I.J. Information Technology and Computer Science, **2014, 07, 65-76**
Published Online June 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2014.07.09

VoIP Technology: Investigation of QoS and Security Issues

Amor Lazzez
Taif University, Kingdom of Saudi Arabia
Email: a.lazzez@gmail.com

***Abstract*—**Voice over IP (VoIP) is the technology allowing voice traffic transmission as data packets over a private or a public IP network. VoIP allows significant benefits for customers and communication services providers. The main are cost savings, rich media service, phone and service portability and mobility, and the integration with other applications. Nevertheless, the deployment of the VoIP technology encounters many challenges such as architecture complexity, interoperability problems, QoS concerns, and security issues. Due to the inability of the IP networking technology to support the stringent QoS constraints of voice traffic, and the incapability of traditional security mechanisms to adequately protect VoIP systems from recent intelligent attacks, QoS and security issues are considered as the most serious challenges for successful deployment of the VoIP technology. The aim of this paper is to carry out a deep analysis of the security issues and QoS concerns of the VoIP technology. Firstly, we present a brief overview about the VoIP technology. Then, we discuss the QoS problems encountering the deployment of the VoIP technology. The presented discussion mainly address the QoS issues related to the use of the IP networking technology, the QoS concerns related to voice clarity, and the QoS mechanisms proposed to support voice traffic QoS constraints. After that, we investigate the security issues of the VoIP technology. The presented investigation mainly address the vulnerabilities and security attacks of VoIP systems, as well as the countermeasures that should be considered to help the deployment of secured VoIP systems.

***Index Terms*—**VoIP, Security Issues, QoS Concerns, Analysis

I. INTRODUCTION

Voice over IP (VoIP) [1-6] has been prevailing in the telecommunication world since its emergence in the late 90s, as a new technology transporting multimedia over the IP network. The reason for its prevalence is that, compared to legacy phone system, VoIP allows significant benefits such as cost savings, the provision of new media services, phone portability, and the integration with other applications [1, 2, 4, 5]. Despite these advantages, the VoIP technology suffers from many hurdles such as architecture complexity, interoperability issues, QoS concerns, and security issues [2, 7-9]. Due to the inability of the IP networking technology to support the stringent QoS constraints of voice traffic, and the incapability of traditional security mechanisms to adequately protect VoIP systems from recent intelligent attacks, QoS and security issues are considered as the most serious challenges for successful deployment of the VoIP technology [2, 4-6, 10].

Because of the nature of the IP networking technology, data packets sent via an IP network are subject to certain transmission problems such as packet delay, packet delay variation (jitter), packet loss [3-5, 11-12]. On the other hand, voice traffic is very sensitive to delayed packets, lost packets, and variable delay [4, 11, 13-14]. The effects of these problems manifest as choppy audio, missing sounds, echo, or unacceptably long pauses in the conversation that cause overlap, or one talker interrupting the other [11, 15]. To help an efficient deployment of the VoIP technology, QoS mechanisms making the IP technology able to support the stringent QoS constraints of voice traffic have been considered. In addition to the QoS concerns that are related to the use of the IP networking technology to transmit voice traffic, a number of concerns related to voice clarity should be considered to help the deployment of a successful VoIP system [11-13, 16]. The clarity of the audio signal is of highest importance. The listener must be able to recognize the identity and sense the mood of the speaker. Voice clarity can be affected by different factors including fidelity, echo, and side tone, and the background noise [11, 12].

In addition to the QoS concerns, the deployment of VoIP technology encounters serious security problems [2, 4-6, 10, 17-18]. Actually, VoIP technology is characterized by a set of vulnerabilities coming from VoIP applications as well as the infrastructure (network, operating system, etc.) are running on. The majority of components involved in the deployment of VoIP service have vulnerable elements that affect it directly or indirectly. The main vulnerable components in a VoIP system are the operating system of the VoIP application, the VoIP application itself, the VoIP protocols, the management interface, and the network devices (switch, router). These vulnerabilities can be exploited to carry out different kinds of security attacks including attacks against availability, attacks against confidentiality, and attacks against integrity. To prevent these attacks, and hence help the deployment of secured VoIP systems, VoIP protocols define specific security mechanisms as part of the protocols, or recommend combined solution with other security protocols [10, 17]. In addition to the security capabilities of the VoIP protocols, specific security devices have been designed to enhance the security of VoIP systems. Examples of those devices are VoIP-aware firewall, NAT, and SBC (Session Border Controller) [10, 17].

The remaining of this paper is organized as follows. Section 2 presents an overview about VoIP technology. First, we present the VoIP architectures. Then, we highlight the benefits leading to the ever-growing of the VoIP popularity. Next, we present a brief overview about the main VoIP protocols. Finally, we investigate the main disadvantages of the VoIP technology. Section 3 discusses the QoS problems encountering the deployment of the VoIP technology. First, we present the QoS requirements of voice traffic. Then, we highlight the QoS problems that may arise on IP networks, and we present the considered QoS mechanisms to make the IP technology able to support voice traffic QoS needs. After that, we discuss the QoS concerns related to voice clarity including fidelity, echo, side tone, and background noise. Section 4 addresses the security issues of the VoIP technology. First, we analyze the VoIP vulnerabilities, meaning the flaws that may be exploited by an attacker to perform a security attacks. Then, we present an overview about the VoIP security attacks. After that, we address the countermeasures that have been considered to help the deployment of secured VoIP systems. We start by the security capabilities of the main VoIP protocols. Then, we present the main VoIP security devices and we show their security potentials. Section 5 concludes the paper.

II. Basics of VoIP Technology

VoIP is a rapidly growing technology that delivers voice communications over Internet or a private IP network instead of the traditional telephone lines [1, 2, 4, 5]. VoIP involves sending voice information in the form of discrete IP packets sent over Internet rather than an analog signal sent throughout the traditional telephone network. VoIP helps the provision of significant benefits for users, companies, and service providers. Cost savings, the provision of new communication services, phone and service portability, mobility, and the integration with other applications are examples of the VoIP benefits. Yet, the deployment of the VoIP technology encounters many difficulties such as architecture complexity, interoperability issues, QoS issues, and security concerns. One of the main features of the VoIP technology is that it may be deployed using a centralized or a distributed architecture [1, 2, 4, 5, 9, 19-22]. Even though they are currently widely used, client-server VoIP systems suffer from many hurdles. In order to overcome the shortcomings of the client-server model, the development community starts tending towards the deployment of the VoIP service using a peer-to-peer decentralized architecture [19-22].

In the following subsections, we first we highlight the benefits of the VoIP technology leading to the ever-increasing of its popularity. Then, we present the main architectures used in the deployment of the VoIP technology. After that, we present a brief overview the most important VoIP protocols. Finally, we mention the main concerns of the VoIP technology.

2.1 VoIP Benefits

The key benefits of the VoIP technology are as follows [1, 2, 4, 5, 9]:

Cost savings: The most attractive feature of VoIP is its cost-saving potential. Actually, for users, VoIP makes long-distance phone calls inexpensive. For companies, VoIP reduces cost for equipment, lines, manpower, and maintenance. For service providers, VoIP allows the use of the same communication infrastructure for the provision of different services which reduces the cost of services deployment.

