Security Principles in Voice over IP (VoIP)

Dr. Bashar M. Nema

Mustansiryah University-College of Science- CS Department

Abstract:

Took the research related to the use and development of speech and voice conversations that occur across the international network occupy the attention of researchers during the recent what this field is of great importance compared to fields that are interested correspondence voice of pressure or other methods. Considered all the systems that are used for the purpose of voice chat systems are important, so for frequent use at the present time. The enormous development and technological progress in the field of information security audio make these systems spread widely and become commonly used.

In the proposed research, will be addressed to all the concepts and key elements of the systems, voice conversations. Also will be recognized by all the information and security secrets to the most prevalent of these systems. A set of comparisons as well as the results have been reached, then search addresses the major components that make up the basis of the VoIP, finally will recognize some current commercial operating systems and scale differentiation between the system and another.

K E Y W O R D S: - Voice, IP, Speech, Skype, Threats, Gateway.

المستخلص

مبادئ الأمان في نقل الصوت عبر الإنترنت (VoIP)

اخذت البحوث المتعلقة باستخدام وتطوير المحادثات الصوتية التي تحدث عبر الشبكة الدولية تستأثر باهتمام الباحثين خلال الآونة الأخيرة لما لهذا الحقل من اهمية كبيرة قياسا بالحقول التي تهتم بالتراسل الصوتي من اساليب الضغط او غيرها. تعتبر جميع الأنظمة التي تستخدم لغرض المحادثة الصوتية انظمة مهمة ، وذلك لكثرة استخدامها في الوقت الحاضر. التطور الهائل والتقدم التكنولوجي في مجال امن المعلومات الصوتية، جعل من هذه الأنظمة تنتشر بكثرة وتصبح شائعة الأستخدام.

في البحث المقترح ، سوف يتم التطرق الى جميع المفاهيم والعناصر الرئيسية لأنظمة المحادثات الصوتية. كذلك سوف يتم التعرف على جميع المعلومات والأسرار الأمنية لأكثر هذه الأنظمة انتشارا. مجموعة من المقارنات وكذلك النتائج تم التوصل اليها، ثم يتطرق البحث الى المكونات الرئيسية التي تشكل اساس ال VoIP ، اخيرا سوف نتعرف على بعض الانظمة التجارية الحالية العاملة ومقياس التفاضل بين نظام واخر..

1-Introduction:

Since the dawn of history, humans have tried to communicate with each other. Using different methods. As the language has evolved to become more advanced forms of communication using the letters of the alphabet in various messages written on the leaves or messages. Technological development and got thanks to the emergence of computer tools, has become the method of communication and conversation take different styles using software packages operate according to the concepts of information security and networking. [1]

VoIP conversations, as forms of communication have advanced there have been subsequent efforts to keep those communications secret by one party, and to identify the clear message by a second party. [3]

2-The Internet Protocol (IP):

Delivering speech information in packets has some advantages to the classical telephone system .When you make a 'normal' telephone call; a path is set up between you and the destination of the call. You will then have a fixed amount of bandwidth you can use during the whole call. [2]

To understand the principles of VoIP, it is necessary to explain the role of IP in VoIP. IP prefix stands for Internet Protocol. Internet Protocol is the share of the layered structure in the standard, called the reference model TCP/IP. This model consists of four layers, each of which contains a number of functions, all of which layer above can be used. Internet layer is the one, all which olefins IP. This layer makes it possible to send data blocks called ended datagram from source to destination. They do so by sending a datagram across all network activity and intermediates. Neighboring networks are linked through devices called routers finished, all that examines incoming IP datagram and forward to the correct network. Supports IP multicasting, a technique to send the package in an effective way for any number of destinations. [1,8]

The main advantage of VoIP can be summarized in the following points: **[1,5]**

1. **Using VoIP, that silent interval can be detected .The VoIP application can examine each packet and detect whether it contains speech information or only silence. If the latter is case, the packet can simply be discarded.**
2. **The possibility of compression .With the compression methods available today, it is possible to reduce the requirement of 64 kbps for uncompressed telephone quality voice communication to amounts ,which are for lower .**
3. **However, a high compression ratio often means that the voice signal will be of lesser quality. We will go deeper into the domain of compression in one of the next chapters.**
4. **Pocketsize voice has certain advantage to the classical telephone system.**

5. **IP is not the only packet –based protocol.**
6. **It has only limited QoS support.**
7. **The TCP/IP architecture has proved to be very popular and nowadays it is very widely used. This fact gives IP a great advantage over other protocols.**

3-Security in PSTN and VoIP: [4]

The public switched telephone network (PSTN) is a global system of interconnected, various sized phone networks that provides users the ability to carry voice conversations with each other.

