Voice over IP (VoIP) software used to conduct telephone-like voice conversations across Internet Protocol (IP) based networks.[3] VoIP services convert the voice into a digital signal that travels over the Internet. VoIP can allow a call directly from a computer, a special VoIP phone, or a traditional phone connected to a special adapter. In addition, wireless "hot spots" in locations such as airports, parks, and cafes allow you to connect to the Internet and may enable you to use VoIP service wirelessly.[5] In early days the two devices can communicate through internet. The communication is in the form of text by typing it from keyboard. If the devices want to communicate through voice, we require PSTN. By using PSTN No free calls possible and installation of PSTN PBX requires extra wiring, expensive proprietary hardware. The main disadvantage of this system is we can communicate with other device by typing the text only. We cannot communicate through voice calls.

IV. RELATED WORK

Our Embedded paper is to design and develop a low cost feature which is based on embedded platform for VOIP media using ARM 32 bit Microcontroller has feature of image/video processing by using various features and classification algorithms The product is be used as VOIP media device communications platform for multiple applications areas. [9]

The design of a VoIP media stream encryption device based on ARM9 micro controller. The device can be deployed between the VOICE OVER INTERNET PROTOCAL (VOIP) terminal, dedicatedly used for the encryption/de-encryption of the VoIP signal and the RTP voice packet. the encryption flow of the packet is described when the VoIP protocol is SIP and the encryption algorithm is RC4. [10]

Our embedded system is designed for transferring voice through Internet protocol for low cost phone calls, which using SAMSUNG Corporation S3C2440 chips as core processor.

V. ETHERNET CONTROLLER

The DM9000 is a fully integrated and cost-effective single chip fast Ethernet MAC controller with a general processor interface, a 10/100M PHY and 4k Dword SRAM. It is designed with low power and high performance process. The DM9000 supports 8-bit, 16-bit and 32-bit micro processor interface to internal memory access for different processors .the DM9000 also supports IEEE802.3X full- duplex flow control. [6]

The VoIP media stream system makes use of providing voice calls through internet which is interfaced to lower power consumptive and highly advanced micro controller like S3C2440. S3C2440 is a Samsung company's microcontroller which is designed based on the structure of ARM 920T family. This microcontroller works for an voltage of +1.8V DC and at an operating frequency of 400 MHz The maximum frequency up to which this micro controller can work is 533 MHz The core part of an operating system we can cal like kernel. Operating system will perform its functionalities like File management, Process management, Memory management, Network management and Interrupt management with the help of the kernel only.[12] Kernel holds the device related drivers that are present on the motherboard. FRIENDLY ARM board supports for operating systems like SYMBION, ANDROID, EMBEDDED LINUX, WIN CE. But in all these operating systems EMBEDDED LINUX will provide high security to drivers and files. So in our current paper we are making use of kernel of EMBEDDED LINUX with which device related drivers that are present on the mother board of FRIENDLY ARM board will automatically come when we load EMBEDDED LINUX related kernel.

VI. ROOT FILE SYSTEM

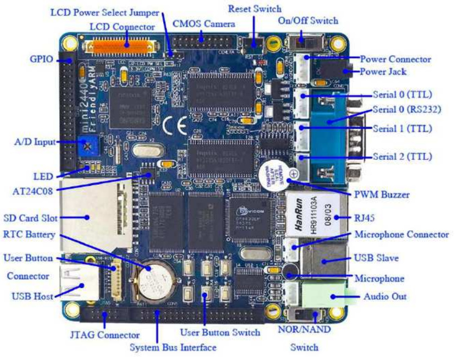
File system will tell how the files are arranged in the internal standard storage devices. In embedded Linux, kernel treats everything as a file even the input and output devices also.[13] In embedded Linux, Root is the parent directory it contains other sub directories like dev, lib, home, bin ,sbin ,media ,mnt ,temp ,proc , etc, opt and etc. According to our application we will interface some external devices also. All the devices means internal devices that are present on the motherboard of MINI 2440 will get their corresponding drivers when we load Embedded Linux related kernel. But these device drivers require micro controller related header files and some other header files which will be present in the lib directory which is present in the root directory.[14] And also the devices related driers will be present in the dev directory which is again present in the root directory. So whenever we will load the Root File System then we will get different directories which will be helpful to the kernel. So compulsorily we need to load the Root File System. MINI 2440 specific Root File System is Root Qtopia.

