International Journal of Advanced Research in Engineering Technology & Sciences ISSN: 2394-2819
April-2016 Volume 3, Issue-4
Email: editor@ijarets.org www.ijarets.org

Review on Techniques for Reduction of Noise over Internet Protocol

Deepika
M. Tech Scholar
Department of ECE
RIMT Rayat Bhahara Group
Chidana, Haryana

Parveen Khanchi
Assistant Professor
Department of ECE
RIMT Rayat Bhahara Group
Chidana, Haryana

ABSTRACT:
In recent years, there has been significant increase in VoIP and internet telephony usage. The users, whether corporate or individuals are subject to the same security risks that have affected data networks for many years This is mainly because voice networks are IP-based and all IP protocols for sending voice traffic contain flaws. In this paper, we study the security risks associated with the VoIP including vulnerabilities, man-in-the-middle attack, and denial-of-service. We will also review the protection measure that can be taken to make VoIP more secure, such as authorization, authentication, transport layer security, and media encryption.

KEYWORDS: VoIP, Noise Detection, Modulation Scheme

I. INTRODUCTION:

In recent years, the telecommunication industry has evolved tremendously that new services are introduced daily. The usage of new services, such as Voice over Internet Protocol (VoIP), has becomes widespread that it has transforms the ways human communicate. While the use of VoIP has-been improving human's life, there has been a great demand for high quality VoIP solution that is ableto provide clear and intelligible conversation without compromise. Users will be annoyed if the received speech is in a noisy condition, making conversation between the users difficult. As such, methods for suppressing, eliminating or compensating echo effects when the near-end speech signal is simultaneously transmitted are needed [1].

Voice over Internet Protocol (VoIP) is a technology that has reached a level of maturity and reliability such that it can now be applied to the enterprise environment. VoIP has the potential to reduce communications costs considerably and opens a new path in the development of new devices. However, like all technologies VoIP comes with a number of inherent risks that while serious can be managed provided the enterprise takes the appropriate precautions.

This paper will examine the risks faced by the VoIP service provider and describe methods to reduce the risk for both the service provider and the enterprise. In addition, we examine the security risks associated with VoIP and has organized these risks in several categories from a layered perspective: weaknesses related to IP, the combined use of legacy and new technology, gateway considerations, security levels associated with VoIP, service provider challenges.

II. BACKROUND HISTORY:

VoIP had been talked about long before Vocaltec, Inc. released Internet Phone Software in 1995. This software was designed to run on a home PC (486/33MHz) with sound cards, speakers, microphone, and modem. The software compressed the voice signal, translated it into voice packets, and shipped itout over the Internet. The technology worked as long as both the caller and the receiver had the same equipment and software. Although the sound quality was nowhere near that of conventional equipment at the time, this effort represented the first IP phone By converting analog voice into compressed digital IP packets, the software enabled PC-to-PC Internet telephony. It's tempting to view the advent of VoIP as a singular technological event.

In reality, however, VoIP is an evolutionary extension of decades-long communications and network technology progress. The highly reliable telephone network has been in a state of constant evolution for more than 100 years. Today, billions of calls traverse the world's phone systems every day withlittle human intervention. This hasn't always been the case. In the early1900s, each call was switched manually by a live telephone company switchboard operator and again with private board operators hired by each company.

An important development for the telephone company network was the automation of the call switching function. With the invention of the Private Branch Exchange (PBX), companies were able to cut their payrolls from many in-house operators to just a handful of receptionists.

The next big step forward for the telephone network was in the early1960s, with the introduction of pulse code modulation (PCM) technology.PCM addressed the inherent signal problems of transmitting voice in the analogworld by converting the analog signal to binary 0s and 1s. This reduced the distance and interference noise on the line. (In fact, on transatlantic calls, one could hear the waves as transient noise moving over the cable.) The binary voice signal became as clear at the receiving end of the line as at the sending end. In the 1980s, Time Division Multiplexing (TDM) became a popular wayto deliver analog voice over digital networks. With TDM, many analog channels were digitized and allocated a specific time slot. The technology allowed different speeds for each channel and supported traffic aggregation. TDMtransformed analogy voice to digital over switched networks, laying very important groundwork for VoIP, because voice could now be viewed as data

TDM provided the major advantage of putting more voice channels ontoa single line. For example, two pair of copper wires could now support a T1line, or 24 channels. The downside of TDM was that allocated channel bandwidth couldn't be dynamically reassigned when not in use. It was for this reason that a different way was sought to transmit voice and data over a single network—a significant challenge because of their differing natures.

Acoustic Echo Cancellation (AEC) has become a necessity in today's conferencing system in order to enhance the audio quality of hands-free communication systems. In recent years, many researchers and manufacturers have developed various AEC algorithms for telecommunication solutions in order to improve the quality of service. Many factors influence the design of an AEC system, such as computational complexity, memory consumption etc [2]. The aim of this work is to review the most recent acoustic echo cancellation techniques and their applicability for current hands free applications. Therefore, this paper presents AEC systems challenges and comparison between these techniques is also presented.