A security breach in either the data sector or voice segment compromises the whole network, especially since PC-based phones straddle both services.

The more familiar possible attacks in VoIP can be as follow:

- **Man in the Middle (eavesdropping and altering)**
- **Denial of Service (DoS)**
- **Compromise of Gateways**
- **Compromise of Endpoints**

4-Voice over IP (VoIP):

Before discuss Voice over IP (VOIP) related topics, it is probably best to give a brief explanation of what it is. This way, the essence of what is discussed here will be clear throughout the document and the details can be worked out at the appropriate time. Voice over IP comes down to trying to transport speech signals in an acceptable way form sender to destination over an IP network Figure (1). [6]

The definition of 'acceptable' depends on the particular situation we are dealing with. If, for example, speech signals are being transported as part of a real-time communication between two persons, it will mean that the real-time aspects of this conversation must be respected: the overall delay between sending and receiving should be low to avoid irritably long gaps of on-line radio show or a lecture –the delay constraints are less strict since the interactive aspect is no longer preset. There is a various proprietary and open-source, paid and free VoIP software clients available for use. These are also called soft phones. A few examples of these are: [4, 7]

(1) Skype.
(2) Google talk.
(3) Yahoo Messenger.
(4) ooVoo.
(5) Nimbuz.
(6) Viber

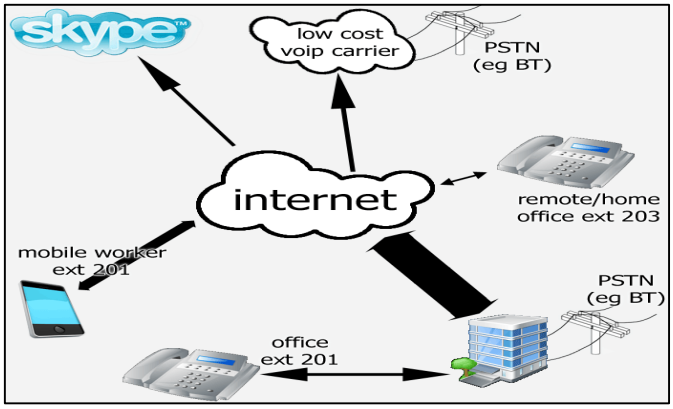

Figure (1): VoIP diagram.

4.1. Uses of Voice over IP: [9]

Currently, when you look what literature can found about VOIP, you will find that most of it is about VOIP as a telephone alternative. This type of use is described first in the section, followed by a discussion about using VOIP in virtual environments.

4.1.1: Telephone Alternative:

The first kind of use is the 'telephone alternative'. This mean that you would use some kind of VoIP system to make a voice call to another person .This can be done in several ways:

- **PC that can be connected to some kind of network is available; it can be used to make a call to somebody else that is also connected to that network. The PC could have a direct connection to a computer network, like in Figure (2). [10]**
- **Telephone is connected to the PC and used in a similar way as you would when making a normal call. The PC does all the necessary work to set up the call and to transmit the speech signal. The connection to the network can be either direct, like in Figure (3), or though a dial-up link. [10]**

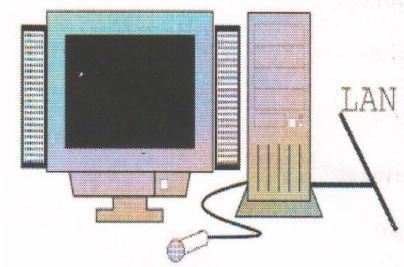

Figure (2): PC to LAN Configuration

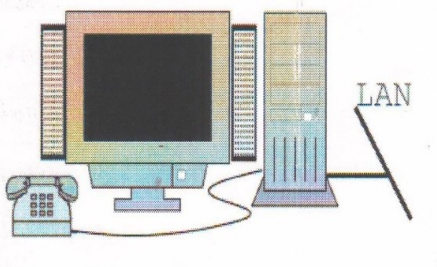

Figure (3): Telephone to PC Configuration

- **VoIP gateway: This is a special device that connects the public telephone network with a computer network. To make a call somebody; you would call the gateway and specify the destination for the call. The call will then be set up and if the other end is available, the conversation can start. This**

configuration would be best for persons who do not have a PC. This configuration is illustrated in Figure (4). [11]

