# Global Information Assurance Certification Paper

# *Security Analysis: Traditional Telephony and IP Telephony*

Alan Klein
Assignment: v.1.4b

## Executive Summary

IP Telephony offers some dramatic benefits over Traditional Telephony in the areas of portability, and accessibility. These enhancements do not come without a cost and require greater effort, planning, and vigilance to ensure high availability and security. "Most users implementing VOIP these days are primarily concemed about voice quality, latency and interoperability"[1] rather than security. Many are "preoccupied with simply making it work."[2] When implemented within an overall security mindset, IP Telephony can successfully address key business problems. It has the potential to dramatically increase the competitive effectiveness of a company and increase shareholder value.

Because of the technologies and skill sets involved, IP telephony transcends the traditional job boundaries of data communications and telecommunications. The goal of this paper is to take a step back and analyze the security implications of migrating from a traditional telephony architecture to an IP telephony architecture. The key components of the two architectures, the phones/stations and the PBX/Gatekeeper/Gateway, are analyzed for vulnerabilities snooping/eavesdropping, theft of service, and denial of service.

## Introduction

It is only upon understanding both the threat vectors that are introduced by any new technology and the technology it supplants that a strategy can be formulated to help contain the risks of that technology. Security vulnerabilities are a fact of life. Security professionals need to strike a balance between risks versus reward. It is necessary to ensure an equitable allocation of time and resources.

I have organized this paper with an initial overview of the components in a traditional distributed PBX architecture as compared to the components in an IP-PBX architecture. BCR magazine provides a generalized definition of IP Telephony as "…call-control signaling and provisioning of software features, and/or voice communications signaling and using an IP-based LAN/WAN infrastructure."[3]

"In the span of five years, IP stations have increased from less than 1 percent to more than 16 percent of total PBX shipments. Last year, circuit-switched (TDM/PCM) station shipments declined 11 percent, while IP station shipments doubled."[4] From a security standpoint, most enterprises will be managing a combination or hybrid system of circuit switched and packet switched telephony networks.

## Traditional distributed PBX architecture

Figure 1 below shows a traditional telephony architecture.

In this topology, there are two sites, Boston and New York. Boston provides all the "intelligence" in the topology - the "brain". New York is a port network off of Boston.

New York requires the services of the Boston "brain" for call set-up/tear-down and other call control functions. A helpful way of understanding this topology is to think of the New York PBX cabinet as a logical extension of the Boston PBX cabinet. This topology is used for this example because of the distant separation of sites and the desire to centrally control and administer the call processing system from one main site (Boston).

Areas of interest in Figure 1 include the telephones (terminals), the New York remote site (Gateway), the Boston – central site (Gatekeeper) and the physical separation (isolation) of the telephony network from the data network. The terms in parentheses - terminals, gateway, and gatekeepers - is the terminology used in the ITU-T H.323 standard. Steve Taylor and Larry Hettick provide a good summary of these terms in their article, H.323 basics[5].

Matching these terms with their traditional telephony counterparts helps in comparing and contrasting the traditional telephony and IP telephony architectures.

