International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences
(NCDATES- 09th & 10th January 2015)

RESEARCH ARTICLE OPEN ACCESS

Security Threat Prevention For Voip Networks

[1]Mrs.M.SHANTHI, [2]Mr.G. SANTHOSH KUMAR
[1]Department of Electronics and Communication Engineering
CMR Engineering College, Hyderabad.
shanthi3011@gmail.com
[2]Department of Electronics and Communication Engineering
AVANTHI Engineering college, HYDERABAD.
santhosh_gangi@yahoo.com

ABSTRACT
With the development of computing technology, Voice over Internet Protocol (VoIP) has been established as an alternative to carry out a tele-phone conversation over a data network. VoIP products promise converged telecommunication and data services that are cheaper, more versatile and provide good quality and security as compared to traditional offerings. There are a number of VoIP solutions for mobile phones and the VoIP telephony supports the management functions. Security threats of VoIP devices are Denial of service attack, Eavesdropping, Man-in-the Middle attack, Call Hijack, Spoofing attack, Call Fraud. In this, the major threat of the VoIP is eavesdropping attack. In this proposed work the eavesdropping attack is prevented by Proxy.
Key Words: VoIP, SIP, RTP, SDP, Security Issues.

I. INTRODUCTION

To Date, the Public Switched Network (PSTN) has been used to conduct telephone calls over a wired network. With the development of computing technology, Voice over Internet Protocol (VoIP) has been established as an alternative to traditional telephony networks. VoIP allows telephone conversations to take place over a data packet-switched networks like the Internet.

VoIP products promise converged telecommunications and data services that are cheaper, more versatile and provide improved voice quality as compared to traditional offerings. Although VoIP is widely used, VoIP on mobile devices is still in its infancy.

The mobile device has become the most personal computers. Mobile devices contain personal information, access sensitive networks and are now utilized for financial transaction. Mobile devices are quickly evolved from phones to fully functional mobile computers enabling web browsing, multimedia, advanced communication, downloading application, accessing public wi-fi hotspots and use of Bluetooth are all common place and targeted by hackers. So, the mobile devices are subject to viruses, malware and hackers. There are a number of VoIP solutions for mobile phones, class VoIP telephony support QoS (quality of service), security and management functions which will present a tremendous opportunity to network and service providers of the world to offer both traditional as well as a range of creative new services in the near future.

II. RELATED WORKS

In the year 2009, Remi Badonnel, Olivier Festor, Khaled Hamlaoui, LORIA- Nancy University,France, proposed the Monitoring and Counter- profiling for Voice over IP Networks and Services. In that paper done a counter measure strategy for preventing VoIP profiling.They proposed two functional architechtures with different noise generation functions in order to dynamically generate fake VoIP messages and deteriorate the profiling performances based on Principal component analysis (PCA).

In the year 2008 Weilai Yang and Paul Judge, Secure computing corporation , Atlanta, proposed the VISOR: VoIP security using Reputation. This paper summarizes the security challenges and proposes the VISOR, a VoIP security architecture.VISOR is a reputation system that monitors VoIP activity, analyse the global traffic patterns, and distinguishes between wanted and unwanted participants.

In the year 2007 Dimitris Zisiadis, Spyros Kopsidas, Leandros Tassiulas, Computer Engineering and Telecommunications Department, University of Thessaly, proposed an Architecture for Secure VoIP and Collaboration Applications.In that paper proposed a new architecture that leverage security for user communications carried over the Internet. The proposed work ensures end to end security through the implementation of the biometric based procedures followed by the VoIPSec (Voice Interactive Personalized Security) protocol..

III. ARCHITECTURAL OVERVIEW

From an architectural standpoint, the minimum requirement to enable a VoIP call is to have two listening parties, each having a calling device equipped with a VoIP codec and connected over an IP network.

However, as VoIP becomes a mainstream service with user demanding services that match and supersede the PSTN-level services, new functional components are being introduced into the VoIP architecture. Consequently, the current VoIP architecture is evolving rapidly by adding new services over VoIP and in addressing various issues specific to the deployment of VoIP over carrier networks, Enterprise LAN, etc.