Provision of new communication services: In addition to the basic communications services (phone, fax), the VoIP technology allows users to check out friends' presence (such as online, offline, busy), send instant messages, make voice or video calls, and transfer images, and so on.

Phone portability: VoIP provides number mobility; the phone device can use the same number virtually everywhere as long as it has proper IP connectivity. Many businesspeople today bring their IP phones or soft-phones when traveling, and use the same numbers everywhere.

Service mobility: Wherever the user (phone) goes, the same services will be available, such as call features, voicemail access, call logs, security features, service policy, and so on.

Integration and collaboration with other applications: VoIP allows the integration and collaboration with other applications such as email, web browser, instant messenger, social-networking applications, and so on.

2.2 VoIP Architecture

One of the main features of the VoIP technology is that it may be deployed using a centralized or a distributed architecture [1, 2, 4, 5, 9, 19-22]. The majority of current VoIP systems are deployed using a client-server centralized architecture. A client-server VoIP system relies on the use of a set of interconnected central servers known as gatekeepers, proxy servers, or soft-switches. The central servers are responsible for users' registration as well as the establishment of VoIP sessions between registered users. Figure 1 shows an example of a VoIP system deployed using the client-server architecture. As it is illustrated in the figure, each central server handles (registers, establishes a session with a local or a distant user, etc.) a set of users. Each user must be registered on one of the central servers (registrar server) to be able to exchange data with other registered users. A user gets access to the service only over the registrar server.

Even though they are currently widely used, client-server VoIP systems suffer from the following many hurdles. The main issues of the client-server VoIP systems are the presence of single points of failure (central servers), scalability, availability, and security [2, 9]. In order to overcome the shortcomings of the client-server model, and help the development of scalable and reliable VoIP systems, the development communities start tending towards the deployment of the VoIP service using a peer-to-peer decentralized architecture. Actually,

a peer-to-peer VoIP system [9, 19-22] allows service provision through the establishment of a symmetric collaboration between the system nodes (peers) communicating according to a given logic architecture (overlay). This helps the deployment of scalable, cost-effective, and more reliable systems VoIP systems.

2.3 VoIP Protocols

The deployment of any multimedia application such as VoIP, videoconference, or network gaming requires a signaling protocol to set up sessions between end points, and a media transport protocol to transmit the media streams [1, 2, 4, 5, 9].

In the following subsections, we present an overview about the main VoIP signaling protocols.

a. VoIP Media Transport Protocols

The majority of VoIP systems rely on the use of the Real-Time Transport Protocol (RTP) for data transmission during a VoIP session. Secure RTP (SRTP) has been recently proposed by the IETF as a secured version of the RTP protocol.

RTP Protocol: Defined in RFC 3550, RTP protocol defines a standardized packet format for delivering audio and video over IP networks [1, 2, 6]. RTP is used in conjunction with the RTP Control Protocol (RTCP). While RTP carries the media streams (audio and video), RTCP monitors transmission statistics and the provided QoS and aids synchronization of multiple streams.

SRTP Protocol: SRTP protocol defines a security profile of RTP, intended to provide the authentication, the confidentiality, and the integrity of RTP messages [1, 2, 6]. Since RTP is used in conjunction with RTCP, SRTP is closely related to SRTCP (Secure RTCP) which is used to control the SRTP session.

b. VoIP Signaling protocols

Given that the majority of current VoIP systems are deployed using a client-server centralized architecture, in the subsequent, we only consider the main signaling protocols used for the deployment of client-server VoIP systems; H323, SIP, and IAX.

H323: Standardized by the International Telecommunication Union (ITU), H323 [1, 2, 6] is the first signaling approach publicly used for the deployment of VoIP systems in conjunction with RTP protocol. H323 standard encompasses many protocols such as H225, H245, and H235. H.225 defines call setup messages and procedures used to establish a call, as well as messages and procedures used for users registration, and call admission. H.245 defines control messages and procedures used to exchange communication capabilities such as the supported codec. H235defines security profiles for H.323, such as authentication, message integrity, signature security, and voice encryption.

SIP: Allowing system flexibility and security, SIP is nowadays the most used VoIP signaling protocol [1, 6, 20, 21, 23]. SIP is an application layer protocol that works in conjunction with several other application layer protocols that identify and carry the session media. Media identification and negotiation is achieved with the Session Description Protocol (SDP). Media streams (voice, video) are transmitted using RTP protocol which may be secured by the SRTP protocol. For secure transmissions of SIP messages the Transport Layer Security (TLS) may be used. SIP also provides a suite of security services including DoS prevention, authentication, integrity, and confidentiality.

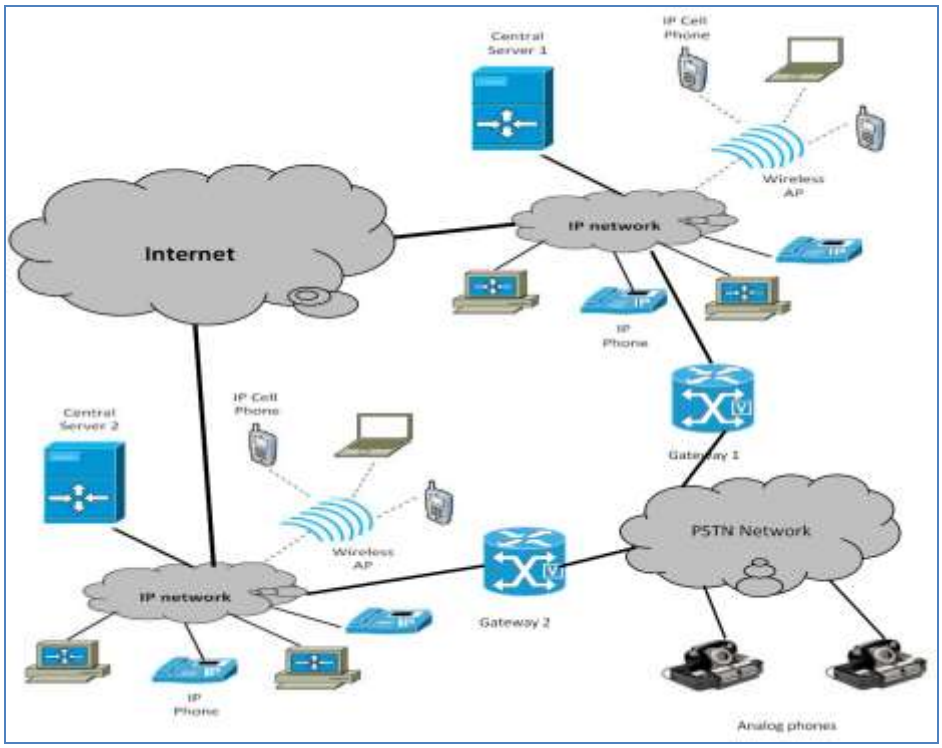

Fig. 1. Client-Server VoIP Architecture: An illustrative example

IAX: Currently, IAX (Inter-Asterisk Exchange) is one of the most used approaches for the deployment of VoIP systems [24-26]. In contrast with H323 and SIP protocols which are limited to signaling tasks, IAX protocol ensures both signaling and media transmission in an IAX-based VoIP system. IAX provides a suite of security services. Actually, it allows message authentication and confidentiality, and supports NAT traversal.

