

# White Paper

## SECURITY IN VoIP NETWORKS

Version 1  
March 2006



# SECURITY IN VoIP NETWORKS

## White Paper

---

### Table of Contents

Introduction..... 3

Securing the Media Stream ..... 5

Securing the Signaling & Control Transport ..... 5

Securing the Network Management Plane ..... 5

Interface Separation ..... 6

Traversing a Secured Network ..... 6

Call Restriction and Filtering..... 6

Denial of Service Protection ..... 7

Summary ..... 7

About AudioCodes ..... 7

Disclaimer..... 8

### Table of Figures

Figure 1: Figure 1..... 4

Figure 2: Securing the Media Stream ..... 5

Figure 3: Securing the Signaling and Control Transport ..... 5

Figure 4: Securing the Network Management Plane..... 5

Figure 5: Interface Separation ..... 6

Figure 6: Traversing a Secured Network ..... 6

## Introduction

### Security in VoIP Networks

*The move from TDM networks to VoIP has created a new challenge for network operators – security. Unlike in a TDM world, where the telephony network was practically isolated from the data network and the internet – most VoIP networks have a number of interface points with the data network, and with the dangers in the internet world. A poorly designed VoIP network can easily be exposed to security threats like denial of service attacks, computer viruses and eavesdropping. On the other hand, the technologies available today, in addition to a well designed network, can offer a greater level of security.*

Security is not a new concept for telephony managers. Telephony networks were always exposed to security threats like eavesdropping, impersonation, fraud and denial of service – similar to data networks.

Moving away from a separated, dedicated TDM network to the well known, widely used IP network has exposed the telephony networks to a growing number of hackers, originating from the data world.

In the aged TDM telephony world, hacking was only an interest to a small number of individuals. These individuals had to break into PBX systems and application servers specifically designed for telephony services only, using proprietary protocols, which were not connected to the internet.

Alternatively, many telephony networks today are based on the well known IP protocol, using well known, Windows, Linux or Unix based call manager and application servers, and could be directly connected to the internet.

Taking these factors into account, it seems that VoIP networks are inherently more vulnerable than TDM voice networks. That assumption is true, for a badly designed, unsecured VoIP network. But, if you design and secure the VoIP network the correct way, you can actually build a VoIP network that is at least as secured as the typical TDM telephony network. Securing a VoIP using standard based protocols and features is far easier and cost effective than securing a TDM telephony network, assuming the right VoIP equipment is being used.

Observing the differences between VoIP networks and TDM telephony networks, a number of security threats exist that need to be addressed:

- Eavesdropping – the ability to listen to another party’s phone conversation without authorization
- Impersonation – the ability to impersonate someone else and to have a phone call with the other party
- Fraud (Call theft) – have a call on the network without paying
- Local denial of service – the ability to block phone calls from or to a specific location out to the network
- Network denial of service – the ability to bring down the network or large portions of a telephony network

A Typical VoIP network will include a number of key components. In order to fully secure the VoIP network, all communications between these components need to be secured. Those key components include:

- Call Control Server / Soft Switch
- IP-PBX
- IP Phones

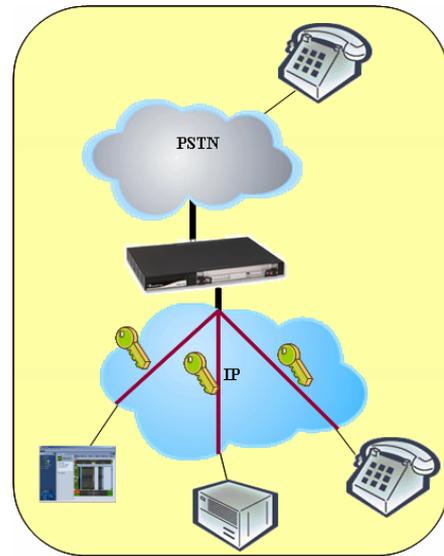
- Media Gateways
- Application Servers
- Media Servers
- Network Management Servers

One of the native features of the VoIP network is the complete separation of the call control traffic, the media streams, and the management traffic. Each has its own protocols and can actually take a different route in the IP network. Each of these protocols must be secured in order to create a fully secured network. These protocols include:

- Media Stream (RTP)
- Call Control Protocols (H.323, SIP, MGCP, MEGACO, etc.)
- Network Management (SNMP, Telnet, RADIUS, HTTP, FTP, TFTP, etc.)

