"A Study on VoIP over Wireless Network and Choosing the Best and Secure Way of using VoIP"

[1]Deepak Singh, [2]Garima Tyagi
[1,2]Department of Computer Application,
School Of Computer Sciences,
Career Point University, Kota

Abstract:- **As we all know that wireless networking is a new technology and it is replacing the traditional wired infrastructure for networking. Due to this change there is a dramatic increase in the portability of computer network. For the wired network, basically the TCP protocol is in use the algorithm and parameters of TCP protocol have been optimized for wired networks. VoIP provides an attractive approach to use voice traffic with different types of IP networks; but a specific problem of 802.11 wireless networks is its ability to handle real-time voice applications. In the presence of TCP the performance of VoIP becomes undesirable.**

The main objective of this paper is to focus on the acceptable architectures or the analysis of different service architectures for delivering these services. In the systems where they are implementing VoIP technologies to cut the communication cost, should not overlook the security risks interconnected with the transfer of voice and data over wireless network

Besides giving the analysis of the architectures the secure transfer of voice and data should be managed as there are numerous threats involved in the VoIP transfer.

Keywords- VoIP, 802.11 wireless networks, MGCP, Megaco/H.248, Session Initiation Protocol, H.323

INTRODUCTION

A wireless 802.11 network is a group of computer systems that can communicate without using a system of wires. In the last few years wireless network is gaining popularity and these devices are present everywhere. Generally the wireless 802.11 networks are present in the places like restaurants, hotels, airports,universities for using internet.
The issues those are present with wireless network is its failure in supporting TCP and real time traffic like Voice over internet protocol (VoIP). VoIP is becoming an important application due to its inexpensiveness & can provide a good quality on a broadband internet connection, so the focus will be on the performance of VoIP over wireless network.

VoIP OVER IP

The transmission of voice over packet-switched network is one of the most emerging trend in communication. As VoIP is enriched with new technologies, but it is also having security risks. Instead of using traditional circuit-based telephony a different architecture is used in VoIP and so it may have a variety of security issues. The main features of VoIP are its low cost, greater flexibility, but it can not be installed without dealing with security problems.
This paper explains the challenges of VoIP architecture and security for wireless network and the requirements for a secured VoIP networks.
VoIP system is having a wide range of architectures and forms. It includes traditional handsets, conferencing units and mobile units. In addition to these units, it also includes call processors/call managers, gateways, routers, firewalls and protocols. It is generally assumed that in VoIP digitized voice travels in packets just like other data, so existing network and tools can be used without any change but VoIP adds a number of complications to the existing network technologies and these problems are extravagant by security considerations.
The implementation of different security measures can decrease the QoS. These complications may be from firewalls delaying on blocking call setup to produce latency and delay variation (jitter). As VoIP is having low tolerance for disruption and packet loss, many security measures are not applicable to VoIP like firewalls, intrusion detection system and they must be specialized by VoIP.

IMPLEMENTATION OF VoIP

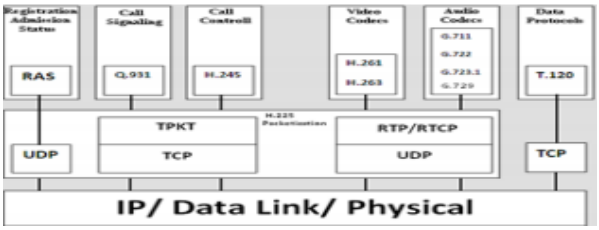
In this First section we will discuss VoIP protocols and after that data processing in VoIP, at last we will discuss about quality of service in VoIP systems.

A) Protocols: (set of rules)

There are currently three types of protocols which are widely used in VoIP implementations: the H.323 family of protocols, the Session Initiation Protocol and the media Gateway Controller Protocol (MGCP). The protocols and services used in VoIP are detailed in Table 1.

Application Layer	Audio RTP, RTCP,(SIP,H.323)
Transport Layer	UDP
Network Layer	IP
Physical Layer	Ethernet, SDH...

H.323 family of Protocol: H.323 is a set of recommendations from the International Telecommunication Union (ITU) and consists of family of protocols that are used for call set-up, call termination, registration, authentication and other functions. These protocols are transported over TCP or UDP protocols. H.323 family of protocol consists of H.225 which is used for registration, admission, and call signalling. H.245 is used to establish and control the media sessions. H.323 uses RTP for media transport and RTCP is used for purpose of controlling RTP sessions.



SIP: The SIP is a signaling protocol which is simple and light weighted, it is most commonly implemented on top of the User Datagram Protocol (UDP), but it can also be implemented on top of the Transmission Control Protocol (TCP).The modification and termination sessions between two or more participants used by SIP (session initiation protocol). The SIP protocol which is also a text-based Protocol it is similar to HTTP and offers an alternative to the complex H.323 protocols.

