International Journal of Networks and Communications: 2011; 1(1): 1-5
DOI: 10.5923/j.ijnc.20110101.01

An Assessment of Security in Voip Using Secret Sharing

K. Maheswari[1,*], M. Punithavalli[2]

[1]Dept. of Computer Applications, SNR SONS College, Coimbatore, 9487458466, India
[2]Dept. of Computer Applications, Sri Ramakrishna Engineering College, Coimbatore, India

Abstract A major change in telecommunication industry is Voice over Internet Protocol (VoIP). VoIP offers interactive communications. It differs from conventional circuit switched networks. It allows people to communicate with each other at very low rates. The transmission of Real time voice data is not as easy as ordinary text data. The real time voice transmission faces lot of difficulties. It suffers from packet loss, delay, security and quality. These factors will affect the communication, degrades the performance and quality of a VoIP. This paper addresses the security aspects of VoIP to improve the quality.

Keywords Security, Quality, Telecommunication and VoIP

1. Introduction

Shamir's secret sharing is an algorithm. The secret or message is divided into parts. Each participant gets their own unique part. Some part of the secret or all parts of the secrets are needed to reconstruct the secret. The properties of shamir's threshold schemes are

- Secure – protecting information
- Minimal – size of each piece does not exceed the size of the original data
- Extensible – the pieces can be added or deleted dynamically
- Flexible – Each participant gets their part according to their importance

Secret sharing is a method for distributing a secret among group of participants. Individual shares are allocated to each participant. The secrets can be reconstructed when a sufficient amount of shares are combined together. Whenever there is a need for information storing, that is highly sensitive and important, the secret sharing is played more in that place. There are more opportunities to catch the data by wrong hands. Secret sharing addresses this problem. To attain the increased level of confidentiality and reliability, this algorithm is anticipated.

The secret "secretsh" is divided into the share se,cr,et and sh and is shown in Figure1. A person with zero shares knows only that the word secretsh consists of eight letters. Any T out of n shares are used to reconstruct the secret Lagrange polynomial interpolation scheme is used.

When the use of internet grows, automatically the complexity of the security problem increases. It becomes very difficult to solve the security problem. Actually, many application services do not consider the security. User authentication, confidentiality and integrity of signaling message or media stream are required for secure VoIP communication system[7].

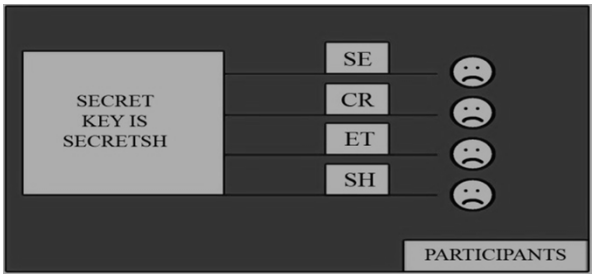

Figure 1. Secret Sharing.

The security threats[8] are

- Eavesdropping and recording phone calls
- Tracking calls
- Stealing confidential information
- Modifying phone calls
- Making free phone calls
- Pranks / Practical jokes
- Board room bugging
- Sending spam (voice or email)
- Denial of service (DoS),
- Alteration of voice stream,
- Toll fraud,
- Redirection of call,
- Accounting data manipulation,
- Caller ID impersonation,
- Unwanted calls and messages

A number of literatures, such as[1-6], cover a wide range of possible attacks on VoIP and SIP. The above mentioned threats had the greatest impact on the design of the security architecture. Eavesdropping is a major threat to confidentiality. The implementation of security in VoIP is very com-

* Corresponding author:
maheswarisnr@gmail.com (K. Maheswari)
Published online at http://journal.sapub.org/ijnc

plex than other data applications.

2. History

Denial of Service (DoS) Attack

A DoS attack is a hateful or malicious attempt. This may be happened by a

- single person or
- a group of public

This attack causes the victim, site, or node to decline the service to its clients. The attempt from a single host in the network forms a DoS attack. In contrast, it is also possible that a lot of malicious hosts coordinate to flood the victim with a plenty of attack packets, so that the attack takes place simultaneously from multiple hosts. This kind of attack is a Distributed Denial-of-Service[9].

Non-authorized Users

The physical access to the IP enabled phones can make calls using un authorized IP-enabled phones or IP – enabled users. Even authorized users may disrupt the service for the other authorized users. VoIP security architecture provides optional user authentication procedures to eliminate these threats.

