Global Information Assurance Certification Paper

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b

VOIP : A NEW CHALLENGE

Chairil Hidayat Abdul Razak
March 26, 2004

Abstract

The main character of this paper can best be expressed in the form of a question: "What are the new challenges that we face by implementing VOIP?" Objectives of the paper are to first briefly introduce about VOIP in general, then identify some security issues which is related with VOIP and finally to analyse the best practise for implementing VOIP.

This paper is not written to address all issues related to VOIP security, and give detailed technical features about VOIP. The scope is only covered the surface and give introduction on some of the most important existing and identified, security issues.

1. Background

Voice over Internet Protocol (VOIP) provides a communication between people and continuous access to networked services in such flexibility. It is a new era of telecommunications technology which is increasingly in demand. VOIP is a combination of hardware and software technology which allow voice to be transferred through the internet. It is a process where people use the internet protocol as transport medium for voice communications. It is understood that VOIP take voice as another form of data and use an algorithm as a compression agent to ensure optimal use of the bandwidth.

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. Solutions applied to traditional direct phone infrastructure cannot be applied in this environment.

In this paper, I am discussing the challenges and security issues associated with VOIP. Where appropriate, I identify the promising approaches that researchers have applied, as well as their limitations.

In section 2, I am looking into the reliability of VOIP in networking. Discussion on difficulties associated with extending services or networks to operate on VOIP is included. Section 3 surveys on the security issues in the VOIP environment. An issue such as threat for security and best practice for implementation is discussed as well. Finally, section 4 concludes remarks as well as opinions of future work considerations.

With this paper, I hope to highlight the challenges and problems that a VOIP user might face. This is in order to give clear picture for those who are looking into this unique environment foresee what is ahead.

2. Reliability

As we know, VOIP as an alternative to traditional telephone direct line helps reducing telephone and facsimile costs and to set the stage for advanced multimedia applications and services such as unified messaging, in which voice, fax, and e-mail are all combined.

Despite the features that make Voice over IP so attractive from the standpoint of cost and flexibility of telephone services, businesses will only adopt it once they've determined whether, and under what circumstances, the quality of VOIP will be satisfactory to users. I will discuss the reliability of VOIP have in a single view of VOIP network performance and voice quality.

Network performance

Deploying a real-time application like VOIP across a network designed for data presents unique challenges for network managers. Concepts native to data transmission such as jitter, packet loss and delay can cause significant frustration in the realm of telephony, where users and customers expect nothing less than toll quality reliability on every call.

- **Jitter.** In IP networks, not all packets suffer the same amount of delay. Variations in packet delay also known as jitter; cause VOIP packets to arrive at their destination in uneven patterns. This can result in degraded voice quality. Typically, the solution to jitter problems is to increase the size of the jitter buffer in VOIP components. However, this solution increases overall delay and must take into consideration network delay characteristics. [1]

- **Packet Loss.** Because of the small size of VOIP data packets, an occasional lost voice packet will have negligible impact. However, as packet loss nears or exceeds one percent, voice quality is degraded. This is especially true if packet loss occurs in bursts. [2]

- **Delay.** Because voice calls are real-time, full-duplex communications, end-to-end delay of packets can have severe repercussions on usability of the VOIP solution. Delay of less than 150ms is considered acceptable, while delay of more than 400ms is considered to be unusable. [3]

Voice Quality

Voice quality is the most important criteria that people aspect when migrating to these new technologies. It depends on several things which are

related. Specific algorithm is been used in order to transform voice into data. This requires coded and decoded process. Transmitting the voice data from the source to destination must be able to succeed without delay, loss or corruption. Traditional phone direct line provides a continuous data tunnel to ensure the flow of data voice. The transmitting success is determined by amount of bandwidth available in the network connection, the smoothness flow of packet data and any corruption of data that occurs.