RTP: The RTP is an essential streaming protocol. It is evidently essential for real time applications that are designed for synchronization of traffic streams compensating for delay variations and de-sequencing. However not ensure on-time delivery or traffic signals or address the issue of QoS, relevant to guaranteed bandwidth availability for specific applications. RTP is generally used in conjunction with UDP, but it can surely make use of any packet-based lower layer protocol.

RTCP: The RTCP is a companion protocol of RTP that is used to transmit periodic control packets on the periodic transmission of control packets to all participants in the session, using the same distribution mechanism as the data packets. RTCP provides QoS feedback and session information. The packets of RTCP carry information related to the state of end points and the statistical information regarding the current RTP stream such as delay times, packet loss and jitter. Both RTP and RTCP run on the top of User Datagram Protocol (UDP) that provide better real-time responsiveness and lower overhead.

IP: IP is responsible for sending and receiving data packet over internet. In VoIP, audio samples are placed into data packets for transmission over the IP network. Typically, a single packet will contain anywhere from 10-30 milliseconds of audio. TCP and UDP are two of the most commonly used connection protocols used for data traverse.

UDP: UDP is connectionless, which means that data packets can be sent without warning, preparation, or negotiation. There's no handshake or setup, just packets of data. UDP also lacks any kind of error control. Not only can packets be delivered in an incorrect order, but they can also get completely left out. UDP is meant for applications where you are more concerned with keeping the stream of information going than making sure you receive every single packet. This makes UDP ideal for real-time services such as Voice over IP.

B) Data Processing in VoIP Systems

There are three types of essential components in VoIP: CODEC (Coder/Decoder), packetized and play out buffer.

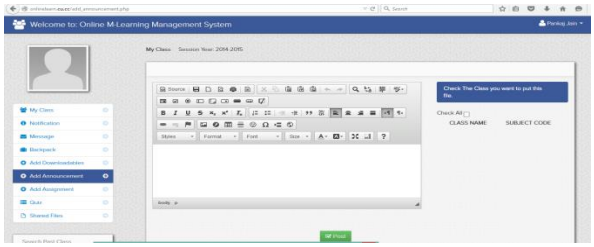
CODEC: The analog voice signals are converted into digital signals at sender's side, after that these digital signals are compressed and then encoded into a predetermined format using voice codec. There are various voice codec such as G.711, G.729, and G.723 etc which are developed by International Telecommunication Union-Telecommunication (ITUT).

Packetized: The packetization process is performed by distributing fragmented encoded voice into equal size of packets. And header are designed and added for each voice packet.

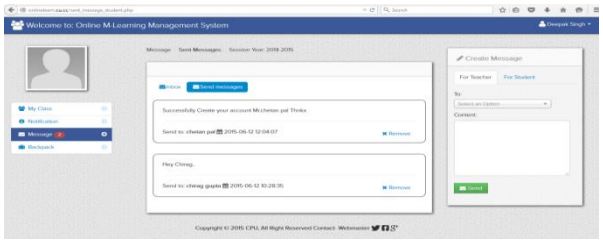
IMPLEMENTATION

A website named M-Learning website has developed for college student which have lots of useful functions related to certain functions used during the education of a students. This website is using the functions of H.323 PROTOCOL?

Visit For Teacher http://onlinelearn.cu.cc/



Visit For Student http://onlinelearn.cu.cc/



CONFIGURATION OF VoIP

Dedicated routers:

These devices allow any user to use its own traditional phone to place VoIP calls. They are connected to cable/DSL
modems (or any high-speed internet source) and allow any user to attach an ordinary telephone. Once these routers are configured with an appropriate VoIP provider and service plan, There is no need of special software or interaction with
a computer. In fact, there is only need to pick up your phone
and dial a number at the dial tone. You can also bring your own adapter with you when you travel and make calls whenever broadband internet access is available.

Adapters (USB):

USB devices also allow you to use a traditional phone to place VoIP calls. They usually come in the form of USB adapters that are slightly larger than the typical thumb drive.
They feature a standard modular phone jack to which you can attach an ordinary phone line. Once connected, your phone behaves as if it were connected to standard phone service.

Software-controlled VoIP applications: "softphones"

There are many software applications ("softphones") that allow you to place VoIP phone calls directly from an ordinary computer with a headset, microphone, and sound card. Internet telephony service providers usually give away
their soft phones but require that you use their service. Together, these applications and services enable users to talk to other people using the same service at no cost, and to the rest of the world for a fee. Software-based VoIP applications
are quite attractive to consumers because they often already
have most of the components necessary to get started at little
to no cost.

Quality of Service (QoS) in VoIP Systems

Quality of service (QoS) can be defined as the network ability to provide good services that satisfy its customers. In other words, QoS is used for measurement of the degree of user satisfactions. When degree of user satisfactions is higher than it means the QoS is also higher. QoS are briefly described as given below:

Delay: Delay can be defined as the total time it takes since a
person, communicating another person, speaks words and hearing them at the other end. Delay can be categorized into three categories: delay at the source, delay at the receiver and network delay.

Jitter: IP network does not guarantee of packets delivery time which introduces variation in transmission delay. This variation is known as jitter and it has more negative effects on voice quality.