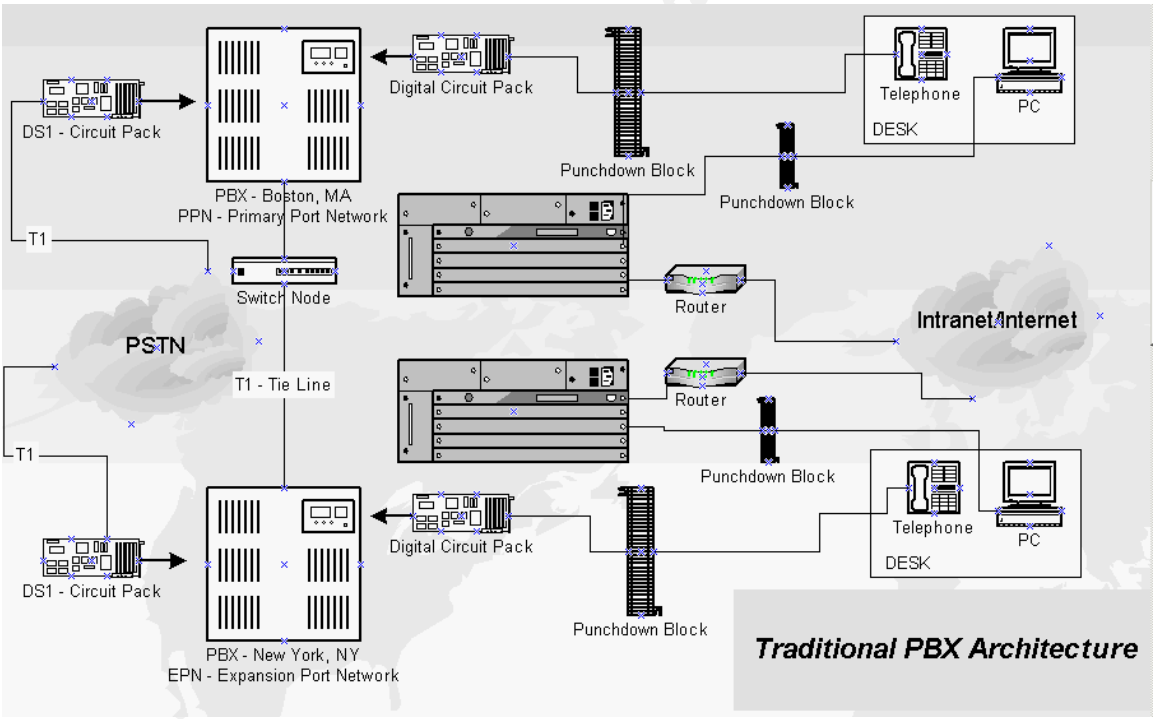


**FIGURE 1**

## Traditional Telephony Environment

### Stations (terminals)

The stations are connected into the PBX via dedicated twisted-pair wiring to a punch down block.

The punch down block is connected to a circuit pack in the PBX (a line card) via an RJ-21X (25-pair amphenol connector). Each station line card, depending on the model, can handle up to 24 individual digital stations.

**Snooping/Eavesdropping**

A number of factors protect against these types of attacks and the integrity and confidentiality of the telephone conversation. These factors include the physical separation (isolation) between the data network and voice network. In fact, each telephone has a dedicated connection between itself and the PBX. It has been incorrectly surmised in some articles that "alligator" clips be used to easily listen in on the conversation as long as physical access to the cabling plant is available. This assumption is incorrect for digital telephone sets because they use vendor proprietary protocols and digitize the voice on the stations before transmission to the PBX. The ability to decode and listen in on the conversation would require much more specific technical expertise and resources.

**Theft of Service**

The term theft of service means the ability of an individual to use the telephone set for nefarious purposes. This includes placing unauthorized calls by assuming the identity of the legitimate user of the telephone. From the perspective of the traditional digital telephone set, a number of factors limit the opportunities for these types of attacks. The primary limiting factor is the physical mapping of each telephone port to a physical port on the PBX line card. This prevents the easy relocation of the telephone set to another location along with the authorized access the extension provides. In addition, the attacker is restricted from "re-programming" the telephone via the keypad to assume another users extension and associated authorization (calling privileges) that extension provides.

A number of large traditional PBX vendors have enhanced functionality that allows the telephone administrator to move the telephone set without rewiring the physical connection. This applies to analog and digital end-points. This movement, however, can be restricted to the system administrator because it requires a feature access code and authorization code be entered before the move. In addition, the station being moved must be defined beforehand on the PBX as one that can be moved.

Another area of attack, which is minimized in the traditional telephony environment, is the use of publicly accessible phone sets, for example lobbies and guest areas. Because the digital (or analog) sets are physically bound to a port on the PBX line card, there is little likely hood of an attacker removing the telephone set from the wall jack and replacing the set with an unauthorized device to gain elevated access or access to the underlying data network for that matter.

Basically, theft of service is limited to physically using the telephone set in the absence of the authorized user or the use of social engineering to convince the telephone user to perform a certain set of actions, which provides an outgoing trunk.

**Denial of Service**
Because of the physically separate networks, the signaling and bearer channel traffic between the telephones and PBX are protected against denial of service attacks. Denial of service attacks are relegated to physically removing the telephone from the wall jack or severing the wire connecting the telephone set to the punch down block or punch down block to the PBX.

