www.ijecs.in

*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 3 Issue 2 February , 2014 Page No. 3879-3883*

# Security issues in Voice over IP: A Review

***Rajni*** [a]***, Preeti*** [a]***, Ritu Baniwal*** [b]

[a] CSE, SES, BPSMV
[b] CSE Deptt., GJUS&T,Hisar

## Abstract:

VOIP and Internet multimedia system technologies are rapidly being used by consumers, government, enterprises and militaries for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as Internet. These technologies offer more features than traditional PSTN (Public Switched Telephone Network). VoIP provide more flexibility and cost is also reduced in VoIP than PSTN[2]. Also, VOIP systems are more complex in architecture, protocols and implementation terms with increase in the potential of misuse. This paper presents an overview of VoIP system and some of its security issues to provide a direction towards the future research in similar technologies. This paper also gives a brief overview of SIP, one of the most important technology of VoIP.

**Keywords: VOIP, Service Convergence, PSTN, Network consolidation, SIP, H.323**

## Introduction:

Voice over Internet Protocol (also called as VOIP, Internet telephony) provides communication facilities over Internet [2]. It is the process of routing voice conversation on Internet. The voice data flows over a packet switched network instead of a circuit switched network. The voice data is transmitted over IP based network. So the voice needs to be transmitted to digital form and encapsulated in packets and converted back to the original voice signal at destination. The VOIP services are cost saving than traditional telephone system by placing long distance calls over an IP network. The advantages of VOIP are toll bypass, network consolidation and service convergence. The data, voice and video all are transmitted over a single line. This reduces the setup and maintenance costs. Because of these benefits, VOIP has been adopted by the enterprises and consumers at a rapid rate. The VOIP is integrated with the data networks. So securing VOIP is more challenging than securing pure data network. All security problems related with data networks come in VoIP because they share same network hardware and infrastructure.

**VoIP components:** The main components of VoIP network are gateway, server and end user equipments. The voice compression or decompression, call routing, packetization all are done by the gateway. The gateway also interfaces with the external controllers. The server performs network management functions. The end user equipments are terminals that can be connected to a network. The terminal may be a hard phone or a soft phone. VoIP needs two protocols: signaling protocols and media protocols. The signaling protocols manage call setup and teardown. The important signaling protocols used in VoIP are SIP and H.323.The media protocols manage the transmission of voice over the IP network. The media protocol used in VoIP is RTP (real-time transport protocol).

