International Journal of Recent Trends in Engineering & Research
ISSN : 2455-1457 Impact Factor : 3.344

VOIP TECHNOLOGY: ANALYSIS OF SECURITY ISSUES

P Y Shinde[1], R Sheth[2]
B. E Student, Gujarat Technological University
E-mail: p.shinde0059@gmail.com

Abstract- Voice over IP (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are IP telephony, Internet telephony, broadband telephony, and broadband phone service. 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 Users can make the telephone calls over an IP network using this technology. 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, 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 of the VoIP technology.

Keywords-- VoIP, Internet Protocol, Security Issues, Analysis0.

I. INTRODUCTION

A major development that started in 2004 was the introduction of mass-market VoIP services that utilize existing broadband Internet access, by which subscribers place and receive telephone calls in much the same manner as they would via the public switched telephone network (PSTN). To transmit voice conversations over a data network using IP, VoIP technology is used. Such data network may be the Internet or a corporate Intranet or managed networks which are specially used by long distance and local service traditional providers and ISPs (Internet Service Provider).

Voice over IP (VoIP) 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][8][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, security issues are considered as the most serious challenges for successful deployment of the VoIP technology [2][4][5][6] be considered to help the deployment of a successful VoIP system. The presented discussion 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.

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 [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,

@IJRTER-2015, All rights Reserved

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]. 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

2.1 IMPLEMENTATION OF VoIP

In this section first we will discuss VoIP protocols and after that data processing in VoIP.

Protocols

There are currently three types of protocols which are widely used in VoIP implementations: the H.323 family of protocols, the Session Initiation Protocol and the media Gateway Controller Protocol (MGCP). The discussion of these protocols is as follows:

H.323 Family of Protocols

H.323 [12][13] is a set of recommendations from the International Telecommunication Union (ITU) and consists of family of protocols that are used for call set-up, call termination, registration, authentication and other functions. These protocols are transported over TCP or UDP protocols. The following figure.1 shows the various H.323 protocols with their transport mechanisms. H.323 family of protocol consists of H.225 which is used for registration, admission, and call signaling. H.245 is used to establish and control the media sessions. T.120 is used for conferencing applications in which a shared white-board application is used. The audio codec is defined by G.7xx series by H.323, while video codec is defined by H.26x series of specifications. H.323 uses RTP for media transport and RTCP is used for purpose of controlling RTP sessions. The following figure.2 & figure.3 shows the H.323 architecture and call set-up process.

Session Initiation Protocol (SIP)

The modification and termination sessions between two or more participants the IETF is used which is defined by SIP (session initiation protocol) [13]. These sessions are not limited to VoIP calls. The SIP protocol which is a text-based protocol, it is similar to HTTP and offers an alternative to the complex H.323 protocols. SIP protocol become more popular in comparison to H.323 family of protocol because it is more similar than it. The following figure 4 and figure 5 shows the SIP architecture, call set-up and tear down process

