Security and Risk Analysis of VoIP Networks

S.Feroz and P.S.Dowland

Network Research Group, University of Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

This paper address all major issues related to VoIP security, and provides detailed technical information about VoIP. The focus of this paper is to highlight, discuss and introduce security issues relating to VoIP networks given the expansion in the usage of VoIP within large corportations. This paper discusses current threats and future security measures related VoIP.

Keywords

Security measures, vulnerabilities, risks, solutions and best practices.

1. Introduction

Voice over Internet Protocol (VoIP) is developing telephony solution that brings voice and data traffic together on the same IP-based network. Telecommunication networks are now getting replaced with data communication networks and voice signals are now getting transferred over data networks by converting them into data packets. In VoIP calls are transmitted over an IP network instead of using PSTN. Because Internet network is getting widely available at various high bandwidth place of world VoIP that's why VoIP is becoming the best option.

The focus of this paper is to highlight, discuss and introduce security issue regarding VoIP networks, since VoIP is spreading rapidly and getting adopted by every other multinational and end user. There are rapidly increasing security threats taking place. This report discusses current threats and future security measures related VoIP.

2. VoIP Over view

Voice over Internet Protocol (VoIP) provides a communication between people and continuous access to networked services in such flexibility. A VoIP technology deals with the routing of voice and data between wired and wireless network. Many problems arise, such as poor service quality where data and voice packet shared the same bandwidth. The impact of security in the current environment of VoIP and the concerns related to its security QoS issues, protocol level security of several Threats as well as their impact on VoIP.

VoIP is a technology that is used to make telephone calls over the Internet using broadband connection using computer network instead of a regular phone

connection. VoIP converts the analog signals from the phone to digital signals so that the signals can travel over the Internet (Polaris, 2002).

Anyone can place a VoIP call by just picking up the phone and dialing the relevant number. The call from your local telephone provider is routed to your VoIP provider and through the internet the call goes to the other party's local telephone provider. In this way the VoIP connection is established from the calling person to the caller. Depending on your VoIP provider the call charges may be either flat or he may charge for local calls. Generally a flat per minute rate is charged from VoIP service providers. That means you can make local call, long distance calls or even international calls.

2.1 Advantages of VoIP

- If you are having a broadband internet connection then you do not need to maintain another line just for making phone calls. Since the same VoIP line can be used to dial any phone number. So, you can save a lot on your telephone bills.
- You can talk to as many people as you want at the same time without paying any extra charges and this facility is known as conferencing.

2.2 Disadvantages of VoIP

- If you think that you can replace your normal telephone with a VoIP connection then you need to be sure as many VoIP providers do not have back up power incase of power outages.
- Mostly through VoIP call do not connect to the emergency numbers.
- VoIP providers generally do not have directory assistance

3. Features of VoIP

3.1 VoIP – Cost effective

If we compare the regular calls charges of the PSTN i.e. Public Switched Telephone Networks especially for long distance calls then the VoIP calls are far cheap (Network world, 2005).

3.2 Quality of Voice in VoIP

VoIP is a very good alternative to PSTN in terms of bandwidth and better quality. But in practical scenarios it does not perform up to the level it guarantees. Since there is a single network maintained, organisations face a lot of data congestion issues. The voice signals need to be transmitted in real time but actually it does not happen and there are significant amount of delay in the packet delivery at the other end that results in voice breakage. Since, VoIP is an emerging technology; research is still going on to deliver better services to the consumers.

3.3 VoIP's legacy and privacy issues

Government rules of monitoring the lines incase of PSTN is absolutely different from the VoIP lines. Security of Call Detail Records (CDR) is one of the privacy issues which fall under the privacy Act of 1974 (Microsoft Tech Net, 2005). Many private VOIP service providers maintain CDR so that they can keep track of the billing, fraud, theft of the resources etc. So, the VoIP service providers keep these records for future purpose but the maintenance of CDR comes under the privacy and security issues of an individual.

3.4 VoIP's Vulnerability

Considering the fact that VoIP systems have some security concerns still the organisations deploy VoIP systems in order to get a better quality service at lower cost. The quality of service provided by VoIP systems is the most important factor in switching to a VoIP System. However, the organisations should realise that voice signals in the form of packets, traveling over the internet are highly susceptible to the amount of attacks as the core data networks. All the packets can be easily intercepted by any hacker and can be manipulated and re-routed. Denial of service and hijacking are major issues in VoIP networks. Even the operating systems are vulnerable as VoIP systems are installed on existing Operating systems and application having no or rather very less security protection.

