International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 1, January-2014, pp: (15-23), Impact Factor: 1.147, Available online at: **www.erpublications.com**

A Review Paper: Voice over Internet Protocol

Rahul Singh[1], Ritu Chauhan[2]
Dept. of Computer Science and Engineering

Abstract: Voice over Internet protocol (VoIP) is a new way of communicating. It is a technology that allows users to make telephone calls over an IP network. This paper will describe Voice over Internet Protocol (VoIP) to a level that allows discussion of security issues and concerns. Business concerns of implementing VoIP, components of a VoIP system, and relevant security issues and concerns as they apply to the topics are explored. The business concerns will be those that affect Quality of Service (QoS). VoIP components will include end-user equipment, network components, call processors, gateways and two of the more common architectures: Session Initiation Protocol (SIP), Denial of service will be discussed and encryption and network address translation (NAT) will be discussed emphasizing how they impact the implementation of VoIP.

Keywords: VoIP; H.323; SIP; MGCP; QoS; Attacks.

I. INTRODUCTION

The technology used to transmit voice conversations over a data network using IP. Such data network may be the Internet or a corporate Intranet, or managed networks typically used by long distance and local service traditional providers and ISPs (Internet Service Provider) that use VoIP.

Voice over Internet Protocol (VoIP) is a form of communication that allows you to make phone calls over a broadband internet connection. Basic VoIP access usually allows you to call others who are also receiving calls over the internet. Interconnected VoIP services also allow you to make and receive calls to and from traditional landline numbers, usually for a service fee. Some VoIP services require a computer or a dedicated VoIP phone, while others allow you to use your landline phone to place VoIP calls through a special adapter.

Voice over IP refers to the diffusion of voice traffic over internet-based networks. Internet Protocol (IP) was originally designed for data networking and following its success, the protocol has been adapted to voice networking. The history of VoIP began with conversations by a few computer users over the Internet. Initially, VoIP required a headset to be plugged into the computer, and the participants could only speak with others who had a similar set up. They had to phone each other ahead or sent a text message, in order to alert the user at the other end of the incoming call and the exact time [2].

In November 1977, the IETF published the ‘Specifications for the NVP (network voice protocol)’. In the preface to this document, the objectives for the research were explained as the development and the demonstration of the ‘feasibility of secure, high-quality, low-bandwidth, real-time, full-duplex1 digital voice communications over packet-switched computer communications networks’ [3].

In the mid-90s, IP networks were growing, the technology had progressed and the use of personal computers had grown extensively. The belief that VoIP could start to make some impact on the market resulted in high expectations and the distribution of the first software packages. In its early stages, the technology was not sufficiently mature. There was a big gap between the marketing hype and the technological reality, resulting in an overall agreement that technical shortages stopped any major transition to VoIP. However, VoIP has continued to make technical and commercial progress and most of the technical problems have been solved, while others arose. Now its presence is no longer restricted to a limited market niche [4].

While communications network providers are hurrying to adopt IP in their infrastructure, enterprises are adopting IP for private corporate networks. By facilitating communications amongst employees whether working at corporate locations, working at home, or travelling, VoIP can augment corporate efficiencies. Many enterprises are testing VoIP, doing a tryout, or engaging in incremental upgrades. The majority of multinational corporations see VoIP not as a remote possibility, but as a business opportunity, which will be a major part of their business operations in the near future [5].

This paper is divided into four parts. Starting with introduction (Section-I), next section covers the implementation of VoIP (Section-II). Moving ahead, Configuration of VoIP is discussed (Section-III) and finally, Conclusions summarizes the last section (Section-IV).

II. IMPLEMENTATION OF VoIP

In this section firstly we'll discuss VoIP protocols and data processing in VoIP and quality of service in VoIP systems.

a. Protocols

There are currently three protocols widely used in VoIP implementations- the H.323 family of protocols, the Session Initiation Protocol and the media Gateway Controller Protocol (MGCP). VoIP vendors are current selling solutions that can work with either of these families of protocols.

