VOIP: Security issues, Security Mechanism and Inherit Dangers of Security

Sangeeta Bhandari
Asstt. Prof. HMV, Jalandhar
sangeetakapoorbhandari@gmail.com

Abstract: Voice communication started in 1878 using PSTN (Public Switched Telephone Network). Slowly and gradually number of telephone users and number of calls per year increased up to year 1900. After year 1900, number of telephone systems and number of calls per year increased like anything. The main issue with conventional telephone system was cost, to reduce the cost and using fast growing internet connectivity, service provider introduced the VoIP (Voice Over Internet Protocol) for organization and residential users. This paper mainly deals with the security issues of VoIP and their countermeasures. The solution or security implemented to avoid security issues further introduced some other issues, so main aim of this paper is to discuss those inherit dangers of VoIP security.

Keywords : software effort estimation, fuzzy inference system, COCOMO.

1. INTRODUCTION

VoIP stands for Voice over Internet Protocol, it refers to carry voice call over IP data network. The main attraction of VoIP is its ability to reduce expenses. In simple words VoIP enables you to make voice calls over data network. VoIP converts your voice to digital data and then it transferred across the network. Advantages of VoIP include toll bypass, network consolidation and service convergence. Thousands of dollars are saved for large enterprises by placing long distance calls over an IP network instead of traditional telephone system. Network consolidation enables the transmission of data, voice, and video over one single network. The integration greatly reduces setup and maintenance costs. With service convergence, enhanced functionality can be implemented through coupling of multimedia services.

Securing VoIP system is more challenging than securing pure data network. First, all security problems related with data network appear in VoIP system since they share same network infrastructure. Secondly, VoIP does not have a dominant standard so far. The support of two standards in products just increases the chance of buggy application. Dozens of proprietary protocols make the matter worse. Thirdly, the QoS (Quality of Service) requirement of VoIP leaves less working room for possible security measures. A very secure VoIP system that cannot deliver good voice quality is not attractive.

2. LITERATURE SURVEY

Upkar Varshney, Andy Snow, Matt McGivern, and Christi Howard (2002) discussed the development, General architecture and functionality of PSTN and VoIP. They also discussed the protocols, adoption and prospect of VoIP [3].

Alan Klein (2003) presented the Security analysis of Traditional and IP telephony. He compared and contrasted the environment and architecture of Traditional and IP telephony. He also discussed the security concerns of traditional and IP telephony [5].

Jianqiang Xin (2007) has discussed and explained the fundamentals of VoIP, its security issues and countermeasures. Jianqiang Xin categorized the VoIP attacks into three main categories that are Confidential, Integrity and Availability threats. He also presents the countermeasures of VoIP security issues [1].

Filip ŘEZÁČ and Miroslav VOZŇÁK (2010) has discussed different VoIP attacks and protection against those attacks. Based on the threat behavior Filip ŘEZÁČ and Miroslav VOZŇÁK divided the VoIP attacks into different categories that are Scanning and Enumerating a VoIP, Exploiting the VoIP Network, VoIP Session and Application Hacking, Social Threats. Filip ŘEZÁČ and Miroslav VOZŇÁK introduced the concept of SPITFILE to avoid the security attacks on VoIP [2].

Fisher, Danneis (2002) Bednarz, Phillip (2002), R. Barbieri, D. Bruschi, E Rosti (2002), Conry-Murray (2002), Andrew D. Richard Kuhn, Thodiscussing mas J. Walsh, Steffen Fries (2005), discussed various aspects of VoIP security, possible attacks and security requirements of VoIP [12] [14] [16] [19] [15].

We have discussed the VoIP security a lot but we haven't discussed the inherit dangers of VoIP security yet, so in this paper we will try to discuss some of inherit dangers of VoIP security.

3. PROBLEM OF UNIFIED NETWORK

The World of Computer Networks is evolving tremendously, especially in term of speed and new services but new services are also bestowing new complexities. Network services can mainly categorized into three categories that are Data, Voice and Video. These services are different in nature and requirements. Traffic characteristics for different types of traffic remains the same, in simple words traffic characteristics like delay, jitter, throughput, lost packet percentage and burstiness remains the same but values of these characteristics are different for different type of traffic, so it's become very difficult to manage all these types of traffic in same line.

One can assume diverse networks for these services as shown in Figure 1, but that's not possible, in simple words we can't three different networks for these different services, we can't have different lines for different type of traffic.

