Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 1, Number 8; October, 2014 pp. 13-16

http://www.krishisanskriti.org/jbaer.html

A Survey of Security Protocols on VoIP

Deepak Tuteja[1], Dhruv Jain[2], Diksha Goyal[3], Divya Sharma[4]

[1, 2, 3]ITM University, Gurgaon
[4]ITM University, Sector-23A, Gurgaon, India

Abstract: **Media correspondence has influenced different parts of individuals' life. So, various models, corresponding to engineering and systems of media from diverse merchants are developing quickly. Voice over Internet Protocol (VoIP) is a type of voice correspondence that uses sound information to transmit voice indicators to the end client. VoIP is a standout amongst the most essential advances in the World of correspondence. Around, 20 years of research on VoIP, a few issues of VoIP are still remaining .In this paper the security conventions connected with VoIP have been examined.**

1. INTRODUCTION

[1]VoIP is a method for taking analog signals and turning them to digital data that can be transmitted over the internet. It is a way to place free phone calls. While voice is a key aspect in VoIP, video and other capabilities are supported. The key VoIP providers include Vonage and AT&T (already setting up VoIP calling plans). VoIP uses packet switching to provide phone services. Packet switching allows several calls to occupy same amount of space which is occupied by only one call in circuit switched networks. Phone companies use VoIP to streamline networks i.e. routing thousands of calls through a circuit switch and then into an IP gateway. This helps them reduce the bandwidth they might be using currently.

[2] VoIP is employed in the public sphere is through VoIP Internet phone service. Skype and Google Talk are both platforms for free Internet phone service. Online real-time gaming uses VoIP technology to allow players to communicate directly with each other as they play. In online role playing games, gamers can build teams with other gamers. These teams can be fairly large, and can be composed of gamers living all over the world. VoIP is a very secure means of transferring voice data and many branches of the government and military use VoIP for their internal telephone services. Military phone correspondences have a percentage of the most elevated necessities for secure systems, and VoIP has remained up to these prerequisites.

2. PLACING A CALL IN VOIP

1. [3] ATA (Analog Telephone Adapter)

We simply connect a phone to an internet connection or a computer. The ATA acts as an analog to digital converter. It receives the analog signals from the phone and converts it to digital signals on the internet.

2. IP phones

IP phones use RJ-45 Ethernet connectors instead of the usual RJ-11 phone connectors. The IP phones are directly connected to our router. Corresponding hardware and software is used to handle the IP calls.

3. Computer to computer

Requirements for such communication are: speakers, microphone, sound card, software and internet connection. This is the easiest way to use VoIP irrespective of the distance.

3. CIRCUIT SWITCHING

At the point when a call is made between two gatherings, the association is kept up for the length of time of the call. Since 2 focuses are associated in the same bearing, the association is known as a circuit. Working: a dial tone demonstrates that one is associated with the nearby office of the phone transporter. In the wake of dialing the number, the call is steered through a switch at the neighborhood bearer to the gathering one is calling. A few switches are utilized along the best approach to associate the two gatherings. Somebody answers the call and opens the circuit. In the wake of hanging up the circuit is shut once more.

4. PACKET SWITCHING

While a discussion on a normal telephone call, just a large portion of the association is being used at a purpose of time since stand out gathering is talking and the other is tuning in. For seconds on end, not, one or the other party is talking. So the quiet interims could be evacuated to abbreviate the record size. In this way, as opposed to sending a constant stream of bytes, Packets could be sent.

The information system rate will be upgraded by basically sending and recovering information as we need it. This is bundle switching. The sending segment sends little parcels

wherein every parcel advises the systems administration gadgets where to send the parcel. Inside every bundle is a Payload (piece of messages, records to be transmitted).the parcel is sent to a close-by switch and overlooked by the sending part. The getting part gets the parcels and reassembles them.

A codec (coder+ decoder) turns an analog audio into packets for VoIP transmission. It converts an audio signal into compressed digital form for transmission and back into an uncompressed audio signal for replay. They sample the audio signal several thousand times per second.

The ATA sends a dial tone which signifies a connection to the internet. After a no. is dialed, the tone is converted into digital data and temporarily stored. The data is sent to VoIP Company's call processor to check its validity and then the phone no.is mapped to an IP address. A soft switch connects the 2devices on either end of the call. A signal is also sent to other's ATA. A session is established between the 2computers. A uniform protocol must be used by both systems to communicate. The packets are translated and converted into analog audio signals by the ATAs at each end. The session is terminated on hanging up.

5. RECENT STUDY

5.1 H.323

[4] H.323 is a recommended set of protocols for voice, video and data conferencing over the Internet. H.323 was designed to support real time transfer of audio and video over IP. The H.323 is maintained by International Telecommunication Union (ITU-T).

The H.323 protocol stack operates above the transport layer of the underlying network. It uses IP for internetwork conferencing.

H.323 specifies components, protocols and procedures for real time communication. In this heading, they should be Times 11-point boldface, initially capitalized, flush left, with one blank line before, and one after.