In addition to these special requirements for VoIP networks, any VoIP stream must be able to traverse the existing IP network, allowing end-to-end connectivity transparently, traversing security-related elements and mechanisms such as Session Border Controllers (SBCs), NAT devices, firewalls, etc.

Like in TDM telephony networks, and especially in enterprise VoIP implementations, not all users are allowed to call ubiquitously. This is a further security element that should not be neglected implementing VoIP networks. Call restriction and call filtering are important mechanisms that should be implemented in any VoIP network.



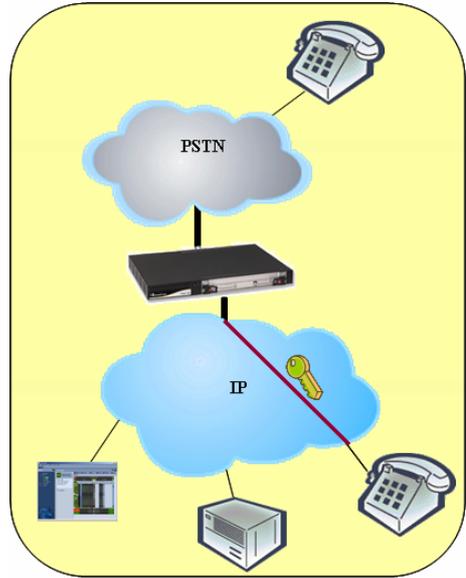
## Securing the Media Stream

The voice stream in VoIP networks is a peer-to-peer communications connection between the end points of the VoIP call. These end points can be IP-phones, soft-phones or media gateways connected to analog phones, PBX and PSTN Switches. In order to achieve maximum protection against eavesdropping, the encryption must be performed in the edge device (IP phone / Media Gateway) and not in the network (IP-SEC tunnels between routers). IPSec tunnels between routers encrypt (in most cases) only the WAN portion of the connection. This allows eavesdropping to clear-channel voice packets between the phone and the router.

RTP is the most commonly used protocol for VoIP media streams. According to RFC 3711, secured RTP (SRTP) is used to encrypt RTP and RTCP transport. This function is widely supported across AudioCodes' media gateway platforms.

In PacketCable based VoIP over Cable core networks, media encryption is conducted by using IPSec in ESP mode.

In both cases, the encryption algorithm being used is AES 128, for maximum level security. Implementing this option into AudioCodes' Media Gateways and Blades, results in minimum affect on the media gateway channel capacity.



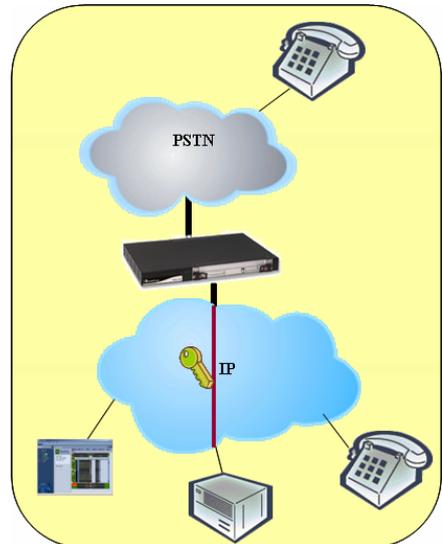
## Securing the Signaling & Control Transport

Unlike the media streaming, where one dominant protocol (RTP) is widely used in a VoIP network, currently many signaling and control protocols are used in parallel across VoIP networks.

H.323 and SIP enable direct or indirect call signaling, while MGCP and MEGACO (H.248) are used for CallServer / SoftSwitch to Media Gateway Control.