DoS/DDoS attack can affect an enterprise in a remarkable loss of revenue due to the loss of interactive communication.

Eavesdropping (Call Interception)

Call interception is the possibility of unauthorized monitoring of RTP traffic. It can occur especially from within the network, and it exploits the vulnerability of SIP servers to registration hijacking, impersonation, and DoS/DDoS. The server can be tricked in acting as a codec converter between the two SIP clients, allowing voice traffic to be recorded or routed to other destination.

Signal Protocol Tampering

It occurs when a malicious user captures and changes the packets involved in the initiation of the call. Thus he can change different fields in VoIP packets, acting for the VoIP network as an authorized network user. In that way, the thief can make expensive VoIP calls.

Presence Theft

Presence theft consists in the impersonation of an authorized user sending or receiving data. It is linked with the Signal Protocol Tampering.

Toll Fraud

The ability of a hacker to use the resources of the VoIP network in order to make unauthorized VoIP calls. The security infrastructure guards against the introduction of worms and other viruses that may affect system and network element availability. It prevents unauthorized users from accessing systems and network elements, makes sure that authorized users do not make changes that may affect system availability, and allows for a quick recovery should there be a problem.

Cloning

The copied set of credentials and authorization information is used in addition to the real CPE. To detect fraud attempts the IP address of the clone is compared with the IP addresses of the real customer's network. A centralized Fraud Management System may also be used to detect patterns that may indicate cloning.

The security objectives[10] are

Integrity

All parts of the VoIP infrastructure must function properly without interference by internal or external users. To realize this, the VoIP security architecture ensures that only authorized users have access to the network elements. The VoIP security architecture takes necessary steps to ensure that weaknesses may not be exploited in a way that may compromise system integrity. The security architecture includes controls that discourage authorized users from making unauthorized changes by holding them accountable for their actions. In addition to securing network elements and systems, the security architecture ensures that internal and external systems may not make unauthorized changes to signaling messages and media. This is achieved in part by preventing other systems from masked as VoIP infrastructure systems.

Theft of Service and Fraud Prevention

"Theft of Service" means billing information does not accurately reflect the resources used, and "Fraudulent use of the Service" means the billing information is incorrectly assigned to the wrong customer. The VoIP security architecture includes a lot of functions that avoid or prevent unauthorized access and theft of service. All use of VoIP services can be accurately identified and billed to a specific customer and cannot be repudiated during a billing dispute. The security architecture should also deploy advanced fraud detection mechanisms tailored to the new VoIP technology.

IP Spoofing

Is a common attack method, it is used in DoS (Denial of Service) attacks. Attackers send flooding of spoofed packets to the destination host and quickly consume the available resources. The UDP packets can easily be manipulated, because it lacks the sequence number, the attack stream will be recognized as DNS response by the victim. TCP/SYN flood uses TCP's handshake procedure to continuously send SYN packets, the victim server or PC will wait for the ACK message that will not arrive[3].

Call Interception

This attack is often regarded as the 'man-in-the-middle attack'. One of the famous attack is 'ARP (Address Resolution Protocol) poisoning'. ARP poisoning modifies the ARP message by adding spoofed MAC address to the IP address. ARP poisoning is often used in VoIP eavesdropping. Fortunately, call interception require physical access to the network often through compromised nodes/servers[3].

The review of security in VoIP are:

[1] The author presents the publicly verifiable secret sharing with several applications. Improved performance and simplicity is achieved. It can be verified explicitly or publicly release shares may be verified by anybody against the output of the distribution protocol. The running time of this scheme is significantly lower than from other schemes. This scheme works for any group of prime order.

[2] Simulation analysis to various types of attack by NS2 was carried out. Simulated several queue including FIFO, DROPTAIL, SFQ, DRR, FQ and RED. The results of the packet loss with variety queue for DDoS was obtained.

[3] The study of identifying the key security issues within the content of software based VoIP is focused. The author pays attention to the key similarities and differences between softphone and hardphone. The VoIP security protocol is analyzed and proposed a model for softphone security. The softphone and hardphone are distinguished. The hardphone has the advantage over security and reliability which is compared to the softphone. Softphone is more flexible. It is easily integrated into web services. The proposed model is to maximize the the softphone adaptation of VoIP security. It secures both external and internal access.

Table 1. Summary of security aspects in VoIP.