VoIP requires some basic components and a signaling and transmission protocol for its deployment. The components include the customer premise equipment, Call processing and Management Application and Voice Handling Server.

3.5 Hardware and Software Requirement for VoIP System

In order to create a VoIP System you need to have a Computer with full duplex capable Sound card and a broadband internet connection. You also need the appropriate dialer software and headset with mike if you are dialing through keyboard. We need a duplex sound card else one cannot hear anything while speaking. This is the minimal requirement for a VoIP system but you need special cards with hardware accelerating capabilities like Quicknet and Voice Tronix (VoIP NEWS," Articles of VoIP). Operating systems like Windows or Linux are good enough for VoIP to take place.

Microsoft Windows NetMeeting provides some VoIP services and in Apple Macintosh they have something similar known as iChat. Even Linux has a lot of VoIP applications.

3.6 VoIP Communication

With VoIP communication coming into existence the internet technology has really changed. Now the voice packets are inserted into data packets using some real time protocol. Next thing is to use some signaling protocol to call the users. When the data packets have reached the destination then those packets have to be decompressed and the data needs to be extracted from the packets.

3.7 VoIP Components:

- Customer Premise Equipment
- Call Processing and Management Application
- Voice Handling Server

4. Security Measures to Threats

- Denial of Service (DOS)
- Toll Fraud
- Call Recording
- Eavesdropping
- Call Hijacking
- Message Integrity

This attack generally relates to IP issues that include VoIP, email, e-commerce and Domain Name service**.**

4.1 VoIP Security Issues

The popularity of VoIP increasing day by day the VoIP security issues are also increasing. Before VoIP came into existence, people were only considering the data security but now voice security is also important. Anyone can intercept the call and can easily gain access to that information if the voice packets are not encrypted.

4.1.1 Why security has been overlooked?

Currently there are not much cases heard about the breach in security of VoIP communication. Once people start thinking in terms of security automatically they would start investing in security infrastructure in order to protect their VoIP systems and VoIP network communication resources.

4.1.2 Security Challenges

Once, VoIP reaches to the masses, security will gain importance amongst VoIP service providers, with the happening of few incidents concerning security breach (Tyson and Valdes, 2004). If we talk about the organisation's usage of VoIP network, they have started feeling the lack in security infrastructure as the packets have to travel through an un-trusted medium known as internet. So, gradually there is a growing demand for security systems to protect VoIP network components from nasty attacks from any intruder in and outside their domain area.

4.1.3 Security and VoIP

The VoIP application running on the organisation data network. If an organisation is considering security planning for VoIP systems then they might consider the following:

Since we all know the potential of VoIP like lower costs and greater flexibility, we should be careful before deploying VoIP components into existing IP networks. In case the existing network is already congested and overburdened then the integration of a VoIP system would cause serious issues.

Generally people think that since the voice packets are also digitised they can be easily used over the existing data network architecture with similar security measures. But actually there is a lot more to VoIP security than the data security. NIST has also laid down some of the security guidelines for VoIP systems. (Rosen. B, 2005).

4.1.4 Is VoIP Scary?

VoIP without security is just like a person without mind. Mind controls the body and in VoIP security controls anyone entering your system. So, security is one of the preconditions for the deployment of VoIP system. Majority of the VoIP attacks are application based. Some of the indications of security issues in VoIP systems are dropped calls and hearing issues. Once the companies start broadcasting their SIP addresses in VoIP communications then VoIP security would be a major concern for most IT experts. According to Internet Security Systems (ISS), Cisco's VoIP is not designed with security in mind and have so many security flaws. An implementation flaw in Cisco's Call Manager that handles call routing and signaling, could allow an overflow in buffer that would grant an intruder to access the VoIP system and listen all calls routed through it (Internet Security Systems Inc. 2004"VoIP). ISS warns the companies using the new VoIP technology to take VoIP security seriously else they might loose enough money if some intruder steals some important information.

5. Quality of Service (QoS)

Quality of Service (QoS) refers to the quality of the usual or traditional telephone network compared to the quality of the voice in VoIP network. Although calls in VoIP systems are far cheaper than that of the usual PSTN telephone calls but still of VoIP cannot guarantee the equivalent quality of service which traditional PSTN offer then it is of no use. Any VoIP network should address these QoS issues before the VoIP system is actually deployed.

