A SECURITY ANALYSIS IN VoIP USING HIERARCHICAL THRESHOLD SECRET SHARING

E.S. Thirunavukkarasu
Research Scholar, Dept. of Computer Science, Bharathiar University, Coimbatore-46
Email: arasu_igr@yahoo.co.in

E. Karthikeyan
Asst. Professor and Head, Dept. of Computer Science, Govt. Arts College, Udumalpet- 642026, Tirupur Dist.
Email: e_karthi@yahoo.com

----------**ABSTRACT**----------
Voice over Internet Protocol (VoIP) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. VoIP provides a protected transmission of private voice data between two endpoints. A tremendous change in telecommunication industry is Voice over Internet Protocol (VoIP). VoIP presents interactive communications. It varies from conventional circuit switched networks. Voice over IP permits people to communicate with each other at lower cost. The transmission of Real time voice data is not simple 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. In VoIP using a collection of hierarchical structure causes the threshold secret sharing tribulations. In those settings, the participants between in secret sharing scheme into a variety of levels. This paper addresses the security aspects of VoIP to improve the quality using hierarchical threshold secret sharing.

Keywords: Voice over IP, Security, Secret Sharing, Threshold Secret Sharing

1.INTRODUCTION Secret sharing is a method for dispensing a secret among set of participants. The secret or message is divided into parts. Individual shares are allocated to each participant and they will get their own unique part. Some part of the scheme or

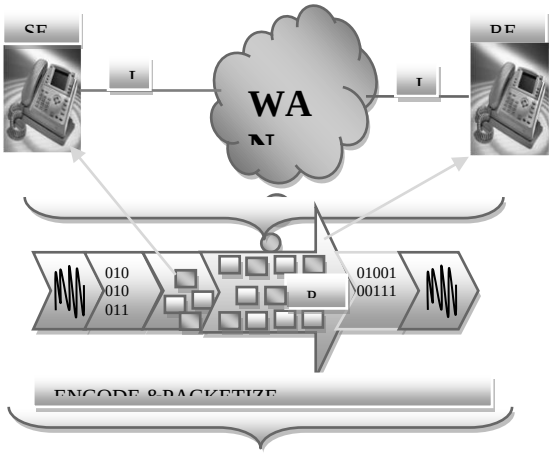

Figure 1.1 Secret sharing scheme

rises, routinely the complication of the security problem increases. It happened 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 [2]. Figure 1.1 described the novel scheme in VoIP Whenever there is a necessity for information storing, that is highly sensitive and important, the secret sharing is played vital role in that place. When the use of internet shares are combined together. Some part of the secret or all parts of the secrets are needed to reconstruct the secret.for sharing the secret messages and for the conjunctive all parts of the secret are needed to reconstruct the secret. The secret can be reconstructed when an enough amount of hierarchical threshold access structures may be altered for the correctness of disjunctive type of hierarchical threshold access structure.

The security threats [3] 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

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 complex than other data applications [15].

2. LITERATURE SURVEY

Leggieri *et al* (2008), They investigates many of the security mechanisms available in the field of Open Source VoIP communications, according to the specific protocol architecture selected for implementation, and provides an extensive evaluation of their impact on quality, by considering a number of network traffic related parameters. Lien *et al* (2009), In this paper, the fusion of temporal and texture background model, multi-mode tracking scheme, color-based difference projection, and ground point detection are proposed to improve the abovementioned problems [6].

Guo *et al* (2013), they express many efficient secret sharing schemes for general access structures have been developed in efforts to deal with the problems of multi-party computations (MPC), threshold cryptography, and access control. In this study, they have proposed a novel secret sharing scheme with general access structures that is based on the key-lock-pair mechanism. Kim *et al* (2008), TLS and S/MIME are proposed for SIP signaling message protection and SRTP for media protection. MIKEY is also a standard protocol for key management. In this study, they analyzed and implemented security protocols for VoIP. And then, they accomplished performance test of them by applying implemented security protocols to hardware VoIP phone and SIP proxy[7].

Piloyan *et al* (2006), it talks about the problems of the current methodology to transfer Voice or Video traffic over IP (VoIP), and proposes a solution to these problems. This proposed solution consists of a new protocol that routes Voice and Video traffic over the Internet infrastructure. This novel protocol runs in parallel and independently from the Internet data routing protocols. Then it gives more detailed design description of this new protocol, and discusses different implementation methods.Farras *et al* (2010) exposes in this paper, they proved that every ideal hierarchical access structure is the port of a representable matroid and, more specifically, they prove that every ideal structure in this family admits ideal linear secret sharing schemes over fields of all characteristics. In addition, methods to construct such ideal schemes can be derived from the results in this paper and the aforementioned ones on ideal multipartite secret sharing [8].