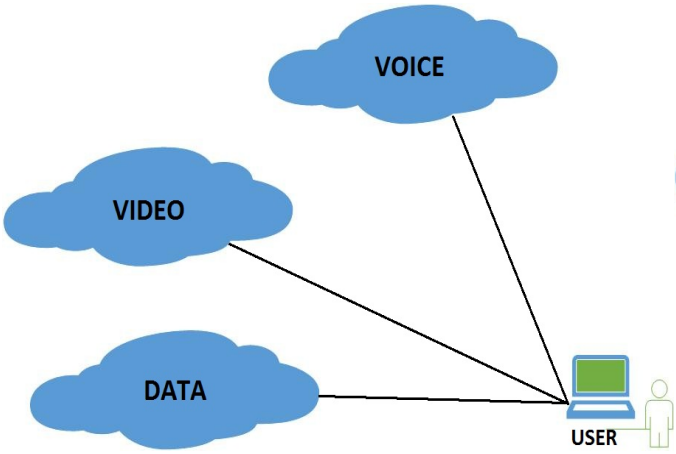

Figure 1

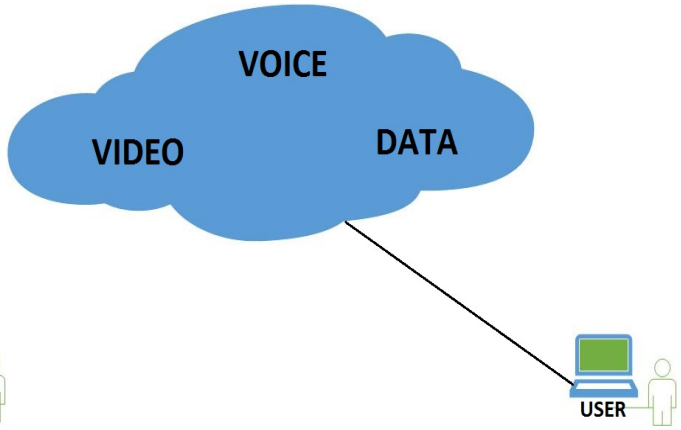

Figure 2

The Biggest challenge these services presenting is unified networks, means the single network with Data, Voice and Video as shown in Figure: 2.

In this paper we will be discussing voice services. We will discuss why corporate should move to Voice networks? How corporate can move to voice networks? , and security of voice networks and its inherent dangers.

4. VOIP: STRUCTURE AND WORKING OF TYPICAL VoIP NETWORK

VoIP Network mainly consists of three types of devices: Infrastructure Devices, Call Processing Devices and Endpoint Devices.

Infrastructure Devices: Infrastructure includes Router and Switches. These devices are the building blocks of not only VoIP network but of all the networks.

Call Processing Devices: Call processing devices are the brain of the VoIP network, these devices are responsible for running VoIP network. Call processing Devices includes Call Manager.

Endpoint Devices: These devices include IP Telephone, VoIP devices.

Figure 3 represent the typical architecture of VoIP network:

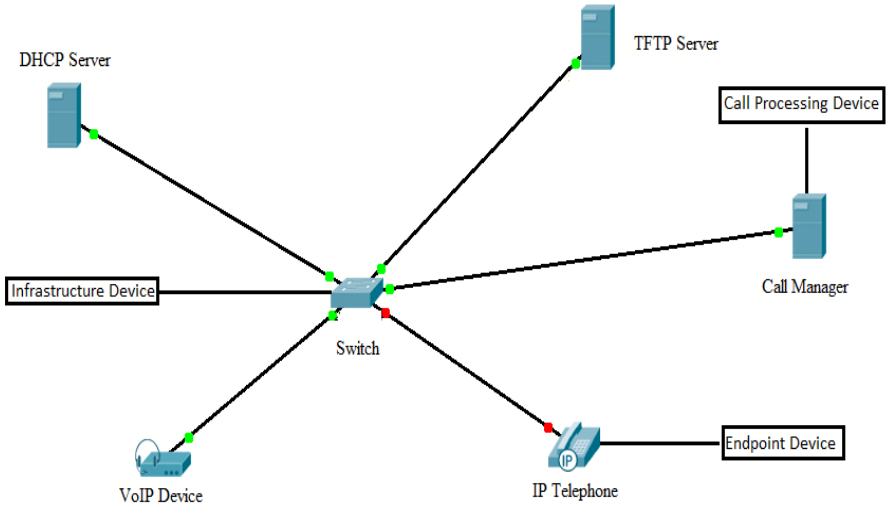

Figure 3

Endpoint Device initialization process:

Startup process of endpoint device can be explained as follows:

1. Switch detect unpowered device and supplies power through PoE (Power over Ethernet).
2. End device loads its OS.
3. Switch provide VLAN information to end device.
4. End device send IP request to DHCP server and acquire IP address.
5. End device with help of DHCP contacts the TFTP server and load configuration file.
6. End device contacts first Call Manger present in configuration file.

