International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 5 Issue 5 May 2018

Study of Securing Voice over Internet Protocol

Aditi Rawal
IES IPS Academy, Indore, India
aditie.23@gmail.com

Abstract: *Voice over Internet Protocol (VoIP) is a transmission technology which integrates the entire world of telephony and data; it has been widely deployed as it reduces the management cost and effort in comparison with services provided by the PSTN. But the combination of telephony and data in one untangled network brings both gains and hindrances to the users. Among several issues that are discussed while using this technology, security is the most vital one. This paper will describe the security threats associated with VoIP and the counter-measures to eradicate the problem. The paper also includes recommendations in respect to the risks and vulnerabilities.*

Keywords: *Authentication, Encryption, Firewall, Security, Threats, VoIP.*

1. INTRODUCTION

This VoIP stands for Voice over Internet Protocol; it is the transmission process of voice and the contents of multimedia over computer networks. Over the internet, it carries traffic of voice and the stimulating force for the progress of VoIP is that it provides simpler network design, more multimedia features, improved quality, reduced management efforts and reduced prices. Over the last decade, VoIP has become immensely popular, attracting millions of subscribers every year. It is estimated that 14 millions U.S. dollars users use VoIP and it will increment drastically in coming years. The major incentives for corporations is cost effectiveness, as it creates enormous revenue prospective for service providers and has increased its usage and implementation in the market place thus moving to the invention of new devices. But VoIP doesn't only include decreased costs; it also brings risks and vulnerabilities unparallel to the telecommunication industry. This is mainly because VoIP is based on IP protocols and all IP protocols for transmitting the traffic of voice contain flaws therefore it is susceptible to greater number of threats which is also an inexperienced platform in comparison to traditional PSTN which is robust and possess mature platform. Therefore the two systems work in completely different manner and each has its demerits and merits. However, like all the technology, VoIP comes up with a number of inherit threats while these serious issues can be managed provided the enterprise takes the appropriate actions.

This paper will analyse the threats faced by VoIP service providers and the users and also describes the methods to reduce the risks both for service providers and users. Researches in the entire world are carrying out different studies to secure the voice transmission over IP. They have discussed using the principle of CIA (Confidentiality, Integrity and Availability) about the particular security threats and also the countermeasures to diminish the problem of threats [1].VoIP promised to provide secure connection and reduce the overall value of ownership of telecommunications and networking through eliminating various charges and services [2]. The combination of data and voice in one simplified network leads to both constraints and benefits to the users where security is the most crucial which must be addressed while adopting this technology [3].The main threats were analysed and probability of threats along with their impacts are estimated from low to immense on the scale [4]. It describes various security threats, encryption methods and firewalls in order to diminish the threats problem [5].VoIP is quietly different from conventional telephone technology which is based on circuit switching, which results in particular security problems on VoIP network. It also brings opportunities for the potential and QoS of VoIP network which have been applied by security strategies [6]. Its main aim is to identify the security issues with the trending VoIP systems and to give a solution idea since it utilizes the existing computer networks and thus decreases the overall costs for long-distance-calls [7].

A. VoIP versus PSTN

VoIP uses packet switching technique to transmit the voice data while PSTN uses method of circuit switching. Therefore, the table shows the comparison between two systems that has its own merits and demerits.

Table 1. VoIP vs PSTN [4]

VoIP	PSTN
Over a same connection, multiple signals can be processed.	Dedicated lines for every signal.
The bit rate of audio compression decreased significantly.	Each line is 64 kb/s (in each direction).
Tracing of emergency calls to a specific geographical location is not possible always.	When placing an emergency call caller's location can be traced.
Long distance calls often cost as same as regular calls.	Long route calls are usually charged per minute.
If there are no backup powers in place, system will go down during power loss.	During power outrage, activeness of hardwired landline phones usually remains.

2. SECURITY THREATS AND COUNTER MEASURES

No VoIP systems depend on data networks only because initially the voice signal is divided into frames first which are then converted into data packets and finally transmitted over the network of IP using voice protocols. This is based on IP and network protocols which mean security weakness and the type of attacks linked with any data networks are possible. As voice gets converted into data packets and transported over the network, possible points of attack might get exposed more that could be used by intruders for interdiction, thus exploiting the security. Thus in order to secure the devices from harm, these types of risks and threats must be concerned. The paper will discuss the principle of CIA (Confidentiality, Integrity and Availability) for VoIP specific security threats, as these three are the most crucial elements of security. But when these are not taken care of, it leads to the threats i.e. Threats against confidentiality, Threats against integrity and Threats against availability. This paper will also describe the taxonomy for VoIP analysis. Few threats are omitted as they offered little or no threat to either providers or consumers because they are considered being redundant.

