VoIP techniques

A. Mentsiev, Kh. Supaeva

Chechen State University, Grozny

Abstract: As with any other technological advancement in use in today's age, security threats are proving to be the major challenges and risks. Knowledge about these security vulnerabilities presents an avenue of protecting organizational assets against virtual attacks. VoIP phone systems are becoming increasingly popular in today's society for business and personal purposes. VoIP services are increasingly productive and cheap, thereby, providing adopters a competitive edge. The paper explores a brief overview of VoIP techniques including network components, structure, standards and protocols, data processing techniques and quality of service.

Keywords: VoIP, VoIP components, VoIP structure, Cybercrime, Computer security.

I. VoIP overview

Voice over Internet Protocol or IP telephony refers to the routing of voice communications over the internet or an IP-based network. The voice data flows over a generalized packet-switched network in contrast with the traditional dedicated circuit-switched voice transmission lines.

VoIP are increasingly adopted due to its beneficial factors, Toll bypass, network consolidation and service emergence are some of the beneficial merits it accords users. Million worth of resources have been saved for large organizations replacing traditional telephone systems for long distance calls with IP network-based solutions. Network consolidation has enables the transmission of data, voice, and video signals over a single network, thereby reducing initial set up costs and maintenance. Different multimedia services coupled together has resulted in enhanced functionalities. According to telecommunication devices and service firm, Juniper, the rapid growth in the adoption of VoIP globally accounted for over $ 18 billion in revenues in 2010 and is expected to increase exponentially [1].

In spite of this, security for VoIP is more challenging and difficult to implement than conventional data networks. This is because all the problems associated with data networks are replicated in VoIP systems due to the same service infrastructure. Further, the lack of dominant standards in VoIP compounds the problem. The support of two standards in products elevates the chances of insecure applications. Finally, the most challenging reality emanates from Quality of Service requirements in VoIP that sacrifices security and vice versa. Security and privacy in VoIP systems has been the core consideration for device manufacturers at the expense of other essential requirements such as return on investment and convenience. Putting security and privacy in the context of VoIP systems has seen the adoption of three models.

A. Basic multiparty freedom model applicable to any public communication system.

B. B. Basic privacy-based model and a social responsibility model founded on acceptable principles under civil and common laws [2][3].

Together, these models have provided the foundation for balancing between security and privacy in VoIP equipment and service design.

Before we dealt in security issue in VoIP, a basic understanding of operational techniques is inevitable. VoIP is a widely deployed technology implemented in the market yet it is far from maturity. Currently, there is no dormant and unanimous protocol standard in the market. With varied protocols and standards such as Signaling Connection Control Part (Cisco), H.323 (Avaya), Unified Network Stimulus (Nortel), Session Initiation Protocol, and Remote Voice Protocol Over IP Specification, there is no coherent standard to be followed. This makes product inter-connection between different players difficult [4].

II. Components of VoIP systems

VoIP network architecture is a set of network gateways which are interconnected and constituting a telephone network. VoIP framework characterizes some system components that cooperate keeping in mind the end goal to convey rich interactive media correspondence proficiencies. Those components are Terminals, Multipoint Control Units (MCU), Gateways, and

Gatekeepers. They provide the interface and encode, compress and transmit data packets. Operation of interaction between all gateways performs the gatekeeper. For ease of management and administration of the network there can be used a Multipoint Control Unit (MCU). All these components from different manufacturers can be called quite differently, but they all perform similar functions listed below. In addition to these functions and requirements, VoIP equipment must support a number of specific features [5]

Gateway is binding device simultaneously connected to the IP network and the telephone network. There can be of two types of networks: PBX and PSTN. First network is a network of office or institution, and the second - the general telephone network which is accessible to everyone. It allows the transmission of voice traffic from the circuit switched network for packet-switched networks. The main functionality of the gateway is to convert the voice information or the fax signal received from the PSTN to a digital form suitable for transmission over the IP network and the inverse conversion for transmission to the telephone network. In addition, the gateway acts as a user interface, responding to the calls of the caller and establishing connection with the callee.

Gateways from different manufacturers have different hardware and software implementation, connection method, capacity, interface and other features, but they all perform the above functions, and are the basis of IP-telephony.

Gatekeeper is an independent logical unit that specifies the algorithm of IP-telephony network, managing terminals and gateways. Gatekeeper is needed in any IP-telephony network comprising more than two gateways. Functionality of gatekeeper is authentication and authorization of client, distribution of calls and management of gateways interaction, as well as support the work of billing systems.

