STUDY OF NETWORK SECURITY IN VOIP

Sudarshan K. S.[(1)], Shreyas R[(1)]
Pradeep Kumar. V[(1)]
[(1)]Student, RV College Of Engineering, Bangalore.

Abstract— Voice over IP is one of the quickest developing Internet services and slowly replaces traditional telephony. However, while moving telephony to the public IP platform broadens its service capabilities, some security problems may occur. It is because the amount of threats existing in IP networks is much bigger than in case of traditional telephone networks. Therefore security challenges of VoIP public network are considered in this work in detail. Full security analysis is performed that covers many issues like protocol vulnerabilities, risks due to the voip infrastructure, sip vulnerabilities and voip services are also mentioned. Considerations regarding how those requirements may be compromised are also carried out, including threat analysis, overview of vulnerabilities and attack techniques against technologies underlying VoIP and specific for VoIP. Finally, some study of existing security mechanisms that could counteract vulnerabilities and prevent attacks is performed. Risk analysis is also carried out in this work. The most serious problems of VoIP public networks are this way identified and security solutions are proposed.

Keywords- VoIP, Network Security, vulnerability , network architecture , threats.

I. INTRODUCTION

VoIP is a technology for producing telephone services on IP-based networks. Traditionally, these tele-phone services have been provided by the public switched telephone network (PSTN/ISDN), which has been managed and completely controlled by single, national operators in each country in Europe, and for GSM the situation initially was similar. The risks were known, and managed. Since the mid '90s this situation has been evolving in Europe. The national operators still exist, but in addition second operators, third party vendors, ISPs and mobile providers (GSM, GPRS, UMTS) are also interconnecting and providing a multitude of services such as VoIP, video conferencing, video on demand etc.[1] This dynamic new situation has given rise to new threats and risks, which are more complex and unpredictable than for any one service or technology in isolation. This enriched threat model requires extensive countermeasures in order to be able to deliver services of acceptable quality, reliability and security.

In this paper we introduce the security issues inherent in this new complex situation and address how some of them can be mitigated. VoIP caused a lot of excitement towards the end of the 90s, with the promise of providing a viable technology for the migration from the monolithic public switched telephone network (PSTN/ISDN) to next generation networks, for which telephone services are produced on an IP-based network. At the turn of the millennium, it was announced that the IETF's Session Initiation Protocol (SIP) standard would be chosen as the basis for the 3GPP IP multimedia subsystem (IMS). [1] SIP at this point, was still in an early phase of development. Problems with poor voice quality for the early Internet-based offerings, along with the added barrier of cumbersome technology, e.g., having to phone from the PC made it difficult for consumers to embrace the new technology, and lead to slow adoption rate. The immaturity of the emerging SIP standard contributed largely to the slowdown of the roll out of VoIP services along with uncertainty in the economic and market related factors, and the lack of a solid business model.

In the early days of VoIP, there was no big concern about security issues related to its use. People were mostly concerned with its cost, functionality and reliability. But today, VoIP is being used everywhere with different levels of success. Home users may use an Analogue Terminal Adapter (ATA) to use their legacy POTS telephone sets and make telephone calls over the Internet. PC users have a choice of applications that allow them a rich user experience and address book facility, and VoIP telephones are available both as desktop models and cordless handsets using WiFI. Even mobile nomadic users may use their VoIP accounts wherever they find a broadband Internet connection. Because of this widescale use of Voip, security has become a major issue. The security threats cause even more concern when we think that VoIP is in fact replacing the oldest and most secure communication system the world ever known – POTS (Plain Old Telephone System). But still VoIP security has not received sufficient attention during the development phases and is lagging behind in the deployment and hence there is a need to improve their security. [1]

In this paper we present in section II VoIP architectures and use cases for some aspects of the VoIP infrastructure, then we present in section III many of the possible attacks that could be done on a VoIP system. Section IV gives us a brief overview of the primary goals in VoIP security. Section V deals with understanding the countermeasures used to prevent attacks against VoIP. Section VI presents conclusion and in Section VII we present the future work that can be done to improve the security in the future. Nonetheless, we believe that this paper will serve for understanding the bigger problem and act as a basis for a more comprehensive analysis in the future.