Unfortunately, there exists no standardized VoIP architecture that can cover all the possible deployment scenarios and functionalities. Currently, different VoIP vendors and service providers have created their own unique architectures in order to differentiate themselves in terms of their functionalities. Yet, it is possible to refer to a generic VoIP architecture as shown in Figure 3.1 for discussing the functional requirements and associated functional components of a next-generation VoIP architecture

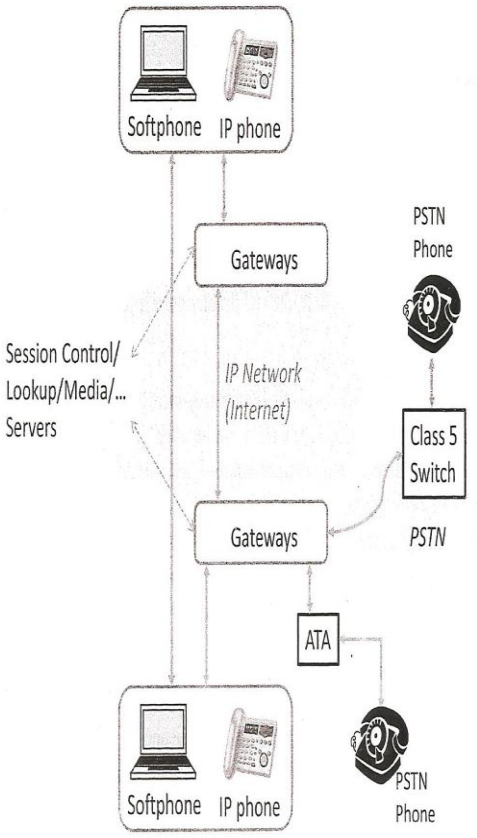

Figure 3.1 VoIP Architecture

3.1 Architectural requirements

The basic architectural requirements are derived from the deployment scenarios that enable a flexible communication model. Since the VoIP architecture is meant to enable voice calls over a packet-switched IP network such as the Internet, there are certain types of communication model that it must support. These can be listed as:

Internet-to-Internet: This type of call includes those that originate on a phone connected to the Internet terminate at a phone connected to the Internet and the entire route remains inside the Internet.

Internet-to-PSTN: These calls have the caller having a phone connected to the Internet whereas the callee is connected to the PSTN. Here the call traverses through both the PSTN segment and the Internet.

PSTN-to-Internet: In this setting, the caller is connected to the PSTN whereas the callee has a phone connected to the Internet. Here also, the call traverses both the PSTN segment and Internet.

PSTN-to-PSTN via the Internet: There is a case where the call originates and terminates on devices connected to the PSTN but the call's routing is done over the Internet. This can be done as communication over the Internet is cheaper and typically used for international calls.

Internet-to-Internet-via-PSTN: Lastly, there can be a case where the call originates and terminates on devices connected to the Internet but a part of the call's route is over the PSTN. This can be the case when the circuit-switched link through the PSTN reduces the communication delay whereas the end-to-end Internet path may have a higher expected delay.

In order to support these models, the architecture must meet the following functional requirements:

Address Discovery: When a call is initiated, there is a need to figure out the destination's location. The destination can be an IP phone for which the address may be an IP address or an Internet Uniform Resource Identifier (URI). The address can also be a unique user ID as used in many P2PnVoIP applications. For supporting the PSTN phones, the destination can be a PSTN phone number. The address discovery service is important in any VoIP architecture for forwarding the call request to the appropriate entity.

Device Interoperability: A VoIP calling device from different vendors should interoperate by being able to communicate using the same protocol. A VoIP phone from vendor A should be capable of calling a VoIP phone from Vendor B. Following the standards ensures that such diverse devices remain interoperable.

Inter operability with PSTN phones: In order to enable calling to and from PSTN phones, the

architecture must provide functionalities that provide protocol level translation and VoIP data level Transcoding. With these functionalities the call generated from the IP network can be forwarded to and from PSTN network class 5 switches.

Session -level Control: In different deployment scenarios, various session-level control functionalities become important. Such functionalities include session-level authorization, authentication, user billing, etc.

Media-Level Functionalities: Media-level functionalities refer to services provided to the actual voice over data that is transported over media transport protocols such as RTP. Such functionalities include various media-level processing to enable call mixing for multiparty conferencing, transcoding to enable transport over heterogeneous network links, etc.

Interoperability among Components:

All the functional components of a VoIP architecture should be interoperable by using standard protocols (such as SIP/H.323). This will enable (a) multivendor equipments to inter-operate; and (b) multiple VoIP service providers to coordinate in carrying each others' VoIP traffic.

The requirements listed above are not exhaustive. They merely represent the high-level requirements that are required for VoIP. Fortunately, these requirements are well addressed by the recently proposed VoIP architectures at different levels. Each of these high-level requirements may lead to various deeper level functionality requirements.