Tassa *et al* (2006), they presents introduction of bivariate interpolation and its potential power in designing schemes for multipartite settings, as different compartments may be associated with different lines in the plane. In particular, they show that the introduction of a second dimension may create the same hierarchical effect as polynomial derivatives and Birkhoff interpolation were shown to do.Oriol *et al* (2012) Multipartite secret sharing schemes are those having a multipartite access structure, in which the set of participants is divided into several parts and all participants in the same part play an equivalent role. In this work, the characterization of ideal multipartite access structures is studied with all generality. Their results are based on the well-known connections between ideal secret sharing schemes and matroids and on the introduction of a new combinatorial tool in secret sharing, *integer polymatroids*[9].

Ballico *et al* (2006) represents that secret sharing schemes provide a natural way of addressing security issues in ad hoc networks. To this aim, a flexible framework for secure end-to-end transmission of confidential information is proposed which exploits multipath source routing and hierarchical shares distribution. Such a goal is achieved by designing an ideal, perfect, and eventually verifiable secret sharing scheme based on Birkhoff polynomial interpolation and by establishing suitable hierarchies among independent paths.Bilien*et al* (2005) this paper presents the possibility of establishing a secure VoIP telephone call using SIP. Different security services relevant for VoIP are presented and also argue that end-to-end authentication and encryption should be provided by default. For media protection they evaluate the possibility of using either SRTP or IPSec, and they examine several alternatives of how a secure VoIP call can be established. The solution they suggest is based on SRTP for media protection, S/MIME and MIKEY for end-to-end authentication and keying, and TLS for hop-by-hop protection of SIP messages [10].

Beimel *et al* (2008), they characterize all weighted threshold access structures that are ideal. They show that a weighted threshold access structure is ideal if and only if it is a hierarchical threshold access structure (as introduced by Simmons), or a tripartite access structure (these structures generalize the concept of bipartite access structures due to Padró and Sáez), or a composition of two ideal weighted threshold access structures that are defined on smaller sets of users. They further show that in all those cases the weighted threshold access structure may be realized by a linear ideal secret sharing scheme. The proof of their characterization relies heavily on the strong connection

between ideal secret sharing schemes and matroids, as proved by Brickell and Davenport [11].

Cui *et al* (2010),they proposed a hybrid key management solution for the Ad Hoc network that the network architecture is hierarchical and distributed. Among them, telecommunications network using the traditional centralized management solution, while mobile backbone network and radio sub-network using the part of distributed management program, which is based on RSA system (t,n) threshold scheme constructed[12].

Wang *et al* (2008), they proposed a dynamic threshold and verifiable multi-secret sharing scheme. Some secrets are protected by distributing them among many participants, whereby only an authorized group of participants can reconstruct the secrets. In our scheme, the secret will change periodically and the dealer will periodically publish some of the information, in addition, the participants can verify the information which they have received.Wei *et al* (2007), they presents a new dynamic threshold secret sharing scheme was proposed, which is based on bilinear maps. The basic idea of this scheme is as follows: The system is consisted of some participants and a dealer. Each participant holds only one permanent private key. The dealer is responsible to choose the shared secret, and to construct a system of linear equations by using the participants 'public keys. The dynamic threshold is realized by adjusting the number of linear equations. Compared with most existing schemes, the proposed scheme is not dependent on any secure channel between the dealer and the participant [13].

Park *et al* (2011), they presents a Packet Loss Concealment (PLC) algorithm for CELP-type speech coders is planned to facilitate recover the quality of decoded speech under burst packet loss conditions in a wireless sensor network. Conventional receiver-based PLC algorithms in the G.729 speech codec are usually based on speech correlation to reconstruct the decoded speech of lost frames by using parameter information obtained from the previous correctly received frames. Though, this approach has complexity in reconstructing voice onset signals because the parameters such as pitch, linear predictive coding coefficient, and adaptive/fixed codebooks of the preceding frames are typically related to silence frames. [14].

3. TYPES OF ATTACKS IN VoIP

3.1 Denial of Service (DoS) Attack

A denial-of-service (Dos) attach is a special form of cyber attack that focuses on the interruption of network service. This is achieved when an attacker sends high volumes of traffic or data through the target network until the network becomes overloaded ("Denial-of-Service"). A DoS attack is a hateful or malicious attempt. This may be happened by a single person or a group of public.

There are multiple ways to execute a DoS attach. Some of the different forms of execution include:

- **Teardrop** – sending irregularly shaped network data packets
- **Buffer Overflow** – flooding a server with an overwhelming amount of data
- **Smurf** – tricking computers to reply to a fake request, causing much trafficz
- **Physical** – disrupting a physical connection, such as a cable or power source

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 [4].

3.2 Brute-Force Attack

This type of attack is typically used as an end-all method to crack a difficult password. A brute-force attack is executed when an attacker tries to use all possible combinations of letters, numbers, and symbols to enter a correct password.

3.3 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.

3.4 Eavesdropping

Eavesdropping is a passive, and often difficult to detect, MitM attack in which the attacker copies or listens to communication between two hosts. VoIP eavesdropping can be performed on signaling and media. Attackers eavesdrop signaling traffic to discover credentials, calling patterns, or identity or other sensitive information. Attackers eavesdrop media traffic to capture, replay or rebroadcast audio, video, or (text) messaging.