YEAR	AUTHOR	CONCEPT	FINDINGS	DRAWBACK
1999	Berry Schoenmakers	Publicly verifiable secret sharing with several applications	Improved performance and simplicity is achieved.	Costly key generation protocol
2009	Chung-Hsin Liu, Chun-lin Lo	Simulated several queue including FIFO, DROPTAIL, SFQ, DRR, FQ and RED	The packet loss with variety queue for DDoS was obtained	Processors will use lot of computing resources
2008	Dannan Lin, Charles A	VoIP security protocol is analyzed and proposed a model for softphone security	It secures both external and internal access	Maintaining high quality
2010	Eric Y.Chen, Mistutaka Itoh	Methodology was formulated based on SIP protocol and is capable of keeping the most comprehensive and up-to-date information about the legitimate SIP clients	It overcomes the limitation by combining this approach with some black list mechanism such as PIKE in SER	Dealing with attacks from a compromised PCs With valid user testimonial
2008	Gauravkumar raval,Amitava pal	A layered approach and solution is proposed	Security architecture is proposed to monitor, detect, analyze and counter attacks relevant for a SIP based VoIP infrastructure	For high traffic ,New analyzer nodes and FSNs can be installed
1998	Hugo Krawczyk	Robust secret sharing scheme is presented	It preserves the space efficiency	Once a key is opened all messages encrypted with that key can be open.
2009	Hui Tian ,Ke Zhou,Hong Jiang,Jin Liu,Yongfeng Huang, Dan Feng	To eliminate the correlation among secret messages, to resist the statistical detection and to protect the short term secret message, to recover secret messages at the receiver side a synchronization method based on the RSA key agreement is proposed	It provides good security and transparency for transmitting secret messages in the real time is achieved.	Consists of critical componenets
2008	JoongMan Kim, SeokUng Yoon,Hyuncheol Jeong, Yoojae Won	Secure and flexible method is discussed for Session Border Controller/firewall management	VoIP security issues are analyzed	The application of security protocols influence on call set up delay than voice quality
2009	Rafael Mendes Pereira and Liane margarida Rockenbach Tarouco	Identifying maximum of each call grouping method is proposed	Overhead reduction with fixed and variable multiplexing method in a favorable set up is presented	Higher compression rate in favorable cases and better quality in unfavorable cases.
2010	Rainer Falk,Steffen Fries, Hans Joachim	The overview of authentication and identity management for voice communication is focused	Provided number of options for integrating an ePA based user authentication in the SIP	Concentrated only authentication and not for integrity, protection and confidentiality
2010	Ryouichi Nishimura,Shun-ichiro Abe,Norihiro Fujita and Yoiti Suzuki	The secret sharing scheme is proposed to convey information from one person to the other	Packet loss is reduced and security level is increased	The probability of occurrence of missing frame expected is increasing
	William Marshall, Alireza Farid Faryar, Kevin Kealy, Gustav de los Reyes, Israel Rosencrantz,Rachel Rosen crantz and Chaim Spielman	Security objectives are specified and summary of security threats are analyzed	Real time services over IP architecture are outlined	The architecture used is to protect AT & T's VoIP infrastructure

[4] Considered DoS attacks against Sip and web services which categorized into

- Fuzzing
- Flooding

SIP based VoIP infrastructure must achieve the same level of reliability, availability and security as in PSTN. This methodology was formulated based on SIP protocol and is capable of keeping the most comprehensive and up-to-date information about the legitimate SIP clients. The author studied the impact of various flooding attacks on a SIP server. This approach is effective in most attack scenarios. It overcomes the limitation by combining this approach with some black list mechanism such as PIKE in SER.

[5] Security architecture is proposed to monitor, detect, analyze and counter attacks relevant for a SIP based VoIP infrastructure. A layered approach and solution is proposed. Fsns can be installed to deal higher loads in terms of algorithmic processing load, filter rule, complexity or message traffic.

[6] Robust secret sharing scheme is presented. Some shares can be corrupted. This scheme correctly recovers the secret even in the presence of a number of corrupted shares. It preserves the space efficiency. The time of share distribution is considered. The encrypted secret E as well as the key share K_i is signed. During the reconstruction the public verification key is used to verify the correctness of the shares. The total amount of information added to each share depends only on the security parameter and not on the shares.

[7] To eliminate the correlation among secret messages, to resist the statistical detection and to protect the short term secret message, to recover secret messages at the receiver side a synchronization method based on the RSA key agreement is proposed. The communication system can be extended to other steganography schemes based on real time system. This approach is evaluated with effectiveness of the ITU G.729a as the codec. It provides good security and transparency for transmitting secret messages in the real time is achieved.