IV. SECURITY ISSUES

At the moment the Voice over IP Security makes the headlines of all major specialized media. All major IT medias seem to be interested in this subject. The reasons are simple: the promises of this technology and the lack of expertise and standards in VoIP Security. Many security experts have warned that up until now VoIP has been developed and deployed with a purely commercial goal in mind, overlooking security and focusing on functionality. As the technology matures, becomes widely available and usable, security issues gain interest. However, no real standards exist yet. VoIP SA (Voice over IP Security Alliance), aims to be the first organization building a sold and coherent taxonomy of vulnerabilities and attacks threatening VoIP infrastructures.

4.1 Denial of Service

A denial-of-service attack (also, Dos attack) is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system.

A DoS attack can be perpetrated in a number of ways. There are three basic types of attack:

1. Consumption of computational resources, such as bandwidth, disk space, or CPU time.
2. Disruption of configuration information, such as routing information.
3. Disruption of physical network components

4.2 Eavesdropping

Eavesdropping is the intercepting and reading of messages and conversations by unintended recipients. In VoIP, eavesdropping is an attack giving an attacker the ability to listen and record private phone conversations. Eavesdropping can have important, unexpected consequences as people may use telephone systems for divulging crucial information such as Social Security numbers, Credit card numbers or any other confidential information. Inside a company, eavesdropping could allow access to confidential business information.

4.3 Man in the Middle

Man in the middle attack (MITM) is an attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims. MITM attack can be used for conducting other sub attacks such as eavesdropping or DoS.

4.4 Call hijack

In VoIP and classical telephony, Call Hijack attack refers to a situation where one of the intended end points of the conversation is exchanged with the attacker. Call hijacking can have common consequences with eavesdropping attacks (access to confidential information). Generally if an attacker is able to conduct a Call Hijacking attack, he will evolve it into a MITM attack to avoid raising suspicions.

4.5 Spoofing attack

A spoofing attack, in computer security terms, refers to a situation in which one person or program is able to masquerade successfully as another.

4.6 Call Fraud

Call fraud is an attack specific to telephony and VoIP, in consists in the illicit use of a VoIP infrastructure to place phone calls. These phone calls seem to originate from legitimate users inside the attacked network/system.

V. DESIGN & IMPLEMENTATION

Below network shows the sample network architecture of a VoIP network.That is wire less or ISTN or PSTN or PBX network or Enterprise

network or other terminals are interconnected through gateway and connected to the IP network so we can achieve the communication between Internet to Internet, PSTN to Internet, PSTN to PSTN via the Internet and Internet to Internet via the PSTN.

In the proposed system, the client 1 make a call to client 2 mobile first the clients get validation and authentication by the proxy server.

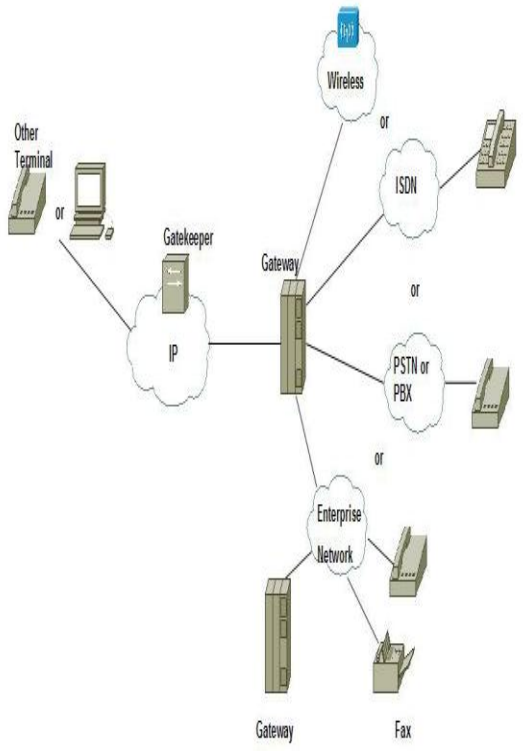

FIG:5.1 Sample VoIP Network

Then they get authorized by the mobile server and then allow the users to communicate between them and to use the free call of VoIP structure. Other unauthorized users not able to call like a VoIP free call instead they go for the normal telephone call and it takes a normal telephone call cost.

In this proposed system the client is validate by the proxy server then the Eavesdropping threat is avoided that is unauthorized user not able to use VoIP structure

This VoIP communication is very useful for call centers or BPO's and KPO's and some commercial enterprises which is globally distributed over the world for their transaction.

