Securing VoIP Systems: A QoS-Oriented Approach

Amor Lazzez

Taif University,
Kingdom of Saudi Arabia

Abstract

Voice over IP (VoIP) is a communication technology allowing voice traffic transmission as data packets over a private or a public IP network. VoIP allows significant benefits for customers and service providers including cost savings, services integration, and systems extensibility. Nevertheless, the VoIP technology suffers from many hurdles such as architecture complexity, interoperability problems, security issues, and QoS concerns. The main challenging matter encountering the deployment of VoIP systems is the mutual interaction between the QoS and the security issues. Actually, the strict performance requirements of voice traffic have significant implications for VoIP system security, particularly in terms of service availability. On the other hand, the use of IP network security standards (firewalls, NATs, IPSec) to overcome security issues results into a degraded VoIP QoS. In this paper, we focus on the effects of the security measures on the VoIP QoS, and we aim to propose a QoS-oriented system allowing the deployment of secured VoIP networks without adversely affecting the provided QoS.

Keywords: *VoIP, Security Issues, QoS Concerns*

1. Introduction

Voice over IP (VoIP) [1-6] is a communication technology allowing voice communications and multimedia sessions over an IP (Internet Protocol) network, such as the Internet. VoIP has been prevailing in the telecommunication world since its emergence in the late 90s, as a new IP communication service. The reason for its prevalence is that, compared to legacy phone system, VoIP allows significant benefits for customers and service providers such as cost savings, the provision of new media services, phone portability, and the integration with other applications [1, 2, 4, 5].

Despite the advantages it may provide, the VoIP technology suffers from challenging issues in terms of security and QoS [2, 4-11]. Actually, initially designed to provide a Best Effort service [3-5, 7, 12-13], the IP networking technology cannot support the stringent QoS requirements of voice traffic [4, 12, 14-15]. This results into QoS problems for voice communication over IP networks [12, 16-17]. On the other hand, in addition to the vulnerabilities of the VoIP devices and protocols, VoIP systems are affected by the vulnerabilities of the infrastructure they are running on (network, operating system, etc.) [2, 4-6, 8, 10, 11, 18, 19]. This multiplies the security attacks that may target the integrity and the confidentiality of voice traffic transmitted over an IP infrastructure.

Different schemes have been proposed to address the security and QoS issues encountering the deployment of the VoIP technology. Actually, QoS approaches (Diffserv, Intserv) have been developed to help a better support of the performance requirements of voice traffic over an IP network [7, 11, 20]. Moreover, specific security mechanisms have been defined as part of VoIP protocols to help securing VoIP systems [10, 18].

Even though different schemes may be considered to address separately VoIP QoS and security issues, an efficient deployment of the VoIP technology is frustrated by a mutual interaction between system security and QoS support [21]. In fact, the strict performance requirements of voice traffic have significant implications for VoIP system security, particularly in terms of service availability [21]. On the other hand, the use of IP network security standards (firewalls, NATs, IPSec) to overcome security issues results into an expanded latency, jitter, and traffic loss, and thus a degraded VoIP QoS [21].

In this paper, we focus on the effects of the security measures on the VoIP QoS, and we aim to propose a QoS-oriented system allowing the deployment of secured VoIP networks without adversely affecting the provided QoS. The proposed system relies on the use of security capabilities of VoIP protocols and the adjustment of the IP data network security standards to make advantages of theirs security abilities while avoiding their negative effects on the VoIP QoS. First, we present a brief overview about the VoIP technology. Then, we present the QoS issues associated with the deployment of the VoIP technology and that may be affected by IP network security standards. After that, we analyze the effects of the

traditional security measures on the VoIP QoS issues. Finally, we present the proposed QoS-oriented VoIP security system.

The remaining part of this paper is organized as follows. Section 2 presents a brief overview about the VoIP technology. Section 3 presents the VoIP QoS issues that may be affected by IP data network security standards. Section 4 highlights the security issues of the VoIP technology. Section 5 discusses the effects of the IP data network security standards on the VoIP QoS, and presents a QoS-oriented security system that overcomes VoIP security issues without affecting the provided QoS. Section 6 concludes the paper.