5. WHY CORPORATE SHOULD USE VoIP

Corporate tends to reduce investments and improve saving, now VoIP offers corporate a cost effective model. The main benefit is in term of cost. Main things that reduce cost are as follows:

1. Move, Add, Change (MACs): VoIP offers MACs, the one of the biggest feature in IT world. VoIP devices enables portability, scalability and flexibility. Relocation of VoIP devices require no or very less configuration.

2. Reduced Cabling and Wiring: By moving to VoIP a corporate can get rid of huge amount of wiring used in conventional telephone network. Single wire will connect IP Telephone and Computer offering Data and Voice services.

3. Solitary Location for different services: VoIP present single location or inbox for different messages. For example: Voicemail, FAX, email and conferencing.

4. Website Integration: VoIP also offer you the option of integration of its voice services with internet website. That's really a great feature to increase customer satisfaction.

5. Open Architecture: IP Telephony world is based on Open architecture, in simple words multi-vendor support is there in VoIP through universally accepted protocol SIP.

6. HOW A CORPORATE CAN MOVE TO VoIP

As we discussed VoIP helps in cost reduction but now suppose a company is running conventional PBX, they will say if we will move to VoIP all our investments in PBX go in vain and wasting our investments in PBX just for low cost distance call is meaningless. So the solution of this problem lies in upgrading the routers of company with the capabilities of PSTN. This can be full filled by adding VWIC (Voice in WAN Interface Card) module. This way company will continue enjoying conventional PBX and they will also have the features of VoIP, and moreover backup line will be there every time as shown in figure 4.

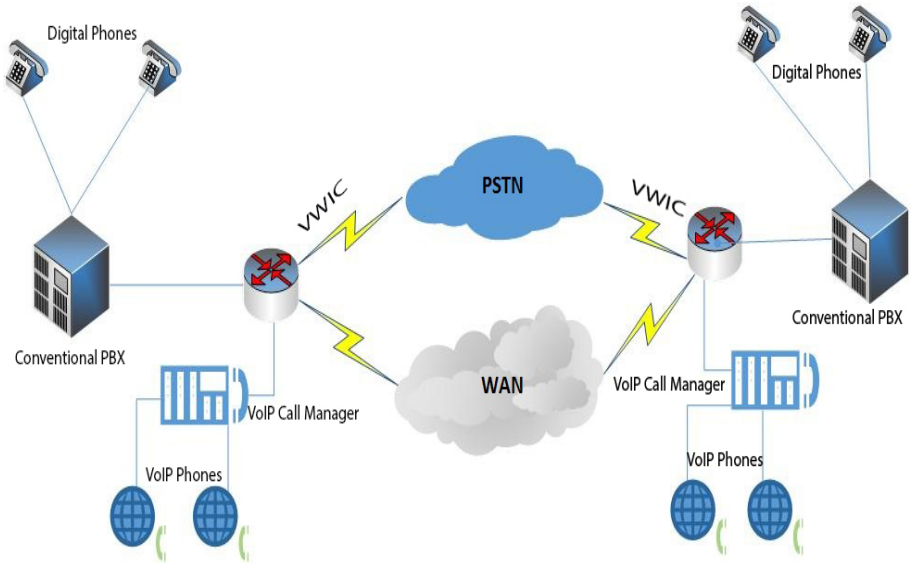

Figure: 4

7. VoIP SECURITY THREATS AND COUNTERMEASURES

In this section we will discuss VoIP security threats and there countermeasure. VoIP systems rely on a data network, which means security weaknesses and the types of attacks associated with any data network are possible. For example, in a conventional telephone system, physical access to the telephone lines or a compromise of the office private branch exchange (PBX) is required for in order to conduct activities such as wire-tapping. But for VoIP, voice is converted into IP packets that may travel through many network access points. Therefore the data is exposed to many more possible points of attack that could be used for interception by intruders. In fact, all the security risks associated with IP, such as computer viruses, Denial of Service and man in the middle attacks, are also dangerous to VoIP systems. In particular, PC-based IP Phone hosts are more susceptible to attacks due to the prevalence of attack techniques pinpointing PC systems. These include operating system vulnerabilities, application vulnerabilities, service vulnerabilities, worms, viruses, and so on. A PC-based IP Phone is also at risk from any attack aimed at the entire data segment upon which it is residing.

We can broadly categorized security threats into three categories: Confidentiality Threats, Integrity threats and Availability threats, we also have some challenges associated with NAT and Firewall. We will discuss these issues one by one.