- **H.323 Family of Protocols**

H.323 [8] [9] 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. The following figure.1 shows the various H.323 protocols with their transport mechanisms. H.323 family of protocol includes H.225 is used for registration, admission, and call signaling. H.245 is used to establish and control the media sessions and T.120 is used for conferencing applications in which a shared whiteboard application is used. The G.7xx series of specifications defines audio codec used by H.323, while the H.26x series of specifications defines the video codec. H.323 uses RTP for media transport and RTCP for control of the RTP sessions. The following figure.2 & figure.3 shows the H.323 architecture and call set-up process.

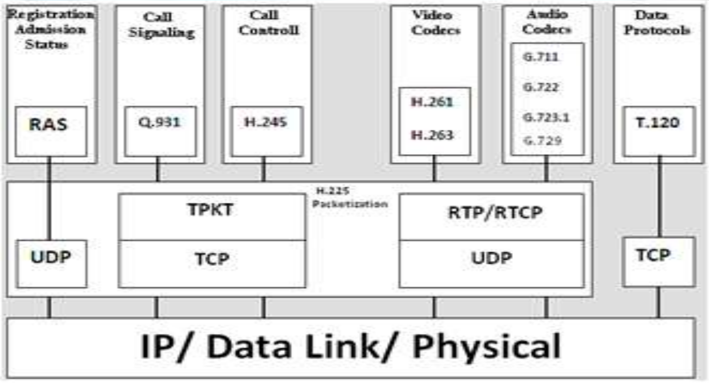


Figure 1: H.323 Protocol Family

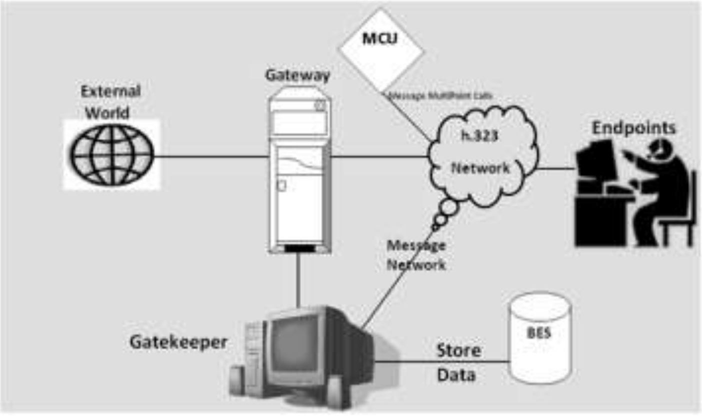


Figure 2: H.323 Architecture

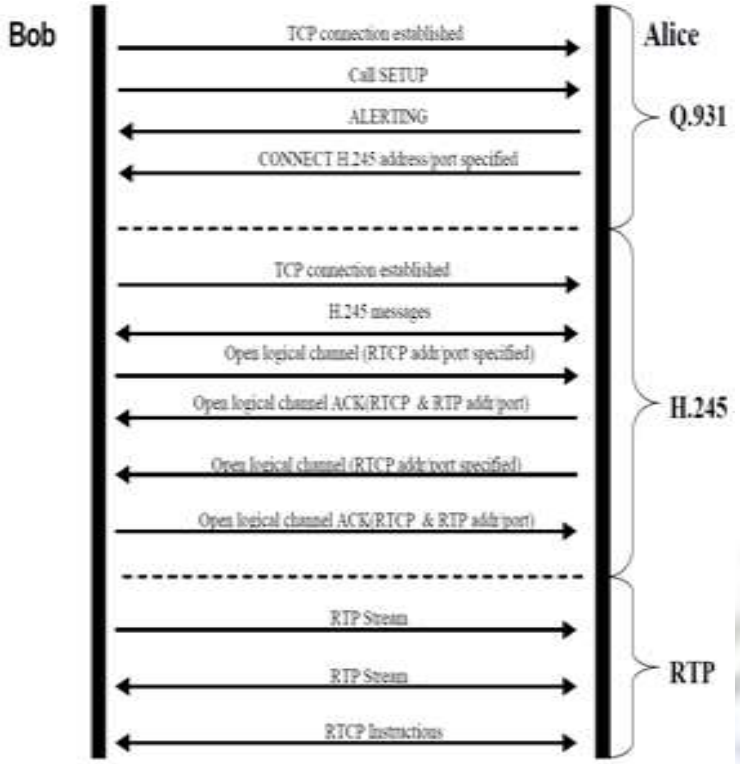
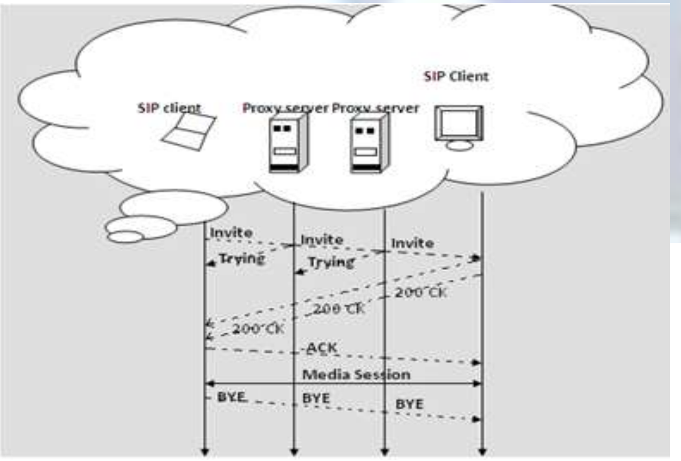