III. INTERNET PROTOCOL WEAKNESSES:

RESOURCE EXHAUSTION (DENIAL OF SERVICE:

Resource Exhaustion, carried out via Do's (Denial of Service) attacks which reduces the number of available IP addresses, bandwidth, processor memory, and other router/server functions. A VoIP based Do's attack bombards a call processing/managing application with large amounts of simultaneous requests that it cannot process, causing the application to shut down, thereby denying service to authorized or intended users.

Before describing how to safely secure a VoIP network, its weaknesses must first be understood. VoIP is carried across the backbone of the Internet using Internet Protocol (IP) addresses to locate customers operating on the voice communications network [3]. However, IP has its own flaws, which are then inherited by all VoIP networks.

NETWORK SNIFFING:

Network Sniffing attacks occur when an individual is observing network traffic. Typically, any system on a network sharing a transmission medium has the ability to view other system traffic (Univ. of London Information Security Group, 1998, pp.6-7).

MESSAGE REPLAY ATTACKS:

According to the University of London Information Security Group [4], this type of attack occurs when network sniffing is done between two systems. Recording of the conversation is done during the sniffing which may be replayed to other parties in an altered state.

IV. FUTURE OF VOIP:

As with any new technology, widespread adoption depends on a complex mix of market needs and market resources set against the new application's potential to transform the user experience. Customers must see the clear advantages of the new technology over their present systems; they must have financial incentive to adopt the new technology; and they must feel confident that it will make them more productive, save money, or fulfill other pressing business or personal requirements. More and more every day, VoIP is living up to these tough criteria. Still, as illustrated earlier, there are important issues that the industry must continue to address. The continual evolution of complementary standards and robust product offerings are just a few.

So where is the VoIP market today, and where is headed? Currently, the enterprise, in the form of corporate intranets and commercial extranets, holds the most immediate promise VoIP is particularly attractive in these environments because IP-based infrastructures allow operators to decide who can and cannot use the network.

The VoIP gateway is another factor propelling the proliferation of packet voice technology. Gateway functionality, which once resided on a PC-based platform, has now migrated to robust embedded systems, each able to process hundreds of simultaneous calls. For corporations, the economies of scale from this integration will allow them cost-effectively to deploy large numbers of VoIP connections that merge data, voice, and video into integrated networks. In fact, the reduced expenses and competitive cost advantages associated with integrated IP networks will be the most compelling factor for many companies.

Outside of the corporate intranet setting, commercial extranets are also pushing VoIP acceptance. These carefully engineered IP networks are already delivering voice and fax over the Internet to customers. As an example, many of the calling cards available at the local convenience store checkout stand are really private IP extranets that earn a profit on the margins that data networks enjoy over traditional switched networks.

V. CONCLUSIONS:

This paper has addressed VoIP security in terms of its configuration, risks, and potential usage by service providers who need to manage those risks. While VoIP is certainly a viable technology great care must be taken in its use and configuration. A number of VoIP specific recommendations conclude the paper.

However, beyond these specific recommendations, an enterprise must use a layered security architecture, which provides the most effective defense against VoIP attacks. Defensive layering must start beyond the enterprise border and originate in the service providers network to insure the secure transport of VoIP to the enterprise. Enterprises must continue to review their security posture in terms of risk mitigation, not risk avoidance because new technology and vulnerabilities will always arise alongside the new technology, like VoIP.

REFERENCES:

1. S. M. Hanshi, Y.-W.Chong, S. Ramadass, A. N. Naeem, and K.-C.Ooi, "Efficient Acoustic Echo Cancellation joint with noise reduction framework," in Computer, Communications, and Control Technology (I4CT), 2014 International Conference on, 2014, pp. 116- 119.
2. Sabri M. Hanshi, 1yung-Wey Chong, 1adel NadhemNaeem, “Review Of Acoustic Echo Cancellation Techniques For Voice Over IP”, Journal of Theoretical and Applied Information Technology 10th July 2015. Vol.77. No.1.
3. Casteel J. (2005). Sound Choices for VoIP Security . Retrieved October 20, 2006
4. University of London Information Security Group (1998). Internet Protocol Security Flaws
5. Barbieri R., Bruschi D., Rosti E. (2002). Voice over IPsec: Analysis and solutions. 8 th Annual Computer Security Applications Conference. pp. 261.
6. Berger T. (2006). Analysis of current VPN technologies.First International Conference on Availability, Reliability, and Security. Pp. 108-115.
7. Bednarz P. (2002). How VoIP is changing the network security equation. Retrieved October 16, 2006.