VoIP Security Threats and Vulnerabilities

S.M.A.Rizvi and P.S.Dowland

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

Abstract

This paper presents the assessment of Voice over Internet Protocol (VoIP) security threats and vulnerabilities along with current security technologies and security patterns. Although these threats and vulnerabilities are mentioned in many research papers but they are still need to be acknowledged for future. The convergence of voice and data in one simplified network brings both benefits and constraints to users. Among the several issues that need to be addressed when deploying this technology, security is one of the most critical. This paper presents recommendations with security patterns for VoIP that are specific to four attacks. The paper is helpful in giving a different perspective of vulnerabilities and risks of VoIP.

Keywords

Security, Technologies, Patterns, Threats, Vulnerabilities

1. Introduction

The VoIP technology being deployed as major infrastructure of organizations and companies have since remained in a cloud of doubt. The question would this technology prevail, while prone to a number of vulnerabilities and exposed to threats, is answered by increasing usage in Western Europe and recent heavy investments by British Telecom in United Kingdom. With the popularity and benefits of VoIP, there are number of increasing security threats taking place. Considering the fact that VoIP systems have security concerns, it is important to continue researches on any existing risks and presenting appropriate solutions.

This paper discusses security in terms of VoIP with threats and vulnerabilities identified. Existing technologies are discussed followed by recommendations and VoIP patterns.

2. Security

The VoIP technology is based on the previously threatened IP network and adds telephony threats as well. As the VoIP technology is evolving, it is collecting vulnerabilities and threats of both Internet and Telecom technologies. Although there have been many articles on security issues but the organizations are still lacking any implementation of security infrastructure steps for VoIP. According to (Schwartau, 2005) the communication world that is moving towards VoIP technology have no security expertise available. The reason is a little amount of budget is set aside for the security. Security needs to be classified in terms of VoIP. The security concept

related to VoIP has many different aspects but there are three main fundamentals Confidentiality, Integrity and Availability (CIA) (Pfleeger and Pfleeger, 2002).

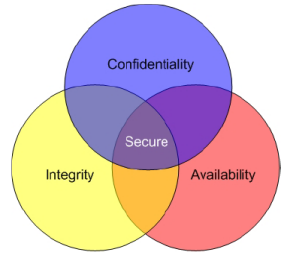

Figure 1: CIA relationship

2.1 Confidentiality

Confidentiality refers to mechanisms ensuring that only intended recipient have access to the VoIP call. Man-in-the-middle attacks are considered to be confidentiality breaches including eavesdropping, sniffing and application attacks. Many free sniffing tools such as dsniff, ethereal, and tcpdump (uses vomit) are available (Porter, 2006). Sniffing packet headers could lead to network and infrastructure disclosure, while sniffing packets leads to leak of private data. ARP monitoring, encryption, VPN are some techniques to mitigate such attacks.

2.2 Integrity

Integrity refers to the prevention of any unauthorized modification in voice packets. Any unauthorized activities must be checked upon. Password breaches are common when a switch reactivates and boots with default settings (Kuhn et.al, 2005).Further attacks include IP spoofing, quality-degradation, registration/session hijacking and server insertion attacks (Ransom and Rittinghouse, 2005).Any rouge packets must be blocked by using VLAN(segmentation),Caller ID verification and fixed routing mechanisms (Green, 2002) should be applied.

2.3 Availability

Availability refers that the VoIP services is always available when needed. Denial of Service which is a threat to availability could have an adverse effect if the VoIP call centre network is hit by such attack. Other attacks include TCP SYN, SIP INVITE flood (Goode B, 2002) and Spam over Internet Telephony (SPIT). Actions needed are using state-full firewalls, Intrusion detection and spam filters on servers (Eyeball, 2006).

3. Threats and vulnerabilities

There are a number of risks associated to VoIP network. Different threats and vulnerabilities are classified in attack categories. The technology needs to be secured as the packets take an unspecified route while traversing from source to destination

end. Analyzing the vulnerabilities and threats while implementing the security measures, is known as 'Risk Identification'.

3.1 Registration attacks

These are such type of attacks where the attacker tries to hack into the system or could be defined as those in which an attacker takes advantage of vulnerabilities in registration injecting themselves into the signal path of the VoIP network. Various type of registration attacks include IP Spoofing, Theft of Service, Reflection Attack, Brute Force Attack

3.2 During a call attacks

These attacks that are carried out mainly when a person is making or receiving a call. The attacker intercepts the route where voice/data packets are being sent. Call Hijacking, Eavesdropping, ARP spoofing (Porter, 2006), Connection Hijacking, Signal Protocol Tampering are some of the attacks in this classification.