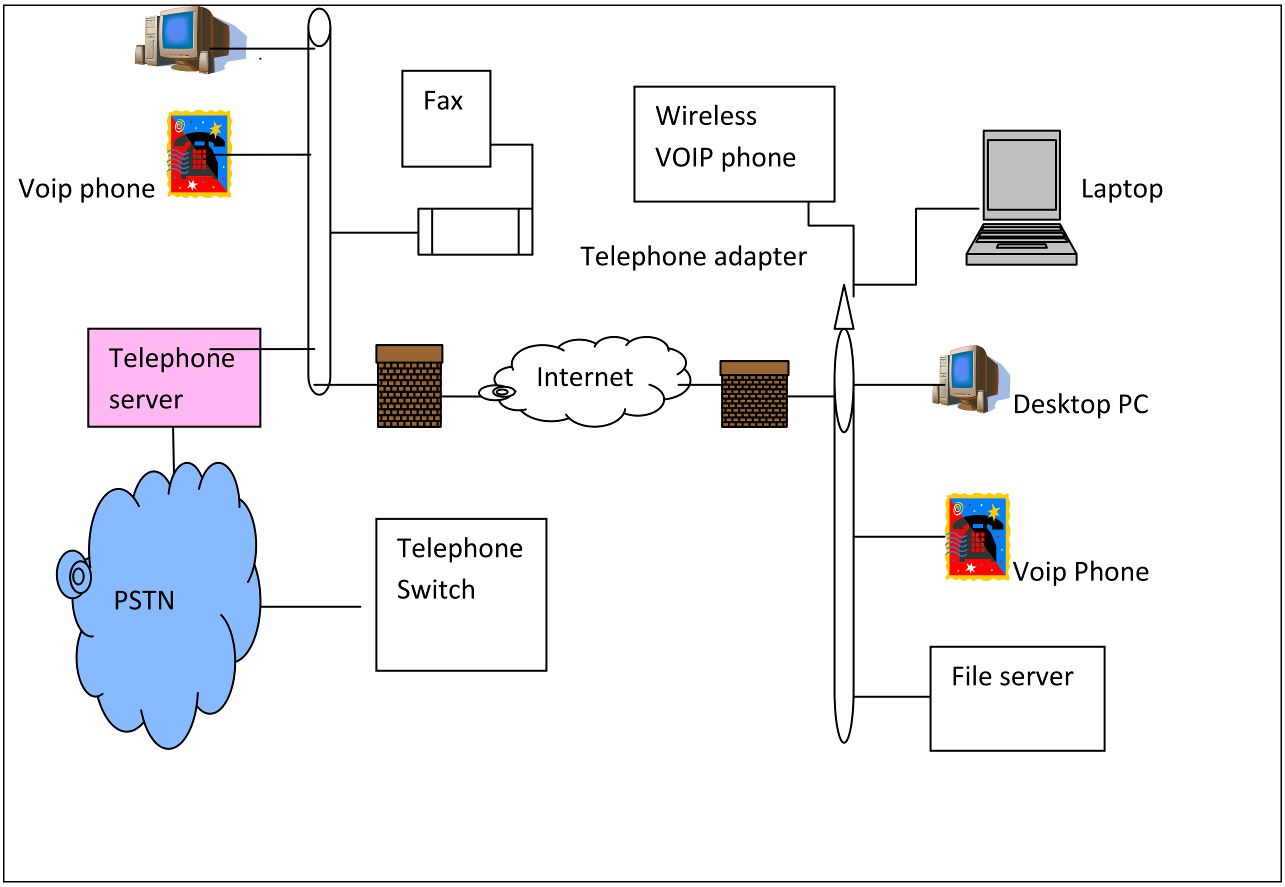

**Figure 1: Components of a VoIP Network**

**H.323 Protocol:** This protocol was created by ITU (International Telecommunication Union).It can be easily integrated with the PSTN. This protocol can transmit voice, data and other multimedia that require PSTN. The various components in H.323 are gateway, terminals, gatekeeper and multipoint control units.

**SIP:** Session initiation protocol is created by the IETF (Internet Engineering Task Force) [8]. This protocol is an application layer protocol and used for creating; modifying and terminating sessions. It can be used to create two-party, multiparty or multicast sessions.SIP is a text based protocol like HTTP that uses messages. It also supports both TCP and UDP. The components of SIP are end points, proxy server, redirect server, location server and registrar. The location of end point is registered at registrar. This information is saved in external location server.SIP messages are forwarded either by proxy server or redirect server.

