Journal of Theoretical and Applied Information Technology
30th September 2015. Vol.79. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

END-TO-END SECURITY WITH IPSEC AND BIOMETRIC TECHNOLOGY IN VOIP OVER IPV6

[1]MOHD NAZRI ISMAIL, [2]MOHD SHUKRAN, [3]KAMARUZAMAN MASKAT, [4]NORHATTA MOHD

[1,2,3]National Defence University of Malaysia, Department of Computer Science, FSTP

[4]Universirty of Kuala Lumpur, Department of General Studied, MIIT

E-mail: [1]m.nazri@upnm.edu.my, [2]afizi@upnm.edu.my, [3]kamruzaman@upnm.edu.my, [4]norhatta@miit.unikl.edu.my

ABSTRACT

Voice over Internet Protocol (VoIP) nowadays is the popular communication technology. This paper is about adding face recognition as the biometric authentication for VoIP architecture and added on the end-user workstation for user login. We compare the VoIP performance on IPv6 and IPv4 LANs in presence in difference uses of softphone codecs. Softphone is uses to making call and SIP server at the voice gateway. The performance measures are jitter, packet loss, delays and Mean Opinion Score (MOS). Together with this, Window 7 IPSec is added to ensure end-to-end security through the implementation of VoIP architecture. This paper divided into difference chapters.

Keywords: *VoIP; SIP; IPv4, IPv6, biometric, IPSec, LAN, softphone.*

1. INTRODUCTION

VoIP technology uses Internet Protocol (IP) network to transmit voice. Voice is packetized and sends over the IP network to the destination [1]. Currently, VoIP is one of the famous communication technologies in the world. At the state of the art this infrastructure we use Session Initial Protocol (SIP) as signaling protocol for VOIP. SIP signaling protocol used to establish, modify, and terminate multimedia sessions between two or more end points [2].

Softphone is used to making call for this VoIP architecture. IPv6 is the next generation network layer protocol that was designed as a replacement for the current IPv4 protocol [3]. As the growing popularity of VoIP in the world technology, it is of interest to compare VoIP performance over IPv6 to IPv4. In this VoIP architecture, we focus on comparing VoIP performance with IPv6 and IPv4 during the exchange of voice data and the difference usage of voice codecs [4].

Performance is measured using jitter, packet loss, delays and Mean Opinion Score (MOS). During this measure, the quality of the VoIP calls is also very much dependent on factors such as latency and jitter. Latency occurs when data are delivered too slowly, usually due to congestion and jitter is a variation of packet delays. Latency and jitter can cause packets to be dropped [5].

The main objective of these studies is to add security to the end-user of VoIP which is biometric authentication and Window7 IPSec. We focus to the user's workstations. This is because VoIP works over the Internet world, and there are many type of malware, virus and attacker over the internet.

This paper divided into difference chapters. Section 1 discuss about the introduction of this study, Section 2 about the Biometric Authentication that used to secure this VoIP architecture. In Section 3 is Using Window7 IPSec policies to secure user's workstation, Section 4 is the Voice Codecs, section 5 is the product developments, and section 6 testing and results. Last but not least section 7 is the conclusion of this study.

2. LITERATURE REVIEW- BIOMETRIC

Biometric is a technique for identifying people by using a unique physical characteristic [5]. Biometric devices verify someone's identity by comparing a saved measure of a particular physical characteristic to a current measurement [6]. Why using biometric authentication instead of key-in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

password technique? This is because Biometric recognition provides a strong link between an individual and a claimed identity. One area where biometrics can provide substantial help is in guarding against attempts to establish fraudulent multiple identities or prevent identity fraud. Benefits of using biometric authentication:

- Accurate discrimination between individuals
- Speed of operation
- The ability to deal with present and future numbers of individuals
- Ease of use
- Social acceptability, i.e. people are happy to use it
- Secure and robust against potential attackers.

On this study, we use KeyLemon [7] Face Recognition software. As a Windows and frequently internet user, you probably deal with lots of passwords every day. Remembering each set of login details and typing them in can be time consuming and very frustrating. KeyLemon is a simple solution to log on to your personal Windows account by using your face. The computer has multiple users the software automatically logs into the right Windows account. When users leave the computer, it will automatically lock it and then unlock it when users are back.

For secure authentication the biometric system must be convinced that the presented biometric measurements are coming from a trusted and unmodified input device and are fresh [8]. The biometric system should verify the liveness; otherwise the system could be cheated with copies of biometric characteristics. Which mean that, the human itself should present there together with the biometric device to pass the authentication? Not by duplicate someone else or it's unable to be present on behalf for someone to pass the authentication [9].