3.3 Denial of Service attacks

These attacks have no concern about gaining any valuable information. This simply isolates the endpoint of network from rest of the world by jamming the switches and IP PBX with loads of rouge requests. Different categories include SIP INVITE Flood, TCP SYN Flood, and Malicious RTP Streams (Reynolds and Ghosal, 2002)

3.4 Attacks on VoIP components

These attacks are primarily on the devices, as they seem to be affected easily. The most common attacks are on IP PBX, Soft phones and IP phones

Further attacks include Application layer and SPIT attacks.

4. Security Technologies

It is fundamentally important to establish a security policy to design a secure VoIP system which can guarantee confidential delivery of services to subscribers. Some existing best practises are discussed as follows.

4.1 Virtual LAN

They allow the network administrators to logically divide a LAN in to a number of VLANs. This method provides security if any other VLAN is attacked other remains safe and secure. VLANs use Segmentation which separates voice from data VLAN.

4.2 Virtual Private Network

This technology establishes a private network within the public network. Mainly there are three subsets of VPN of technology, LAN VPN services, Dial-up VPN

services and Extranet VPN services (Venkateswaran, 2001)VPN is based on tunneling. The most popular technologies in VPN are Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP) and IP Security (IPSec).

4.3 Encryption

Voice packet encryption is the best defence against call interception. The major benefit of VoIP based telephony is the ability to encrypt the digital signals representing the voice stream. VoIP designers can also perform encryption at routers.

4.4 Authentication

It is the best to counterattack against registration problems. Authentication is based on cryptography using common secret or public and private key based methods along with signatures and certificates.

4.5 Firewall and NAT Issue

They are handled by a number of methods such as Stateful Firewall that checks each connection present at on any interface of the firewall to make sure they are legitimate Other method is Application Level Gateway (ALG) which intercepts the packet headers and perform modification if appropriate so they correspond to the correct source or destination IP address. Next approach is Demilitarized Zone (DMZ) which is a zone created between a trusted internal network, such as a private LAN, and an un-trusted external network, such as the Internet. (Tanenbaum, 2003).Placing an Intrusion Detection System (IDS) on firewall is also effective. An IDS detects intrusions and malicious behaviour on networks and hosts.

5. Recommendations

Based on the different threats and technologies that were discussed some recommendations might be given as follows

- The endpoint at user's premises shouldn't need any access to the Internet. A connection to the call manager and other phones is feasible.
- The phone or endpoint should not have any access to the normal data, a possible virus outbreak or DoS could result in spread of the virus on the data systems.
- When there is a confidential conversation traversing in the public network a very highly encryption is needed. The information can contain secret key as well.
- Just as the data networks the phones should also be protected by a firewall remotely. The firewall may deny any unencrypted traffic to the phone from Internet.
- The internal data network should be implemented separately with the voice network.
- Any upgrades or configuration required on any devices must need authentication.

- Any ports opened must be closed after call disconnection.

6. VoIP related patterns

Security patterns are better solution to recurring information security problems. (Schumacher and Roedig, 2001). It consists of an overview, problem description and solution with consequences. In this paper it is reduced to two headings. The four patterns are described in this section are Voice/data Segmentation, Tunneling, Call authentication and Call confidentiality.

6.1 Voice/Data Segmentation

The Voice/Data Segmentation pattern separates the voice and data services in order to counter against the threats to voice VLAN from an attacker in data VLAN. The converged services provide the ability to implement the telephony on the existing IP based data network. An economical factor for moving towards VoIP is the ability to use a single network to run both voice and data services. The problem domain consists of finding methods to prevent any attacks from data networks to the voice traffic in a VoIP environment. If an Accountancy company has implemented voice services for example starting a VoIP based customer call centre for marketing and sales purpose. If there is an attack on the data system, there are backup services available to retrieve the data, but the management is doubtful what if an attack leads to the VoIP call centre. The disruption in service would be very costly. How to prevent the voice network from such attacks?

6.1.1 Solution

Two different VLANs for voice and data could be isolated, by using layer three segmentation. All the inter VLAN traffic has to pass through the routing device that filters traffic using access control lists. The deployment of IP telephony services and IP data services should be segregated on two logically separate VLANs **(**DISA**,** 2004).
The terminal devices such as IP phones should reside in VLANs that support only IP telephony services. Similarly, the VoIP servers must be protected by a VoIP aware firewall residing on a separate segment. The packet filtering could be easily configured on routing device e.g. routing switches etc. that connects voice and data VLANs. Implementing a state full firewall at Voice VLAN could provide better protection from data VLAN.