VII. RC4 ALGORITHM

SAMSUNG's S3C2440A 16/32-bit RISC microprocessor. SAMSUNG's S3C2440A is designed to provide hand-held devices and general applications with low-power, and high-performance microcontroller solution in small die size.[15] To reduce total system cost, the S3C2440A includes the following components.[16]The S3C2440A is developed with ARM920T core, 0.13um CMOS standard cells and a memory complier. Its low power, simple, elegant and fully static design is particularly suitable for cost- and power-sensitive applications. It adopts a new bus architecture known as Advanced Micro controller Bus Architecture (AMBA).[17]The S3C2440A offers outstanding features with its CPU core, a 16/32-bit ARM920T RISC processor designed by Advanced RISC Machines, Ltd. The ARM920T implements MMU, AMBA BUS, and Harvard cache architecture with separate 16KB instruction and 16KB data caches, each with an 8-word line length. By providing a complete set of common system peripherals, the S3C2440A minimizes overall system costs and eliminates the need to configure additional components. The integrated on-chip functions that are described in this document include The ARM (Acorn RISC Machine) architecture is developed at Acorn Computer Limited of Cambridge, England between1983-1985. ARM Limited founded in 1990. ARM became as the Advanced RISC Machine is a 32-bit RISC processor architecture that is widely used in embedded designs. ARM cores licensed to semiconductor partners who fabricate and sell to their customers. ARM does not fabricate silicon itself Because of their power saving features, ARM CPUs are dominant in the mobile electronics market, where low power consumption is a critical design goal. As of 2007, about 98 percent of the more than a billion mobile phones sold each year use at least one ARM CPU.

Today, the ARM family accounts for approximately 75% of all embedded 32-bit RISC CPUs making it the most widely used 32-bit architecture. ARM CPUs are found in most corners of consumer electronics, from portable devices (PDAs, mobile phones, iPods and other digital media and music players, handheld gaming units, and calculators) to computer peripherals (hard drives, desktop routers). [18]

ARM does not manufacture the CPU itself, but licenses it to other manufacturers to integrate them into their own system. It has been developed by integrating features of all the hardware components and software used.



ARM9: (Mini2440 | S3C2440 ARM9 Board)

The paper "DESIGN OF A VOIP MEDIA STREAM ENCRYPTION DEVICE" has been successfully designed and tested. [11] Presence of every module has been reasoned out and placed carefully thus contributing to the best working of the unit. Secondly, using highly advanced ARM9 board and with the help of growing technology the paper has been successfully implemented.[19]

The essential programs that are required in order to work with MINI 2440 like Boot loader, Embedded Linux related Kernel, Root File System will be loaded into the NOR flash which is present on the MINI 2440 board itself. The program that is related with the application will be loaded into NAND flash which is also present on the MINI 2440 board itself. By using boot strap switch that is present on the MINI 2440 will help the user to select either NOR or NAND flash. After that by using DNW tool we can load Boot loader, Embedded Linux related kernel and Root File System into NOR flash by using USB cable and the application related program into NAND flash. Once loading everything into MINI 2440 board it will work based on the application program that we have loaded into theNAND flash. Voice over Internet Protocol (VoIP) is a technology that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions ofthe PSTN. Here we are using two ARM9 boards which are usedto communicate with each other by using VoIP technology. First ARM9 board having one IP address and second board having another IP address. [12] The two ARM9 boards are connected through internet through Ethernet cable. By typing destination IP address the two devices can communicate and transfer the voice through VoIP. The voice can directly given by MIC which is present in the ARM9 board and voice can convert in the form of packets and transfer it to server through ARM9 board.[21] The server will retransmit the packets to the destination IP address.[13] At the other end the ARM9 board retrieves the packets into voice. Like that two devices can communicate over Internet Protocol.