2.4 VoIP Disadvantages

Even though it allows significant benefits, the VoIP technology suffers from many hurdles [1, 2, 6, 11, 12, 18]. In the following a brief presentation of the main VoIP disadvantages.

Complicated service and network architecture: the integration of different services (voice, video, data, and so on) into the same network makes it difficult the design of the network architecture because different protocols and devices are involved for each service, and various characteristics are considered for each media. It also causes various errors and makes it harder to troubleshoot and isolate them.

Interoperability issues between different applications, or products: Different protocols (H323, SIP, IAX, and MGCP) have been proposed for the deployment of VoIP systems. This leads to an interoperability issues between the VoIP devices developed based on different protocols. Interoperability issues still come up between products using the same protocol due to the multitude of protocol versions, and the ways of implementation.

Quality of service (QoS) issues: The QoS aspect was not much considered when the IP technology was designed. That is why, the IP technology remains inefficient to support traffic with different QoS constraints despite the development of different approaches (DiffServ, IntServ) for enhancement of the QoS provided by an IP network.

Security issues: In the legacy phone system (PSTN: Public Switched Telephone Network), the main security issue is the interception of conversations that require physical access to phone lines. In VoIP security issues are much more than that. Actually, in VoIP systems many elements (IP phones, access devices, media gateways, proxy servers, and protocols) are involved in setting up a call and transferring media between two endpoints. Each element has vulnerable factors that may be exploited by attackers to carry out security attacks.

Due to the inability of the IP networking technology to support the stringent QoS constraints of voice traffic, and the incapability of traditional security mechanisms to adequately protect VoIP systems from recent intelligent attacks, QoS and security issues are considered as the most serious challenges for successful deployment of the VoIP technology.

III. VoIP QoS Issues

The deployment of VoIP technology encounters serious QoS problems related to the use of the IP networking technology for voice traffic transmission. Actually, because of the nature of the IP technology, data packets sent via an IP network are subject to certain transmission problems such as packet delay, jitter, and packet loss [3-5, 7, 11, 12]. On the other hand, voice traffic is very sensitive to delayed packets, lost packets, and variable delay. The effects of these problems manifest as choppy audio, missing sounds, echo, or unacceptably long pauses in the conversation that cause overlap, or one talker interrupting the other [3-5, 11-13, 15-16]. To help an efficient deployment of the VoIP technology, QoS mechanisms making the IP technology able to support the stringent QoS constraints of voice traffic have been considered.

In addition to the QoS concerns that are related to the use of the IP networking technology to transmit voice traffic, a number of concerns related to voice clarity should be considered to help the deployment of a successful VoIP system [11-13, 16]. The clarity of the audio signal is of highest importance. The listener must be able to recognize the identity and sense the mood of the speaker. Voice clarity can be affected by different factors including fidelity, echo, and side tone, and the background noise [7, 11-12].

In the following subsections, we first present the QoS problems that may arise on IP networks, and present the considered QoS mechanisms to make the IP technology able to support voice traffic QoS needs. Then, we present the QoS concerns related to voice clarity including fidelity, echo, side tone, and background noise.

3.1 VoIP QoS Concerns

The main issues that should be addressed by the QoS aspect to adequately transport voice traffic over an IP network are the following: bandwidth, network delay, delay variation, and traffic loss [3-5, 7]. In the following, we describe the main VoIP QoS issues, and we show how they can be addressed to guarantee the required QoS for voice traffic.

a. Bandwidth

The bandwidth of a transmission media (optical fiber, coaxial cable, etc.) defines its data transmission capacity in bits/second. The bandwidth of a network path composed of different LAN and WAN links corresponds to the bandwidth of the slowest link on the path. The network link with the lowest bandwidth on a network path is often referred to as a bottleneck. Bottlenecks on a network cause congestion which results into QoS problems for voice traffic. Figure 2 presents an example of a network path between two VoIP terminals over an IP network. The figure shows the location where a bottleneck is most likely to occur on the considered path. The figure also illustrates the calculation of the path bandwidth which corresponds to the bandwidth of the IP WAN link; the slowest link on the considered path.

To adequately transport voice traffic over an IP network, and hence help the deployment of a successful VoIP system, congestion should be avoided. This can be achieved using several ways including the increase of the bandwidth, traffic prioritization, and traffic compression [3-5, 7, 11-16].

b. Link capacity increasing

The best way to increase bandwidth is to increase the link capacity to accommodate all applications and users, with some extra bandwidth. Even though this solution sounds simple, increasing link capacity is expensive and needs time to be implemented. Fortunately, various QoS mechanisms can be used to effectively increase available bandwidth for priority applications.

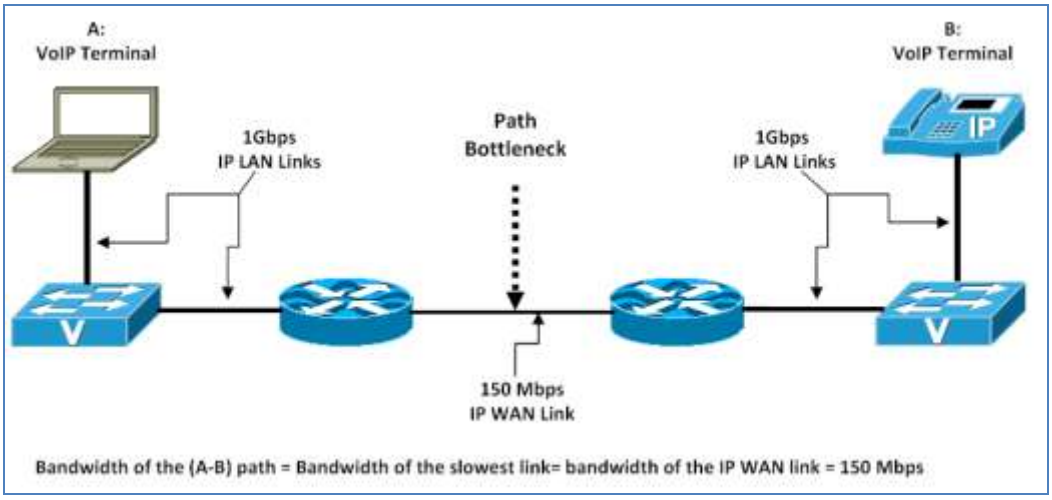

Fig. 2. Network Bottleneck

c. Delay-sensitive traffic prioritization

It consists to:

- Classify traffic into different classes according to their QoS constraints in terms of delay, jitter, and packet loss.
- Assign a priority level to each traffic class. The highest priority level is assigned to the traffic class or real-time applications including VoIP, and videoconference.
- Ensure priority-based traffic forwarding through the network. Assigned a high priority level, real-time applications such as VoIP can get sufficient bandwidth to support their QoS requirements; voice traffic will get prioritized forwarding; and the least-important traffic will get whatever unallocated bandwidth is remaining.

d. Traffic compression

Different techniques have been proposed for the compression of IP traffic so that it consumes less bandwidth. We mainly distinguish payload compression, and header compression.