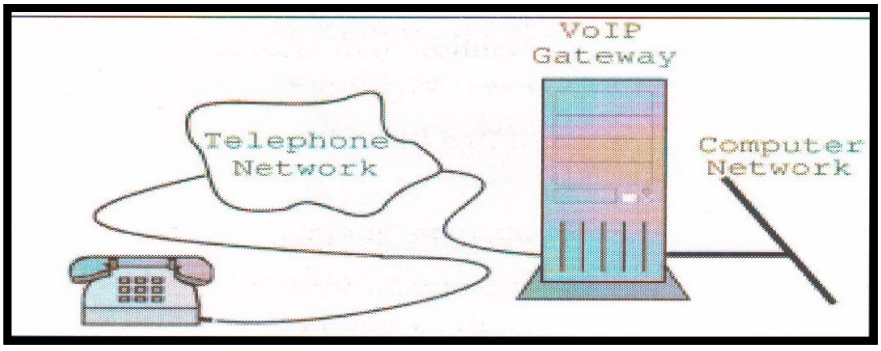

Figure (4): VoIP via Gateway configuration.

4.1.2: Benefits of using VoIP:

In this paragraph, there are many reasons for using VoIP as a telephone alternative while the telephone itself is quite handy? Well, there are several arguments that can be made in favor of VOIP. Suppose that somewhere. [10, 12]

- ***There is less cabling and equipment required.***
- ***Capacity of the computer network will be better utilized.***
- ***The available bandwidth of a network within an organization is usually quite large and rarely fully used.***
- ***By using VoIP, more of the network's capacity will be used.***
- ***If Voice over IP could be used over a large distance, it would be much cheaper than making that same long distance all using the telephone network.***
- ***With VoIP, not only the normal telephone features can be made possible, but also a wide range of new features could be created, especially when using VoIP on a PC:***

  (1) white boarding could be used to make working together easier,
  (2) a log book with information about incoming and outgoing calls could be kept,
  (3) conversations could easily by recorded and ,
  (4) Security could be enhanced by using encryption algorithms.

4.1.3. VoIP in Virtual Environment:

The use of VoIP for virtual environments can be seen as a replacement of the textual interface of chat facilities like Internet Relay Chat (IRC).the virtual environment can be made quite abstract by using the same kind of interface as IRC chat programs, but using voice input instead of text. [7]

Because we are dealing with a virtual environment, several signals can be expected to go to several destinations, all the same time. This means that considerable attention

should be paid to limiting the required bandwidth. This is especially true when people can access the virtual environment through a dial-up link which has a very small capacity compared to LAN for example, Figure (5).

Figure (5): VoIP via Virtual configuration.

The importance of VoIP software packages and the rapid development of such software, as well as the reasons that I mentioned earlier. With the emergence of devices iPhone and iPad has become a process of communication across thus Systems process easy and simple. The following figure shows the rapid growth and the ratio of the number of users. [12]

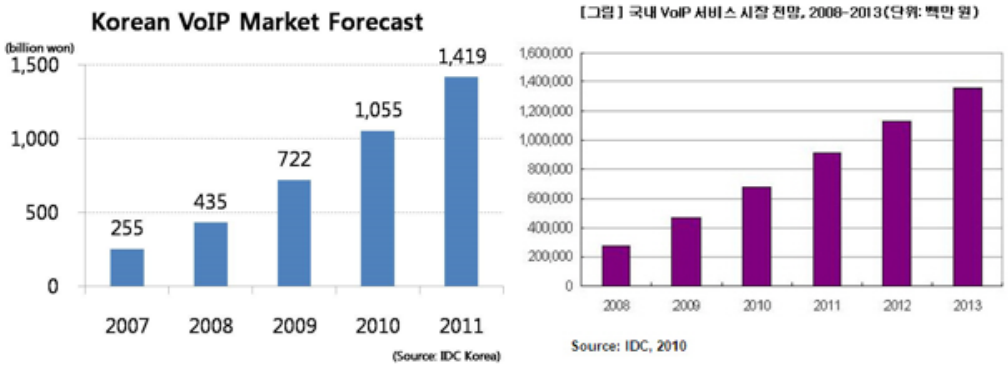

Figure (6): Indicators of growth and development of VoIP. **[13]**

4.2 Components of A VoIP System:

The core components of a VoIP for virtual environment will be illustrated. With core components, I mean the parts of the VIOP system that are at work *during the conversation*, so when the VoIP connection has already been establish. The entire process of the core VoIP system for virtual environments is depicted in Figure (7). The arrows that point downward define the path, which is followed when *sending speech signals*; the arrows that point upward define the processing sequence when speech signals are received. when the label of a box contains two items , the left one is about the sending of speech signals and the reception of such signals .they are grouped together because they operate at the same level : the right item does approximately the opposite of the left one . [12]