## Primary Port Network/Expansion Port Network -Gatekeeper/Gateways

The PPN/EPN are connected to each other via a dedicated T1 circuit. Additionally, PSTN connectivity is provided via dedicated T1 circuits. These circuits terminate on a circuit pack in the PBX (trunk cards).

**Snooping/Eavesdropping**
From Figure 1, intercepting the communications between the sites or PSTN would require physical access to the digital circuit and the technical expertise and specialized tools to recover the communications. A more plausible attack vector would be via the PBX itself through an insecure maintenance port, possibly via a modem or insecure system console. Once administrative access is gained, many PBX's can be configured with a service-observing feature that can be used to silently listen in on otherwise confidential communications between parties.

**Theft of Service**
Theft of service has been the highest risk factor in traditional telephony environments. Attackers have crafted extremely creative techniques to bypass security restrictions, ultimately resulting in toll fraud. Many traditional PBX vendors have complete manuals dedicated to this topic. Attack vectors are many and include: maintenance ports, voice mail systems, automated attendants, remote access (DISA), and social engineering. Interestingly enough, many of these exploits are similar in the data communications world. Examples include weak passwords or barrier codes (the password is the extension, the password is the extension backwards, etc). Administratively defined trunk restrictions can be bypassed by attackers via "privilege escalation" attacks on call prompting vectors of automated attendants. These attendants can run with privileged access to lines and trunks.

**Denial of Service**
The separation of physical facilities between the voice network and data network makes denial of service type attacks unlikely yet not impossible.

Examples include co-coordinated calling from internal or external parties to overwhelm the call carrying capacity of the trunks or TDM backplane. Finally, privileged access by unauthorized individuals to the maintenance port or system console to reprogram the system.

## IP Telephony Environment

Figure 2 provides a "feature rich" example of a distributed IP Telephony architecture. In this example, the benefits of the accessibility and portability become apparent. The terminals (stations) have been extended from the office desk environment to include mobile 802.11b wireless IP handsets sets, IP Softphones, and remote IP hardphones connected over an IPSec VPN. The dedicated T1 circuit connecting Boston to New York has been replaced by an IP trunk. The telephony and data network have converged onto a common physically shared network.

The functionality of the Boston PBX (Gateway/Gatekeeper) has been moved to the "Call Processing Gatekeeper/Gateway" and New York PBX (Gateway) to the "Call Processing Gateway". The intelligence (brain) is still handled out of the Boston, MA office. Figure 2 below provides a topology for a distributed IP telephony architecture.