To ensure the voice quality meets high standard requirements by the users, the ability of a network to transport voice data packet fast and consistent is needed. This requires a very high Quality of Service (QoS) network.

3. Security Issues in VOIP

Many major corporations are in the move towards VOIP technologies to cut communications cost. Therefore security is a very important aspect to be considered in order to maintain the integrity and privacy of corporate operations. We have to realize and shouldn't overlook the security issues when voice and data merge together in one network connection.

I believed that common things people like maintain when implementing a new technology is integrity, confidentiality, authentication and non–repudiation of information.

"Life was simple before World War II. After that, we had system"

Admiral Grace Hopper

To ensure security in a new technology is not an easy task. The convergence between data and voice in one single network require users to focus more on the security aspect for VOIP to make into the corporate world.

This converged technology can be seen as a huge threat, not only to users but to the industry as well. As we can see, VOIP is solely relying on the electricity for supporting its operation. Comparing to traditional phone line, we don't have to rely on the electricity for its operation. Disaster such as, power failure, natural disasters etc which can destruct the electricity contribute directly for the failure of using this technology. Imagine how it would be when we need to use the phone to make a very important phone calls but there is no electricity.

VOIP use IP as its main backbone for operation. This inherits the good and bad aspect of the internet. We know that IP address can be spoofed, hacked sniffed, sent viruses to and totally open to get a Denial of Service attack. We have to realize that it is the same when talking about security on data networks and VOIP network.

A network that connects outside the world opens the gate for unfriendly and unknown people. This situation creates an environment for hackers and crackers come out with new attack and other network compromises tools that could failed call process. We can say that VOIP is vulnerable to all security threats in IP.

Some security issue face by VOIP is:

Eavesdropping

Eavesdropping is the secret listening of others conversations without their consent. [4] VOIP will transform the voice into a digital packet and segment it into several packets before routing it through the network. Tapping the VOIP call seems like impossible to do but there no such thing as impossible. We might think that the only way to listen the line is by using the telephone system it self. Now day's packet sniffer software can be downloading for free and it is easy to operate. VOMIT is use to transfer packet sniffer output to WAV file. The utility converts a Cisco IP phone conversation into a wave file that can be played with ordinary sound players.[5] Physical access to the line or wire itself can make eavesdropping done easily. Therefore access to the phone, VOIP equipment and network (physical wire) should be considered as a security issue and must be monitored without any doubt.

Call Hijacking

Many VOIP service providers will use web as a user interface for user to get access to their phone system. Using the web interface, an authenticated user can alter the Call Forwarding settings. Setting all calls to be forwarded to another Session Initiation Protocol (SIP) URL or phone number enables an attacker to divert all telephone traffic to a 3rd party. [6]

Denial of Service

Denial of Service (DoS) attack can caused user unable to access data from the network. In this case is voice data packet. There are several methods that can be use to create DoS attacks. One way is by flooding the network with too much traffic. DoS attack also can be done by prevention of access to a network service by bombarding SIP proxy servers or voice-gateway devices on the Internet with inauthentic packets. According to tests conducted by Secure Test on its own VoIP network, Cisco 7900 VoIP phones are susceptible to both DoS attacks and communications interception vulnerabilities. Cisco 1760 VoIP routers can be crashed with malicious traffic [7].

There are various DoS attacks to VOIP could take place. Dos attack which exploit problem in software. This type of attack can be addressed by upgrading the software or disabling the service component. DoS attack also can be launch

on protocols. The newer and more serious attack such as DDoS cannot be prevented technically and must be dealt with by developing and implementing a disaster recovery policy to handle this type of attacks

4. Best Practice.

By using VOIP technology, one has to indicate several steps for security purpose.

"*Security is a process, not a product*"

Bruce Schnier

Physical Security

VOIP equipment should be physically protected from security threats and environmental hazards. The equipment should be sited or protected to reduce the risk from environmental threats and opportunities for unauthorized access. VOIP equipment should be protected from power failures and other electrical anomalies. Option to achieve continuity of power supply includes:

- Multiple feeds to avoid a single point failure in the power supply.
- Backup generator
- Uninterruptible Power Supply (UPS).