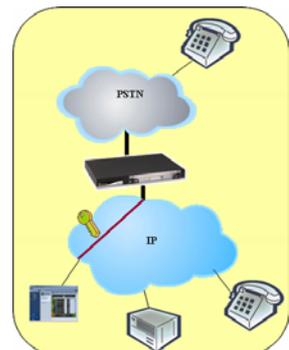
Each of these protocols has its own method of security. AudioCodes, focuses on interoperability and flexibility of its products, supports all required protocols to secure all types of signaling and control protocols:

- H.323: H.235 Annex D based security
- SIP: SIP/TLS, SIPS (Secured SIP) & MD5 Authentication
- MGCP / MEGACO: MGCP/MEGACO over IPSec with IKE pre-shared keys



## Securing the Network Management Plane

VoIP network management, like any service management across IP networks, involves many protocols and systems running in parallel. These protocols are extremely sensitive to security threats. Implementing security in the management plane must include the protection of all management-related protocols and systems in the network. The following table outlines the different management-related protocols supported across AudioCodes' EMS, Media Gateways, Media Servers and Blades their use in the network and the supported way to secure them.



<i>Management Task</i>	<i>Peers</i>	<i>Protocol</i>	<i>Secured Protocol</i>
<b>Configuration and Monitoring</b>	Management Station & Media Gateway	SNMP	SNMP over IPSec
<b>Remote Terminal</b>	Remote Terminal & Media Gateway	Telnet	Telnet over SSL / SSH
<b>Web Console</b>	Remote Browser & Media Gateway	HTTP	HTTPS
<b>File Transfer</b>	Remote File Server & Media Gateway	FTP	SFTP
<b>Management User Authentication</b>	Web / Telnet User & Authentication Server		RADIUS

## Interface Separation

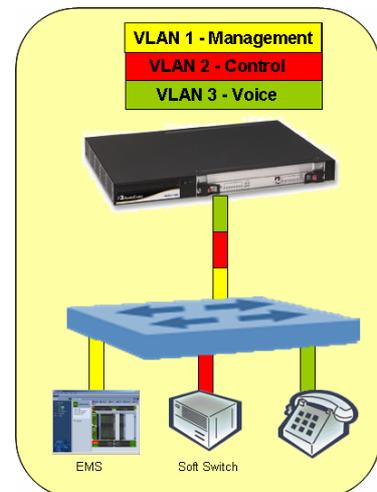
The logical separation between the media streams, the signaling & control protocols and the network management protocols in VoIP networks allows new ways of network configuration.

AudioCodes' Media Gateways, Media Servers and Blades support interface separation between the different types of transport.

In the case of low density Media Gateways, this support is achieved using 802.1Q based VLAN tagging. A different VLAN and a different subnet can be used for each type of transport.

In the case of the carrier grade, high density Media Gateways and Media Servers, physical interface separation is also supported. The various types of transport can run on different physical interfaces, dissimilar VLANs on contrasting interfaces, and different VLANs on the same interface (or interface bundle using 802.3ad Trunking) or the same interface.

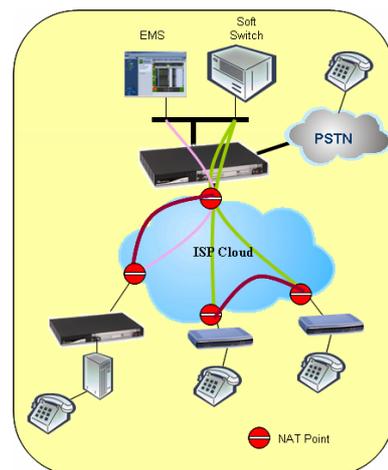
Using the above functionality, a more secure network can be built, separating the management and control traffic from the users' traffic, protecting them from malicious network attacks.



## Traversing a Secured Network

Today's VoIP networks run on very complicated IP networks. For scalability and security reasons, many of these networks implement features like NAT (Network Address Translation), and security network devices such as firewalls and SBCs (Session Border Controllers).