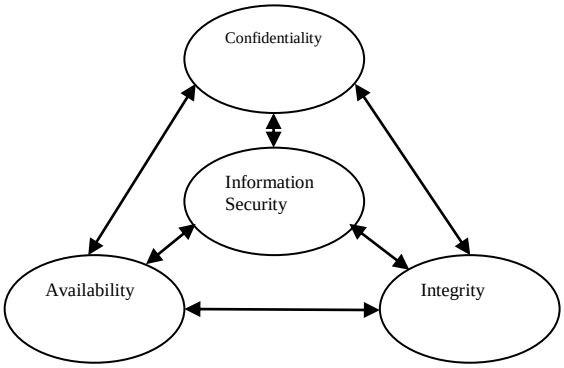

Figure 1: CIA Triad [3]

Classification of Threats

Threats have been classified according to the CIA triad. Security of transmission of data and voice over network is most important and thus threats are classified mainly in these three divisions i.e. Confidentiality, Availability and Integrity. This taxonomy presents different types of threats according to this triad.

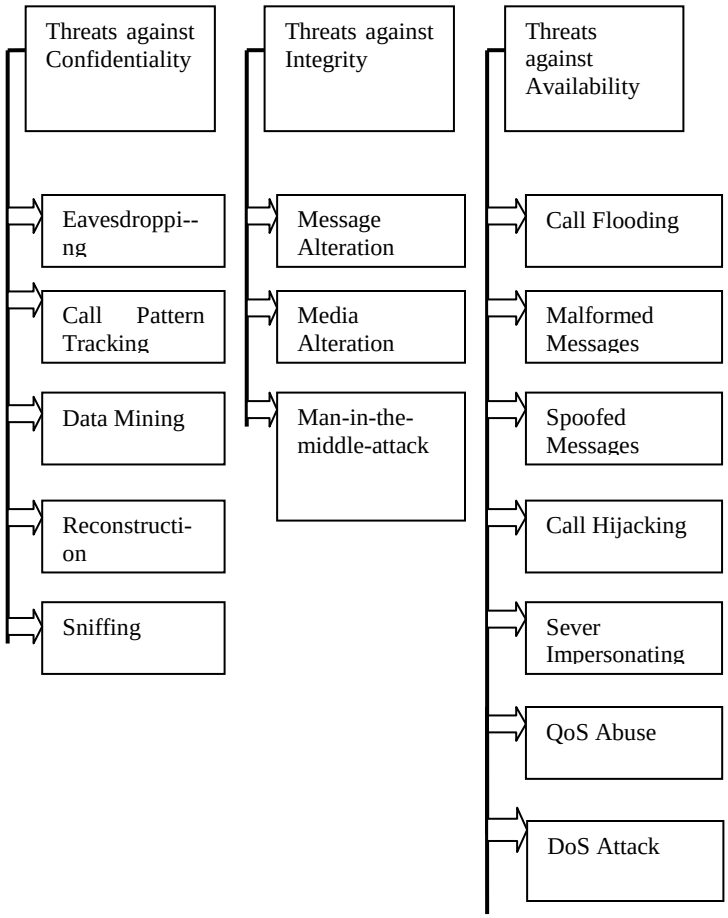

Figure 2: Taxonomy of Threats

A. *Threats against Confidentiality:* Confidentiality is defined as the set of rules that restricts access to the useful information. The main aim of confidentiality is that only recipients who are intended can access the information. But the threat against confidentiality provides an unauthorised way of capturing credentials, identities and access. VoIP transactions mostly suffer from this threat as most of the services of VoIP don't provide full confidentiality from source to destination. It includes eavesdropping, call pattern tracking, sniffing etc.

1) *Eavesdropping:* It happens when an intruder intercepts the stream of data between source and destination without changing the data; it gains access over the conversation. As there are large number of nodes present in the medium between two conversation entities. If the attacker gains control on any of these nodes, he can access the data packets flowing through that node. This method targets the media. Few of the eavesdropper are VOMIT (Voice over Misconfigured Internet Telephony), SIPtap.