3. METHODOLOGY – FRAMEWORK DEVELOPMENT

IPSec is a framework of open standards for ensuring private, secure communications over IP networks through the use of cryptographic security services [10]. The Microsoft Window implementation of IPsec is based on standard developed by the Internet Engineering Task Force (IETF) IPsec working group. IPsec establishes trust and security from a source IP address to a destination IP address [11].

Vioce Codecs - The important things in VoIP architecture is bandwidth saving. The bandwidth is used more efficiently with the application of voice compression codec. Voice codec is used to compress and decompress analogue voice signal into digital format for transmitting in the packet network. During call setup, voice terminal or gateway can automatically negotiate on which codec to be used from the codec selection list that these equipments support [12]. The popular voice codec used in the telecommunication industry are G.711 which is widely used in the PSTN environment.

Software and Hardware Requirements - During the development of these studies, there is several software and hardware are used to deploy this architecture. Brekeke SIP Server v2 and v3, X-Lite Softphone for IPv4, PortGO Softphone for IPv6, PRTG VoIP monitoring software and VQManager for the VoIP monitoring. Cisco 2500 series router is used to distribute IPv6 to the VoIP workstation. Each workstation is run under Window7 operating system. . Window 7 IPSec policies are used to establish trust and security from a source IP address to a destination IP address. On the biometric authentication, we use KeyLemon face recognition software.

VoiP Network Design - To develop the IPV6 for VOIP, a Cisco 2500 router is added into this architecture. Figure 1 show the network architecture for VoIP over IPv6 on a Local Area Network (LAN). There are two workstations which both workstation installed with SIP Softphone, has enabled Window 7 IPSec, and received a distributed IPv6 address from the CISCO router. This Cisco 2500 Series router is used to distribute an IPv6 address to both workstations. However, it's only required to install one SIP server in any workstation. This architecture is similar to the VoIP over IPv4 just without the Cisco router.Voice codecs used during this VoIP testing are:

a. G.711alaw
b. Speex
c. iLBC
d. BroadVoice

Journal of Theoretical and Applied Information Technology
30th September 2015. Vol.79. No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

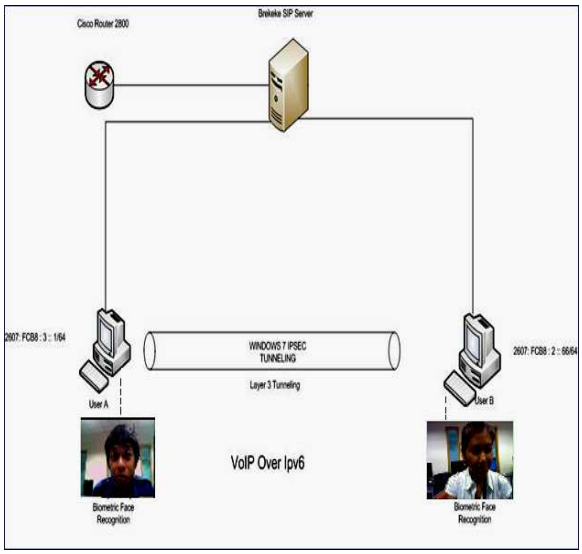

Figure 1. Voip Over Ipv6 Network Architecture

4. RESULTS AND EXPERIMENTAL

In this section, we discuss the results performance of the VoIP IPv6 using biometric technology. Several method of testing are involve to collect data such as:

- Network environment of VoIP is Local Area Network (LAN).
- Duration of the analysis take part is one (1) hour. This analysis taken with PRTG VoIP monitoring tools and VQManager. Graph delay, jitter, packet loss and MOS are taken from here.
- Comparison between IPV4 and IPV6 performance are tested to compare the voice quality of VoIP architecture.
- All result is taken after the adding of biometric authentication and window 7 IPSec.

VoIP result maybe vary from difference codecs, the effect from difference addressing protocol IPv6 and IPv4, and also workstation performance after adding biometric authentication.