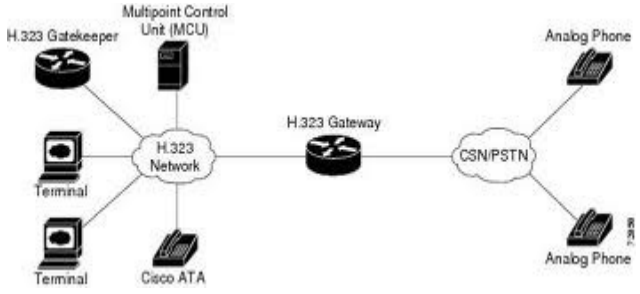

Fig. 1: Architecture of H. 323 and call through ATA

5.1.1 Architecture

Implementation of H.323 requires four logical entities. (Collectively known as end points). They are:

1. **Terminal -** The H.323 data streams and signaling originate and terminate at the terminal / client. It may be a multimedia PC or a standalone device such as a USB IP telephone. Audio communication must be supported by a terminal, video and data communication support is optional.

2. **Gateway-** (optional) when communication is required between different networks, a gateway is needed at the interface. e.g. A H.323 terminal is able to set up a conference with terminals based on other H.32X terminals through an appropriate gateway. A gateway provides data format translation, control signaling translation, audio and video codec translation and call setup, termination functionality on both sides of the network.

3. **Gatekeeper-** (optional) in order to ensure reliable, commercially feasible communications, gatekeepers are needed. Gatekeeper provides control services and manages network centrally and is hence referred to as the brain of the H.323 enabled network. It provides services such as :

   - Address Translation: Gatekeeper maintains a database for translation Admission and access control of endpoints: This control is based on bandwidth availability, number of calls.
   - Bandwidth Management: bandwidth can be managed by network administrators by specifying limitations on the no. of simultaneous calls.
   - Routing capability: all calls can be routed by a gatekeeper. In this way, accounting information of calls can be maintained for billing and security purposes. Secondly, calls can also be re-routed to an appropriate gateway based on bandwidth availability.

5.1.2 Security

[5]Recommendation H.235 specifies the security requirements for H.323 communications .Four security services provided are as follows;

1. Authentication- It is provided by admission control of endpoints. This is handled by the gatekeeper that handles the zone.
2. Integrity – Data Integrity is provided by encryption
3. Privacy- Privacy is also provided by encryption.
4. Non -Repudiation- it ensures that no endpoint can deny that it participated in a call. Gatekeeper services provide non repudiation.

To implement these security service H.235 can use existing standards such as IP security and transport layer security.

5.2 SIP (Session Initiation Protocol)

[4]It is an application layer protocol standardized by the Internet Engineering Task Force (IETF) and it is designed to support the setup of bidirectional communication sessions (including VoIP calls). It supports interaction with multiple network components.

- A proxy server, a registrar, a redirect server and a location server are the main entities in a SIP architecture. Endpoints communicate with a registrar to indicate their presence.
- The correspondence data is put away in the area server. Numerous endpoints might at the same time enlist a client. The endpoints correspond with the substitute server amid the call to focus the course of the call with the assistance of the area server. Instead a redirect server is utilized to figure out where a call ought to be administered to.
- After the foundation of an end to end channel, the SIP arranges the genuine session parameter

5.2.1 SIP Threat Classification

[6]Social threats: These are pointed straightforwardly against people. For example, misconfigurations, bugs or terrible convention between activities in VoIP frameworks may empower or encourage assaults that distort the personality of noxious gatherings to clients. Such assaults might then go about as venturing stones to further assaults, for example, phishing, burglary of administration, or undesirable contact (spam).

Eavesdropping, interception and modification threats: Covers situation where an adversary can unlawfully and without authorization from the parties concerned listen in on the signaling (call setup) or content of a VoIP session, and possibly modify aspects of that session while avoiding detection. Examples of such attacks include call re-routing and interception of unencrypted RTP sessions.

Denial of service threats: can possibly deny clients access to VoIP administrations. This may be especially tricky on account of crises, or when a Dos assault influences the majority of a client's or association's correspondence capacities (i.e., when all VoIP and information correspondences are multiplexed over the same system which could be focused through a Dos assault). Such assaults may be VoIP-specific (misusing flaws in the call setup or the execution of administrations). They might additionally include assaults with physical parts (e.g., physically separating or disjoining a link) or through figuring or different foundations (e.g., crippling the DNS server, or shutting down power)

Service abuse threats: Blankets the disgraceful utilization of VoIP administrations, particularly (yet not solely) in those circumstances where such administrations are offered in a business setting. Samples of such dangers incorporate toll extortion and charging evasion.

Physical access threats: refer to inappropriate/ unauthorized physical access to VoIP equipment, or to the physical layer of the network (following the ISO 7-layer network stack model).