2. Brief overview of VoIP

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 technology helps the provision of significant benefits for users, companies, and service providers. The key benefits of the VoIP technology are as follows [1, 2, 4, 5, 7-9, 11]:

- Cost savings: less expensive phone calls, reduced service deployment and maintenance cost.
- Provision of new communication services: instant message, presence check, image transfer, etc.
- Service mobility: Wherever the user (phone) goes, the same services will be available.
- Integration and collaboration with other applications: integration and collaboration with web browser, instant messenger, social-networking applications, etc.
- The provision of a user control interface: a web GUI allowing user to change features, options, and services dynamically.

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 that are responsible for users' registration as well as the establishment of VoIP sessions between registered users [9, 11]. Figure 1 shows an illustrative example of a client-server VoIP system. As it is illustrated in the figure, each central server handles a set of users. Each user must be registered on one of the central servers to be able to exchange data with other registered users.

The deployment of a client-server VoIP system relies on the use of a signaling protocol to set up a communication session between two end points, and a media transport protocol to transmit voice traffic between communicating terminals once a session has been established [1, 2, 4, 5, 9, 11, 21]. The main signaling protocols used for the deployment of VoIP systems are H323, and SIP. Standardized by the International Telecommunication Union (ITU), H323 [1, 2, 6] is the first signaling protocol publicly used for the deployment of VoIP systems. Allowing flexibility and security features, SIP protocol [1, 6, 22] is nowadays more used than H323 protocol. For media transport, the majority of VoIP systems rely on the use of Real-Time Transport Protocol (RTP) for data transmission during a VoIP session [1, 2, 6, 11]. Secure RTP (SRTP) has been recently proposed by the IETF as a secured version of the RTP protocol [1, 2, 6, 11].

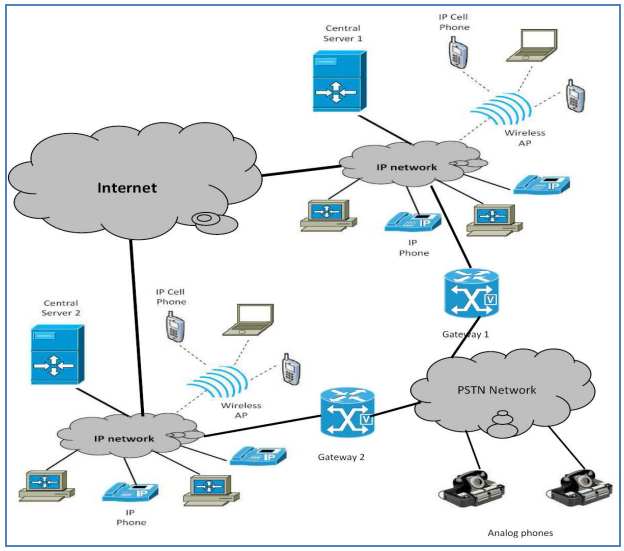

Figure1: Client-Server VoIP Architecture: An illustrative Example

3. VoIP QoS Issues

The main QoS issues encountering the deployment of the VoIP technology and that security may affect are: bandwidth, network delay, delay variation, and traffic loss [3-5, 7, 11, 21].

3.1 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. 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, 12-17].

3.2 Network Delay

Referred to as latency, network delay is the amount of time it takes a packet to travel from a source to a destination through the network. Latency mainly includes the processing delay, the queuing delay, the serialization delay, and the propagation delay [11-13].

- 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, 12]. 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, 11-17]:

3.3 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. 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, 12]. Given the annoying effects of Jitter, a QoS mechanism referred to as de-jitter or play out delay buffering has been considered [12, 13]. 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.

3.4 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, 12]. Voice traffic loss may be minimized using the following strategies [3-5, 11-17]:

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

4. VoIP Security Issues

VoIP technology is characterized by a set of vulnerabilities coming from VoIP applications as well as the infrastructure are running on (network, operating system, etc.). These vulnerabilities can be exploited to carry out different kinds of security attacks including attacks against availability, attacks against confidentiality, and attacks against integrity. In the following subsections, we first present the main vulnerable components in a VoIP system. Then, we present a brief overview about the VoIP security attacks.