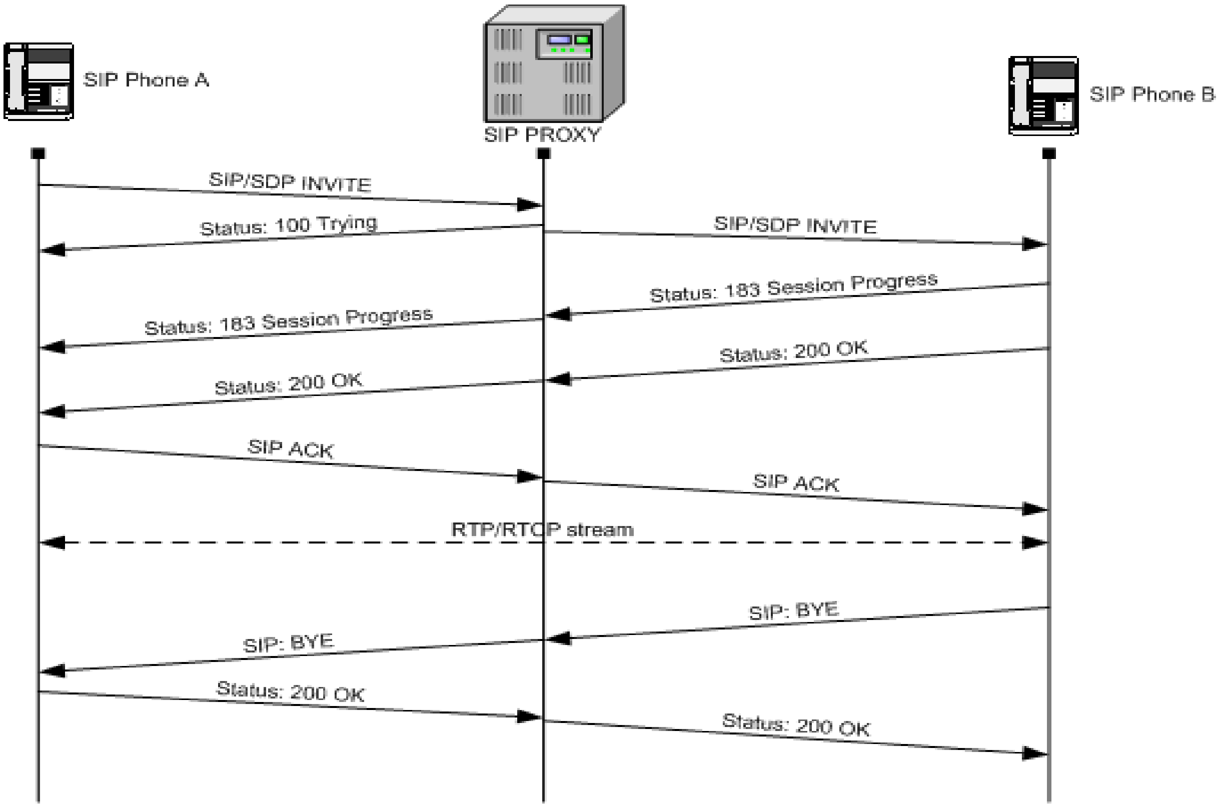

**Figure 2: SIP protocol**

**VoIP threats:** This section presents various threats to the confidentiality, integrity and availability of VoIP systems. In August 2006, S. Niccolini submitted a draft to the IETF outlining taxonomy for VoIP threats [5]. Earlier, the VOIPSA (Voice over IP security alliance) had created an enormous classification for VoIP threats and attacks. The various threats in VoIP are:

- **Social threats:** Social threats are aimed directly against humans**.** The social threats include misrepresentation, theft of services and unwanted contact.
- **Security threats:** The various security threats are confidentiality threats, eavesdropping of telephone conversation, unauthorized access, integrity threats.
- **Service abuse threats:** This category includes improper use of services. The threats are call conference abuse, improper adjustment to billing.

## Security threats:

**Confidentiality threats:** Confidentiality means information cannot be accessed by an unauthorized party. The confidential information of the users may include private documentation, financial information, and security information like passwords.

**Eavesdropping of telephone line:** In VoIP, the chances for eavesdropping increase because of the large no. of nodes between the path of two conversation parties. If the attacker is one of these nodes, he can access the IP packets flowing through that node.

**Unauthorized access:** Unauthorized access means that the attacker can access resources on a network that they do not have authority.

**Integrity threats:** Integrity means information remains unaltered by unauthorized users. A legitimate user may perform an incorrect or unauthorized operation.