- Payload compression: By compressing the payload of a packet, the total size is reduced. This compression method does not affect the headers, which makes it appropriate for links that require the header to be readable to route the packet correctly.
- Header compression: On point-to-point IP links where the header information is not needed to route the packet, header compression may be used.

Even though, it may increase the available bandwidth, Compression takes time and CPU resources, which may increase the end-to-end network delay.

e. Network Delay

Network delay is the amount of time it takes a packet to travel from a source to a destination through the network. Network delay, mainly includes the processing delay, the queuing delay, the serialization delay, and the propagation delay [11-12].

- Processing delay: The time it takes a router to take a packet from an input interface and put it into the output queue of the appropriate output interface. The processing delay mainly depends on the router architecture, and the router processing speed.
- Queuing delay: The time a packet resides in the output queue of a router. Due to bottlenecks, the queuing delay depends on the traffic load, the processing speed, the bandwidth of the output interface, and the queuing mechanism.
- Serialization delay: The time it takes to place a packet on the physical medium for transport.
- Propagation delay: The time it takes a signal to transit a media. It depends on the type of media, and the type of signal transporting the data.

Due to bottleneck conditions, improper queuing, or configuration errors, network delay may increase and hence leads to QoS issues especially for delay-sensitive applications such as VoIP. The ITU-T G.114 specification recommends that the end-to-end network delay should not exceed 150 ms [11].

Different strategies have been considered to minimize the network delay through an IP network to make the IP technology able to support real-times applications with stringent constraints in terms of delay. Network delay may be minimized using the same strategies used for the increasing the available bandwidth [3-5, 7, 11-16]:

f. Increase the transmission speed of the network links

It helps the reduction of the serialization and transmission delays, and hence the decreases of the overall network delay.

g. Increase the processing speed of the network nodes

It allows the decrease of the processing delay, which helps the reduction of the queuing delay, and thus the decrease of the end-to-end network delay.

h. Prioritize delay-sensitive traffic

This approach helps the reduction of the queuing delay for delay sensitive-traffic such as voice traffic, which helps the support of the stringent delay constraints of such applications.

i. Compress the transmitted traffic

As it is mentioned above, traffic compressions allows the reduction of the amount of data transmitted over the network, which reduces the network traffic load, and hence decreases the queuing and the serialization delays.

j. Delay variation

Jitter is defined as a variation in the arrival of received packets. On the sending side, packets are sent in a continuous stream with the packets spaced evenly. Due to bottleneck conditions, this steady stream can become uneven because the delay between each packet varies instead of remaining constant. Figure 3 illustrates the jitter QoS issue.

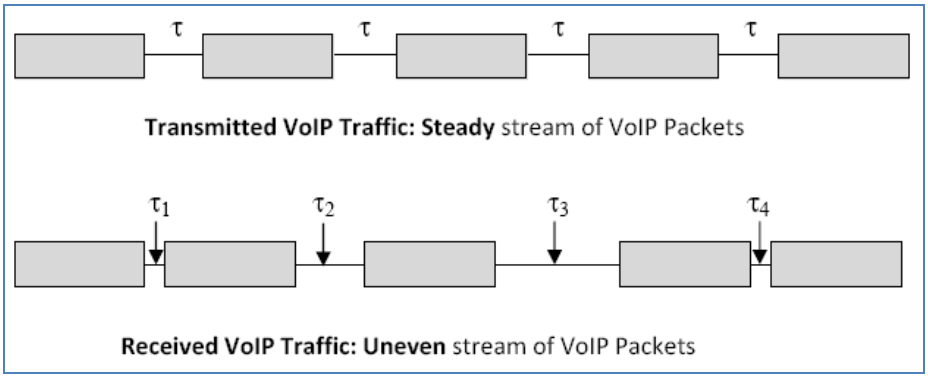

Fig. 3. Jitter Issue

This variation in the receiving of packets can cause the voice stream to skip and stutter, which can be very annoying to the listener. To adequately transport voice traffic over an IP network, the ITU-T G.114 specification recommends that the jitter should be reduced to 30 ms or less on average [11].

k. De-Jitter Buffering Mechanism

Given the annoying effects of Jitter, a QoS mechanism referred to as de-jitter or play out delay buffering has been considered [11-12]. Implemented at the input interface of the receiving end, the de-jitter buffering mechanism relies on the use of a specific buffer known as de-jitter buffer to slow down and properly space down the received packets before being played out in a steady stream like to the transmitted one. Even though, it helps the avoidance of the jitter effects, the de-jitter mechanism affects the overall network delay.

l. Traffic loss

The main reason for packet loss over an IP network is network congestion. Lost data packets may be recovered by retransmission. However, lost voice packets cannot be recovered by retransmission because voice traffic must be played out in real time. Therefore QoS mechanisms minimizing voice traffic loss should be considered. For an efficient deployment of the VoIP application, The ITU-T G.114 specification recommends that the overall total of packets lost for a voice call never exceed 1 percent [11].

Voice traffic loss may be minimized using the following strategies [3-5, 11-16]:

- Network congestion prevention,
- Voice traffic prioritization,
- Packet loss concealment.

In the following, we present a brief overview about these strategies.

m.Network congestion prevention

The following procedures can be used to prevent network congestion:

- **Increase of the network bandwidth:** this can be achieved through:
  - Increase of the transmission capacity of the network links,
  - Increase of the buffering capacity of the network routers
  - Increase of the processing speed of the network routers.
- **Decrease of the traffic load:** This can be achieved through:
  - Traffic compression: it makes the data that needs to be transmitted smaller which reduces the traffic load.
  - Delay-insensitive traffic shaping: It consists to delay delay-insensitive traffic and send it at a configured maximum rate. For example, if an FTP server is generating a 512 kbps stream, shaping could limit the generated traffic to 256 kbps, delaying the transmission of the excess traffic.
  - Call Admission Control: It consists to accept a new traffic on the network only if the needed transmission bandwidth is available [13, 16].
- **Traffic policing:** it consists to drop lower-priority packets in excess a configured threshold to prevent congestion. WRED (Weighted Random Early Detection) scheme can be used start dropping these lower-priority packets before congestion occurs.

n. Voice traffic prioritization

It consists to delay or drop low-priority data packets to guarantee the required bandwidth for the transmission of voice traffic.

o. Packet Loss Concealment

Despite the above presented mechanisms which aim to reduce voice traffic loss, we cannot avoid the loss of a voice packet. The loss of a voice packet causes voice clipping and skips. As a result, the listener hears gaps in the conversation. To assist with packet loss on voice calls, a specific mechanism, referred to as Packet Loss Concealment (PLC), has been proposed [7, 11-12]. The PLC mechanism intelligently analyzes missing packets and generates a reasonable replacement packet to improve the voice quality. Cisco VoIP technology uses 20-ms samples of voice payload per VoIP packet by default. Effective codec correction algorithms require that only a single packet can be lost at any given time. If more packets are lost, the listener experiences gaps

3.2 Voice Clarity Considerations

In addition to the QoS concerns that are related to the use of the IP networking technology to transmit voice traffic, a number of concerns related to voice clarity should be considered to help the deployment of a successful VoIP system [7, 11-13, 16].