6.2 Tunneling

The Tunneling pattern ensures the provision of confidentiality and integrity of voice packets in IP telephony. A voice link has to be established between two or more VoIP end user at remote location on different intranets. The communication link either could be established through a private Metropolitan Area Network (MAN), a Wide Area Network (WAN) or a public medium such as Internet. The Voice traffic is suspected of exposion to hackers while passing through a public network like the Internet. The traffic running on public medium is visible to other private networks.

The problem domain consists of finding methods to counter man-in-the-middle attacks and similar attacks on voice packets running on VoIP network. If an organization that is spanning round the globe wants to connect all its branch offices with the head office so that the communication is better and faster. But the problem is the organization has to choose public medium as the main path because having special leased lines is too much expensive. How would be the confidential information of a company be secure on the public network?

6.2.1 Solution

Virtual Private Networks (VPN) technology provides a tunneling mechanism through the public network to carry any confidential traffic from the private networks. The two locations can communicate securely over these end to end tunnels. One of the end points initiates the connection to establish a secure channel. Appropriate network nodes form the starting and termination points of the intermediated transport network.

VPN technique consists of encapsulation technique. Voice traffic is secured by encapsulating it inside an IPSec or similar tunneling standard. The fundamental mechanism behind tunneling is encryption that ensures confidentiality and data integrity in VoIP networks. Prior to establishing a connection tunneling makes use of Authentication Protocol to set up a trust relationship between the network terminal devices. Encryption could slow down the performance and it's a big issue to quality of service. A symmetric encryption algorithm should be preferred for the voice transportation that would help up in speeding up the process while providing confidentiality. VPN could use public key cryptography.

6.3 Confidential Call

In confidential call pattern security mechanisms such as encryption is provided at the hardware level such as IP phones. When two or more subscribers are engaged in a confidential voice call over a public channel, end users need to be sure that there message delivered from one end to other regains its secrecy. The voice conversation might be intercepted in between the originating and terminating points of VoIP network. The public network such as Internet is not a secure medium; therefore network administrators should apply cryptographic algorithms and techniques in order to ensure security of voice packets. A voice stream on the Internet is vulnerable to eavesdropping. The problem domain consists of deducing techniques to prevent attacks from sniffers while making or receiving a call on the public network. If general home users or a small company which haven't got a big infrastructure such as number of servers and gateways for the VoIP network, like to communicate securely. Applying encryption without tunneling, will that provide similar results?

6.3.1 Solution

To address confidentiality issue, the Secure VoIP Call pattern uses encryption and decryption techniques for VoIP calls. As mentioned earlier latency is an important issue in many converged services, symmetric encryption algorithms are preferred.

This algorithm generates a common cryptographic key i.e. shared secret key passed on both sides of the channel.

Preferably IPSec standard can be used, if so, then it is mandatory for the caller and callee participating in a voice conversation to agree previously on a data encryption mechanisms that must be included in IPSec i.e. DES, MD5, SHA along with a shared secret key. The originator encrypts the call using a common secret key at his end and sends it separately to the person at other end. The receiver decrypts the voice call using the key and playback the information.

Public key cryptography could be used as the other encryption mechanism where latency is not a big issue. This is regarded as the most secure method. In this scenario the receiver must obtain the senders public key before any voice connection is established. The sender encrypts the voice/data with his private key, callee must obtain caller's public key before establishing a connection. Caller encrypts the voice call with callee public key and sends it to him. Callee decrypts the voice call and recovers the original voice packets.

Properties of both symmetric and asymmetric cryptography could be fused together. The symmetric key that needs to be distributed among the end terminals and transported along the same medium could make use of asymmetric cryptography which is feasible for small amount of data. In this way both symmetric and asymmetric cryptography techniques are combined to provide fast and secure results.

6.4 Call Authentication

In Call Authentication pattern user authentication along with the dice authentication is verified when a VoIP call is made on the public network. A voice conversation which is using the public access as a medium could give rise to confidentiality and authentication issues. Subscriber who is imitating a VoIP call could be in doubt whether he is talking to intended recipient or an attacker. Similarly A person at the end of VoIP conversation could not prove the authenticity of Caller, as Caller can decline the authorship of any calls made by him. On top of that, as Public keys are widely available, any attacker could intercept the encrypted data, although he cannot read it but can append any false information or send entirely a new packet encrypted in receivers public key. The receiver may not authenticate the message integrity. The problem domain consists of any methods ensuring attackers are not able to masquerade the call. Solution is needed on how to prove the callers and message authentication so that caller is not able to deny a call made to callee. While making a payment over the IP phone a customer is not sure that the details he is giving to a legitimate party or not, on the other hand the company need to know whatever the customer gives detail, if proved wrong he must not be able to deny it. What should be the mechanism addressing both issues?