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, 11, 18, 19]. 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. The

following are the main vulnerable components involved in the deployment of a regular VoIP system.
- 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 types of security attacks. An attacker 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. The following is a brief presentation of VoIP security attacks as it is presented in [8, 10, 11, 18, 19].

Attacks against availability: Attacks against availability aim at VoIP service interruption, typically in the form of Denial of Service (DoS). The main attack methods against availability are: call flooding, malformed messages, spoofed messages, call hijacking, server impersonating, and Quality of Service (QoS) abuse.

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.

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.

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.

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.

5. Securing VoIP Systems

Efficient measures have been proposed for the deployment of secured IP data networks. The main are firewalls, network address translation (NAT), and traffic encryption using IPSec protocol. The standard IP data network security measures may be used to secure VoIP networks. However, they complicate several aspects of VoIP and affect the provided QoS [21, 23, 24]. In order to help the deployment of an integrated IP network allowing the transmission of data and voice traffic while taking into account their requirements in terms QoS and security, adjustments have been considered for the main IP data network security standards to be able to support security in the new fast paced world of VoIP [20, 21, 25, 26]. In addition to adaptation of the existing security schemes to help the integration of voice and data over a secured IP network, specific security mechanisms have been defined as parts of the VoIP protocols to enhance the security of voice communication over an IP network [10, 17].

In the following subsections, we first discuss the effects of the main IP data network security standards on the VoIP QoS. Then, we present a QoS-oriented VoIP security system that relies on the security capabilities of VoIP protocols and the use of VoIP-aware security devices obtained by the adjustment of the IP data network security standards to make them able to secure voice traffic while allowing efficient support of VoIP QoS constraints.

5.1 Effects of IP Data Network Security Standards of VoIP QoS

In this subsection, we discuss the effects of the main IP data network security measures on the VoIP QoS issues. Mainly, we focus on the analysis of the effects of firewalls, NATs, and IPSec traffic encryption.

Effects of Firewalls: Firewalls are a main of security in today's IP networks. A firewall is the first line of defense against intrusion, blocking traffic that deemed to be invasive, intrusive, or malicious. A firewall is a central access point that filters the input/output traffic based on a set of rules programmed by the network administrator (security policies). There are two types of packet filtering firewalls, stateless and stateful. Stateless firewalls retain no memory of traffic that has occurred earlier in the session. Stateful firewalls do remember previous traffic and can also investigate the application data in a packet. Thus, stateful firewalls can handle application traffic that may not be destined for a static port.
Even though, it may prevent intrusions, the introduction of firewalls to VoIP networks results into the following QoS issues [21, 23]:

Increased latency: every packet needs to pass through the firewall to be checked. This incurs an extra delay for each transmitted packet, which corresponds to the sum of the queuing delay at the input of the firewall and the needed time to check a packet. This incurred extra delay may result into more latency for voice traffic especially with low throughput firewalls.

Introduced jitter: Transmitted over the firewall, voice packets undergo various delays. This results into a non-uniform packet delays, and hence a jitter issue.

Traffic loss: As it is mentioned above, a firewall acts as a bottleneck on the network because every packet needs to pass through it to be checked. Therefore, a traffic loss may occur at the input of the firewall due to a buffer overflow.

Effects of the Network Address Translation: Network Address Translation (NAT) is a powerful tool that enables several endpoints within a LAN to use private addresses for local accesses and to share the same public IP address for wide connections [21, 25]. In addition to the efficient use of the global IP addresses, the NAT scheme contributes indirectly to security for a LAN, making internal IP addresses less accessible from the public Internet. Thus, all attacks against the network must be focused at the NAT router itself. Like firewalls, this provides security because only one access point must be protected. Like firewalls, the introduction of the NAT in the deployment of VoIP networks complicates several aspects (ex., making a call into the network) and affects the provided QoS. The following are the results of the introduction of the NAT may affect the VoIP QoS [21].