The clarity (that is, the "cleanliness" and "crispness") of the audio signal is of highest importance. The listener must be able to recognize the identity and sense the mood of the speaker. Voice clarity can be affected by different factors including fidelity, echo, and side tone, and the background noise.

a. Fidelity

It is defined as the degree to which the voice transmission network accurately reproduces the transmitted voice signal. Fidelity depends on the sampling frequency band and the compression ratios. When audio is sampled using the frequency band [300-3400 Hz] (narrowband) and is then highly compressed, the audio is considered to be low fidelity. However, when it is sampled using the frequency band [50–7000 Hz] (wideband) and transported using lower compression ratio is called high fidelity.

The human voice covers the wide frequency band (50-7000 Hz). Voice sampling using the narrowband allows an acceptable QoS given that 90 percent of the most significant elements of the human voice are contained in the narrow band. Voice sampling using the wideband offers a clearer and fuller-sounding voice representation but at the cost of higher bandwidth requirements.

b. Echo

Echo is a result of electrical impedance mismatches in the transmission path. Echo is always present, even in traditional telephony networks, but at a level that cannot be detected by the human ear. The two components that affect echo are amplitude (loudness of the echo) and delay (the time between the spoken voice and the echoed sound). To reduce the annoying effects of the echo phenomenon, a specific system, referred to as echo canceller or suppressor has been considered for a more efficient deployment of the VoIP technology.

c. Side tone

Side tone refers to the fact that the telephone allows the speakers to hear their spoken audio in the telephone earpiece. Without side tone, the speaker is left with the impression that the telephone instrument is not working.

d. Background noise

It corresponds to the low-volume audio that is heard from the far-end connection to prevent the illusion that the call has been disconnected.

IV. VoIP Security Issues

In addition to the QoS concerns, the deployment of VoIP technology encounters serious security problems. VoIP security issues are becoming more serious because traditional security devices, protocols, and architectures cannot adequately protect VoIP systems from recent security attacks.

VoIP technology is characterized by a set of vulnerabilities coming from VoIP applications as well as the infrastructure (network, operating system, etc.) are running on. These vulnerabilities can be exploited to carry out different kinds of security attacks including attacks against availability, attacks against confidentiality, and attacks against integrity. To prevent these attacks, and hence help the deployment of secured VoIP systems, VoIP protocols define specific security mechanisms as part of the protocols, or recommend combined solution with other security protocols. In addition to the security capabilities of the VoIP protocols, specific security devices have been designed to enhance the security of VoIP systems [8, 10, 17-18]. Examples of those devices are VoIP-aware firewall, NAT, and SBC (Session Border Controller).

In the following subsections, we first present the main vulnerabilities of VoIP systems. Then, we present a brief overview about the VoIP security attacks. After that, we present the security capabilities of the main VoIP protocols. Finally, we present the main VoIP security devices and show the security potential of each device.

4.1 Vulnerabilities of VoIP systems

In system and network security, vulnerability is a flaw or a weakness that may be exploited by an attacker to carry out a security attack. VoIP has two types of vulnerability [8, 10, 17-18]. The first one is the inherited vulnerability which comes from the infrastructure (network, operating system, web server, and so on) used for the deployment of VoIP applications. The other is the vulnerability coming from VoIP protocols and devices, such as IP phone, voice gateway, media server, signaling controller, etc.

In the following, we present the sources of vulnerabilities as well as the vulnerable components in a VoIP system.

a. Sources of Vulnerabilities

IP-Based Network Infrastructure: As the name VoIP implies, all traffic flows over IP networks and inherits the vulnerability of IP networks, such as malicious IP fragmentation, network viruses, or worms.

Public Networks: In most cases, VoIP traffic is transmitted over Internet where anonymous people including hackers may send and receive traffic.

Open VoIP Protocol: Most VoIP protocols, such as SIP or H.323, are standardized and open to the public. Hence, an attacker can create malicious client or server program based on the protocol specification in order to get access to a target VoIP servers or clients. Moreover, the openness of a VoIP protocol helps malicious people to identify and take advantage of its vulnerabilities.

Voice and Data Integration: Even though it allows significant benefits, the integration of voice and regular data traffic in the same network results into new traffic engineering issues. Actually, the integration of traffic with different QoS and security requirements makes the traffic engineering tasks (securing, switching, queuing, and s on) more complex and difficult.

Lack of Specific Security Mechanisms: While many data security mechanisms like firewalls may enhance the security of VoIP systems, it is still not enough to protect VoIP systems from today's malignant attacks.

Real-Time Media Transfer: Unlike common communication services like email, VoIP service requires a real-time transfer of media traffic which involves hard QoS constraints in terms of packet delay, and packet delay variation (jitter). Hence, minor packet delay or jitter could be recognized by users and impact the overall QoS. An attacker may overload the VoIP network (Calla flooding for example) to affect the provided QoS, and thus the system reliability.

Exposed Interface: The majority of current VoIP systems are deployed using a client-server architecture. Even though, VoIP servers are located in a protected network, the interface modules receiving call requests are open to clients that are located in an open or public network. This allows attackers to perform a ports scan to find out the exposed interface modules, and then carry out a security attack (DoS for example) by sending malicious traffic.

Endpoints Mobility: The PSTN (Public Switched Telephone Network) phone system assigns a dedicated phone line to a certain number. Thus, an attacker requires physical access to spoof the identity (the telephone number or line) of a regular user of the PSTN phone system. Unlike PSTN technology, VoIP phone systems allow endpoints mobility, which makes the protection against identity spoofing harder.

b. Vulnerable Components

In the following of this subsection, we present subsequent, a brief overview of the main vulnerable components involved in the deployment of a regular VoIP system [8, 10, 17-18].

Operating system: VoIP applications are affected by the vulnerabilities of the operating systems are running on. The frequent security patches for the regular operating systems (Windows, Unix, Lunix) prove that they always have vulnerabilities.

VoIP application: A VoIP application (Skype, Google Talk, etc.) itself may have security issues because of bugs or errors, which could make VoIP service insecure.

VoIP protocols: The deployment of a VoIP application involves a signaling protocol (H323, SIP, IAX), and a media transmission protocol (RTP, RTCP). These protocols are vulnerable to different kinds of attacks which may affect the VoIP service provided based on these protocols.

Management interface: For management purposes, the majority of VoIP devices have different service interfaces such as SNMP, SSH, Telnet, and HTTP. A service interface may be a source of vulnerability, especially when being configured carelessly. For example, if a VoIP device uses the default ID/password for its management interface, it is easy for an attacker to break in.

TFTP Server: Many VoIP devices download their configurations from a TFTP server. An attacker could impersonate a TFTP server by spoofing the connection, and then distribute a malicious configuration to the VoIP equipment.

Access device (switch, router): All VoIP traffic flows through access devices (switch, router) that are in charge of switching or routing. Compromised access devices could create serious security issues because they have full control of packets.

Network: VoIP traffic is affected by the vulnerabilities of the IP network through which it is transmitted. An IP network vulnerability may be due to a bad configuration of a network device (switch, router, firewall, etc.) or a bug in one of the involved protocols (IP, UDP, and so on).