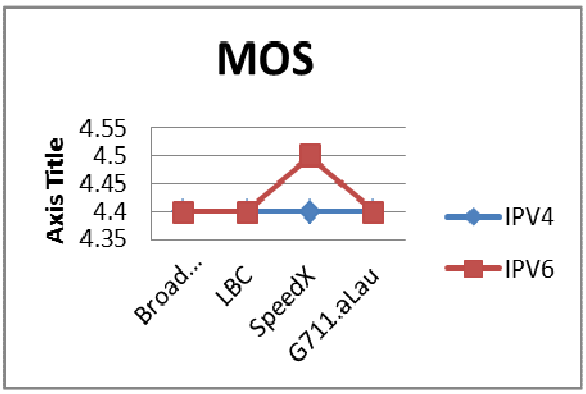

Figure 2. MOS Of Ipv4 And Ipv6 With Difference Type Of Codec

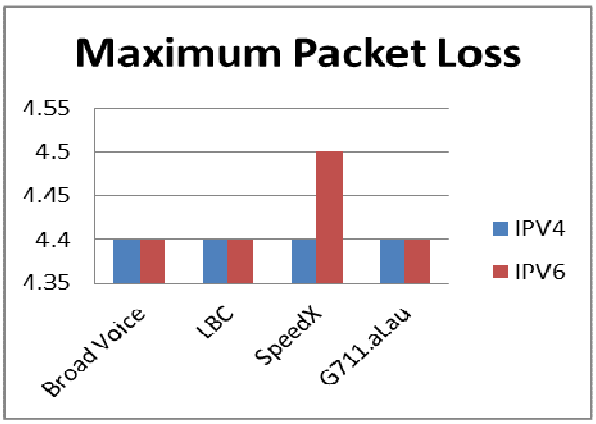

Figure 3. Maximum Packet Loss Of Ipv6 And Ipv4 With Difference Codecs In %

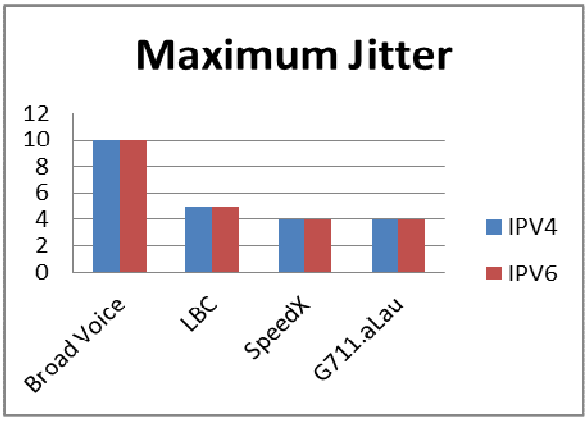

Figure 4. Maximum Jitter On Ipv6 And Ipv4 With Difference Voice Codec In Ms

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

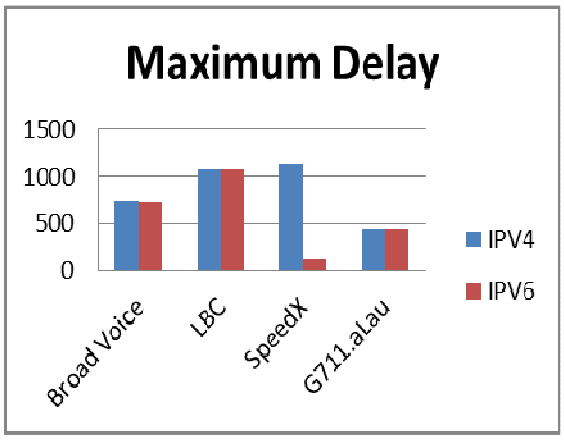

Figure 5.Maximum Delay On Ipv6 And Ipv4 With Difference Voice Codec

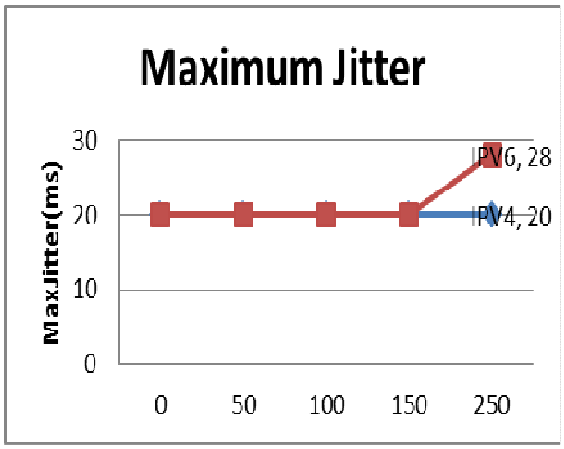

Figure 6. Maximum Jitter On Ipv4 And Ipv6

Figure 2 shows the average MOS taken in both VoIP on IPv6 and IPv4 with difference of audio codecs. According to figure 2, codec Speex has the almost perfect MOS value on IPv6 architecture at 4.5. However, in figure 3 codec Speex show high packet loss with 4.54% loss. Meanwhile both result on IPv6 and IPv4 show almost significant value and have the same MOS rate. With both IPv4 and IPv6 packet loss also is measure according to difference voice codecs. Packet loss was found to me much significance in both IPv4 and IPv6. However, there is high packet loss on IPv6 by using Speex audio codec. Thus, quality of service support in future IPv6 with using PortGo SIP Softphone may prove to be useful in preventing VoIP packet loss and the resulting degradation in voice quality.