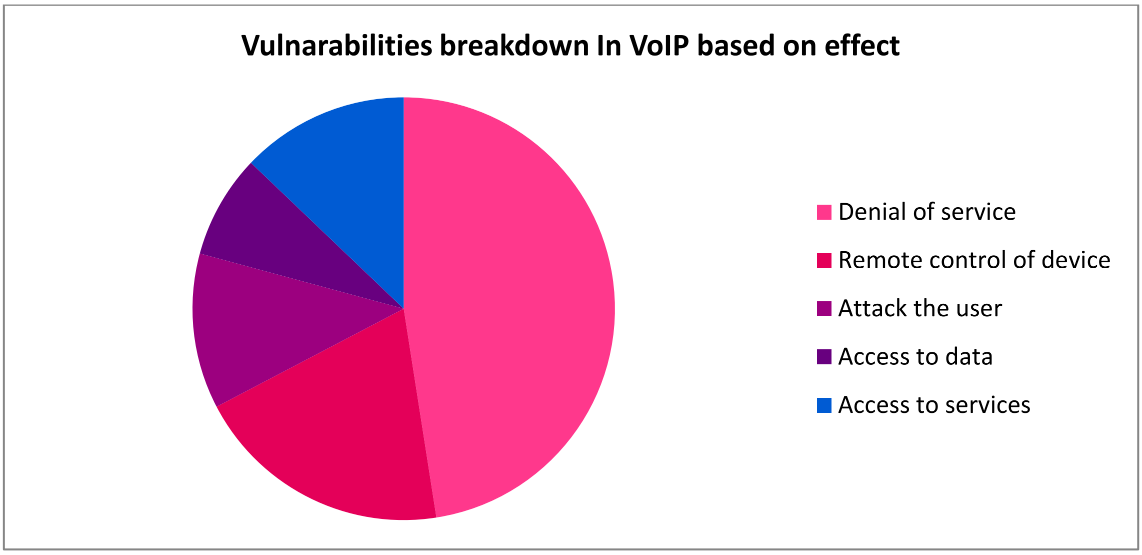

**Figure 3: Vulnerabilities breakdown based on effect**

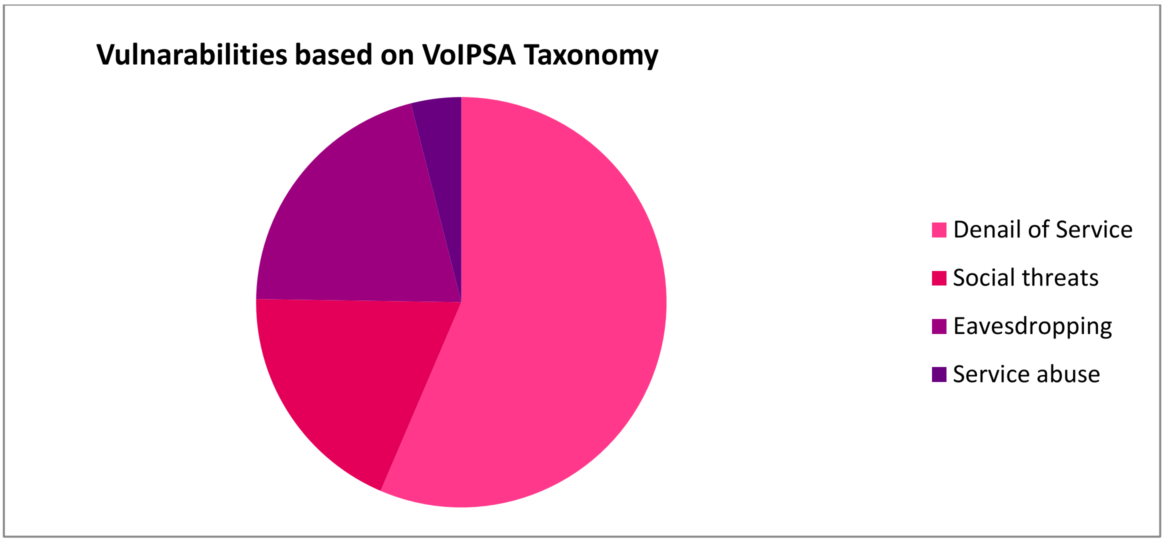

**Figure 4: Vulnerabilities based on VoIPSA Taxonomy**

**Interruption threats:** These are non-intentional threats that cause VoIP services to become unusable or inaccessible. Examples are performance issues that degrade call quality.

**Attack the user** refers to the vulnerabilities that permit the attacker to effect the user of the device. Traffic eavesdropping attacks fall in this category. The attacks that compromise the data on a system fall in the category of **Attack the data.**

## Security Guidelines for VOIP:

There are various security measures that can minimize the risk of attack on VOIP system [7].

Some of these are:

**1. Develop appropriate network architecture**: It is good to separate data and voice on logically different networks, if feasible due to their QoS requirements.

**2. Do not use soft phone system:** Viruses and other malicious software are common on PC connected with the Internet and very difficult to defend against.

**3. VoIP firewalls and other appropriate protection mechanisms should be used**.

## References:

**[1]. Mark Collier, “The Current State of VoIP Security”,** http://download.securelogix.com/library/The_Current_State _of_VoIP_Security.pdf

**[2].** A.D. keromytis. Voice over IP Risks, Threats and Vulnerabilities. In Proceedings of the Cyber Infrastructure Protection (CIP),June 2009.

[3]. http://www.voip-info.org/wiki/

[4]. A.D. Keromytis,”Voice over IP Security: Research and practice,”IEEE security &Privacy magazine, vol. 8, PP. 76-78, March/April 2010.

[5]. VoIP Security Alliance,”VoIP Security and Privacy Threat Taxonomy Version 1.0”, http://www.voipsa.org/Activities/taxonomy.php , Oct 2005

[6]. A.D. Keromytis,”Voice over IP: Risks, Threats and Vulnerabilities”, Symantec Research Labs Europe.

[7]. Jianqiang Xin, GIAC Security Essentials,” Security issues and countermeasure for VoIP “

[8] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler. SIP: Session Initiation Protocol.RFC 3261(Proposed Standard),June 2002.