4.2 VoIP Security Attacks

The VoIP vulnerabilities presented in the previous section may be exploited by hackers to carry out different kinds of security attacks. Attackers may disrupt media service by flooding traffic, collect privacy information by intercepting call signaling or call content, hijack calls by impersonating servers or impersonating users, make fraudulent calls by spoofing identities, and so on.

There are many possible ways to categorize the security attacks. The first version of the IETF draft classified the security attacks into the following four categories: Interception and modification attacks, Interruption-of-service attacks, abuse-of-service attacks, and social attacks [18]. In [17], the authors consider the following categories of VoIP security attacks: service disruption and annoyance, eavesdropping and traffic analysis, masquerading and impersonation, unauthorized access, and fraud. In [1], the author classifies the security attacks into four categories as follows: attacks against availability, attacks against confidentiality, attacks against integrity, and attacks against social context.

In the following of this section, we present a brief overview about the main VoIP attacks according to the taxonomy presented in [10], which we adopt as it is the newest presented taxonomy compared to the other listed ones.

a. Attacks Against Availability

Attacks against availability aim at VoIP service interruption, typically in the form of Denial of Service (DoS). The main attacks against availability are: call flooding, malformed messages, spoofed messages, call hijacking, server impersonating, and Quality of Service (QoS) abuse. In the following, we present a brief overview of these attacks.

Call Flooding: an attacker floods valid or invalid heavy traffic (signals or media) to a target system (for example, VoIP server, client, and underlying infrastructure) which breaks down the system or drops its performance significantly.

Malformed Messages: An attacker may create and send malformed messages to the target server or client for the purpose of service interruption. A malformed message is a protocol message with wrong syntax. The server receiving this kind of unexpected message could be confused (fuzzed) and react in many different ways depending on the implementation. The typical impacts are as follows: infinite loop, buffer overflow, inability to process other normal messages, and system crash.

Spoofed Messages: An attacker may insert fake (spoofed) messages into a certain VoIP session to interrupt the service, or steal the session. The typical example is call teardown. For this example, the attacker creates and sends a call termination message (for example SIP Bye) to a communicating device to tear down a call session. This attack requires the stealing of session information (Call-ID) as a preliminary.

Call Hijacking: Hijacking occurs when some transactions between a VoIP endpoint and the network are taken over by an attacker. The transactions can be a registration, a call setup, a media flow, and so on. This hijacking can make serious service interruption by disabling legitimate users to use the VoIP service. It is similar to call teardown in terms of stealing session information as a preliminary, but the actual form of attack and impact are different. The typical examples are registration hijacking, and media session hijacking.

QoS Abuse: The elements of a media session are negotiated between VoIP endpoints during call setup time, such as media type, coder-decoder (codec) bit rate, and payload type. An attacker may intervene in this negotiation and abuse the Quality of Service (QoS), by replacing, deleting, or modifying codecs or payload type. Another method of QoS abuse is exhausting the limited bandwidth with a malicious tool so that legitimate users cannot use bandwidth for their service.

b. Attacks Against Confidentiality

Attacks against confidentiality provide an unauthorized means of capturing media, identities, patterns, and credentials that are used for subsequent unauthorized connections or other deceptive practices. The main types of confidentiality attacks are eavesdropping media, call pattern tracking, data mining, and reconstruction.

Media Eavesdropping: An unauthorized access to media packets. Two typical methods are used by attackers. One consists to compromise an access device (layer 2 switch for example) and duplicate the target media to an attacker's device. The other way is that an attacker taps the same path as the media itself, which is similar to legacy tapping technique on PSTN. For example, the attacker may get access to the T1 itself and physically splits the T1 into two signals.

Call Pattern Tracking: Call pattern tracking is the unauthorized analysis of VoIP traffic from or to any specific nodes or network so that an attacker may find a potential target device, access information (IP/port), protocol, or vulnerability of network. It could also be useful for traffic analysis; knowing who called who, and when.

Data Mining: The general meaning of data mining in VoIP is the unauthorized collection of identifiers that could be user name, phone number, password, URL, email address, strings or any other identifiers that represent phones, server nodes, parties, or organizations on the network. These information may be used by an attacker for subsequent unauthorized connections such as service interruptions, confidentiality attacks, spam calls, etc.

c. Attacks Against Integrity

Attack against integrity consists in the alteration of the exchanged traffic (signaling messages or media packets) after intercepting them in the middle of the network. The alteration can consist of deleting, injecting, or replacing certain information in the VoIP message or media. Call rerouting and black holing are typical examples of attacks against the integrity of the signaling traffic. Media injection and degrading are examples of media integrity attacks.

Call Rerouting: An unauthorized change of call direction by altering the routing information in the signaling message. The result of call rerouting is either to exclude legitimate entities or to include illegitimate entities in the path of call signal or media.

Media injection: An unauthorized method in which an attacker injects new media into an active media channel. The consequence of media injection is that the end user (victim) may hear advertisement, noise, or silence in the middle of conversation.

Media degrading: An unauthorized method in which an attacker manipulates media or media control packets relative to an established communication session in order to reduce the quality of data communication (QoS). For instance, an attacker intercepts RTCP packets in the middle, and changes the sequence number of the packets so that the endpoint device may play the media with wrong sequence, which degrades the quality.

d. Attacks Against Social Context

An attack against social context focuses on how to manipulate the social context between communicating entities so that an attacker can misrepresent himself as a trusted entity and convey false information to the target user (victim). The typical attacks against social context are misrepresentation of identity, authority, rights, and content, spam of call and presence, and phishing.

Misrepresentation: It corresponds to the intentional presentation of a false identity, authority, rights, or content as if it were true so that the target user (victim) or system may be deceived by the false information. Identity misrepresentation is the method of presenting an identity with false information, such as false caller name, organization, email address, or presence information. Authority or rights misrepresentation is the method of presenting false information to an authentication system to obtain the access permit, or bypassing an authentication system. Content misrepresentation is the

method of presenting false content as if it came from a trusted source of origin. It includes false impersonation of voice, video, text, or image of a caller.

Spam: Call spam is defined as a bulk unsolicited set of session initiation attempts (INVITE requests), attempting to establish a voice or video communications session. If the user should answer, the spammer proceeds to relay their message over real-time media. Presence spam is defined as a bulk unsolicited set of presence requests (for example, SIP SUBSCRIBE requests) in an attempt to get on the "buddy list" of a user to subsequently carry out a call spam (INVITE request).

Phishing: An illegal attempt to obtain somebody's personal information (for example, ID, password, bank account number, credit card information) by posing as a trust entity in the communication. The typical method is that an attacker picks target users and creates request messages (SIP INVITE for example) with spoofed identities, pretending to be a trusted party. When the target user accepts the call request, the phisher provides fake information (for example, bank policy announcement) and asks for personal information. Some information like user name and password may not be directly valuable to the phisher, but it may be used to access more information useful in identity theft.