Bob
Alice
TCP connection established
Call SETUP
ALERTING
CONNECT H.245 address/port specified
Q.931
TCP connection established
H.245 messages
Open logical channel (RTCP addr/port specified)
Open logical channel ACK(RTCP & RTP addr/port)
Open logical channel (RTCP addr/port specified)
Open logical channel ACK(RTCP & RTP addr/port)
H.245
RTP Stream
RTP Stream
RTCP Instructions
RTP

Figure 3: Call Setup Process in H.323

- **Session Initiation Protocol (SIP)**

The Session Initiation Protocol (SIP) [9] was defined by the Internet Engineering Task Force (IETF) for creating, modifying and terminating sessions between two or more participants. These sessions are not limited to VoIP calls. The SIP protocol is a text-based protocol similar to HTTP, and offers an alternative to the complex H.323 protocols. Due to its simpler nature, the protocol is becoming more popular than the H.323 family of protocols. The following figure.4 and figure.5 shows the SIP architecture and call set-up and tear down process.



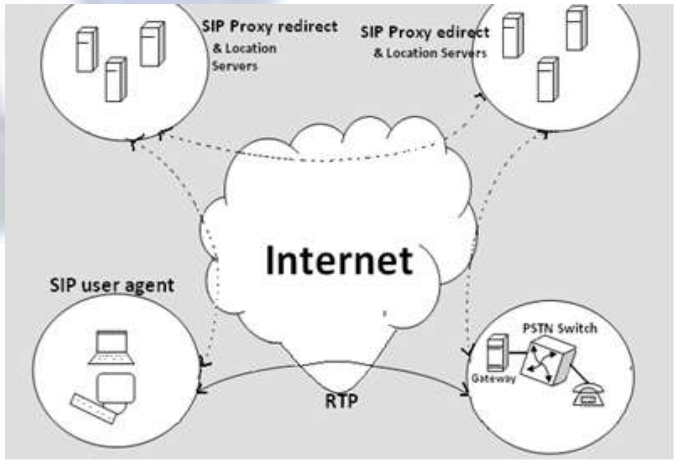

SIP Proxy redirect & Location Servers
SIP Proxy edirect & Location Servers
Internet
SIP user agent
PSTN Switch
Gateway
RTP

Figure 4: SIP Network Architecture

Figure 5: Call setup and tear down in SIP

Media Gateway Control Protocols (MGCP)

MGCP [9] is used to communicate between the separate components of a decomposed VoIP gateway. It is a complementary protocol to SIP and H.323.Within MGCP the MGC server or "call agent" is mandatory and manages calls and conferences, and supports the services provided (see Figure 6). The MG endpoint is unaware of the calls and conferences and does not maintain call states. MGs are expected to execute commands sent by the MGC call agents. MGCP assumes that call agents will synchronize with each other sending coherent commands to MGs under their control. MGCP does not define a mechanism for synchronizing call agents. MGCP is a master/slave protocol with a tight coupling between the MG (endpoint) and MGC (server).