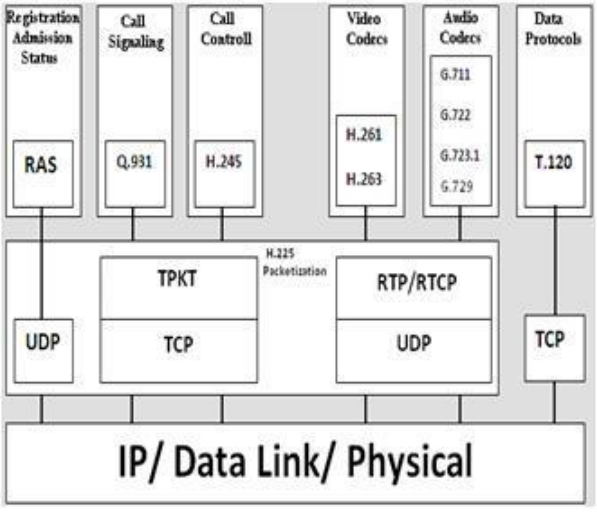


Fig.1 H.323 Protocol family

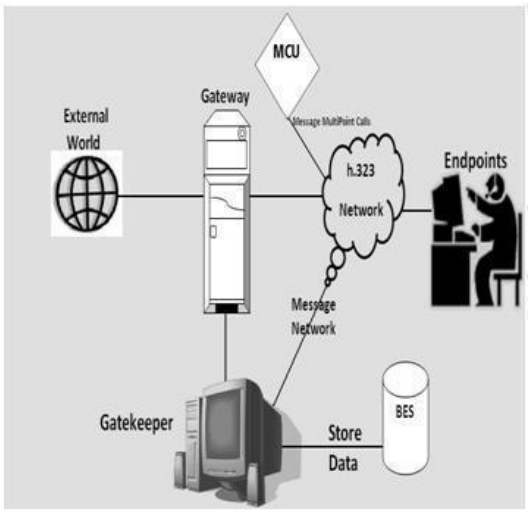


Fig. 2 H.323 Architecture

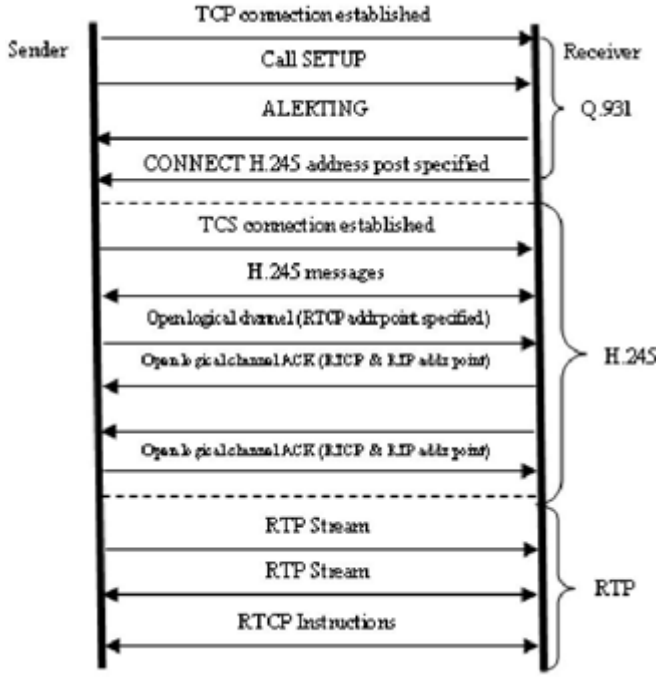


Fig. 3 Call Setup Process in H.323

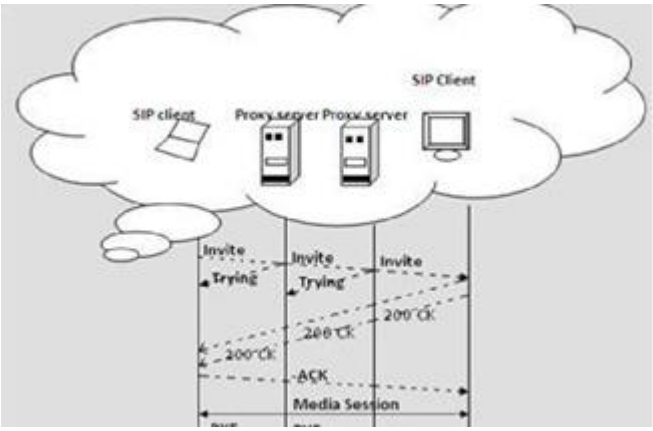


Fig. 4 SIP Network Architecture [9]

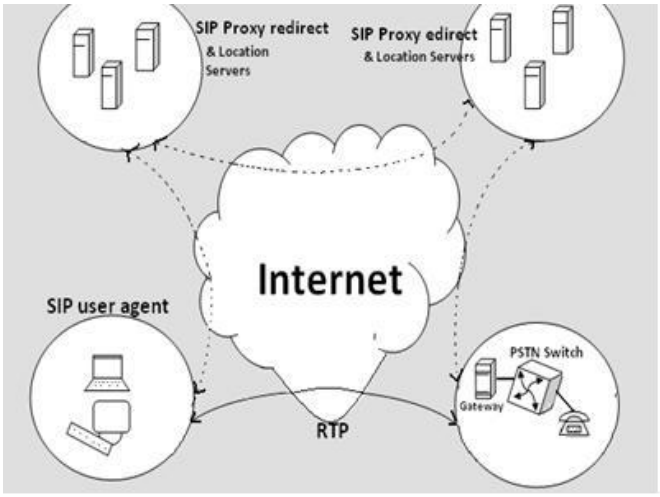


Fig. 5 Call setup and tear down in SIP

Media Gateway Control Protocols (MGCP)

The communication between the separate components of a decomposed VoIP gateway is done by media gateway control protocol. It is a complementary protocol to SIP and H.323. "Call agent" is mandatory and manages calls and conferences, when we are using MGCP and MGC server (Figure 6). The MG endpoint is not responsible for calls and conferences. It does not maintain call states. MGs are responsible to execute commands sent by the MGC call agents. MGCP assumes that call agents will synchronize with each other sending coherent commands to MGs under their control. MGCP does not define a mechanism for synchronizing call agents. MGCP is a master/slave protocol with a closely coupling between the MG (endpoint) and MGC (server).