4.3 Security Abilities of VoIP Protocols

To prevent the above presented attacks, and hence help the deployment of secured VoIP systems, VoIP protocols (SIP, H.323, IAX) define specific security mechanisms as part of the protocols, or recommend combined solution with other security protocols (IPSec, SRTP, etc.) [10, 17]. In the following subsections, we present a brief overview about the security abilities of the dominating protocols in the current VoIP systems: H323, SIP, and IAX for signaling and RTP/RTCP for media transport.

a. H.323 Security Abilities

Security for H.323 is described by the ITU-T standard H235"Security and Encryption for H-Series Multimedia Terminals" [1, 10, 17]. The scope of this standard is to provide authentication, privacy and integrity for H-323. Different profiles have been defined for the use of the H235 security protocol. Each profile is defined by a specific annex. Annex D describes a simple, password-based security profile. Annex E describes a profile using digital certificates and dependent on a fully-deployed public-key infrastructure. Annex F combines features of both annex D and annex E.

Annex D: Defines a simple, baseline security profile. The profile provides basic security by simple means, using secure password-based cryptographic techniques. This profile is applicable in an environment where a password/symmetric key may be assigned to each H.323 entity (terminal, gatekeeper, gateway, or MCU). It provides authentication and integrity for H.225 protocols (RAS, and Q931), and tunneled H.245 using password-based HMAC-SHA1-96 hash. Optionally, the voice-encryption security profile can be combined smoothly with the baseline security profile. Audio streams may be encrypted using the voice-encryption security profile deploying Data Encryption Standard (DES), RC2-compatible or triple-DES, and using the authenticated Diffie-Hellman key-exchange procedure.

Annex E: Describes a security profile deploying digital signatures that is suggested as an option. H323 entities (terminals, gatekeepers, gateways, MCUs, and so on) may implement this signature security profile for improved security or whenever required. Typically, it is applicable in environments with potentially many terminals where password/symmetric key assignment is not feasible. The signature security profile overcomes the limitations of the simple, baseline security profile of Annex D.

Annex F: Describes an efficient and scalable, public key infrastructure (PKI)-based hybrid security profile deploying digital signatures from Annex E and deploying the baseline security profile from Annex D. With this security profile, digital signatures from the signature security profile in annex E are deployed only where absolutely necessary, and highly efficient symmetric security techniques from the baseline security profile in Annex D are used otherwise. The hybrid security profile overcomes the limitations of the simple, baseline security profile of Annex D as well as certain drawbacks of Annex E, such as the need for higher bandwidth and increased performance needs for processing, when strictly applied.

b. SIP Security Abilities

The SIP protocol describes several security features [10, 17]. The main security features of the SIP protocol are: message authentication, message encryption, media encryption, transport layer security, and network layer security. Only message authentication is ensured by SIP protocol, and the others abilities are allowed by other security protocols such as S/MIME, SRTP/SRTCP, TLS, and IPSec. In the following, a brief presentation of the main security features of the SIP signaling protocol.

Message Authentication: SIP ensures the authentication of signaling messages (REGISTER, INVITE, and BYE) to avoid registration hijacking attacks and prevent unauthorized calls and DoS or annoyance attacks.

Message Encryption: SIP relies on the S/MIME (Secure/Multipurpose Internet Mail Extensions) protocol to encrypt the headers of the signaling messages (except the "Via", and "Route" headers) which helps end-to-end confidentiality, integrity, and authentication between participants. S/MIME provides the flexibility for more granular protection of header information in SIP messages as it allows a selectively protection of SIP message fields.

Media encryption: SRTP (Secure RTP) protocol ensures the encryption of media packets encryption which helps the guarantee of the confidentiality and integrity of exchanged media. Section 5.4 details the security capabilities of SRTP protocol.

Transport Layer Security (TLS): TLS protocol is used to provide a transport-layer security of SIP messages (requests, responses). Actually TLS ensures the

encryption of entire SIP requests and responses which ensures the confidentiality and integrity of messages.

Network Layer Security: SIP relies on the use of IPSec at the network layer which enhances the security of IP network communications by encrypting and authenticating data. IPSec is very useful to provide security between SIP entities, especially between a user agent (UA) and a proxy server.

c. IAX Security Abilities

As it is mentioned above, IAX allows message authentication and confidentiality, and supports NAT (Network Address Translation) and firewall traversal [3-5]. Actually, IAX protocol was deliberately designed to work behind firewalls and devices performing NAT. Moreover, IAX includes the ability to encrypt the streams between endpoints with the use of an exchanged RSA key, or dynamic key exchange at call setup, allowing the use of automatic key rollover.

d. RTP/RTCP Security Abilities

Secure RTP (or SRTP) [10, 17] defines a profile of RTP Protocol, intended to provide confidentiality, integrity, and authentication to media streams in both unicast and multicast applications. In addition to protecting the RTP packets, SRTP provides protection for the RTCP streams. The designers of SRTP focused on developing a protocol that can provide adequate protection for media streams but also maintain key properties to support wired and wireless networks in which bandwidth or underlying transport limitations may exist.

4.4 VoIP Security Devices

In addition to the security capabilities of the VoIP protocols, specific security devices have been designed to enhance the security of VoIP systems [10, 17]. The security devices are primarily designed for providing security services like access control, intrusion detection, DoS protection, and so on. Examples of those devices are VoIP-aware firewall, Network Address Translation (NAT), and Session Border Controller (SBC).

a. VoIP-aware firewall

A firewall is a key security device in an IP network allowing the protection of the internal network from external attacks. The general function is to block certain types of traffic based on the source/destination IP address, the used transport protocol (TCP, UDP), the source/destination port number, the traffic direction (input, output), and the traffic type (RTP, HTTP, SMTPP). VoIP traffic may be handled using a regular or a VoIP-aware firewall. Compared to a regular firewall which handles packets only at the network and transport layer, a VoIP-aware firewall has the additional capability to inspect and manipulate VoIP packets at the application layer [10]. Actually, a VoIP-aware firewall allows:

Inspection of protocol messages: consists to check out the integrity of protocol messages (SIP messages), and blocks the originator if it detects any malformed messages.

Protection against DoS attacks: consists to detect any flooded messages and blocks the originator for a certain amount of time, based on a given policy. The policy may include number of call attempts per second, number of messages per second, number of invalid messages, etc.

Control of the bandwidth utilization: It can assign maximum bandwidth for each endpoint (or group), and block any overused endpoint.

b. Network Address Translation

Network Address Translation (NAT) [10, 17] is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. This allows home users and small businesses to connect their network to the Internet cheaply and efficiently. NAT automatically provides firewall-style protection without any special set-up. That is because it only allows connections that are originated on the inside network. This means, for example, that an internal client can connect to an outside FTP server, but an outside client will not be able to connect to an internal FTP server because it would have to originate the connection, and NAT will not allow that. It is still possible to make some internal servers available to the outside world via inbound mapping, which maps certain well know TCP ports (21 for FTP) to specific internal addresses, thus making services such as FTP or Web available in a controlled way.

c. Session Border Controller

Session Border Controller (SBC) [10, 25] is a controlling device located in a border of two network sessions. A network session may be an access network, a core network, and so on. For instance, from a VoIP service provider's perspective, there are two network borders. One is between the customer's access network and the core network (service provider's network). The other is between the core network and the other service provider's network (peer network). The role of a session border controller is to resolve border concerns that include interoperability and security issues. Security issues are mainly due to the exposure of a network session (a core network for example) to other network sessions (peer network, or a customer access network) which may help malicious users form a network session to attack resources (VoIP server, proxy, etc.) in another network session. However, interoperability issues are basically due to the interaction between network sessions using different devices and protocols.