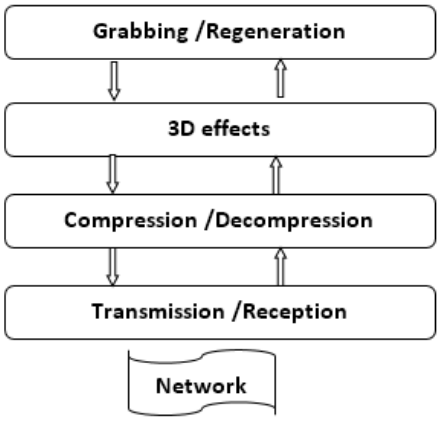

Figure (7): Components of VoIP system. [12]

5. Security of VoIP:

In this paragraph, we will explain all the concepts that belong to the security of information that must be on all users of the VoIP systems can recognize them and are significantly attention. In our proposal we will take care of those concepts statement, and we are trying to focus through this paragraph on a set of points that we set in order to reach the expected results and drawn from the proposed research. [13]

The security of VoIP resources, as with other data resources on networks, is dependent partly upon an organization's existing network infrastructure to maintain its security strength. This is in reference to building security, router, firewall, host, and OS security, password policies, etc.

The methods of securing VoIP phones and VoIP IP PBXs/call management servers, in some respects are not much different then securing data networks. The physical gear must be restricted to access by only authorized users. Just as with securing confidential data, rigorous access controls must be in place to specifically permit certain users and phones from making calls, what services are permitted, etc. and deny all others. Also VoIP phones and servers should have the latest patches and/or firmware updates available, and they should be delivered/installed via a sound patch management policy. However firewalls or VoIP network edge devices must be VoIP protocol aware.

5.1: VoIP Threats Categories:

Similar to the Confidentiality, Integrity, and Availability (CIA) of voice, the following is a clever way of remembering VoIP threat categories:

Table (1): VoIP threats categories.

Inx.	Threat Type	Example
1	Confidentiality	▪ Call eavesdropping. ▪ Voicemail tampering ▪ Call recording.
2	Availability	▪ Denial of Service (DoS). ▪ Buffers overflow attack. ▪ Worms and Viruses.
3	Authenticity	▪ Registration hijacking. ▪ Caller ID spoofing. ▪ Sound insertion.
4	Latency	▪ Service theft. ▪ Data theft.
5	SPIT (Voice spam)	▪ Unsolicited calling. ▪ Voice mailbox stuffing. ▪ Voice Phishing.

The following points must be considered(from our viewpoint as a researcher):

- **Segment their data and VoIP traffic into separate Virtual Local Area Networks (VLANs).**
- **If VoIP traffic is seen sourcing from a 'data only' network, the host producing the VoIP traffic should be investigated to identify what is causing,**
- **A stateful firewall should be used to block all outbound traffic for known destination VoIP service ports.**
- **Some vendors such as Cisco Systems include authentication and encryption measures in their proprietary VoIP deployments as a means of securing VoIP traffic to and from call manager servers, TFTP servers, and VoIP phones.**

5.2: Methods of attacking VoIP:

This can be illustrated breifly in the following points:

- **Denial of service attacks (DOS),**
- **man-in-the-middle attacks,**
- **call flooding,**
- **eavesdropping,**
- **VoIP fuzzing,**
- **signaling and audio manipulation,**
- **voice SPAM (called 'SPIT'), and voice phishing attacks.**

6. Skype system: [12]

Skype is a softphone, which means its a software VoIP application phone that runs on a PC. Skype, along with other softphones, require either a headset or a microphone with speaks to have a successful conversation.

The definition of Skype is defined by UKERNA as aproprietary, peer-to-peer resource discovery , directory access ,and call signaling protocol . Skype is a worldwide phenomenon that offers a Voice over IP service based on a free-to-download voice client and a central register of all Skype users .

6.1: Key Components of the SKYPE Software:

A Skype client listens on particular ports for incoming calls maintains a table of other skype nodes called host cache uses wideband codecs maintains a buddy list encrypts messages end-to-end and determines if it is behind a firewwall. this section discusses these components and functionalities in detail.