II. VOIP ARCHITECTURE

The VoIP infrastructure consists of endpoints (telephones), Control nodes, gateway nodes, and the IP-based network. The IP network can utilize various media including Ethernet, fiber, And wireless. The VoIP system interacts with both local and Remote VoIP phones using the intranet and Internet as well as

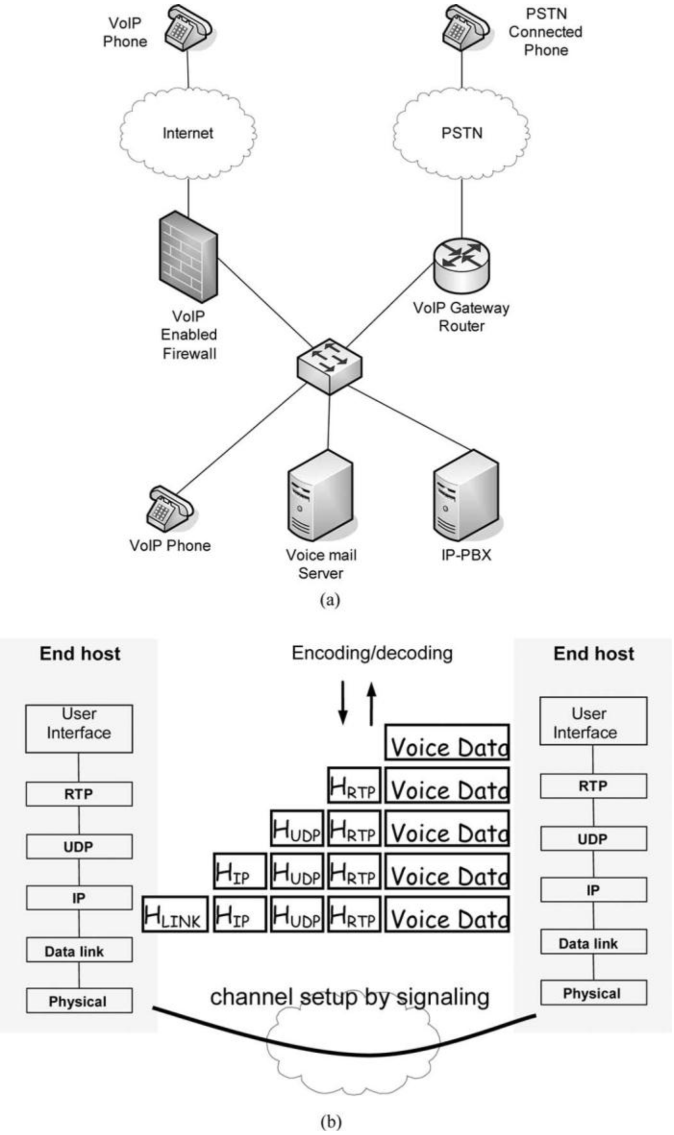


Fig. 1. (a) Typical VoIP network structure. (b) Voice data processing of the VoIP.

Interacting with phones connected to the public-switched telephone network (PSTN) through gateways. Fig. 1(a) illustrates a simple VoIP setup. The VoIP data processing consists of the following four steps:

1) *Signaling* : The purpose of the signaling protocol is to create and manage connections or calls between endpoints. H.323 and the session initiation protocol (SIP) are two widely used signaling standards for call setup and management.

2) *Encoding and Transport:* Once a connection is setup, voice must be transmitted by converting the voice into digitized form, then segmenting the voice signal into a stream of packets. The first step in this process is converting analog voice signals to digital, using an analog-to-digital converter. Here a compression algorithm can be used to reduce the volume of data to be transmitted. Next, voice samples are inserted into data packets to be carried on the Internet using typically the real-time transport protocol (RTP). RTP packets have header fields that hold data needed to correctly reassemble the packets into a voice signal on the other end. Lastly, the encapsulated voice packets are carried as payload by the user datagram protocol (UDP) for ordinary data transmission. At the other end, the process is reversed: the packets are disassembled and put into the proper order, and then the digitized voice is processed by a digital-to-analog converter to render it into analog signals for the called party's handset speaker. Fig. 1(b) illustrates the basic flow of voice data in a VoIP system.