Expanded latency: Because the payload of each transmitted packet must be changed at the application level to correspond to the NAT translated source or destination address and ports, an additional delay is incurred for each voice packet. This results into more latency for voice traffic especially with the use of low throughput NAT devices.

Introduced jitter: Transmitted over the NAT device, voice packets undergo various delays. This results into a non-uniform packet delays, and hence a jitter issue.

Traffic loss: As it is mentioned above, NAT devices act as a bottleneck on the network because every packet needs to

pass through to be changed the NAT translated source or destination address and ports. Therefore, a traffic loss may occur at the input of a low throughput NAT device due to a buffer overflow.

Effects of the Encryption: Encryption is a standard security scheme used to prevent network traffic against tapping attacks by making it unintelligible. The encryption process relies on the use of an encryption/decryption algorithm and a secret key. Encryption may only interest payload to provide traffic confidentiality, or both header and payload to ensure confidentiality and prevent traffic analysis. IPSec is the standard method used to secure an IP network against tapping attacks through the encryption of the exchanged traffic at the network layer [21, 24, 27]. Even though it may prevent voice communication against tapping attacks, the transport of voice traffic of IPSec protocol (VoIPSec) results into various QoS issues that lead to degraded voice quality [21, 24]. The main effects of the use of the encryption scheme in a VoIP network are:

Encryption/decryption latency: this results form:

- The computation times of the encryption process at the transmission side and the decryption process at the reception side.
- The queuing delay at the input of the encryption/decryption engine. This delay may be excessive in the presence of heterogeneous traffic (data, voice) IP packets) due to the standard FIFO scheduling algorithm employed in today's encryption engines.

Jitter: The computation time of the encryption/decryption algorithm varies with the variation of packet lengths. Therefore, the presence of heterogeneous traffic in the network (voice packets, data packets) results into variable encryption/decryption latencies. This leads to variable delay times for fairly uniform voice packets, causing them to arrive in spurts.

Traffic loss: given the excessive delay introduced by the encryption/decryption process**,** the encryption/decryption engine constitutes a severe bottleneck in a VoIP network. Therefore, a traffic loss may occur at the input of the encryption engine due to a buffer overflow.

Reduction of the effective bandwidth: The encryption process expands the overhead of the transmitted IP packets. This results into the reduction of the effective bandwidth, which may cause a latency issue for voice traffic.

5.2 A QoS-Oriented VoIP Security System

The aim of this subsection is to present the QoS-oriented security system that we propose to help a secured deployment of the VoIP technology that provides an efficient support of VoIP QoS constraints. The proposed system relies on the security capabilities of VoIP protocols and the adjustment of the IP data network security standards to make advantages of theirs security abilities while avoiding their negative effects on the VoIP QoS as detailed in the previous section. This helps the integration of voice and data traffic over a secured IP network while allowing an efficient support of the stringent QoS constraints of voice traffic.
In the following, we first present the main solutions that have been proposed to adjust the main IP data network security standards to support security without affecting VoIP QoS. Then, we present the security abilities of the main VoIP protocols.

Adjustment of the IP Data Network Security Standards: In order to help the deployment of an integrated IP network allowing the transmission of data and voice traffic while taking into account their requirements in terms QoS and security, solutions have been considered to adjust the main IP data network security standards (Firewalls, NATs, IPSec Encryption) to support security in the new fast paced world of VoIP [21, 25-27]. In the following subsections, we present the main considered approaches to overcome the VoIP QoS issues of Firewalls, NATs, and IPSec encryption.

Solution to Firewall/NAT VoIP QoS Issues: In the absence of a universally accepted solution to the traversal and QoS issues associated with firewall/NAT in the deployment of the VoIP technology, product developers have proposed a solution that has come to be known as a Session Border Controller (SBC) [21, 25, 26]. SBCs are dedicated appliances that offer one or more of the following services to a VoIP network: Firewall/NAT traversal, Call Admission Control, Service Level Agreement monitoring, support for legal intercept, and protocol interworking. Therefore, SBCs allow the use of Firewall/NAT security schemes in securing VoIP networks while avoiding their effects on the quality of voice traffic transmission over an IP network (VoIP QoS).