6.4.1 Solution

Authentication could be provided by different means. The subscribers can make use of public and private keys to produce digital signatures technique. The public keys need to be exchanged before the voice conversation starts. Sender can sign the voice

packets by using his private key and re-encrypt the result with the receiver's public key. In this scenario only receiver could decrypt the information with his private key and then repeat the same process by using sender's public key. This would provide authentication of the call that has been generated from the legitimate caller.

Another option could be used by applying using MD5.The caller takes the hash of voice signal and encrypt the original message and the hash with callee public key. When the callee receives the call he decrypts using his private key and if the hash of the voice signal is the same as the hash received it means the message is original without any modifications.

Both of the above mentioned techniques could be applied to make the voice conversation more secure but the limiting factor is QoS.

7. Conclusions

The VoIP security issues and solutions play a significant role in the success of VoIP services. Most of the threats discussed above are the threats from public networks. The above discussed recommendations and patterns would be helpful in determining an exact solution to the most common issues in VoIP patterns etc. These VoIP patterns make use of various techniques that are readily available. More information on related patterns is given in (Braga, 1998).

This paper gives an overview of some of the main threats and vulnerabilities posed to VoIP networks. We have also covered some technologies which are incorporated to mitigate such risks. The solutions for VoIP would continue to be researched on as it is a long process, but it would help the end users be aware of security implications and know how they can protect them selves from the VoIP related security threats. Finally in summary VOIP is still an emerging technology, so it is important to counter the emerging and unforeseen threats and vulnerabilities associated with the converged services. As this unique environment of VoIP develops and increase at rapid pace, new challenges and problems would arise.

8. References

Braga, A.M., Rubira, C.M. & Dahab, R. (1998) "Tropyc: A Pattern Language for Cryptographic Software", http://hillside.net/plop/plop98/final_submissions/P25.pdf (accessed August 2006).

Defense Information Systems Agency (DISA) (2004), "Voice over Internet Protocol (VOIP) Security Technical Implementation Guide", iase.disa.mil/stigs/stig/voip_stig_v1r1.pdf, (accessed July 2006)

EyeBall Networks Inc. (2006) "Eyeball Anti-SPIT™ Technology", http://www.eyeball.com/technology/anti_spit.html (accessed August 2006)

Goode, B**.** (2002) "Voice over Internet protocol (VoIP)", Proceedings of the IEEE Volume 90, Issue 9, Sept. 2002 Page(s):1495 – 1517.

Green, J. (2002) "Voice and Video over IP", McGraw-Hill Professional, USA, ISBN: 0071382488.

Kuhn, R., Walsh T. and Fries, S. (2005) "Challenges in securing voice over IP" ; Security & Privacy Magazine, IEEE Volume 3, Issue 3, May-June 2005 Page(s):44 – 49.

Pfleeger, C. and Pfleeger, S. (2002) "Security in Computing" (3 rd ed.) Prentice Hall, USA, ISBN: 0130355488.

Porter, T. (2006) "Practical VoIP Security", Syngress Publishing, USA, ISBN: 1597490601.

Ransom J. & Rittinghouse J. (2005) "VoIP Security", Elsevier Digital Press, USA.

Reynolds, B. and Ghosal, D. (2002); "STEM: Secure Telephony Enabled Middlebox", Communications Magazine, IEEE, Volume 40, Issue 10, Oct. 2002 Page(s):52 – 58.

Schwartau, W. (2005) "With VoIP, it's all over again", http://www.networkworld.com/columnists/2005/111405schwartau.html?page=2 (accessed June 2006).

Schumacher, M. and Roedig, U. (2001) "Security Engineering with Pattern", http://www.cs.ucc.ie/misl/publications/files/plop01schumacher.pdf, (accessed August 2006).

Tanenbaum, A.S. (2003) "Computer Networks" (4th ed.) Prentice Hall, USA, ISBN: 0130661023.

Venkateswaran, R. (2001) "Virtual private networks"**;** Potentials, IEEE, Volume 20, Issue 1, Feb-Mar 2001 Page(s):11 – 15.