3) *Gateway Control:* The IP network itself must then ensure that the real-time conversation is transported across the telephony system to be converted by a gateway to another format—either for interoperationwith a different IP-based multimedia scheme or because the call is being placed onto the PSTN.

III. REVIEWING VOIP SECURITY

A. *Voip Protocols*

Voice-over Internet Protocol (VoIP) communications are supported by a complex environment of standards. Transmission Control Protocol/Internet Protocol (TCP/IP) is involved in the transport of communication, and other critical protocols are involved in the voice aspects of the communications. A number of protocols should be considered when reviewing the security of a VoIP network

1) *H.323* - It is a recommendation from the ITU Telecommunication Standardization Sector (ITU-T) that defines the protocols to provide audio-visual communication sessions on any packet network. The H.323 standard addresses call signaling and control, multimedia transport and control, and bandwidth control for point-to-point and multi-point conferences.

a) H.225.0 - The main objective of H.225.0 is the definition of messages and procedures for:

Call Signaling: establish, control and end an H.323 call. The call signaling of H.225.0 is based on the call setup procedures for ISDN, Recommendation Q.931.

RAS Signaling Function: perform registration, admission, bandwidth changes, status and disengage procedures between endpoints and an H.323 Gatekeeper. The RAS signaling function uses a separate channel (RAS channel). This set of messages is called Registration, Admission and Status (RAS).

b) H.245-control protocol for multimedia communication, which describes the messages and procedures used for capability exchange, opening and closing logical channels for audio, video and data, control and indications.

c) Real-time Transport Protocol (RTP) - defines a standardized packet format for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications and web-based push-to-talk features.RTP is used in conjunction with the RTP Control Protocol (RTCP). While RTP carries the media streams (e.g., audio and video), RTCP is used to monitor transmission statistics and quality of service (QoS) and aids synchronization of multiple streams. When both protocols are used in conjunction, RTP is originated and received on even port numbers and the associated RTCP communication uses the next higher odd port number

d) H.235 – It covers security and encryption for H.323 and other H.245 based terminals

2) *Session Initiation Protocol (SIP)*—Created by the Internet Engineering Task Force (IETF) and used for initiating a two- way communication, SIP is text-based and simplifies communications. It is an application-level protocol that exists independently from the protocol layer[2]. The Internet Society's request for comments (RFC) 3261 describes the security features on SIP, including the use of PGP encryption. SIP can be protected using S/MIME, Transport Layer Security (TLS), IPSec, and SIP Authenticated Identity Body (AIB)[3]. One feature common to the different standards used is that the signaling and the actual real-time data are transmitted via different channels across the same network. Additionally, the same network is used to transport a number of other communications and sessions, shared with corporate function such as e-mail, web browsing and file access.

B. VOIP Infrastructure Risks

The VoIP network inherits all the vulnerabilities linked with the underlying data network; it also shares the problems with the data network. A *denial-of-service* (DoS) [3]attack is a typical example of this situation, as any excessive load on the data network affects the VoIP service. Attackers may use a data network attack to cause failures on the VoIP network. The operating systems of all elements within the VoIP network must be hardened to avoid security incidents; regardless of the function, intruders may be able to exploit security problems on the components. VoIP networks share some vulnerability with conventional phone systems. Intruders may be able to exploit vulnerabilities leading to toll fraud. This is a common situation within voice networks and causes significant economic losses.

IP phones also pose a significant risk to internal security. Intruders may be able to exploit vulnerabilities on the IP phones, using them as a platform for attacking the corporate network, capturing information, exploiting other systems or causing a distributed denial-of-service (DDoS)[3] attack against the local network.

C. SIP Vulnerabilities

- *Hijack registration*—This type of attack is based on the lack of any security mechanism that ensures the validity of SIP requests[4]. Intruders are able to impersonate the originator and deregister or add information into the communication exchange.
- *Impersonation of server*—Attackers can impersonate the remote server in some communications, including the user agent request. Intruders can embed their own information into the communication path and appear as the valid destination or participant on communications.
- *Message body exploitation*—Intruders may be able to change the payload on the message body; this can be used to modify session keys and content exchanges[4]. Intruders may be able to use this attack to capture sessions or eavesdrop on a communication exchange.