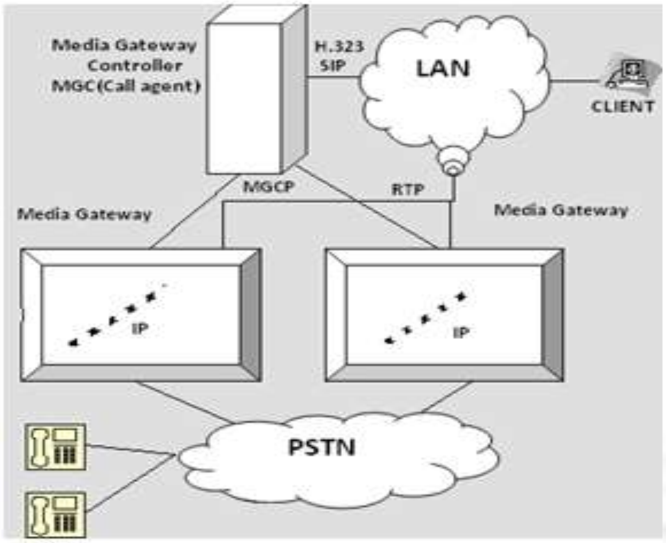


Figure 6: MGCP Architecture

b. Data Processing in VoIP Systems

VoIP consists of three essential components: CODEC (Coder/Decoder), packetizer and playout buffer [10], [11]. At the sender side, an analog voice signals are converted into digital signals, compressed and then encoded into a predetermined format using voice codec. There are various voice codecs developed and standardized by International Telecommunication Union-Telecommunication (ITU-T) such as G.711, G.729, and G.723 etc. Next packetization process is performed which fragment encoded voice into equal size of packets.

Furthermore, in each packet, some protocol headers from different layers are attached to the encoded voice. Protocols headers added to voice packets are of Real-time Transport protocol (RTP), User Datagram Protocol (UDP), and Internet Protocol (IP) as well as Data Link Layer header. In addition, RTP and Real-Time Control Protocol (RTCP) were designed at the application layer to support real-time applications.

Although TCP transport protocol is commonly used in the internet, UDP protocol is preferred in VoIP and other delay-sensitive real-time applications. TCP protocol is suitable for less delay-sensitive data packets and not for delay-sensitive packet due to the acknowledgement (ACK) scheme that TCP applies. This scheme introduces delay as receiver has to notify the sender for each received packet by sending an ACK. On the other hand, UDP does not apply this scheme and thus, it is more suitable for VoIP applications.

The packets are then sent out over IP network to its destination where the reverse process of decoding and de-packetizing of the received packets is carried out. During the transmission process, time variations of packet delivery (jitter) may occur. Hence, a play out buffer is used at the receiver end to smoothen the playout by mitigating the incurred jitter. Packets are queued at the playout buffer for a playout time before being played. However, packets arriving later than the playout time are discarded. The fig.7 shows the end –to- end transmission of voice in VoIP system.
Besides, there are signaling protocols of VoIP namely Session Initiation Protocol (SIP) and H.323. These signaling protocols are required at the very beginning to establish VoIP calls and at the end to close the media streams between the clients.