5.1 Different Protocols used in VoIP

- H.323 Standard
- H.323 Multipoint Control Units, Gateways, and Gatekeepers
- SIP

5.2 Benefits

H.323 products and services offer the following benefits to users:

- Since various companies have adopted H.323 as a standard for audio transmission over the internet. All products services developed by different manufacturers using the H.323 standard protocol can interoperate. H.323 conferencing clients, bridges, servers, and gateways support this interoperability.
- Different bit rates are used for formatting of the data with audio codecs that are provided by H.323. It is up to the users to choose the codec that is best supported by their computer and network selections.
- Audio-visual teleconferencing can be done with the support of T.120 with H.323

5.3 Components of SIP

- SIP Servers
- SIP User Agents

5.4 Best Practices for moving to secure VoIP

- **Network Architecture**: We need to have strong network architecture. By strong we mean that the architecture or the network design should be such in which we have separate networks for voice and data. Ensure that all the VoIP related communication is through some standard firewall.
- **Legal advisors**: You should regularly visit your legal advisor to verify about any possible new law or concern that the company needs to give some extra attention. You should be aware of any new law if passed that may affect your company at a later stage
- **Soft phones**: Always try to avoid using soft phones with headphones and special software's as the computers use data networks and that may interfere with the voice network.
- **Risk Analysis**: A proper risk analysis should be done before implementing VoIP in your company as to know the cons and the danger involved is equally important. Also, to know the cost of the implementation is essential.
- **Security Features**: There should be proper security environment to implement VoIP systems. Adequate security layers should be there in order to have a proper security enabled environment
- **Backup Power Supply**: There should be a very good backup power supply system for the office where VoIP systems is implemented. Even the backup power system should be provided for the individual instruments.
- **Physical Controls**: VoIP Networks should be encrypted and this is one of the most important characteristics of voice networks. The landlines can be easily tapped so there is no question of the VoIP networks being interpreted by intruders.
- **Emergency Services**: Dealing with emergency service is one of the major challenges in the implementation (E-911) of VoIP systems as all VoIP system will not be able to identify where the physical location of the office is and route the 911 calls to the right center
- **WiFi Security**: Now since the technology is changing we should consider the need of integration of VoIP systems with Mobiles, since to break the

security of WiFi systems is tougher than that of conventional landline phones. Security features of Wired Equivalent Privacy (WEP) offer very little or rather no protection as WEP security can be easily broken with some publicly available software's.

6. Conclusions

There are some specific additional security measures, mostly dealing with securing the signaling to set up VoIP sessions, but, in general, networks with good practices for IP security will have good VoIP security. Although solutions to some problems have o been proposed, designed and accepted; the research does not stop. This is due to the fact that technologies are an on-going subject evolves everyday. As this unique environment of VoIP develops and increase at rapid pace, new challenges and problems occurred. However, we must not ignore the security impact that relies on how we tackle the situation in handling the security issues. It is important to know the various threats in VoIP technology. Something that is will end up suffering due to poor security implementation. Usually some times is required for a new technology to gain adequate level of security. The awareness of risk factors described in this paper will help to prepare for VoIP and should help mitigate potential security breaches and raise internal security awareness within organisations to significantly reduce risks from unwarranted attacks in order to provide reliable operations and services in the VoIP. In order to meet user requirements and to satisfy user needs for reliable operations over VoIP, some sort of guidelines are needed. This paper has highlighted the challenges faced by user of VoIP environment and the various kinds of approaches that can be used to tackle those problems.

7. References

Internet Security System Inc. (2004), "VoIP: *The Evolving Solution and the Evolving Threat*", http://www.documents.iss.net/whitepapers/ISS_VoIP_White_paper.pdf (21/07/05)

Jupiter Web Network (2002), "Whitepaper: *Advantages of SIP for VoIP*", http://www.webpedia.com (02/09/05)

Network World (2005), "*VoIP security can not be ignored*" http://www.findarticles.com/p/articles/mi_qa3649/is_200508/ai_nl4879749 (25/07/2005)

Planchard, C. (2005), "*The Future of VoIP: Secure, Integrated Collaboration?*", http://www.tmcnet.com/usubmit/2005/Aug/1171625.htm (28/07/05)

Polaris (2002), "*A reference guide to all things VoIP*", http://www.voip-info.org, (12/06/05)

Rosen. B. (2005), "*VoIP and Frauds*", http://www.voipsa.org/pipermail/voipsec_voipsa.org/2005-February/000072.html (08/7/05)

Tyson and Valdes (2004), "*How VoIP Works*" http://www.computer.howstuffworks.com/ip-telephony.htm (10/07/05)