D. Risk To VOIP Service

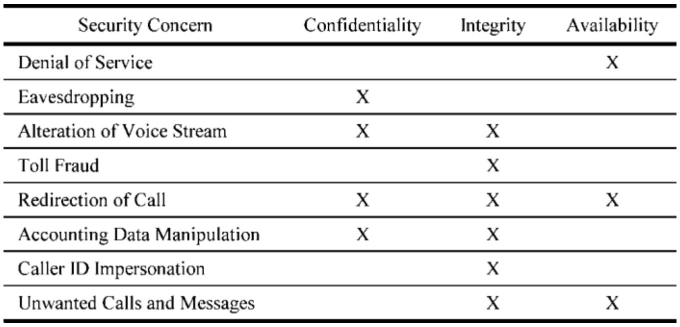
There are a number of risks specific to the VoIP environment, including the following:

- *IP phone hijacking*—Intruders may be able to take control of the IP phone and change the configuration parameters, including modifying the greeting and call-forwarding configuration.
- *Modification of accounting data*—Intruders may be able to manipulate the data used to control accounting functions, charging calls to a different phone or even eliminating the charges completely. This type of attack would seriously compromise the integrity of the VoIP environment.
- *Phone-based DDoS*—Intruders may use all the IP phones within a corporate network to launch a DDoS or phishing attack using a recording and dialing hundreds of numbers to try and play a message or to clog the lines of a victim[5]. Thousands of simultaneous calls may bring down the victim's phone system.
- *Change caller ID*—Intruders may be able to modify the caller ID records to impersonate valid users
- *Identity theft*—Intruders may exploit vulnerabilities on the VoIP environment to impersonate a user, redirect calls to a secondary phone and gather information to support the identity theft process.
- *Session hijacking*—Intruders may be able to hijack an ongoing call and redirect it to a different end point.

This can also be used for intercepting or monitoring the calls[5].

- *Insertion of content*—Intruders can exploit weaknesses on the communication when in cleartext, and insert data into the stream including the contents of a .wav file.

TABLE I
OVERVIEW OF SECURITY CONCERNS AND IMPACTS IN A VOIP SYSTEM



Security Concern	Confidentiality	Integrity	Availability
Denial of Service			X
Eavesdropping	X		
Alteration of Voice Stream	X	X	
Toll Fraud		X	
Redirection of Call	X	X	X
Accounting Data Manipulation	X	X	
Caller ID Impersonation		X	
Unwanted Calls and Messages		X	X

IV. PRIMARY GOALS OF VOIP SECURITY

The commercial objectives of any commercial network that impact on security are to ensure profitabil-ity of the network, availability of the network and customer confidence. This is to be realized by addressing the following technical issues.These commercial objectives break down to the following technical security issues for VoIP; charging fraud, protection of privacy, and ensuring availability of the VoIP services[6]. The goals for VoIP should therefore aim to reduce these risks by reducing the ability to mount these attacks and to limit their impact.We therefore define the following technical objectives for VoIP Security:

- *Prevention of masquerade*. This means being able to determine that a user claiming to be Alice is always Alice, Bob is always Bob, and Bob cannot pretend to be Alice, and this applies to both mas- querade of the user and of the system or service.
- *Ensure availability of the VoIP services*. By this we mean that the service must be accessible and usable on demand by an authorised entity. This is crucial for e.g. emergency services. In general, a user expects to be able to place a call and complete the call without being cut off in the middle.
- *Maintain privacy of communication*. In many cases, the parties to a call communicate across public networks, and mechanisms must be in place to prevent eavesdropping [7]. Furthermore, the only delivery points for communication have to be the legitimate parties to the call.