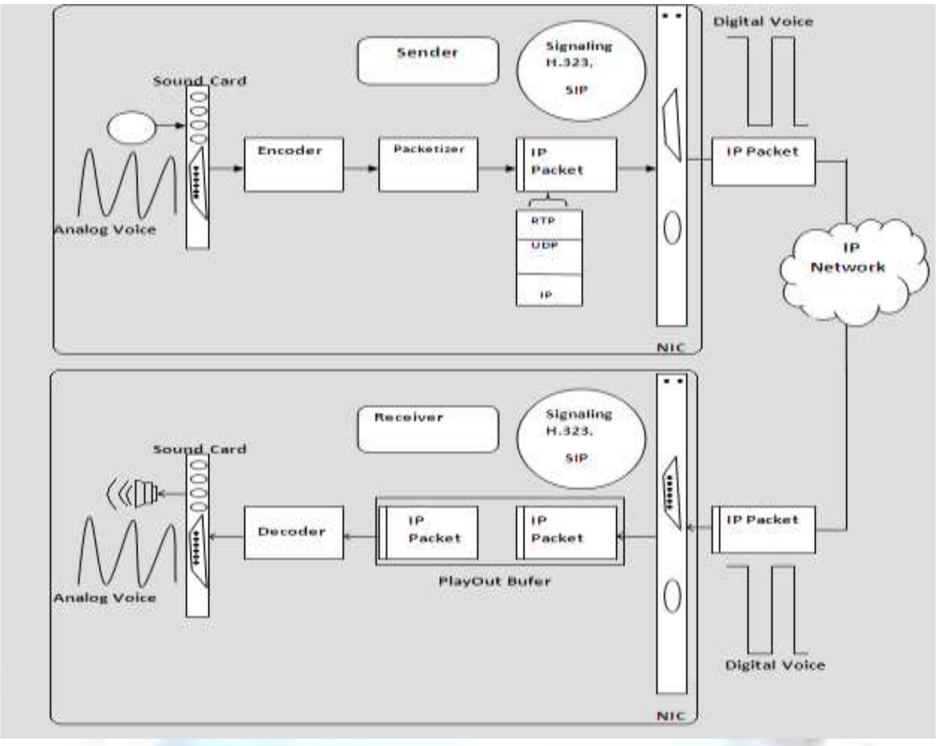


Figure 7: End-to End Voice Transmission

c. Quality of Service (QoS) in VoIP Systems

Quality of service (QoS) [3] can be defined as the network ability to provide good services that satisfy its customers. In other words, QoS measures the degree of user satisfactions; the higher the QoS, the higher degree of user satisfaction. QoS are briefly described in following sections.

- 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: delay at the source, delay at the receiver, and network delay [3].

- 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 [3], [4].

- 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 the total loss occurs due to network congestion and late arrival [5]. In case of packet loss, the sender is informed to retransmit the lost packets and this would cause more delay and thus affecting transmission QoS.

- Echo

In VoIP, Echo is experienced when caller at the sender side hears a reflection of his voice after he talked on the phone or the microphone whereas the callee does not notice the echo. Echo is the term of the reflections of the sent voice signals by the far end. Echo could be electrical echo which exists in PSTN networks or acoustic echo which is an issue in VoIP networks [6].

- Throughput

This parameter concerns about the maximum number of bits received out of the total number of bits sent during an interval of time.

III. CONFIGURATIONS OF VOIP

Dedicated routers

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

Adapters (USB)

These 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 softphones 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.

Dedicated VoIP phones

A VoIP phone looks like an ordinary corded or cordless telephone, but it connects directly to a computer network rather than a traditional phone line. A dedicated VoIP phone may consist of a phone and base station that connects to the internet or it may also operate on a local wireless network. Like the VoIP adapters mentioned above, dedicated VoIP phones also require a provider and service plan.

a. VoIP attacks

VoIP attacks can be divided into two categories: SIP attacks and RTP attacks. Since SIP takes significant roles of session initiation, connection and termination, we need to consider SIP attacks first.

Malformed Message Attack

This is one of the most representative case using the vulnerabilities of text-based protocol. Attackers are able to cause malfunctions of proxy server or UA by manipulating SIP headers. For instance, overflow-space, overflow-null, specific header deletion and using non-ASCII code are involved in malformed message attacks.

SIP Flooding Attack

IP phones generate requests or responses to send to a specific UA, called by victim. As a result, a single UA is overwhelmed by receiving excessive SIP messages within a short duration of time, so that the UA cannot provide normal services. INVITE flooding is one of the most typical attacks. Basically, flooding attack is also the issue of IP layer. In case of INVITE flooding, however, it could be more annoying attack for the VoIP user because the one should see many call requests and hear ringing.