The Implementation modules of the secure VoIP structure is shown below

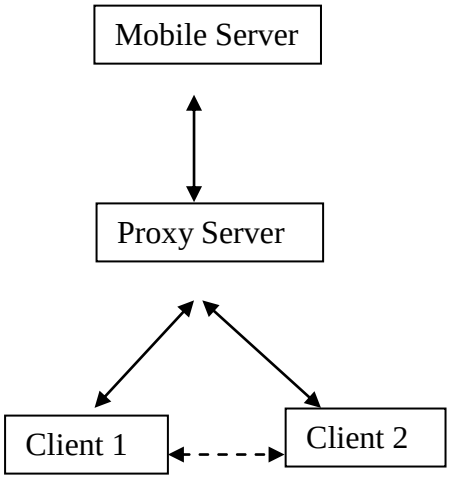

Figure 5.2: Implementation Module

VI. CONCLUSION & FUTUREWORK

IP telephony provides a viable alternative to traditional wired line and wireless telephone systems. Critical signaling infrastructure is vulnerable to many security threats arising due to message structure, message content, misbehaving signaling nodes and traffic analysis etc. Because of the technology limitations, achieving large enterprise level security is not possible. Based on this fact, the proposed model is simple and gives the maximum performance over the VoIP network.

The proposed system considers the major threat of Eavesdropping attack. The proposed implementation module provides the security and avoids the Eavesdropping attack across the users.

Like wise in the future work we can integrate the secure network structure across the enterprises and achieve the secure voice communication across the users.

REFERENCES

[1.] M. Nassar, R. State, and O. Festor, "Voip honeypot architecture." In Integrated Network Management. IEEE, 2007, pp. 109–118

[2.] J. Quittek, S. Niccolini, S. Tartarelli, and R. Schlegel: "On Spam over Internet Telephony (SPIT) Prevention", Vol. 22, No. 5, 2008

[3.] J. Seedorf, F. Ruwolt, M. Stiemerling, S. Niccolini: "Evaluating P2PSIP under Attack": IEEE Globecom 2008, November 2008

[4.] I. Arce and E. Levy, "An analysis of the slapper worm," IEEE Security and Privacy, vol. 1, no. 1, pp. 82–87, 2009
[5.] M. Luo, T. Peng, and C. Leckie, "CPU-based DoS attacks against SIP servers," IEEE, April 2008
[6.] H. Sengar, R. Dantu, and D. Wijesekera, "Securing voip and pstn from integrated signaling network vulnerabilities," April 2010
[7.] Weilai Yang and Paul Judge, "VISOR: VoIP security using Reputation," IEEE, 2008.
[8.] Remi Badonnel, Olivier Festor, Khaled Hamlaoui, "Monitoring and Counter-Profiling for Voice over IP networks and services," IEEE, 2009.
[9.] Zahid Anwar,William Yurcik, Ralph Johnson, Munawar Hafiz,Roy H. Campbell, "Multiple design patterns for VoIP security," IEEE, 2010.
[10.] Patrick c.k. Hung,Miguel Vargas Martin, "Security issues in VoIP applications," IEEE, 2009.

Web Sites:

1. http://www.wirlab.net/kphone.
2. http://snad.ncsl.nist.gov/itg/nistnet/
3. http://www.ietf.org/rfc/ rfc3761.txt.
4. http://www.cisco.com/en/us/about/security/intelligence/05_07_voip.html.
5. http://www.foundrynet.com/pdf/wp-ieee-802.1x-enhance-network.pdf

Books:

1. Voice over IP Security A layered approach Amarandei-Stavila Mihai Amarandei-Stavila XMCO Partners

2.Security Considerations for Voice Over IP Systems Recommendations of the National Institute of Standards and Technology D. Richard Kuhn, Thomas J. Walsh, Steffen Fries

AUTHOR PROFILES

Mrs.M.Shanthi received her M.Tech (Embedded Systems) degree from JNT from JNTUH University, TELANGANA, India, in 2012. She is serving as Asst.Prof in the department of Electronics and Communication Engineering, CMR Engineering College, Hyderabad, India, since 2014. She has served as Asst.Prof in the department of Electronics and Communication Engineering, Guru Nanak Institute of Engineering & Technology, Hyderabad, India. Her research interests include Embedded systems, Communication systems, Mobile wireless and Multimedia Technology and Robotics.

Mr.G.Santhosh received his M.Tech (Communication Engineering) degree from VIT University, TamilNadu, India, in 2010. He is serving as Lecture in the department of Electronics and Communication, AVANTHI Engineering College, Hyderabad, India, since 2014. He has served as Lecturer in the department of Electronics and Communication, Guru Nanak Institute of Engineering & Technology, Hyderabad, India. His research interests include Digital signal processing, Digital systems, Mobile Wireless and Image Processing and Artificial Intelligence.