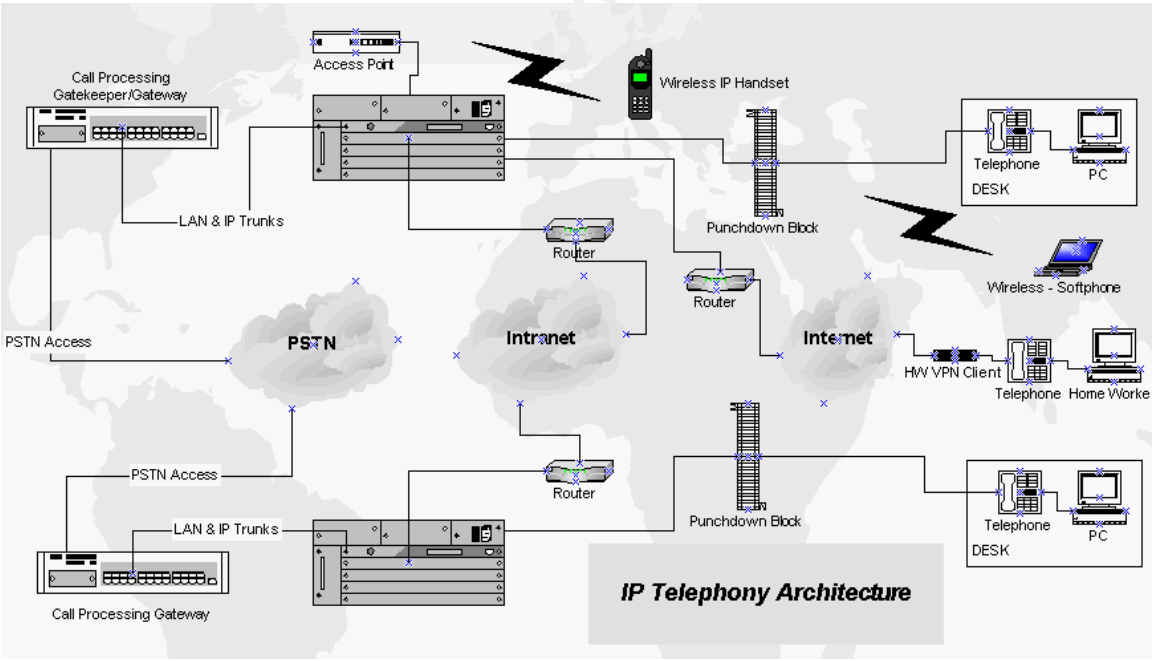


**FIGURE 2**

## Security in a IP Telephony Environment

### Terminals (stations)

The IP hard phones are connected into the IP-PBX via an IP connection over Ethernet.

The terminals connect to a punch down block that in turn is connected to an Ethernet switch. An Ethernet switch has basically replaced the PBX station line card from Figure 1. The IP-PBX is connected to an Ethernet switch. In the diagram, you can see that the desktop computers have their Ethernet patch cord plugged into the IP phone. This allows the desktop PC network connectivity without a second cable drop. The majority of IP telephones ship with a three-port switch. One port is used for the uplink, one port for the phone (internal port) and one port for the desktop computer.

The IP soft phone and wireless IP set use a Wi-Fi (802.11b) connection back to the corporate LAN. This allows for enhanced speech mobility throughout the enterprise. The Internet connected home workers use an IPSec based VPN in combination with a hardware VPN client to tunnel back to the corporate intranet. This provides the employer the cost benefits of bypassing the PSTN while providing the employee the benefits of a full-featured phone set, call processing capabilities, and corporate presence.

**Snooping/Eavesdropping**

The threat of snooping/eavesdropping is much greater on an IP network. "VoIP packets have a well-known and standardized format so even an individual VoIP packet can be 'played' without knowing the contents of previous packets in the packet stream."[6] The majority of IP Telephony vendors have utilized Real Time Protocol (RTP), RFC 1889, for packetized voice transmission. RTP currently provides no form of confidentiality. An IETF draft is underway, Secure Real Time Protocol, to enhance RTP "with confidentiality, message authentication, and replay Protection"[7] Snooping and Eavesdropping are a serious concern in a converged network when compared with the traditional telephony environment where the phone has a dedicated physical connection to the PBX. Some vendors have released interim solutions, which encrypt the RTP media streams for added confidentiality. The International Telephone Union (ITU) has also addressed the topic of snooping and eavesdropping in the H.235 standard, "Security and encryption for H-series (H.323 and other H.245-based) multimedia terminals."

Various points of snooping in Figure 2 include the 802.11b wireless network when used with or without WEP. The 802.11b network provides a shared medium, very similar to an Ethernet hub.

Attackers on the same IP subnet can use man-in-the-middle ARP poisoning tools such as Ettercap or dsniff to re-direct packets to capture and record the RTP streams between hosts. The use of a "switched" Ethernet network does not protect against these types of active attacks.

Less sinister but just as effective, a network administrator can mirror switch port traffic to capture and replay traffic streams. Anyone who can intercept the unencrypted RTP packets between the two communicating end-points can listen in on a conversation.

Phillip Bednarz summed up the state of IP phone market in his article, How VoIP is changing the network security equation by saying, "…the development of security features in new telephones has followed a fixed pattern. First, get it to work and then worry about security. It is a tribute to either the trusting nature of communications engineers or to the enormous pressures to get products to market, that security issues take a back seat to functional features."[6]

The often-mentioned "proof-of-concept" tool to capture and record RTP streams is VOMIT (http://vomit.xtdnet.nl - Voice over misconfigured internet telephones).