V. CONCLUSION

In this paper, we have presented a deep analysis of the QoS and 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 QoS problems encountering the deployment of the VoIP technology. The presented discussion has addressed the QoS issues related to the use of the IP networking technology, the QoS concerns related voice clarity, and the QoS mechanisms proposed to support voice traffic QoS constraints. After that, we have investigated the security issues of the VoIP technology. The presented investigation has addressed the vulnerabilities and security attacks of VoIP systems, as well as the

countermeasures that should be considered to help the deployment of secured VoIP systems.

REFERENCES

[1] Olivier Hersent, Jean-Pierre Petit, and David Gurle, "Beyond VoIP Protocols: Understanding Voice Technology and Networking Techniques for IP Telephony", Wiley; 1 edition (March 4, 2005), Edition 1, ISBN-10: 0470023627

[2] Network World, Cisco Subnet, "Working with VoIP", Internet: http://www.networkworld.com/subnets/cisco/011309-ch1-voip-security.html, May 2013.

[3] Jonathan Davidson, and Tina Fox, "Deploying Cisco® Voice over IP Solutions", Cisco Press, 2001, Print ISBN-10: 1-58705-030-7, Print ISBN-13: 978-1-58705-030-5.

[4] Jonathan Davidson, James Peters, Manoj Bhatia, Satish Kalidindi, and Sudipto Mukherjee, "Voice over IP Fundamentals", Cisco Press, July 2006, Print ISBN-10: 1-58705-257-1, Print ISBN-13: 978-1-58705-257-6.

[5] Theodore Wallingford, "Switching to VoIP", O'Reilly Media, Inc., June 2005, Print ISBN-13: 978-0-596-00868-0, Print ISBN-10: 0-596-00868-6.

[6] Meisel, J.B. and Needles, M. (2005), ''Voice over internet protocol (VoIP) development and public policy implications'', info, Vol. 7 No. 3, pp. 3-15.

[7] Amor Lazzez, and Thabet Slimani, "Deployment of VoIP Technology:QoS Concerns", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue 9, September 2013.

[8] Amor Lazzez, "VoIP Technology: Security Issues Analysis", International Journal of Emerging Trends & Technology in Computer Science, Vol. 2, Issue, July-August 2013.

[9] Amor Lazzez, Wissem Ben fredj, Thabet Slimani "IAX-Based Peer-to-Peer VoIP Architecture", International Journal of Computer Science Issues, volume 10, Issue 3, May 2013.

[10] Patrick park, "voice over IP Security ", Cisco Press, September 2008, ISBN-10: 1-58705-469-8.

[11] Andrew Froehlich, "CVOICE 8.0: Implementing Cisco Unified Communications Voice over IP and QoS v8.0: Study guide", Sybex, Novmber 2011, Print ISBN : 978-0-470-91623-0, Web ISBN: 0-470916-23-0.

[12] Kevin Wallace, "Implementing Cisco Unified Communications Voice over IP and QoS (CVOICE) Foundation Learning Guide: (CCNP Voice CVoice 642-437)", Cisco Press, May 2011, Print ISBN-10: 1-58720-419-3, Web ISBN-10: 0-13-210342-7.

[13] Tim Szigeti - CCIE No. 9794; Christina Hattingh, "End-to-End QoS Network Design", Cisco Press, Print ISBN-10: 1-58705-176-1, Print ISBN-13: 978-1-58705-176-0.

[14] Jonathan Davidson; Tina Fox, "Deploying Cisco Voice over IP Solutions", Cisco Press, November 2001, Print ISBN-10: 1-58705-030-7, Print ISBN-13: 978-1-58705-030-5.

[15] Michael Valentine," CCNA Voice Quick Reference", Cisco Press, July 2008, Print ISBN-10: 1-58714-337-2, Web ISBN-10: 1-58705-810-3.

[16] Vinod Joseph, and Brett Chapman, "Deploying QoS for Cisco IP and Next-Generation Networks: The Definitive Guide", Morgan Kaufmann, April 2009, Print ISBN-13: 978-0-12-374461-6, Web ISBN-13: 978-0-08-092255-3.

[17] Peter Thermos; Ari Takanen, "Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures", Addison-Wesley Professional, August 2007, ISBN-10: 0-321-43734-9.

[18] S. Niccolini. 2006. VoIP Security Threats. http://tools.ietf.org/id/draft-niccolini-speermint-voipthreats-00.txt.

[19] Nico Schwan, Thomas Strauss, and Marco Tomsu, "Peer-to-Peer VoIP & MMoIP for Public Services – Requirements and Architecture", Alcatel-Lucent Deutschland AG, Research & Innovation, Lorenzstrasse 10, 70435 Stuttgart, Germany.

[20] Internet Engineering Task Force, P2PSIP Working Group "draft-ietf-p2psip-service-discovery-08.txt", February 2013.

[21] Mart ínez-Yelmo Isa ás, Bikfalvi Alex, Cuevas Rub én, Guerrero Carmen, and Garcia Jaime, "H-P2PSIP: Interconnection of P2PSIP domains for Global Multimedia Services based on a Hierarchical DHT Overlay Network", Elseiver, Mars 2009, Computer Networks, Vol. 53, Issue 4, March 2009, pp. 556-568.

[22] David Schwartz, "A Comparison of Peer-To-Peer and Client-Server Architectures in VoIP Systems", Internet: http://www.tmcnet.com/voip/0406/featurearticle-comparison-of-peer-to-peer.htm, May 2013.

[23] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261 (Proposed Standard), June 2002. Updated by RFCs 3265, 3853, 4320, 4916.

[24] Internet Engineering Task Force (2009b), "IAX: Inter-Astersik eXchange version 2", RFC 5456, Internet Engineering Task Force, Fremont, CA.

[25] Mohamed Boucadair, " Inter-Asterisk Exchange (IAX): Deployment Scenarios in SIP-Enabled Networks", 2009 John Wiley & Sons Ltd. ISBN: 978-0-470-77072-6.

[26] Jim Van Meggelen, Jared Smith, and Leif Madsen, "Asterisk: The Future of Telephony", O'Reilly Media, September 2005, ISBN-10: 0596009623.

Author's Profiles

Amor Lazzez is currently an Assistant Professor of Computer and Information Science at Taif University, Kingdom of Saudi Arabia. He received the Engineering diploma with honors from the high school of computer sciences (ENSI), Tunisia, in June 1998, the Master degree in Telecommunication from the high school of communication (Sup'Com), Tunisia, in November 2002, and the Ph.D. degree in information and communications technologies form the high school of communication, Tunisia, in November 2007. Dr. Lazzez is a researcher at the Digital Security research unit, Sup'Com. His primary areas of research include design and analysis of architectures and protocols for optical networks.

How to cite this paper: Amor Lazzez,"VoIP Technology: Investigation of QoS and Security Issues", International Journal of Information Technology and Computer Science(IJITCS), vol.6, no.7, pp.65-76, 2014. DOI: 10.5815/ijitcs.2014.07.09