2) *Call Pattern Tracking:* It is an unauthorised study of traffic over channel from or to any particular network so that attacker can access the information by finding potential target device. Call Pattern Tracking is an illegitimate tracking of user's call pattern of phone. This enables the attacker to keep record what number has called, geographical location, recording of phone call, length and time of the phone call. This threat targets directly signal information. Reason for this threat may include theft and extortion.

3) *Sniffing:* The network software which are providing troubleshoot and monitoring VoIP services, can be used as a means for wiretapping easily. For listening and sniffing, VoIP system provides weak protection these sniffing packets leads to the leak of private data and hacking of sensitive information.

Countermeasures

Encryption is a method which is combined to the VoIP information so that it becomes indecipherable to anyone who is sniffing the network traffic. For protection against eavesdropping, encryption of voice message packets is done using deployment of IPSec. The main advantage of VoIP based technology of telephony is its ability to encrypt the digital signals representing the voice stream. In addition, all passwords must be modified before the system is plugged into the network. Even if encryption is used, physical access to VoIP network becomes possible. Therefore, adequate security must be considered to restrict control over VoIP network components.

B. *Threats against Availability:* Availability refers that VoIP services remain available always when required. Threats against availability are a group of threats contrary to the service of availability that runs 24/7. The main aim of these threats is service interruption. It includes denial of service attack, call hijacking, spoofed messages, and quality of service etc.

1) *Denial of Service attack*: DoS attack is an attack in which there are multiple requests on a network server which it cannot handle. It typically floods the servers with traffic so that legitimate users no more able to use

them. It may lead to system instability or even paralysis. Though it doesn't result in theft, it can cost the victim a great amount of time and money to handle. Call flooding is an example of DoS where an attacker floods necessary or unnecessary heavy traffic because of which either performance drops or break down occurs.

2) *Call Hijacking:* It arises when a call is interrupted and rerouted through a different path before the information reaches to the destination. The attacker gets access to the valuable information and results in denying users completely of service. It usually happens when some transactions between VoIP endpoint and network path are captured by an attacker. This transaction can be registration, call setup and etc. This hijacking can make serious interruption by disabling legitimate users to use services provided by VoIP, also by storing these data and making use of data in other ways.

3) *Spoofed Messages:* An attacker may create malformed messages, fake messages and insert it into certain VoIP session with the purpose of service malfunction. Call teardown and toll fraud are the examples of spoofed messaging. An attacker creates spoofed messages on the server to force password assault until he receives authorization. If the client use default password or easily guessed password then it is quiet easier for an attacker to attack maliciously by using password dictionary.

4) *Quality of Service abuse*: Quality of service is vital for the progress of VoIP but because of the delay in transmission of packets, discontinuities it abuses the QoS. The components of a media session are negotiated between VoIP endpoints and network during call setup time of calls. An attacker may intercept in this negotiation and ruin the QoS by deleting, replacing, modifying codecs or payload time. Another reason for degrading the QoS is exhausting the limited bandwidth with malicious tool so that legitimate users cannot use bandwidth for their request over server.

Countermeasures

Device authentication using the MAC address of an IP phone is one solution to threats against availability. The automatic registration working of the call processing server should be blocked. It means if a phone attempts to download network configuration from the call handling servers with an unknown MAC, it will automatically reject the request and will not be granting network configurations. User authentication is also an effective precaution to prevent call masquerading. Authentication (such as user password, ID) is generally based on cryptography using methods along with signatures and certificates. To eliminate this kind of attacks from posing serious damages, software patching is crucial to fix vulnerabilities. Unfortunately, there is no productive and effective way to inhibit caller ID spoofing. The best way is not to trust unknown caller ID at all.

C. *Threats against Integrity:* Integrity of information means that information must remain unaltered by unauthorised users. It inculcates maintenance in terms of consistency, accuracy and trustworthiness of information over its complete cycle form source to destination. When delirious modification in voice packets, destruction and deletion, disclosure of switch software and data or altering media happens in the middle of network it results in the threats against integrity as these are modifying the traffic between among endpoints. An attacker can see the entire signalling and media flow between endpoints as an intermediary. Thus it results in lack of integrity of information. It includes call rerouting, call black holing, man-in-the-middle attack etc.