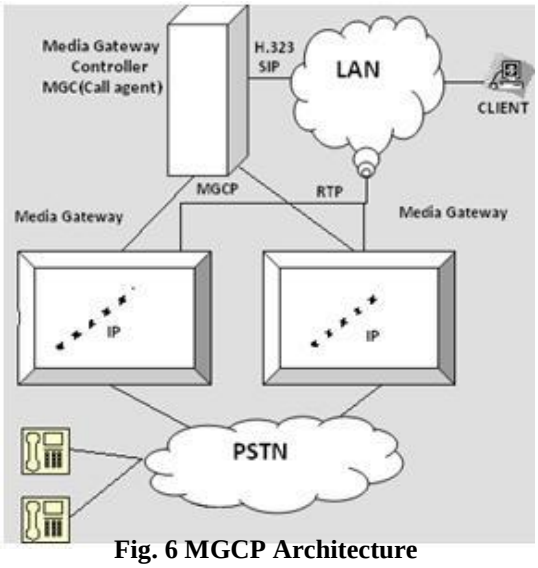


Fig. 6 MGCP Architecture

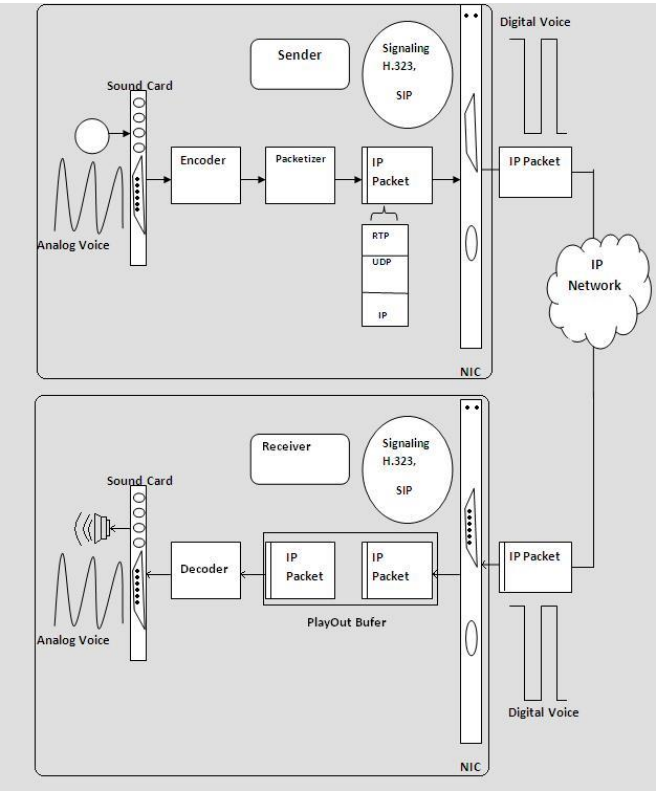
B. Data Processing in VoIP Systems

There are three types of essential components in VoIP: CODEC (Coder/Decoder), packetizer and playout buffer [14], [15]. The analog voice signals are converted into digital signals at sender's side, after that these digital signals are compressed and then encoded into a predetermined format using voice codec. There are various voice codecs developed and standardized by International Telecommunication Union-Telecommunication (ITU-T) such as G.711, G.729, and G.723 etc. The packetization process is performed by distributing fragmented encoded voice into equal size of packets.

@IJRTER-2015, All rights Reserved

Furthermore, in each packet, some protocol headers from different layers are attached to the encoded voice. Protocols headers added to voice packets are of Real-time Transport protocol (RTP), User Datagram Protocol (UDP), and Internet Protocol (IP) as well as Data Link Layer header. In addition, RTP and Real-Time Control Protocol (RTCP) were designed to support real-time applications at the application layer. Although TCP transport protocol is commonly used in the internet, UDP protocol is preferred in VoIP and other delay-sensitive real-time applications. TCP protocol is suitable for less delay-sensitive data packets and not for delay-sensitive packet due to the acknowledgement (ACK) scheme that TCP applies. This scheme introduces delay as receiver has to notify the sender for each received packet by sending an acknowledgement. The UDP protocol cannot be applied to VoIP technology. It is more suitable for VoIP applications. The packets are then sent out over IP network to its destination where the reverse process of decoding and depacketizing of the received packets is carried out. The time variations of packet delivery (jitter) may occur in transmission process. Hence, a play out buffer is used at the receiver end to migrate the package without any interruption. Packets are queued at the playout buffer for a playout time before being played. However, these packets continued to arrive until the playout time is discarded. The fig.7 shows the end –to- end transmission of voice in VoIP system.

Besides, there are signaling protocols of VoIP namely Session Initiation Protocol (SIP) and H.323. These signaling protocols are required at the very beginning to establish VoIP calls and at the end to close the media streams between the clients.



III. 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 [16], 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 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

@IJRTER-2015, All rights Reserved

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

@IJRTER-2015, All rights Reserved

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.

IV. 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.) [16, 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, 16, 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 profiledeploying 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

@IJRTER-2015, All rights Reserved

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.

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.

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”,

[5] Cisco Press, July 2006, Print ISBN-10: 1-58705-257-1, Print ISBN-13: 978-1-58705-257-6.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] [10]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.

[12] 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.

[13] http://www.isoc.org/pubpolpillar/voip-paper.shtml 15.08.2006 http://www.eyeball.com/spit-solution.htm.

[14] K. M. McNeill, M. Liu and J. J. Rodriguez, "An Adaptive Jitter Buffer PlayOut Scheme to Improve VoIP Quality in Wireless Networks", IEEE Conf. on BAE Systems Network Enabled Solutions, Washington, 2006.

[15] C. Lin, X. Yang, S. Xuemin and W.M. Jon, "VoIP over WLAN: Voice capacity, admission control, QoS, and MAC", International Journal of communication Systems, Vol.19, No 4, pp. 491-508, May 2006.

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

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

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

@IJRTER-2015, All rights Reserved