[8] Secure and flexible method is discussed for Session Border Controller/firewall management. VoIP security issues are analyzed. The functionality of SBC is well defined modular design based on model view controller architecture and PHP as a programming language.

[9] Increasing the multiplexing capacity attained a higher compression rate in this work. The architecture consists of two compounds.

- Adaptive multiplexer
- QoS monitor

Identifying maximum of each call grouping method is proposed. Overhead reduction with fixed and variable multiplexing method in a favorable set up is presented. 42% of average compression rate is reached. This approach is based on E-Model recommendation which introduces a non- invasive method that allows a global overview of several settings related to the quality of calls.

[10] The overview of authentication and identity management for voice communication is focused. Provided number of options for integrating an ePA based user authentication in the SIP. A Diffie hellman authentication using a static chip key is activated to authenticate the ePA towards the terminal.

[11] The secret sharing scheme is proposed to convey information from one person to the other. Nobody can obtain any share of the original form. Only a person who collects all shares can reconstruct the original information. A single set of data is transmitted through multiple paths. This is used to achieve load sharing and high reliability. It requires no secret key. The image data is considered promising for scalable coding speech compression coding. Packet loss is reduced and security level is increased.

[12] Security objectives are specified and summary of security threats are analyzed. Real time services over IP architecture are outlined. The architecture is divided in to 3 security domains.

- Signaling media
- Applications
- OAMP operation

3. Future Work

From the above study there is no considerable amount of work towards the secret sharing algorithm in VoIP. The future work concentrates on methodologies to improve quality in terms of packet loss and security using a modified secret sharing algorithm.

4. Conclusions

This survey provides an overview of existing approaches for security techniques of VoIP. It promises to deliver cost savings to users and service providers and is driving the convergence of network and telecom. It offers improvements in quality, interoperability and security applications in the near future. An effort was directed to the development of a security algorithm that would maintain the quality of voice for lost packets.

REFERENCES

[1] Berry Schoenmakers," A simple publicly verifiable secret sharing scheme and its application to electronic voting", CRYPTO 99 vol 1666 of lecture notes in computer science ,springer-verlag,1999,pp: 148-164

[2] Chung-Hsin Liu,Chun-lin Lo,"The simulation for the SIP DDoS attack",2009 Fifth international IEEE conference on INC, IMS and IDC

[3] Dannan Lin, Charles A. shoniregun,Galyna A.Akmayeva,"The softphone security",2008,IEEE international conference

[4] Eric Y.Chen, Mistutaka Itoh," A whitelist approach to protect

SIP servers from flooding attacks", IEEE conference, 2010

[5] Gauravkumar raval,Amitava pal,"VoIprotect: A layered security Architecture",Tenth IEEE international symposium on Multimedia,2008

[6] Hugo Krawczyk,"secret sharing made short", 1998, Springer-verlag

[7] Hui Tian ,Ke Zhou,Hong Jiang,Jin Liu,Yongfeng Huang, Dan Feng,"An M-sequence based steganography model for voice over IP", publication in the IEEE ICC 2009 proceedings

[8] JoongMan Kim, SeokUng Yoon,Hyuncheol Jeong, Yoojae Won,"implementation and evaluation of SIP based secure VoIP communication system",2008,IEEE/IFIP international conference on embedded and ubiquitous computing

[9] Rafael Mendes Pereira and Liane margarida Rockenbach Tarouco,"adaptive multiplexing based on E-Model for reducing network overhead in voice over IP security ensuring conversation quality",2009 fourth international conference on digital telecommunications

[10] Rainer Falk,Steffen Fries, Hans Joachim Hof ,2010 third international conference on advances in human oriented and personalized mechanisms , Technologies and services

[11] Ryouichi Nishimura,Shun-ichiro Abe,Norihiro Fujita and Yoiti Suzuki," Reinforcement of VoIP security with multipath routing and secret sharing scheme",Jouranl of information hiding and multimedia signal processing,2010,Vol 1,number 3, July 2010,ISSn: 2073-4212

[12] William Marshall, Alireza Farid Faryar, Kevin Kealy, Gustav de los Reyes, Israel Rosencrantz,Rachel Rosen crantz and Chaim Spielman,At & T Labs,USA,"Carrier VoIP Security Architecture"

[13] Wei Wang,Soung Chang Liew,Victor o.k.Li,"solutions to performance problems in VoIP over a 802.11 wireless LAN", IEEE transactions on vehicular technology , vol 5, No.1, Jan 2005.