Cabling security is an important aspect in VOIP security. Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage with the following controls:

- Power and telecommunications lines should be underground where possible, or subject to adequate alternative protection.
- Network cabling should be protected such as avoiding routed through public areas.
- Power cables should be separated from communications cables to prevent interference.

Encryption

Encryption is a cryptographic technique that can be used to protect the confidentiality of information. It should be considered for the protection of sensitive or critical information. In this case is voice packet data. Encryption can be done in RTP-layer which is used to transport information streams. Encryption can be utililized packet-by-packet basis, which means that it is up to the specified policy how encryption capabilities are applied to each packet.[8]. To capture, reassemble and decode voice packets, can definitely be done by the attackers. Encryption is the only way to prevent such an attack. To choose a unique, quick, efficient encryption algorithm and employ a dedicated encryption processor is the key to tackle these problems.

Firewall and Intruder Detection System (IDS)

Firewall is innovative solutions to securely accomplish end to end Session Initiation Protocol (SIP) based VOIP communications. A VOIP is quite difficult to manage because of the ever changing requirements. New connections caused for the close and opening of ports. This makes rule management is a difficult process.

SIP is solving the interoperability issue. SIP allows users of realtime communications to connect no matter what providers are used. The problem is ordinary network firewalls does not recognize SIP component. To ensure secure environment in VOIP user must look for SIP capable firewall. Communications such as audio, video and VOIP are the SIP based communications. The VOIP firewall should be able to support Network Address Translation (NAT), Port Address Translation (PAT) and also support Transport Layer Security (TLS) for encrypted signals.

IDS are a technology for detecting any unauthorized access to break or misuse the system through the network. IDS can monitor the network for any interruption or potential misuse. By analyzing the packet captured by the IDS, we can get the early warning about any intrusion to the network.

The 7 Fatal Mistakes

Implementing VOIP technologies in our corporate environment will end up with failure if we commit these 7 fatal mistakes [9].

1) DON'T: Treat VOIP management as a second thought

VOIP is an alternative for traditional phone line. It is crucial to follow the deployment steps and being consulted by the management before it is implemented.

2) DON'T: Ignore priority and quality handling for voice traffic.

Quality of Service (QoS) is an important aspect that shouldn't be overlooked in the implementation of VOIP. VOIP relies on the reliability of the networking system to ensure the service quality and availability. To implement QoS is to have total awareness about your network conditions and to maximize the use of resources.

3) DON'T: Manage data, voice, and QoS on a single network with separate management tools.

An integrated management solution is the best choice to manage data, voice and QoS on a single network. In order to really know what is going on to the network and resources, we must be able to get clear picture of the situations of the data, voice and QoS.

4) DON'T: Assume your IP network is ready to handle the demands of voice traffic.

By assuming that our networks have the ability to handle voice traffic without any pre-deployment testing is like risking the operational of the entire transport system. Therefore network management is an important aspect to inspect the reliability of the equipments in the infrastructure and the availability of bandwidth for traffic handling.

5) DON'T: Wait for end users to complain before addressing voice quality issues.

Voice quality is the main focused thing being questioned by ordinary (non IT background) users before VOIP technology took place in their environment. It is important to have voice quality monitoring methods to measure and plan any contingency plan if voice quality starts to degrade. The measurement results can be included in the VOIP management solutions.

6) DON'T: Ignore the need for technical education for voice and data staffs.

Although there is some IT professional call themselves as data or voice person exist in VOIP environment in term of knowledge and responsibilities, the requirement to understand deep inside the operation of different service on the network shouldn't be neglected by both side. This is to ensure that they know how to manipulate the parameter to totally use the resources and performance. This told us that training is crucial for both side without any differentiate.