1. Confidentiality Threats

Confidentiality means keeping the information from unauthorized users. Confidentiality threat means danger of accessing confidential information by unauthorized users. Confidential threats includes **Eavesdropping of phone conversation** and **unauthorized access attack**.

Eavesdropping of phone conversation: Eavesdropping in conventional telephone requires either physical access to wire, or penetration of a switch. With VoIP, opportunities for eavesdroppers increase dramatically because of the large number of nodes in the path between two conservation entities. If the attacker compromises any of these nodes, he can access the IP packets flowing through that node. There are many free network analyzers and packet capture tools that can convert VoIP traffic to wave files. These tools allow the attackers to save the conversation into the files and play them back on a computer.

Unauthorized access attack: Unauthorized access attack means that the attackers can access resources on a network that they do not have the authority. As we discussed earlier we have call processing devices, switches, and routers in VoIP network, for example call manager. All the call manager stores thesensitive information and if attacker gain access over the call manager then attacker can make any changes.

Countermeasures for Confidentiality Threats:

Encryption of the voice packets can decrease the risk of eavesdropping. IPsec, SRTP can be deployed to increase confidentiality of voice data. Unauthorized access attack can be prevented by securing devices, they should be using Secure Shell (SSH) instead of plain text. And an up-to-date IDS should be there in network.

2. Integrity Threats

Integrity of information means that information remains unaltered by unauthorized users. A legitimate user may perform an incorrect or unauthorized operations function and may cause delirious modification, destruction, deletion or disclosure of switch software and data. An intruder may masquerade as a legitimate user and access an operation port of the switch. Integrity threat means danger of unauthorized alteration of information. Main integrity attacks are **Caller Identification Spoofing**, **Registration hijacking**, **Call redirection**.

Caller Identification Spoofing: Caller identification spoofing means creating a fake caller id for outgoing calls. In this the user on receiving side will not be able to judge the caller because he will be provided with other number from which caller is calling, it might be the number of other user.

Registration Hijacking: Registration hijacking means when an attacker replace the legitimate registration of the victim with his address. The attack causes all incoming calls for the victim to be sent to the attackers address.

Call Redirection: Call redirection means the interception of call and rerouting call through a different path that is not intended before reaching the destination. Possible methods include proxy impersonation and registration spoofing. The attacker can also spoof the response from the recipient and trick the requestor to talk with the attacker.

Countermeasures for Integrity Threats

We can't here to prevent caller ID spoofing, there is no effective way to cop up with this problem yet. The best solution so far is not to trust caller ID at all. Stronger authentication schemes are the solutions to registration spoofing, proxy impersonating and call hijacking. To mitigate this type of attacks, software patching is crucial to fix any known vulnerabilities. VoIP vulnerability scanning tools like Sivus is strongly recommended.

3. Availability Threats

Availability refers to the notion of availability of information, services and resources whenever required by authorized user. Availability threats means the danger or risk of compromising the availability of information and services. VoIP network is susceptible to denial of service attacks since DoS attacks can degrade QoS quickly to unacceptable level. Traditional DoS attacks against data networks are still very dangerous. Here we will discuss about VoIP specifics DoS attacks. We can mainly categorize the availability threats into **VoIP signaling DoS Attack, VoIP media DoS attack, and Physical DoS attack.**

VoIP signaling DoS Attack: In this attack, an attacker can use signaling protocol to create DoS. An Attacker can create huge number of call setup requests that consume the processing power of proxy server or terminal. The attackers can also launch distributed DoS to cover trace and aggregate requests. These activities ultimately results in DoS attack. These type of attack can only be created in LAN.

VoIP media DoS attack: In this attack an attacker can flood VoIP network components with large number of RTP. If the target is enforced to drop the RTP packet, this ultimately result in degradation of voice quality. If attacker will succeeded in attacking key VoIP network component like gateway, and if it will go offline the entire network will be down.

Physical DoS attack: This attack includes the damaging VoIP network component physically.

Countermeasures of Availability threats: To cop up with VoIP signaling and media DoS attacks, strong authentication is the most important weapon. VoIP components should be communicating with authentic counterparts. VoIP firewall should also be implemented to monitor streams and filter out abnormal signals and RTP packets. Media and signal rate limits can be set by observing normal traffic patterns. To mitigate physical DoS attacks, strict physical security schemes should be implemented with restricted areas, access control, locks, guard, etc. To guarantee continuous power supply, backup power generation system should be available.