Multipoint Control Units provide support for conferences of three or more H.323 terminals. All terminals participating in the conference establish a connection with the MCU. MCU manages conference resources, negotiates between terminals used to determine the audio or video codec, and can control the audio streams [6]

The figure below illustrates the major component of VoIP. The gateway converts signal from the conventional telephony interface to VoIP. There are two gateway types in the market; VoIP gateways and VoIP GSM gateways. VoIP gateways provide a link between the conventional telephone networks and equipment to VoIP telephone networks. VoIP GSM gateways enables direct routing between GSM networks, analog, IP or digital networks [5]

The server manages the routing and administrative support processes across the network. For instance, in a system based on H.323, the server is referred as the gatekeeper. IP network provides the connectivity between all the terminals be it private, intranet, or internet. The end user equipment's terminals give native support for VoIP and can directly connect to an IP network [7]

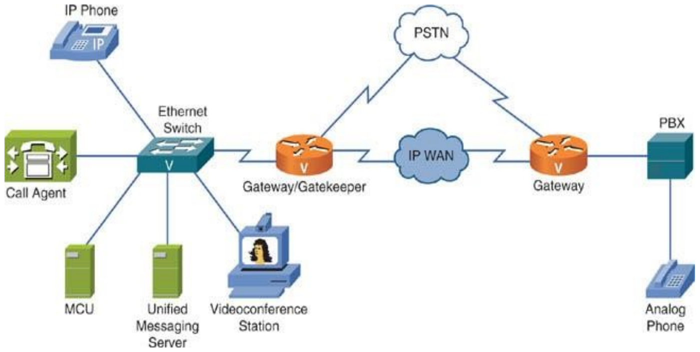

Figure 1. VoIP components

End user equipment's are classified as softphone, conventional phone adapters, and IP phones. Softphone refers to a setup or PC with a headset, software and cheap connection service. A PC can serve as a softphone while some client software such as Skype, Microsoft Net meeting, and SIP-set can also qualify.

Conventional telephone adapters are characterized by a single or more telephone jack and an Ethernet or USB adapter. They connect to a remote VoIP server with the help of analog or digital adapters. Examples include Cisco ATA 18X Analog IP Adapter, D-Link DVG-1402S and Nortel ATA-2 Enhanced Terminal Adapter [7][9].

References

1. Chinedum, Eze Elias, and Sijing Zhang. “Prevalent Network Threats and Telecommunication Security Challenges and Countermeasures in VoIP Networks.” Network and Complex Systems 3.2, 2013. pp. 1-7.

2. Coulibaly, Elhalifa, and Lian Hao Liu. “Security of Voip networks.” Computer Engineering and Technology (ICCET), 2010 2nd International Conference on. Vol. 3. IEEE, 2010. pp. 219-238.

3. Gallo Patrik, Dusan Levicky, and Gabriel Bugar. “Authentication threats in PSTN-VoIP architecture using multi-service gateways.” ELMAR, 2012 Proceedings. IEEE, 2012. pp. 153-156.

4. Hamdaqa Mohammad and Ladan Tahvildari. “ReLACK: a reliable VoIP steganography approach.” Secure Software Integration and Reliability Improvement (SSIRI), 2011 Fifth International Conference on. IEEE, 2011. pp. 189-197.

5. Hoffstadt Dirk, Alexander Marold, and Erwin P. Rathgeb. “Analysis of sip-based threats using a voip honeynet system.” Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012. pp. 541-548.

6. Jiang Hua, et al. “An identity-based security mechanism for P2P VoIP. “Wireless Communications, Networking and Information Security (WCNIS)”, 2010 IEEE International Conference on. IEEE, 2010. pp. 481-486.

7. Keromytis Angelos D. “Voice over IP: Risks, threats and vulnerabilities.” Cyber Infrastructure Protection, 2009. pp. 1-13.

8. Kevin Wallace, CCVP CVOICE Quick Reference, Cisco Press, 2008. 489 p.

9. Abramov E.S., Tarasov Y.V. Inženernyj vestnik Dona (Rus). 2017. №3. URL: ivdon.ru/ru/magazine/archive/n3y2017/4354

10. Mokhov V.A., Georgitsa I.V., Goncharov S.A. Inženernyj vestnik Dona (Rus). 2013. №3. URL: ivdon.ru/ru/magazine/archive/n3y2013/1852