The danger of VoIP eavesdropping depends on the topology and underlying technology (switching systems and communications media) of the IP network used for voice transport. Eavesdropping on packets by tapping into fiber-optic circuits or by breaking into core switches that comprise eavesdropping on the Internet backbone is much more difficult than eavesdropping on traffic in a shared Ethernet segment on an unencrypted wireless link, or by breaking into an access point or broadband access router. Confidentiality measures protect against eavesdropping attacks

3.5 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.

3.6 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 un-authorized access and theft of service. All use of VoIP ser-vices 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.

3.7 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 [1].

3.8 Call tampering

Call tampering is an attack which involves tampering a phone call in progress. For example, the attacker can simply spoil the quality of the call by injecting noise packets in the communication stream. He can also withhold the delivery of packets so that the communication becomes spotty and the participants encounter long periods of silence during the call.

3.9 Man-in-the-Middle

This attack is often regarded as the "Call Interception". The man-in-the-middle (MitM) is the classic attack and many cryptographic systems are designed to protect themselves against it. The assumption is that the attacker has somehow managed to insert himself between the two hosts.

As such, the attacker has the ability to:

- Inspect any packet between the two hosts
- Modify any packet sent between the two hosts
- Insert new packets sent to either hosts
- Prevent any packets sent between the hosts from being received

4. HIERARCHICAL THRESHOLD SECRET SHARING ALGORITHM (HTSS)

A *threshold secret sharing scheme* enables a dealer to distribute a secret among a set of users, by giving each user a piece of information called a *share*, such that only large set of users will be able to reconstruct the secret from the shares that they got, while smaller sets gain no information on the secret. Threshold secret sharing schemes were introduced and efficiently implemented, independently, by Blakley and Shamir. Efficient threshold secret sharing schemes were used in many cryptographic applications, e.g., Byzantine agreement, secure multiparty computations and threshold cryptography.

The properties of hierarchical threshold secret sharing 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

5. FUTURE WORK

From the above evaluation, it is revealed that there is no significant amount of work towards the secret sharing algorithm in VoIP. The future work focuses on methodologies to improve quality of voice transmission in terms of packet loss and security using a Hierarchical Threshold Secret Sharing algorithm.

6. CONCLUSION

This paper provides a summary of on hand available approaches for security techniques of VoIP. It assured to deliver the voice data with high security at lower costs using Hierarchical Threshold Secret Sharing algorithm and is driving the unification of network and telecommunications. It presented the high quality data with interoperability and security applications in the future. An attempt effort was aimed at the development of a security algorithm that would improve the quality of voice for lost packets.

REFERENCES

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

2. 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 proceed-ings

3. 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

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

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

6. Lien, Cheng-Chang, Ya-Lin Huang and Chin-Chuan Han 2009, "People counting using multi-mode multi-target tracking scheme." In Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP'09, Fifth International Conference on, pp. 1018-1021, IEEE.

7. Kim, JoongMan, SeokUng Yoon, HyunCheol Jeong and YooJae Won 2008, "Implementation and evaluation of SIP-based secure VoIP communication system." In Embedded and Ubiquitous Computing, EUC'08, IEEE/IFIP International Conference on, vol. 2, pp. 356-360, IEEE.

8. Farras, Oriol and Carles Padró 2010, "Ideal hierarchical secret sharing schemes." In Theory of cryptography, pp. 219-236. Springer Berlin Heidelberg.

9. Arràs, Oriol, Jaume Martí-Farré and Carles Padró 2012,"Ideal multipartite secret sharing schemes." Journal of cryptology 25, no. 3: 434-463.

10. Bilien, Johan, Erik Eliasson, Joachim Orrblad and Jon-Olov Vatn 2005, "Secure VoIP: call establishment and media protection." In 2nd Workshop on Securing Voice over IP.

11. Beimel, Amos, Tamir Tassa and Enav Weinreb 2008, "Characterizing ideal weighted threshold secret sharing." SIAM Journal on Discrete Mathematics 22, no. 1: 360-397.

12. Wang, Shiuh-Jeng, Yuh-Ren Tsai and Jian-Jhih Shen 2008, "Dynamic threshold multi-secret sharing scheme using elliptic curve and bilinear maps." In Future Generation Communication and Networking, FGCN'08, Second International Conference on, vol. 2, pp. 405-410, IEEE.

13. Wei, Chen, Long Xiang, Bai Yuebin and Gao Xiaopeng 2007, "A new dynamic threshold secret sharing scheme from bilinear maps." In Parallel Processing Workshops, ICPPW 2007. International Conference on, pp. 19-19, IEEE.

14. Park, Nam In, Hong Kook Kim, Min A. Jung, Seong Ro Lee and Seung Ho Choi 2011, "Burst packet loss concealment using multiple codebooks and comfort noise for CELP-type speech coders in wireless sensor networks." Sensors 11, no. 5: 5323-5336.

15. Maheswari, Punithavalli 2011, "An Assessment of Security inVoIP Using Secret Sharing", International Journal of Networks and Communications, 2011; I(I):1-5.