Spoofing Attack

Two kinds of spoofing attacks are possible, IP spoofing attack and URI spoofing attack. IP spoofing attack is to forge IP source addresses in order to pretend a trusted user and IP spoofing is the intrinsic security problem in TCP/IP protocol suites and it is not in the scope of our study on VoIP security. URI spoofing attack is a particular case in malformed message attacks. The attacker who hijacked SIP messages between two UAs forges their URI field, so the attacker can hide himself from tracebacks. If spoofed BYE requests (BYE DoS attack) are sent to a victim, the call will be terminated by the attacker.

b. Requirements, Availability and Service Limitations

When considering VoIP service, you should not assume that its features, functionality and options will equal those of traditional landlines; you should be familiar with the requirements, availability and possible service limitations of VoIP service before switching to VoIP as either a primary means of communication or an enhancement to your current services.

Requirements

VoIP requires a connection to the Internet through an ISP, a VoIP service to extend the reach to traditional landlines, and VoIP software to actually place calls. Plain Old Telephone Service (POTS) requires none of these prerequisites. It is important to note that Digital Subscriber Line (DSL) internet service uses traditional phone lines for your internet connection. In this case, you already have telephone service to begin with. You may wish to weigh the expected benefits of VoIP against these costs given your current operating environment.

Availability due to power outages

During a typical power outage, VoIP becomes unavailable because VoIP devices (computers, routers, adapters) usually rely on a power source to function. Traditional phone lines are usually still available during such an outage, which is a major advantage in an emergency.

Availability due to bandwidth

VoIP communication nearly always requires a high-speed (broadband) internet connection for reliable functionality. Even given typical broadband connection speeds, though, service interruptions or degradation of quality is possible due to high internet traffic. For example, if you are trying to place a VoIP call while other people are using a lot of bandwidth on the same internet connection, the sound quality of your VoIP call or general VoIP availability may be affected.

c. 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.

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.

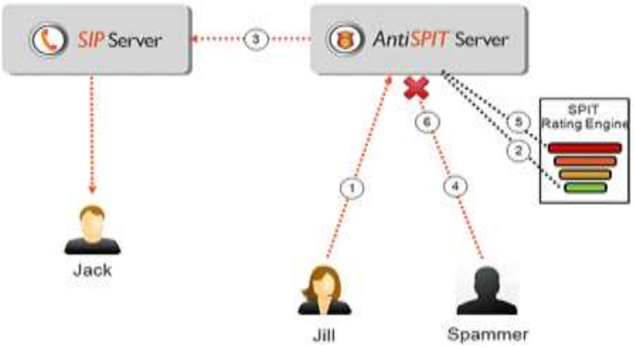


Figure 8: SIP & SPIT server [16]

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.

Confidentiality concerns

The concern is that VoIP data sometimes travels unencrypted over the internet. Therefore, it is technically possible for someone to collect VoIP data and attempt to reconstruct a conversation. Although it is extremely difficult to achieve, some software programs are designed to piece together bits and pieces of VoIP data in an effort to reconstruct conversations. While such activity is currently rare, you should be aware of this possibility as it may increase as VoIP becomes more widespread.

d. How to Protect Against Risks

The "Voice VLAN" is a special access port feature of Ethernet Switches which allows IP Phones to auto-configure and easily associate to a logically separate VLAN. This feature provided various benefits, but one particular benefit is when the Voice VLAN is enabled on a switch port that is also enabled to allow simultaneous access for a regular PC. This feature allows a PC to be daisy chained to an IP Phone and the connection for both PC and Phone to be trunked through the same physical Ethernet cable.