**Theft of Service**

The benefits of portability and accessibility introduced by IP Telephony have a downside of an increased risk of service theft. One of the most popular features of IP Telephony is a concept known as hoteling, hot-desking, or substitution. "While call forwarding moves only calls from one phone to another, substitution moves all the features, including address book, access abilities and personalized speed dial."[8] A practical example of this functionality is the ability for the end-user of an IP Telephone to dynamically login/log-off their telephone. No longer is the end-user at the mercy of the PBX administrator for system moves. This ability provides enhanced mobility and allows the full feature carry forward and rights of a user to any IP Phone they log into with their extension. End-users can easily transfer their extension and personalized set configuration to an IP telephone in a conference room or shared cubicle arrangement.

The downside of this functionality is the primary protection against theft of service in the traditional telephony environment, the physical security of the handset, is no longer enough. Additional reliance and responsibility is placed on the end-user to remember to login/logoff the IP Hardphone. Otherwise, end-users risk the abuse of their telephone extension and associated privileges.

Theft of service can also be perpetrated using falsified authentication credentials. A number of IP Telephony vendors authenticate their end points via Ethernet media access control addresses (MACs). MAC addresses are notoriously easy to spoof. An IP Softphone can spoof the functionality and appearance of an IP hardphone to the call processing platform.

Using tools such as SMAC (Spoof MAC) which the authors describe as a "Windows MAC Address Modifying Utility which allows users to change MAC address for almost any Network Interface Cards (NIC) on the Windows 2000 and XP systems, regardless of whether the manufactures allow this option or not." the IP Softphone can be configured quite easily to assume the full functionality and rights of any extension given only the MAC address of that extension.

Finally, the reduction in costs for Moves, Adds, and Changes (MAC) in an IP Telephony environment has led to the addition of daemons/services on many vendors IP Telephones. Some of the more popular services include HTTP, SNMP, and Telnet. Practical attacks and exploitation of these services which can result in the theft of service has been documented in Ofir Arkins paper, More Vulnerabilities with Pingtel xpressa SIP-based IP Phones. A very important distinction between IP Telephones and Traditional Analog and Digital telephone sets in this case (and others as well) is that the IP Telephones were running on the network as ""fully POSIX compliant network devices with storage space, bandwidth and a CPU".[9]

**Denial of Service**

Many IP Telephones are running networking services such HTTP, SNMP, and Telnet. All are running TCP/IP stacks. The exploitation of these devices is no different than those of the servers and workstations running on our data networks. In fact, the exploitation tools and techniques are the same. Some of the recent DOS attacks against IP Telephones are documented in the Cisco Security Advisory, Multiple Vulnerabilities in Cisco IP Telephones. "The Cisco IP Phones are vulnerable to several network based Denial of Service (DoS) attacks including the well-known attacks for 'jolt', 'jolt2', 'raped', 'hping', 'bloop', 'bubonic', 'mutant', 'trash', and 'trash2'."[10]

The nature of a converged networks leads to DOS attacks against the underlying transport medium, the data network and therefore the phone. This may also be a "side-effect" of another type of attack such as the SQL Sapphire/Slammer worm. One infected Slammer host can consume a large amount of bandwidth and render the underlying data network and phones unusable. These types of attacks must be considered when designing a converged network topology.

Signaling messages between the gatekeeper and IP Telephones can be spoofed because there is no signaling message authentication. These spoofed messages can be used to deny service to the targeted IP Telephone.

## Gatekeeper and Gateways (EPN/PPN)

**Snooping/Eavesdropping**

The communication between the Gateway and Gatekeeper is equally vulnerable to snooping/eavesdropping using the techniques described in the terminals section above. The RTP streams can be intercepted between the IP end-stations or between the Gateway and Gatekeeper (IP Trunk). Another area of importance is the encryption and authentication of the signaling channel between devices. The signaling channel is used for communication between end-points such as key presses, when the phone goes off hook, when the phone should ring, etc.

IP telephones send DTMF out-of-band through the signaling channel.

These DTMF entries could be PIN codes, credit card numbers, or other identification credentials.

**Theft of Service**

The primary threat of toll fraud discussed in the traditional telephony architecture remains the major threat in the IP-PBX environment. There have been many new entrants into the IP-PBX market, often, companies with very little past experience in the telephony world. The obvious concern here is the lack of "insight" and experience on the numerous ways call processing software can be manipulated to commit toll fraud. "Software history has a way of recycling. Since programmers are human, they sometimes fail to look back and avoid the mistakes of the past."[11] As has been the case, "'…when you introduce a new technology, the old problems tend to creep back in if you're not careful."[12]

Given the nature of IP, the connection between devices is not "hard-wired", for example the IP Trunk between Boston and New York. These virtual communication paths must be authenticated to ensure that rogue devices are not allowed to register for services they are not authorized for.