1. **Ports: A Skype client (SC) opens a TCP and a UDP listening port at the port number configured in its connection dialog box.**
2. **Host Cache: The host cache (HC) is a list of super node IP address.**
3. **Codecs: the third unknown codec.**
4. **Buddy List: Skype stores its buddy information in the windows registration.**
5. **Encryption: the Skype uses AES (advanced encryption standard).**

6.2: Skype Conferencing:

We observe the skype conferencing features for a three -users conference for the three network setups discussed below. We use the term user and machine interchangeable .let us name the three users or machine as *A,B and C*. Machine A was a 2G_{HZ} Pentium 4 with 1 GB RAM while machine B ,and C were Pentium 3 1G_{HZ} with 512 MB RAM , and Pentium 2 512MHz with 256 MB RAM , respectively .

In the first setup , the three machine had a Public IP address . A call was established between A and B Then B decided to include C in the conference .from the ethereal dump ,we observed that B and C were sending their oice traffic over UDP to SC on machine A , which was acting as a mixer. It mixed its own packets with those of B and sent them to C over UDP and vice versa as Shawn in Figure (8). the size of the voice packet was 67 bytes ,which is the size of UDP packet .

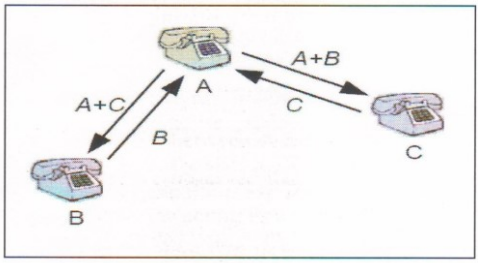

Figure (8): Skype three user's conferencing.

7. Conclusion:

As you can see, there is a wide variety of various VoIP technologies that are vulnerable to a multitude of different attacks. The Internet was not originally designed with security in mind and nor was the PSTN. Many other concluds as follow:

- **The classical use for VOIP is as a replacement for telephone call .**

- **using VIOP like this can reduce costs in various ways, but the quality of the conversation is usually lower than that of a normal telephone call .**
- **using VOIP virtual environment is relatively new .**
- **adding a 3D effect to the speech signal of a user help to create a more natural environment .**
- **many other applications use similar techniques as VIOP , for example the transmission of a video signal.**
- **Several components are require to make VIOP in virtual environment possible .**
- **the speech signal is split in tiny pieces , which are transmitted separately to be reconstructed into a continuous speech signal, which can then be sent to some speakers.**
- **Note that several signals may have to be mixed together if several persons are talking at the same time.**
- **to reduce the amount of required band width to transmit the signal , the digitized speech signal should be compressed. of course, at the other end it must be decompressed before it can be processed .**
- **Finally, there must also be a component, which handles the transmission and reception of packets containing speech data.**

References

1. Larry L. Peterson and Bruce S. Davie; "Computer Network, a Systems Approach", 3rd Ed.; 2003

2. Andrew S. Tanenbaum; "Computer Networks"; 4th Ed.;2003.

3. Stefan Brunner and Akola A. Ali,"Understanding VoIP Network", Juniper Network Inc. , USA, www.Juniper.net, Aug 2004.

4. Selman Arbalest and Henning Schuzrinne,"An Analysis of the Skype peer-to-peer Internet Telephony protocol", Department of Computer Science, Columbia University, 2004.

5. Packetizer-A ,"Resource for packet-switched conversational protocols "http:// www.packetizer Tamu-voip-qos-4.02.pdf ,2005.

6. International Telecommunication Union, http:// www.itu.int 2004.

7. Cisco Systems, http://www.cisco.com2006.

8. Endler, David , "Hacking exposed voIP:Voice over IP security secrets & solutions", New York, NY: McGraw-Hill, 2007.

9. Ramteke, T ,"Networks" Second edition. New Jersey: Prentice-Hall, Inc., 2001.

10. Thermos, Peter," Threats in VoIP", November 1, 2007, from Threats in VoIP Web site: http://www.enterpriseitplanet.com/security/features/article.php/3694056

11. Ramteke, T, (2006, February 19). "VoIP Phone/Gateway Default Password" November 7, 2007,

12. Skype, "Skype and firewalls". Retrieved December 1, 2007, from Skype and firewalls Web site: http://www.skype.com/help/guides/firewalls/technical.html

13. David Persky ,"VoIP Security Vulnerabilities", SANS Institute, Fall 2007.