The traversal of call control, media streams and network management protocols on top of these networks is not transparent. AudioCodes widely supports features such as NAT Traversal (STUN) and interoperability tests with leading firewalls and Session Border Controllers, in order to allow easy implementation of VoIP over secured networks.



## Call Restriction and Filtering

The combination of Call Control Servers and Media Gateways in VoIP networks is replacing legacy TDM switches and PBXs. As in TDM telephony networks, not all users are permitted to call everywhere. AudioCodes supports PBX like telephony functions of its Media Gateways. The Media Gateways allow flexible configuration of call restriction and call filtering rules, enabling full control and security over the organization dialing plans and policies. These policies can be applied at the IP level or at the dialing plan level.

## Denial of Service Protection

Another layer of security of the VoIP network control plane involves the use of denial of service protection mechanisms. In order to limit the source and type of communication allowed with the AudioCodes Media Gateways, Media Servers and Blades, a network firewall function is integrally supported in the products. This firewall function provides the following features:

- Block traffic from known malicious sources
- Only allow traffic from known friendly sources, and block all others
- Mix allowed and blocked network sources
- Limit traffic to a predefined rate (blocking the excess)
- Limit traffic to specific protocols, and specific port ranges on the device

Apart from the aforementioned, the AudioCodes Media Gateways are protected against malicious Denial of Service (DoS) attacks which include:

- SYN floods - sending huge number of TCP SYN packets.
- Jolt (pings to death) - sending huge fragment Ping packet (64KB) when each fragment is very "small" (less than 100 bytes) to create a "shortcut" for receive network buffers.
- Ping floods - sending more than 1K PING packets per second
- Land attack - sending packets with the board network address (MAC/IP) as the source.

## Summary

AudioCodes is well positioned to supply the Media Gateway and Media Server products required to build secured VoIP networks. Its wide range of products supports the required protocols and features to secure all aspects of VoIP communications.

## About AudioCodes

AudioCodes Ltd. (NASDAQ: AUDC) enables the new voice infrastructure by providing innovative, reliable and cost-effective Voice over Packet technology and Voice Network products to OEMs, network equipment providers and system integrators. AudioCodes provides its customers and partners with a diverse range of flexible, comprehensive media gateway and media processing technologies, based on VoIPerfect™ – AudioCodes' underlying, best-of-breed, core media gateway architecture. The company is a market leader in voice compression technology and is a key originator of the ITU G.723.1 standard for the emerging Voice over IP market. AudioCodes' voice network products feature media gateway and media server platforms for packet-based applications in the converged, wireline, wireless, broadband access, and enhanced voice services markets. AudioCodes enabling technology products include VoIP and CTI communication boards, VoIP media gateway processors and modules, and CPE devices. AudioCodes' headquarters and R&D facilities are located in Israel with an R&D extension in the U.S. Other AudioCodes' offices are located in Europe, the Far East, and Latin America.

### International Headquarters

1 Hayarden Street, Airport City  
Lod, Israel 70151  
Tel: +972-3-976-4000  
Fax: +972-3-976-4040

### US Headquarters

2099 Gateway Place, Suite 500  
San Jose, CA 95110  
Tel: +1-408-441-1175  
Fax: +1-408-451-9520

[info@audiocodes.com](mailto:info@audiocodes.com)  
[www.audiocodes.com](http://www.audiocodes.com)

**Disclaimer**

© 2006 AudioCodes Ltd. All rights reserved. AC, Ardito, AudioCodes, AudioCodes logo, AudioCoded, IPmedia, Mediant, MediaPack, MP-MLQ, NetCoder, Stretto, TrunkPack, VoicePacketizer and VoIPerfect are trademarks or registered trademarks of AudioCodes Ltd. All other marks are the property of their respective owners. The information and specifications in this document and the product(s) are subject to change without notice.

**Ref. #** LTRM-80013 V.1 03/06

**Notice**

The information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and changes in the business environment, AudioCodes does not assume any obligation to update or correct any information and does not guarantee or assume liability for the accuracy of the printed material nor can it accept responsibility for errors or omissions. Original Date Published: March 2006