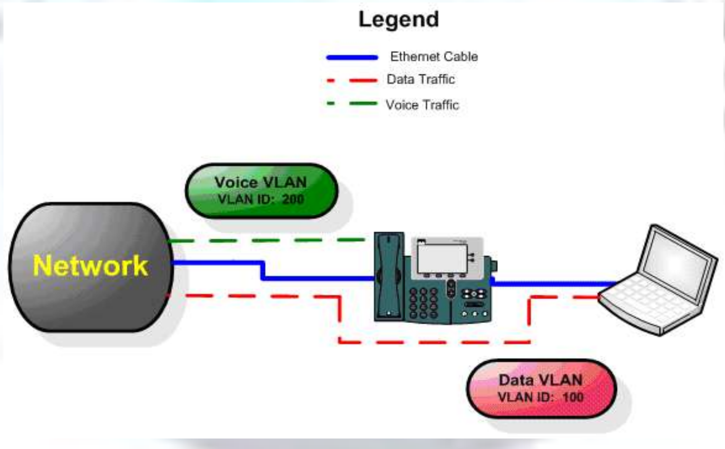


Figure 9: A typical VoIP scenario in which data and voice traffic is transmitted through the same cable [17]

Enabling Voice VLANs raises the complexity to properly secure these physical Ethernet ports. Enabling without the proper security controls in place can increase the risk to an organization.
Many of the principles and practices for safe VoIP usage are the same as those you may already be practicing with other internet applications. Here are some of the key practices of good personal computing:

- Use and maintain anti-virus and anti-spyware programs.
- Be cautious about opening files attached to email messages or instant messages.
- Verify the authenticity and security of downloaded files and new software.
- Configure your web browser(s) securely.
- Use a firewall.
- Identify, back-up, and secure your personal or financial data.
- Create and use strong passwords.
- Patch and update your application software.
- Do not disclose personal information to people you don't know.

IV. CONCLUSION

Security for a VoIP system should begin with solid security on the internal network. It should be protected from the threats of attached hostile networks and the threats of the internal network. The security policy should include any specific VoIP needs. The load of the VoIP system should be accommodated by the network and the servers involved, ensuring that proper resources are in place and available. Conducting a risk analysis of each component and process will identify the vulnerabilities and threats. This will provide the information needed to determine proper measures. Striking a balance between security and the business needs of the organization is key to the success of the VoIP deployment.

REFERENCES

[1]. Comparative Analysis of Traditional Telephone and Voice-over-Internet Protocol (VoIP) Systems Hui Min Chong and H. Scott Matthews* Department of Civil and Environmental Engineering Carnegie Mellon University Pittsburgh, PA USA.

[2]. 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.

[3]. A Survey on Voice over IP over Wireless LANs Haniyeh Kazemitabar, Sameha Ahmed, Kashif Nisar, Abas B Said, Halabi B Hasbullah World Academy of Science, Engineering and Technology 2010.

[4]. 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.

[5]. 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.

[6]. L. Mintandjian, P.A. Naylor, "A Study Of Echo In Voip Systems And Synchronous Convergence Of The µ-Law Pnlms Algorithm", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006.

[7]. J. B. Meisel, M. Needles, Voice over Internet protocol (VoIP) development and public policy implications, Info 7, 2005.

[8]. A comparison of sip and h.323 for internet telephony henning schulzrinne department of computer science, columbia university new York.

[9]. A comprehensive survey on a promising technology Stylianos Karapantazis, Fotini-Niovi Pavlidou Department of Electrical and Computer Engineering, Aristotle University of Thessaloniki, Panepistimioupoli, 54124 Thessaloniki, Greece.

[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.19, No 4, pp. 491-508, May 2006.

[11]. 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. 11, No. 5, Oct. 2003.

[12]. Russel, T., "Session Initiation Protocol (sip) Controlling Convergent Networks" McGrawHill Professional, 2008.

[13]. Seedorf, J., "SIP Security: Status Quo and Future Issues", Talk presented at 23rd Chaos Communication Congress, 2006.

[14]. Qiu, P.Q., Monkewich, O., and Probert, R.L., (2004), "SIP Vulnerabilities Testing in Session Establishment and User Registration" ICETE (2), 223-229

[15]. Advisory Committee on International Communications and Information Policy (ACICIP) (2005). http://www.isoc.org/pubpolpillar/voip-paper.shtml 15.08.2006.

[16]. http://www.eyeball.com/spit-solution.htm

[17]. http://www.symantec.com/connect/articles/voip-hopping-method-testing-voip-security-or-voice-vlans.