1. Call Rerouting: Call rerouting is an unauthorised means of call direction from one or more endpoints by changing its route of instruction in the protocol message. One reason of call rerouting is to either exclude authorised entities or to include unauthorised entities in call signal or media's path. Attackers take this as an advantage and use as an attack for scams. For example, an attacker can reroute the way of incoming calls like of bank to him, etc thus tries to gain control over critical information of user. It doesn't pose a direct harm to the service providers but rather it provides severe damage to the clients in many ways which results in bad reputation of providers or unsatisfied clients.

1) *Call Black Holing*: Call black holing is an unauthorised method of denying or declining to send any necessary components of protocol messages over the communication path. It results in delay call setup, make errors on applications, drop call connections, denying of subsequent messages and many more. An attacker deletes the media session information which leads to only one -way audio on call connection. This attack reduces QoS, as now companies are no longer able to make outgoing calls and users can't make any emergency calls.

2) *Man-in-the-middle attack*: MitM stands for man-in-the-middle attack, in which the attackers secretly intervenes and relay messages between two end parties who believes communication is taking place between them only but the intruder is capturing and manipulating the sensitive information in real time. Sometimes this data in the transmission process is an effort of tricking the user to insert private information, such as login credentials etc. Once the user fails to this bait, the information is collected from the target entity and the original information is then transmitted to the intended destination unaltered. Furthermore, an attacker can redirect the users to initiate the method of DoS attacks.

Countermeasures

Systems which use VoIP servers and gateways should be secured with a personal firewall, along with anti-virus and malicious code software to diminish the threats problem and media attacks. VoIP components is needed to be sure that they are transferring the information to legitimate counterparts. VoIP firewalls should be implemented for monitoring the streams and filtering out odd signals and RIP packets. By observing normal VoIP traffic patterns, limits of media and signal can be set. To check and diminish the integrity threats, strict security methods is necessarily implemented with restricted access control.

3. REASONS BEHIND IMPACT OF THREAT VALUES (VOIP)

This table represents the impact of threats on the voice and data over the network and describes the reasons of these threats as how they are affecting the network channel.

Table 2: Reasons behind impact of threat values (VoIP) [1]

Threat:	Impact of Threat	Reasons
Call Pattern Tracking	Low	Whatever the number user has called, attacker gains the information only regarding the number. He can draw only conclusions but has no proof about them.
Theft of Service	Immense	An attacker can steal assets worth millions by changing the data.
Call Black Holing	High	The company denies the requests and all the services of the clients together.
Call rerouting	Very High	An attacker can take access over conversation completely and can alter in its own way.
QoS Abuse	Low	Reduces QoS but doesn't deny or stop streaming altogether.
Spoofed Messages	High	Attackers can exploit vulnerabilities
Call Hijacking	High	Attackers can deny users completely of the service
Performance Latency	Low	Annoy the users but no other affects
Resource Exhaustion	Low	Viruses can cause resource exhaustion but probably likes to cause damage in another areas.
Physical Intrusion	Immense	If an attacking agent gains control of the restricted areas, he can do severe harm.
Malformed requests and messages	Medium	Attacker targets the single user at a time.

4. REASONS BEHIND PROBABILITY OF THREAT VALUES (VOIP)

This table represents the probability of threats under different circumstances and presents the reasons behind their affecting behaviour on the voice over the networks.

Table 3: Reasons behind probability of threat values (VoIP) [1]

Threat:	Probabili-ty of Threat	Reasons
Distributed	High	If an attacker

Denial of Service		possesses enough phones, then nothing could be done to prevent this attack.
Theft of Service	Medium	There are many attackers who still manage the stealing of phone minutes.
Reconstruct i-on	High	There are many applications available free of cost that makes this attack easy to implement.
Call controller flooding	Low	Servers are well protected.
Performanc e latency	Very High	Latency in calls can cause because of bad servers, service etc.
Alteration	Medium	It is difficult to completely alter the conversation rather than to take over the whole conversation.
Loss of Power	Low	SP's should have some backup power but single users are possibly losing the services.
Traffic Capture	Medium	An attacker can do entire control over to SP's network.
Unwanted Contact	Very High	Spamming through VoIP is easy.
Conversatio n Degrading	Low	The attacker gains little from the attack inspite of annoying.
Misinterpre tation	High	There are various means to misrepresent the identity; innocent unaware users get trapped in such type of attacks.

5. VoIP Results

The results from the analysis of threats involved with every asset are presented in this graph according to the security risks it faces. The graph is made between the security risks and threats.