VIII. DISCUSSION AND CONCLUSION

The results show a low performance in secure robustprotocols. In fact, it’s necessary to establish a relationship between secure polices and bandwidth needs before design the VoIP network. Higher security means low throughput but it’s possible to achieve medium security with a reasonable throughput.

ACKNOWLEDGEMENT

I am thankful to all staff members in E& TC department, & Dr. Ullash Shiurkar also my paper guide, & HOD Prof. R.M. Autee

REFERENCES

[1]. David Endler, “Hacking Exposed VoIP: Voice over IP security Secrets & Solutions,” McGraw Hill Osborne Media.

[2]. Behrouz A.Forouzan, TCP/IP protocol suite Tata McGraw - Hill publication.

[3]. D.Richard Kuhn, “Security Consideration for Voice IP Systems,” NIST Special Publication 800-58.

[4]. http : // www.Friendly ARM MINI 2440 .com Datasheet.

[5]. http:// www.Friendly ARM MINI 2440.com Programming Guide.

[6]. X.Lai, **“** on the Design and security of Block Ciphers ,” ETH Series in Information processing , vo l.1 Konstanz : Hartung_ Georre Verlag, 1992.

[7]. A.F Webster and S.E.Tavares**, “**on the Design of S - Box . Advances in Cryptology- crypto 85,” Springer- verlag.

[8]. Gupta, P. Shmatikov, V. VMWare, Inc. , Palo Alto.“Security Analysis of Voice-over-IP Protocols”. IEEE, Computer Security Foundations Symposium,. 2007.

[9]. R. Blom, E. Carrara, F. Lindholm, K. Norrman, M. Naslund, Ericsson Res., Ericsson AB, Stockhol Sweden. “ Conversationa l IP multimedia security”. IEEEMobile and Wireless Communications Network,2002.

[10]. P. Thermos, A. Takanen. “Securing VoIP networks,Threats, Vulnerabilities, and Countermeasures”. Addison Wesley. August 2007.

[11]. T. Dierks, E. Rescorla. “The Transport Layer Security (TLS) Protocol Version 1.1”. IETF RFC 4346. April 2006.

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

[13]. Eren, Evren. Detken, Kai-Oliver. “Voice-over-IP Security Mechanisms – State_of:the:art, risk assessment, concepts and recommendations”. Chile, 2007.

[14]. L. Wang, P. K. Verma, A Network Based Authentication Scheme for VoIP, School of Electrical and Computer Engineering University of Oklahoma, IEEE, Tulsa, OK, USA.

[15]. C. Roberts. “Voice Over IP Security. Centre for Critical Infrastructure Protection”. New Zealand. 2005.

[16]. M. Baugher, C. McGrew. Naslund, M., Carrara, E., Norrman K. “The Secure Real-time Transport Protocol (SRTP)”. IETF RFC 3711. March 2004.

[17]. M. Spencer, Digium, Inc.,B. Capouch, S. J.College, E. Guy,E. Truphone, F. Miller, Cornfed Systems, LLC,K. Shumard. IAX: InterAsterisk eXchange Version 2. RFC 5456, February 2009.

[18]. Feng Cao and Saadat Malik, Cisco Systems, Inc. .”Vulnerability Analysis and Best Practices for Adopting IP Telephony in Critical Infrastructure Sectors”. IEEE Communications Magazine. April 2006.

[19]. P. Zimmermann. “ZRTP: Media Path Key Agreement for Secure RTP”. IETF draft. Sept 2008.

[20]. E. Kokkonen, M. Matuszewski,. Nokia Res. Center, Helsinki. “Peer-toPeer Security for Mobile Real-Time Communications with ZRTP”. 5th IEEE Consumer Communications and Networking Conference, 2008.

[21]. S. Tangwongsan, and S. Kassuvan. “A Security Model of Voice Eavesdropping Protection over Digital Networks”. proceedings of world academy of science, engineering and technology, volume 20, 2007. ISSN 1307-6884

About the authors:

Mr. Parmeshwar Khawal is born in Partur & completed his Bachelor Degree in E & TC from MSS’s CET Jalna & now pursuing Master Degree in E & TC from DIEMS Aurangabad.

Prof. S.B. Kalyankar is currently working as Professor & HOD in DIEMS in Computer Science Engineering Department.