Maximum Jitter of VoIP on IPv4 and IPv6 is shown in figure 4. The result show that maximum jitter is essentially the same for IPv4 and IPv6 (it is identical or there is less than a millisecond difference). This could be cause in the use of difference SIP Softphone. The use of difference protocol IPv6 and IPv4 does not affect the call quality. This is also after adding the biometric authentication and IPSec. In result figure 5 with IPv6 and IPv4, packet loss and jitter was found to be more significant with the respect to its effect on MOS and voice quality as shown also in figure 6. However, with difference audio codec that been compare as shown in Figure 5, slightly difference in milliseconds (ms). In result, show that using audio codec G.711 show low jitter.

Figure 5 show the maximum delays with difference codecs. The result shows that there is high delay on using Speex codec. Thus, the delay was high on using IPv4 instead of IPv6. This is because the use of difference of SIP Softphone. On IPv4 uses X-Lite softphone while on IPv6 uses PortGo softphone. However, the other codec show slightly significance with minimum time in difference (measure in milliseconds, ms). Based on the result on figure 5, still codec G.711 shows the minimum delay.

Based on all the result, author can concluded that by using codec G.711 is recommended for a better VoIP call quality and also followed by BroadVoice and iLBC codec. However, author does not state that the worse audio codec is Speex, but it is not recommended to use Speex audio codec due to its high delay on the results.

6. CONCLUSION

In this study, we compare the performance of VoIP on IPv6 and IPv4 from difference parameters of measurement which is delay, packet loss, jitter and MOS. IPv6 address said to be replace for IPv4 address to avoid network congested and IPv6 has longer addressing scheme. This does not mean that the addressing scheme could affect the quality of VoIP. Therefore, measurements of several parameters shows that there is not much performance in difference with IPv6 compare to IPv4. For both IPv4 and IPv6, packet loss even under overloaded conditions results in poor voice quality and also significance drop in the MOS.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From the result, is proving that audio codec G.711 gives the best audio codec quality for both VoIP on IPv4 and IPv6. However, according to the result audio codec Speex does not perform the best audio codec for VoIP. This means that, it is not recommended to use Speex audio codec. Securing both end-to-end points with Windows 7 IPSec does not much effect the performance of VoIP call and video. It is important to end user to secure their platform before start using VoIP. Biometric is one of the most appropriate authentications for security end user.

VoIP is deemed as one of the driving forces behind the adoption of IPV6. However, during this research we discover that different softphone also take effect on the call performance. Implementation on IPV6 into VoIP does not degrade the call performance.

REFRENCES:

[1]. Walsh, T. J., & Kuhn, D. R. (2005). Challenges in Securing Voice over IP. Security and Privacy , 3 (3), 44-49.

[2]. Thomas, J. W., D, R. K., & Steffen, F. (2005). Security Consideration for Voice Over IP Systems. Computer Security Division Information Technology Laboratory .

[3]. Lambrinos, L., & Kirstein, P. (2007). Integrating Voice over IP services in IPv4 and IPV6 networks. Proceedings of the International Multi-Conference on Computing in the Global Information Technology . IEEE.

[4]. Yasinovskyy, R., Wijesinha, A. L., Karne, R. K., & Khaksari, G. (2009). A comparison of VoIP performance on IPv6 and IPv4 networks. Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on (pp. 603-609). Towson,MD: IEEE.

[5]. Matyas, V., & Riha, Z. (2010). Security of Biometric Authentication Systems. IEEE , 19-28.

[6]. Thomas, J. W., D, R. K., & Steffen, F. (2005). Security Consideration for Voice Over IP Systems. Computer Security Division Information Technology Laboratory .

[7]. KeyLemon. (n.d.). KeyLemon. Retrieved from www.keylemon.com

[8]. Li, J.-S., Tzeng, J.-J., & Kuo, C.-M. (2009). Building Security Gateway. Information Networking, 2009. ICOIN 2009. International Conference on (pp. 1-3). Tainan: IEEE.

[9]. Ballard, L., Kamara, S., Monrose, F., Reiter, M. K. (2008). " Towards pratical biometric key generation with randomized biometric templates", in Proceedings of the 15th ACM Conference on Computer and Communications Security, Alexandria, Virginia, USA. ACM, New York, NY, USA, 2008.

[10]. Barbieri, R., Bruschi, D., & Rosti, E. (2002). Voice Over IPSec: Analysis and Solutions. Proceeding of the 18th Annual Computer Security Applications Conference. IEEE.

[11]. Technet. (n.d.). IPSec. Retrieved February 2012, from Networking and Access Technology: http://technet.microsoft.com/en-us/network/bb531150.

[12]. Sahabudin, S., & Alias, M. Y. (2009). End-to end delay performance analysis of vacious codecs on VoIP Quality of Service. 9th Malaysia International Conference on Communication (pp. 607-612). Kuala Lumpur: IEEE.