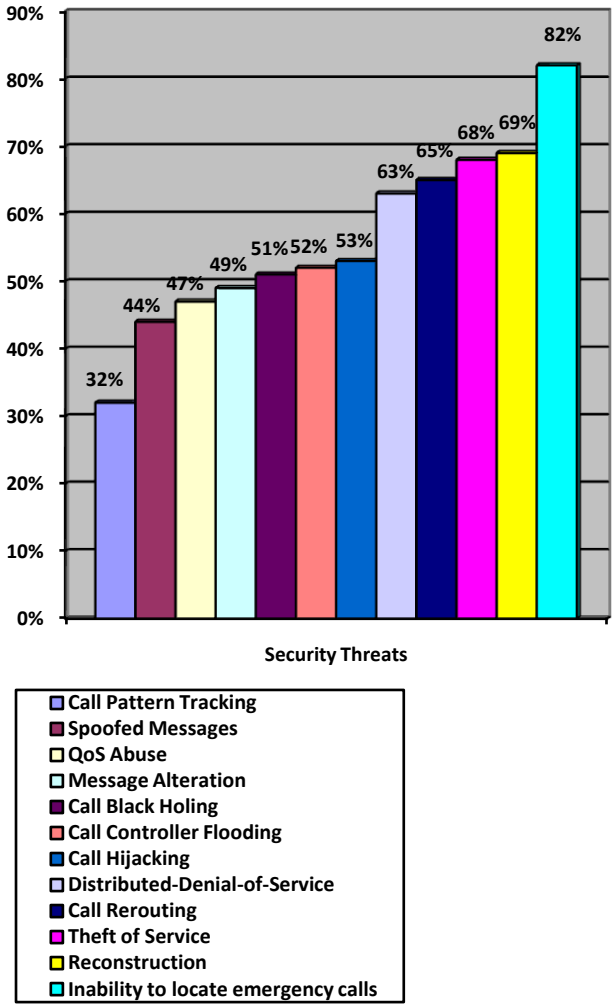

Figure 3: VoIP Results

6. RECOMMENDATIONS

Based on the different threats and preventive measures that were discussed, some recommendations and security guidelines are given which are:

- The port which is opened for connection of call must be closed after call disconnection.
- If in a system, updating or configuring is required then the device and system must be provided with authentication.
- It is a good method to separate data and voice on logically distinct networks if appropriate because of their different requirements of QoS.
- Sufficient backup power should be available for the VoIP switches and it should be checked systematically in a manner to certify that they would be ready if power is out.
- As data networks are provided by firewalls, it should protect remotely the phones also. Firewall will secure the phone from malicious attacks.
- In spite of encryption, there may exist a chance of breaking physical access and possessing control over the components of network. Thus to restrict the access, physical security measures must be considered appropriately.

7. CONCLUSION

VoIP is a developing technology that originates after the birth of PSTN. As PSTN provides good level of security and reliability, the users expect from VoIP the same safety measures and features. The progress of VoIP relies greatly upon the threats which are affecting the efficiency of VoIP systems and the measures which have been taken upon them to eradicate the problems of such attacks. Though, service providers have minimal or no effect because they have resources to safeguard themselves from these dangers. The main concern of service providers is the security of clients thus they are finding the ways to secure the clients from such threats. VoIP is an emerging technology which is having a potential to create advancement in the development of new devices. So, it is necessary to counter the emanating and unforeseen risks related with VoIP services.

REFERENCES

[1] S1. Jianqiang Xin, "Security Issues and Countermeasures for VOIP",SANS Institute Infosec Reading Room,pp.16-24, 2007.
[2] Ransom J. & Rittinghouse J.,"VOIP Security", Elsevier Digital Press, USA, pp.212-223, 2005.
[3] S.M.A.Rizvi and P.S. Dowland, "VOIP Security Threats and Vulnerabilities", Network Research Group, University of Plymouth, UK, pp.114-117.
[4] Knútur Birgir Otterstedt,"Risk Analysis on VOIP Systems", Master's thesis, Faculty of Industrial, Engineering, pp. 69, 2011.
[5] B. Goode, "Voice Over Internet Protocol(VOIP)", Proceedings of the IEEE, VOL. 90, NO. 9, Sept. 2002.
[6] Xiaojun Liu and Chunxia Tu,"Security of VOIP Network", School of Computer Huanggang Normal University, Hubei Huanggang 438000 China, pp.59-60, 2011.
[7] Lawecki, P., "VOIP Security in Public Networks". Stuttgart: University of Stuttgart.pp.6-11, 2007.