Solution to VoIPSec QoS Issues: The main solution that has been proposed to overcome the VoIPSec QoS issues is the Secure Real Time Protocol (SRTP) [21, 27]. SRTP has been proposed to protect voice traffic against tapping attacks while avoiding the effects of traffic encryption on VoIP QoS. SRTP protocol defines a security profile of RTP (Real Time Protocol), intended to provide the authentication, the confidentiality, and the integrity of RTP and RTCP messages. SRTP protocol relies on the use of AES (Advanced Encryption System) protocol for traffic encryption, and HMAC-SHA1 for message authentication

and integrity. Compared to IPSec, SRTP protocol relies on the use of ultra fast encryption and authentication algorithms (AES, HMAC-SHA1). SRTP protocol allows an improved VoIP QoS attained by :

- Low computational cost asserted by the use of speedy encryption and authentication algorithms (AES, HMAC-SHA1);
- Low bandwidth cost and a high throughput by limited packet expansion and by a framework preserving RTP header compression efficiency;

This illustrates that the SRTP protocol may take advantages of the encryption scheme to provide the authentication, the confidentiality, and the integrity of the transmitted voice traffic without affecting VoIP QoS as IPSec does.

Security Abilities of VoIP Protocols: In addition to the use of VoIP-aware security devices obtained by the adjustment of the IP data network security standards to make them able to provides VoIP security issues without affecting VoIP QoS, the proposed QoS-oriented VoIP security system makes advantages of the security ability of the VoIP protocols for more secure VoIP systems. The following is a brief presentation of the security abilities of the dominating protocols in the current VoIP systems: H323, and SIP [10, 17].

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.

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 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.

6. Conclusion

In this paper, we have proposed a QoS-oriented security approach to help the deployment of secured VoIP systems able to support the stringent QoS constraints of voice traffic. The proposed approach relies on the use of the security capabilities of VoIP protocols and the adjustment of the IP data network security standards to make advantages of theirs security abilities while avoiding their negative effects on the VoIP QoS. The proposed approach helps the integration of voice and data traffic over a secured IP network allowing an efficient support of the stringent QoS constraints of voice traffic.

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] Amor Lazzez, “ VoIP Technology: Investigation of QoS and Security Issues”, International Journal of Information Technology and Computer Science (IJITCS), Modern Education and Computer Science (MECS) Press, June 2014, Vol. 06, No. 07, Pages: 65-76.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

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

[17] 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.

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

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

[20] C-N. Chuah, “Providing End-to-End QoS for IP based Latency sensitive Applications.”. Technical Report, Dept. of Electrical Engineering and Computer Science, University of California at Berkeley, 2000.

[21] D. Richard Kuhn, Thomas J. Walsh, and Steffen Fries (January 2005), NIST Special Publication 800-58: Security Considerations for Voice over IP Systems: Recommendations of the National Institute of Standards and Technologies.

[22] 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.

[23] P. Hochmuth and T. Greene, “Firewall limits vex VOIP users”. Network World Fusion, July 2002.

[24] Telcordia Technologies, “Performance and Security Analysis of SIP using IPsec”, National Institute of Standards and Technology, January, 2004.

[25] J. Rosenberg and H. Schulzrinne, “SIP Traversal through Residential and Enterprise NATs and Firewalls”. Internet Draft, Internet Engineering Task Force, Mar. 2001.

[26] Anonymous, “Traversing Firewalls and NATs With Voice and Video Over IP: An Examination of the Firewall/NAT Problem, Traversal Methods, and their Pros and Cons” . Wainhouse Research, Apr. 2002.

[27] R. Barbieri, D. Bruschi, E Rosti, "Voice over IPsec: Analysis and Solutions", Proceedings of the 18th Annual Computer Security Applications Conference,2002.

Amor Lazzez is currently an Assistant Professor at the college of Computer and Information Technology (CIT), Taif University, KSA.
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 primary areas of research include the design and analysis of all-optical network architectures and protocols, VoIP deployment, digital forensics, network security and QoS support.