Interruption of service threats: refer to non-intentional problems that may cause VoIP services to become unusable or inaccessible. Examples of such threats include loss of power due to inclement weather, resource exhaustion due to over subscription, and performance issues that degrade call quality.

5.2 Media Gateway Control Protocol (MGCP)

[7]The media gateway control protocol (MGCP) is a text based application layer protocol used for call setup and call control between the media gateway and the media gateway controller (MGC).

This protocol is based on master/slave call control architecture.

Call control intelligence is maintained by the media gateway controller and instructions from the call agent are carried by the media gateways. UDP is used to transmit both signaling packets and media packets.

Application Layer gateway (ALG)

ALG is a software component that is designed to manage specific protocols such as Session Initiation Protocol (SIP) or File Transfer Protocol (FTP) on J-series routers.

The MGCP ALG has following functions:

1. VoIP signaling payload inspection is conducted by the ALG. It inspects the payload of the incoming VoIP signaling packet based on proprietary standards. Any malformed packet attack is blocked by the ALG.

2. MGCP signaling payload inspection is conducted by the ALG. It inspects the payload of the incoming MGCP signaling packet in accordance with RFC 3435. Any malformed packet attack is blocked by the ALG.

3. Stateful processing is provided .the corresponding VOIP based state machines are invoked to process the parsed information. Any out-of-state or out-of-transaction packet is identified and properly handled.

4. All IP address and port information in the payload is properly translated based on the network topology and

existing routing information. It is then replaced with the translated IP address and port number, if necessary. There are 4 basic entities in MGCP:

- Endpoint: a media gateway is a collection of endpoints. An analog link, a trunk, or any other access point can be considered an endpoint.
- Connection: a media gateway creates connections during call setup. VOIP call involves two connections. A three party call or conference call requires more connections. Media gateways can create, modify, delete and audit a connection.
- A connection ID (created by the Media gateway when requested) identifies a connection. Connection ID is presented as a hexadecimal string with maximum length of 32 characters.
- Call: a call ID identifies a call, which is created by the MGC when establishing a new call. Call ID is presented as a hexadecimal string with maximum length of 32 characters. Two or more connections can have the same call ID if they belong to the same call
- Call agent: MGCP supports one or more call agents to enhance reliability in the VOIP network. The notified entity for an endpoint is the call agent currently controlling that endpoint. An endpoint should send any MGCP command to its notified entity. Different call agents might send MGCP commands to this endpoint.

5.3.1. MGCP Security

MGCP ALG has the following security features:

1. Denial of service (DoS) attack protection – a stateful inspection at the UDP packet level, transaction level and call level is performed. MGCP packets matching the RFC 3435 message format, transaction state and call state are processed. All other messages are dropped.
2. Enforcement of security policy between gateway and gateway controller (signaling policy).
3. Enforcement of security policy between gateways (media policy).
4. Per- gateway MGCP message flooding control.it makes sure that any hacked / malfunctioning gateway does not disrupt the whole VOIP network.
5. Per- gateway MGCP connection flooding control.

6. COMPARISON

H.323	SIP	MGCP
Mature	**Not as mature as H.323**	**Not as mature as H.323**
Uses abstract syntax notation for call control messages	Uses clear text for call control.	Uses clear text for call control.
Uses a peer-to-peer model	Uses a peer to peer model	Uses a client server model
Call reservation for SRST on PRIs	Allows interoperability between vendor equipment	Ideally positioned for service providers (Centrally located call agents).

REFERENCES

[1] http://www.cs.columbia.edu/~angelos/Papers/2011/cst.pdf, A Comprehensive Survey of Voice over IP Security Research, Angelos D. Keromytis

[2] H. Abdelnur, R. State, and O. Festor, “KiF: A stateful SIP Fuzzer, ” in Proceedings of the 1st International Conference on Principles, Systems and Applications of IP Telecommunications, pp. 47–56, July 2007

[3] J. Bilien, E. Eliasson, J. Orrblad, and J.-O. Vatn, “Secure VoIP: Call Establishment and Media Protection, ” in Proceedings of the 2nd Workshop on Securing Voice over IP, June 2005.

[4] H. Abdelnur, V. Cridlig, R. State, O. Festor, and J. Bourdellon, “VoIP Security Assessment: Methods and Tools, ” in Proceedings of the 1st IEEE Workshop on VoIP Management and Security (VoIP MASe), pp. 29–34, April 2006.

[5] P. Truong, D. Nieh, and M. Moh, “Specification-based Intrusion Detection for H.323-based Voice over IP, ” in Proceedings of the IEEE International Symposium on Signal Processing and Information Technology, December 2005.

[6] S. Salsano, L. Veltri, and D. Papalilo, “SIP Security Issues: The SIP Authentication Procedure and its Processing Load, ” IEEE Network, vol.16, pp. 38–44, November/December 2002.

[7] Media Gateway Control Protocol (MGCP) Version 1.0 RFC 2705, IETF, http://www.ietf.org/rfc/rfc2705.txt?number=2705