Packet Loss: Packets transmitted over IP network may be lost in the network or arrived corrupted or late. Packets would be discarded, when they arrive late at the jitter buffer of the receiver or when there is overflow in jitter buffer or router buffer. Therefore, packet loss is equal to the total loss occurs during congestion of network and late arrival. During the packet loss, the sender is informed to retransmit the lost packets. It causes more packet delay and it affects transmission QoS.

Echo: Echo is the term of the reflections of the sent voice signals by the far end. In VoIP, Echo occurs when a caller at the sender side hears the reflection of his own voice

after he talked on the phone or the microphone, whereas the caller does not notice the echo.. Echo could be electrical echo which exists in PSTN networks or echo of sound which is an issue in VoIP networks.

Throughput: The throughput may be defined as the maximum number of bits received out of the total number of bits sent during an interval of time.

VoIP ATTACKS

Spam over internet telephony (SPIT) : VoIP spam is unwanted, automatically dialed, pre- recorded phone calls using Voice over Internet Protocol (VoIP). It is similar to E-mail spam.

Threats / Risks: Many of the threats associated with VoIP are similar to the threats inherent to any internet application. Internet users are already familiar with the difficulties of email abuse in the form of spam. VoIP opens yet another pathway for these annoyances, which can lead to spam over internet telephony (SPIT), spoofing and identity theft.

Spoofing: It is technically possible for an attacker to masquerade as another VoIP caller. For example, an attacker could possibly inject a bogus caller ID into an ordinary VoIP call so that the receiver believes the call to be coming from a known and trusted source. The receiver, fooled by the electronic identification of the caller, may place unwarranted trust in the person at the other end. In such an exchange, the receiver may be tricked into disclosing personal information like account numbers, social security numbers, or secondary authentication factor: a mother's maiden name, for example. This scheme is essentially the VoIP version of traditional phishing, where a user follows links in an unsolicited email and is tricked into providing personal information on a bogus web site. Attackers may use these bits and pieces of personal information to complete partial identity records of victims of identity theft.

HOW TO PROTECT AGAINST RISKS

There are several types of the principles as well as the practices for safe VoIP usage are the same. However, you may already practice with other internet applications. There are some of the key practices of good personal computing.

i. Verify the authenticity and security of downloaded files and new software. Configure
ii. Your web browser(s) securely.
iii. Use Firewall.
iv. Use and maintain anti-virus and anti-spyware programs
v. Be cautious about opening files attached to email messages or instant messages.
vi. Create and use strong password.

CONCLUSION

We have presented a survey of VoIP security research. In this paper, we have presented a deep analysis of the security concerns of the VoIP technology. Firstly, we have presented a brief overview about the basics of the VoIP technology. Then, we have discussed the VoIP Protocol and attacks related to VoIP Implementation. After that, we have presented the countermeasures that should be considered to help the deployment of secured VoIP systems. A future work will address another important issue in the deployment of VoIP technology; the ability to support the QoS constraints of the voice and video applications.

REFERENCES

[1] H. Yong-feng, Z. Jiang-ling, "Implementation of ITU-T G. 729 speech codec in IP telephony gateway" Wuhan University Journal of Natural Sciences, Volume 5, Number 2, June 2000.
[2] M. Habib, N. Bulusu, "Improving QoS of VoIP over WLAN (IQ-VW)", Project Research Paper, for CS522 Computer Communications, University of Colorado at Colorado Springs, December 2002.
[3] P. M. Athina., A. T. Fouad and J. K. Mansour, "Assessing the Quality of Voice Communications Over Internet Backbones", IEEE/ACM Transactions on Networking, Vol. 1 1 , No. 5, Oct. 2003.
[4] Qiu, P.Q., Monkewich, O., and Probert, R.L., "SIP Vulnerabilities Testing in Session Establishment and User Registration" ICETE (2), 223-229., 2004.
[5] J. B. Meisel, M. Needles, Voice over Internet protocol (VoIP) development and public policy implications, Info 7, 2005.
[6] Advisory Committee on International Communications and Information Policy (ACICIP), 2005.
[7] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, Security Considerations for Voice over IP Systems, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-58, 2005.
[8] http://www.isoc.org/pubpolpillar/VoIP-paper.shtml 15.08.2006. http://www.eyeball.com/spit-solution.htm.
[9] K. M. McNeill, M. Liu and J. J. Rodriguez, "An Adaptive Jitter Buffer PlayOut Scheme to Improve VoIP Quality in Wireless Networks", IEEE Conf. on BAE Systems Network Enabled Solutions, Washington, 2006.
[10] C. Lin, X. Yang, S. Xuemin and W.M. Jon, "VoIP over WLAN: Voice capacity, admission control, QoS, and MAC", International Journal of communication Systems, Vol.1 9, No 4, pp. 491 -508, May 2006.
[11] L. Mintandjian, P.A. Naylor, "A Study Of Echo In VoIP Systems And Synchronous Convergence Of The µ-Law Pnlms