8. INHERENT DANGERS OF VoIP SECURITY

We have discussed the security threats in VoIP network and we also discussed the countermeasures of security threats. The countermeasure discussed above some time inherit some dangers. In this section we will discuss some inherent danger of VoIP security. The inherit dangers of VoIP security are as follows:

1. IDS Restraints: as we discussed strong encryption algorithms are required to avoid Confidential and Integrity threats, implementing strong encryption present problems for IDS, which is one of the most crucial component of VoIP security. IDS device can't monitor and scan encrypted data. So if we strengthen the encryption mechanism the IDS will become useless, and probability of outside attacks will be increased.

2. Defense in depth Restraints: Defense in depth means implementing the static packet filtering, stateful packet filtering, NIDS, HIPS, HIDS, HIPS, and antivirus. The hard rule making will ultimately result in packet drops because routing security devices have mainly limitation with VoIP, for example H.23 protocol has many problems related with firewalls and IDS.

3. NAT restraints: NAT (Network Address Translation) contributes a lot in securing internal network from external network, but NAT makes VoIP communication nearly impossible. It is very difficult to make VoIP aware of NAT, some very tricky port forwarding is required in firewall to make two communication of VoIP devices. Though we have solution like STUN, TURN, ICE, B2BUA for NAT restraints but none of these is 100% efficient.

4. Security restraints of Softphone System: It doesn't matter how much network security is tightened but if you have deployed VoIP using Softphone system, you can't be sure of security. Softphone system that are connected to internet usually have lots of virus, worms, Trojans and other malicious.

9. CONCLUSION

We have discussed the building blocks, operation procedure, security issues and countermeasure of security of VoIP. We also tried to introduced the inherit dangers of VoIP security. VoIP service is totally different from conventional Telephony and also requires unique treatment as compare to data traffic, and obviously the security requirements of VoIP are also different. It has been shown that, though we have many security mechanism but these mechanisms are also presenting some dangers that we have discussed in this paper. We conclude that the security techniques used for TCP/IP based networks are not enough or fully appropriate to provide security to VoIP traffic, moreover current security systems have inherit dangers as well, impact and handling of inherit danger is scope of our future work.

REFERENCES

1. Jianqiang Xin "Security Issues and countermeasure for VoIP". SANS institute 2007.
2. Filip ŘEZÁČ, Miroslav VOZŇÁK "security risks in ip telephony", information and communication technologies and services, vol. 8, no. 1, march 2010.
3. Upkar Varshney, Andy Snow, Matt McGivern, and Christi Howard "VOICE OVER IP", COMMUNICATIONS OF THE ACM January 2002/Vol. 45, No. 1.
4. "VOICE OVER IP SECURITY", The Government of the Hong Kong Special Administrative Region, February 2008.
5. Alan Klein "Security Analysis: Traditional Telephony and IP Telephony", SANS institute 2003.
6. Debashish Mitra "Network Convergence and Voice over IP", Tata Consultancy Services, March 2001.

7. P. Mehta and S. Udani, "Overview of Voice over IP", Technical Report MS-CIS-01-31, Department ofComputer Information Science, University of Pennsylvania, February 2001.
8. B. Goode, "Voice Over Internet Protocol (VoIP)", Proceedings of the IEEE, VOL. 90, NO. 9, Sept. 2002.
9. Roberts, C., "Voice over IP security", Center for critical Infrastructure Protection, 2005.
10. Black, U. "Voice over IP". Prentice Hall, Upper Saddle River, NJ, 2000.
11. VOZNAK, M.; REZAC, F.; KYRBASHOV, B.; HALAS, "M. Possible attacks in IP Telephony". In proceedings RTT2008, 9th International Conference, 10-12.9 in Vyhne, Slovakia. SlovakUniversity of Technology in Bratislava, ISBN 978-80-227-2939-0.
12. Fisher, Danneis. "eWeek. Flaws Plague VOIP Phones". July 2002.
13. Cisco Security Advisory "Multiple Vulnerabilities in Cisco IP Telephones". May 2002.
14. Bednarz, Phillip "How VoIP is changing the network security equation", EETimes, October 2002.
15. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, "Security Considerations for Voice Over IP Systems", Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, January 2005.
16. R. Barbieri, D. Bruschi, E Rosti, "Voice over IPsec: Analysis and Solutions". Proceedings of the 18th Annual Computer Security Applications Conference, 2002.
17. James S. Tiller (2000), "A technical guide to IPSec Virtual Private Networks" Auerbach publications.
18. Schulzrinne, H., "Converging on Internet Telephony". IEEE internet Computing (1999).
19. Conry-Murray, Andrew, "Emerging Technology: Security and Voi ce over IP - Let's Talk", Network Magazine, November 2002.