7) DON'T: Take shortcuts.

VOIP is new technologies that arise in corporate world within this past few years. To compare these telecommunications technology with the existing voice communication services is seem to be unfair. Therefore the implementation must be in order and followed step by step with consultancy from the VOIP management. Shortcuts during the implementation should be avoided so that any crucial steps is not miss looked.

5. Conclusion

"Security is a journey not a destination"

Anonymous

VOIP networking has greatly enhances the utility of telecommunications. This provides users with versatile communications with less cost than traditional phone lines. However, VOIP networking is much more to achieve than traditional phone line communication, due to its surrounding environment. Many problems occurred, as solutions to traditional phone line networking technologies are not quit possible to be applied to the VOIP.

Flexibility communication provided by VOIP between people across geographical boundaries and without much impact on the communication cost. The vision enabling VOIP user to access various kind of places made available over future high-speed network is already a reality with current technologies. However, in order to provide reliable operations and services in the VOIP, still lots of task to be done.

In order meet user requirements satisfy user needs for reliable operations over VOIP, some sorts of guidelines are needed. In this paper, I have highlighted the challenges faced by users of VOIP environment and the various kinds of approaches used by researches in tackling those problems. Although solutions to some problems have 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 increases at rapid pace, new challenges and problems occurred.

Therefore, by keeping track of these issues efficiently is very important in order to achieve VOIP environments ultimate goal of providing user communication to a wide variety of unlimited geographical area with total satisfaction.

Voice over IP has made an explosive growth on voice communications market. These technologies keep on bursting into businesses world and networks. 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 new will end up suffering due to poor security implementation. Usually some times is required for a new technology to gain adequate level of security.

References

[1] Packeteer, Inc. "*Is Your Network Ready for VoIP?"*

http://www.packeteer.com/resources/prod-sol/VoIP_FAQ.pdf

[2] *Bob Massad* "Trying To measure VoIP CallQuality" March 2002

http://www.nwfusion.com/news/tech/2002/0318tech.html

[3] CISCO White Paper "Understanding Delay in Packet Voice Networks"
http://www.cisco.com/warp/public/788/voip/delay-details.html#standarfordelaylimits

[4] http://www.yourwindow.to/information-security/gl_eavesdropping.htm

[5] “vomit - voice over misconfigured internet telephones”
http://vomit.xtdnet.nl/

[6] @stake Inc. Security Advisory “Multiple Vulnerabilities with Pingtel xpressa SIP Phones “ http://www.atstake.com/research/advisories/2002/a071202-1.txt.

[7] Revcb “Vulnerable VoIP”
http://www.dslreports.com/shownews/40436

[8] M.Tolga SAKALLI , Ercan BULU• , Ion TUTANESCU “SECURITY AND DSPs IN VoIP (Voice over IP) NETWORKS”
http://eleco.emo.org.tr/ELECO2003/bsession/B3-01.pdf

[9] Paula Daley and Pam Snaith ”VoIP's Seven Deadly Sins” March 15, 2004
http://www.commweb.com/howto/showArticle.jhtml?articleId=18400154

[10]http://www.computerworld.com/securitytopics/security/story/0,10801,74840,00.html

[11] http://whitepapers.zdnet.co.uk/0,39025942,60079775p,00.htm

[12] http://www.sys-security.com/archive/advisories/html/More_Vulnerabilities_with_Pingtel_xpressa_Phones.htm

[13] Amanda D. Parthenious “Hackers Beware” June 18, 2001
http://currentissue.telephonyonline.com/ar/telecom_hackers_beware

[14] Noriyuki Fukuyama, Shingo Fujimoto, Masahiko Takenaka “Firewall-Friendly VoIP Secure Gateway and VoIP Security Issues “ September 26 2003
http://magazine.fujitsu.com/us/vol39-2/paper05.pdf

[15] http://seclists.org/lists/focus-ids/2003/Jan/0006.html