**Denial of Service**

In a recent Business Communications Review article, a suite of a denial of service attacks was executed against popular converged call processing platforms. The "DoS attacks were effective when levied against IP-PBX systems. We attacked the call controllers and the IP phones of all 12 systems tested in both the large enterprise PBX review and the SME systems. Of those tested only two…showed acceptable overall resilience to our attacks". The DOS attacks included "several off-the-shelf scripts against both the call servers and the IP phones of each system tested."[13] Obviously, the affect of an attack on the Call Processing platform can impact hundreds (and possibly thousands of telephony end-points). Almost all of the reviewed calls processing servers were running common operating systems. Of the 12 units tested, the operating systems included: 2-Linux, 3-Windows NT/2000, 5-VxWorks, 2 Proprietary. The spoofing and interference with the in band signaling between terminals, gateways and gatekeepers can also be effectively used to deny service.

## Summary

"Some security experts say that VoIP is enjoying a grace period. Because it's a relatively new technology, the underground community has had little opportunity to play with equipment and develop attack tools."[12] Many of the benefits IP Telephony has to offer are directly related to the "openness" of the architecture. It should be clear that there are many more network entry points to be aware of with IP Telephony. Additionally, there must be a bridge between traditional telecom and data communications departments to fully understand and develop a networking infrastructure that can best minimize the risk.

## References


[1] Jaikumar Vijayan, "VOIP: Don't overlook security," ComputerWorld 7 October 2002. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,74840,00.html (3 Jan 2003)
[2] Vijayan, Jaikumar. ComputerWorld. VOIP Security on the Back Burner. October 2002. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,74778,00.html
[3] Sulkin, Allan. Business Communications Review. Flavors Of IP-PBXs. January 2003. URL: http://www.bcr.com/bcrmag/2003/01/p21s1.asp
[4] Sulkin, Allan. Business Communications Review. PBX Market - The Shift to IP Is On. January 2003. URL: http://www.bcr.com/bcrmag/2003/01/p21.asp
[5] Taylor, Steve, Larry Hettick. Network world Magazine. H.323 basics. October 2002. URL: http://www.nwfusion.com/newsletters/converg/2002/01596969.html
[6] Bednarz, Phillip. EETimes. How VoIP is changing the network security equation. October 2002. URL: http://www.eetimes.com/story/OEG20021014S0072
[7] McGrew, Baugher, Oran, Blom, Carrara, Naslund, Norrman. Internet Engineering Task Force AVT Working Group. The Secure Real-Time Transport Protocol. June 2002. URL: http://www.ietf.org/internet-drafts/draft-ietf-avt-srtp-05.txt
[8] Woods, Darrin. Network Computing Magazine. Hold the IP Phone. June 2002. URL: http://www.networkcomputing.com/1315/1315ws1.html
[9] Fisher, Danneis. eWeek. Flaws Plague VOIP Phones. July 2002. URL: http://www.eweek.com/article2/0,3959,373289,00.asp
[10] Cisco Security Advisory: Multiple Vulnerabilities in Cisco IP Telephones. May 2002. URL: http://www.cisco.com/warp/public/707/multiple-ip-phone-vulnerabilities-pub.shtml
[11] Audin, Gary. Business Communications Review. Packetized Voice: It's the Software, Stupid! September 2002. URL: http://www.bcr.com/bcrmag/2002/09/p48.asp. URL: http://www.webtorials.com/main/resource/papers/BCR/paper46/2002-09-audin.pdf
[12] Conry-Murray, Andrew. Network Magazine. Emerging Technology: Security and Voice over IP - Let's Talk. November 2002. URL: http://www.networkmagazine.com/article/NMG20021104S0004
[13] Percy, Kenneth M., Randall E. Birdsall, Diane Poletti-Metzel, Eric Reichard. Business Communications Review. BCR Best-in-Test-SME IP-PBX Systems. January 2003. URL: http://ftp2.bcr.com/voicecon2003/ippbxtest.pdf