V. COUNTER MEASURES WITHIN VOIP

Some of the general countermeasures required for the VoIP network are:

- *Physical security*—This applies to the network, data center , hardware and equipment used for the VoIP service.
- *Encryption of traffic*—The VoIP traffic must be encrypted to avoid unauthorized access to the calls and modification of contents and session information.
- *Segmentation*—The critical VoIP components must be added to a dedicated virtual local area network (VLAN) where additional controls can be deployed, including VoIP-aware firewalls and intrusion detection system (IDS)/intrusion prevention system (IPS) protections.
- *Duplicate TCP/IP services*—In case of Dynamic Host Configuration Protocol (DHCP), [6]Domain Name System (DNS) and other shared resources, it is useful to have separate servers for the VoIP and data networks. This will be useful in case of simple DoS attacks targeting the service on one of the two networks.
- *Filter traffic*—VoIP-aware firewalls should be deployed, and the switches and routers should be configured to filter unauthorized traffic. In an ideal configuration mode, the network must be able to allow only expected traffic on the specific VLAN where needed and between the valid elements. SIP traffic on the data network may not be allowed, and DHCP requests between IP phones must be blocked. Only valid protocols should be allowed, filtering out unnecessary protocols.
- *Hardening*—All operating systems and applications must be hardened following best practices and vendor recommendations.
- *Separation of traffic*—The VoIP and data traffic must run on separate VLANs[7]. This will provide an initial protection to attacks within the two services and will create a virtual separation between the two.
- *Deployment of application-aware filters*—These can be used to identify the type of calls being made, restrict fax/data traffic on VoIP lines, block outbound international traffic, block calls on lines that are not allocated to employees, log caller activities and provide additional filtering capabilities.

VI. CONCLUSION

VoIP networks have a number of inherent security vulnerabilities that can be easily exploited by intruders. The number of VoIP networks is growing constantly, thus increasing the possibility of VoIP elements becoming a prime target for large-scale attacks. Additionally, the maturity of exploit tools and complexity of attacks is continually changing, allowing intruders to cause more damage with less resources and time[4].

However, it is possible to have a safe VoIP environment. This is achieved by ensuring that all elements are properly hardened, communications are filtered, and VoIP-aware elements are used for filtering and analyzing communications between different networks. VoIP services can be protected and they can converge with data networks[3]; however, security must be considered while designing and deploying the service.

VII. FUTURE WORK

The purpose of this paper is to give a brief overview of the area of VoIP security. This paper is by no means exhaustive it presents just a few directions of research in the area of VoIP security and tries to figure out some existing problems in this area. Based on the discussion of the challenges and requirements on VoIP in this paper, in our view, future efforts regarding securing VoIP systems should focus on two essential areas, summarized as follows. First, a great deal of research is still needed to strengthen security mechanisms and services to support VoIP at different system levels. Technologies to handle attacks aiming at specific VoIP protocols such as SIP and RTP and various components should be given priority including those handling the connection between traditional and VoIP networks. An integrated approach to securing a VoIP system including security mechanisms to secure both the application layer as well as the underlying IP data network can provide a more robust solution. Second, management of security standards and products specific to VoIP and integrating these tightly with IP data network security standards and products will provide an overall solution to securing enterprise data. Although we have witnessed development of standards for VoIP protocols and services, security management of VoIP systems requires continued evolution of these services and protocols to tighten security. Just like IPSec to VPN networks, protocols such as secure RTP are finding their way into VoIP solutions and will continue to be adopted as more individuals and organizations depend on VoIP for their critical communication needs.

REFERENCES

[1] Elhalifa Coulibaly; Lian Hao Liu; “Security of VoIP network”

[2] Judith E. Y.; Rossebo; Paul Siiben; “Security issues in Voip

[3] Henning, T.; A. Resetko; “Security in Voice-over IP Networks,”Alcatel-Lucent, 2006

[4] Ransome, James F.; John W. Rittinghouse; VoIP Security,Elsevier, 2005

[5] Greg Hoglund and Gary McGraw – Exploiting Software : How to break code. Addison-Wesley, August 2004

[6] John Viega and Gary McGraw – Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley, September 2002

[7] Yves Younan – An overview of common programming security vulnerabilities and possible solutions. Vrije Universiteit Brussel, Agust 2003

[8] David Butcher,*;* Xiangyang Li*;* Jinhua Guo,- *Security Challenges and considerations in Voip*