Role of Multiple Encryption in Secure Voice Communication

Himanshu Gupta and Dr. Vinod Kumar Sharma

Abstract **-** Today, for secure voice communication, various encryption techniques are evolved significantly. Traditional analog methods of voice encryption have been replaced by digital technology by using complex and secure encryption algorithms. Using multiple encryption, voice encryption has become much more efficient and secure. This research paper explores the role of multiple encryption in secure voice communication over the insecure network. It provides high level security for voice communication. Multiple encryption of voice data can uproot the problem of information theft during the communication through telephone, mobile phone, etc.

Keyword--- Voice Communication; Multiple Encryption; Voice Encryption.

I. INTRODUCTION

VOICE encryption is a process of converting sound signal in a secure form by using encryption algorithm. In cryptography, secure voice is a term which is used for the encryption of voice communication over the insecure communication medium such as telephone, mobile or IP telephony [1].

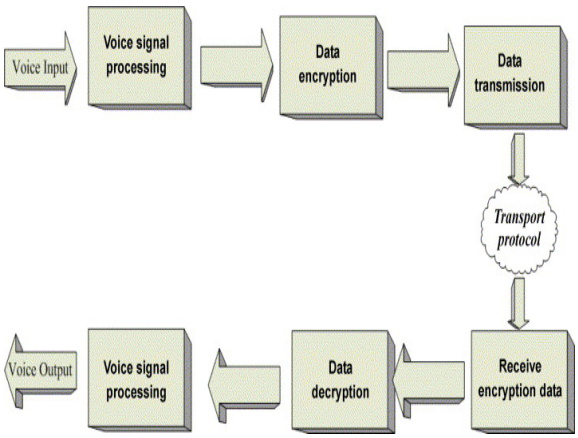

Fig. 1 Operations in Voice Encryption

Himanshu Gupta is Senior Faculty Member, Amity Institute Of Information Technology, Amity University, Noida, Uttar Pradesh, India E-Mail: Himanshu_ Gupta4 @Yahoo.Co.In

Dr. Vinod Kumar Sharma is professor & Hod – Department Of Computer Science, Gurukula Kangri University, Haridwar, Uttarakhand, India E-Mail: Vks_Sun@Ymail.Com

To implement this system, the army gave the contract to Bell Laboratories and they developed a system called as SIGSALY. In SIGSALY, ten channels were allocated to sample the voice frequency spectrum from 250 Hz to 3 KHz and two channels were allocated to sample background hiss and voice pitch. This system included radio transmitter and receiver with large precise phonograph turntables [2].

A secure voice communication system provides the secure transmission of voice communication between the sender and receiver through PSTN (Public Switched Telephone Network). This system implements the multiple encryption techniques to enhance the security of voice communication over insecure network. This system uses an encryption/decryption engine which is capable to execute a number of complex encryption algorithms [3]. During the voice communication, the voice encryption algorithm may be changed session to session.

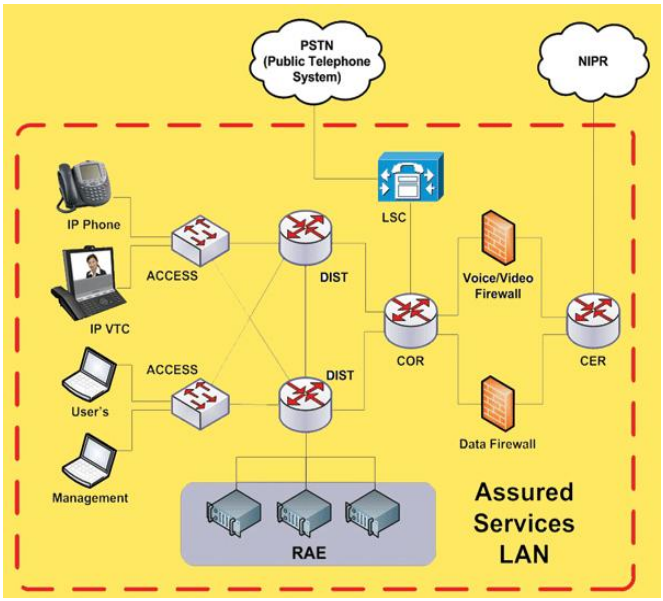

Fig. 2 Voice over Secure IP

II. DESCRIPTION OF DIGITAL SECURE VOICE

A digital secure voice generally includes two components, an encryption system to provide confidentiality and a digitizer to convert between speech and digital signals. Voice coder is used to achieve bandwidth compression of the speech signals.

The standard protocol ZRTP can be used as end-to-end encryption technique for encrypting digital GSM and VoIP. The old secure voice coder or voice compression standards include CELP and MELP, where the latest standard is the MELPe algorithm.

A. Digital Methods using Voice Compression

The MELPe (Enhanced Mixed Excitation Linear Prediction) is a speech coding standard of United States Department of Defense for military applications, secure voice and satellite communication. Its development was supported and led by NSA and NATO. The Enhanced-MELP was adopted in 2001 in form of supplement and annexure for secure voice communication.

In 2002, the MELPe was adopted as NATO standard and it was tested against old secure voice standards. Subsequently, the MELPe won the competition, surpassing the quality of all other secure voice standards. The NATO concluded that MELP substantially improved performance in terms of speech quality, intelligibility and noise immunity and reducing throughput requirements.

In 2005, a new 600bit/s rate MELPe voice coder (vocoder) was added to the NATO standard by France, and there are more advance efforts are made to lower the bit rates to 300 bit/s and even 150 bit/s [4].

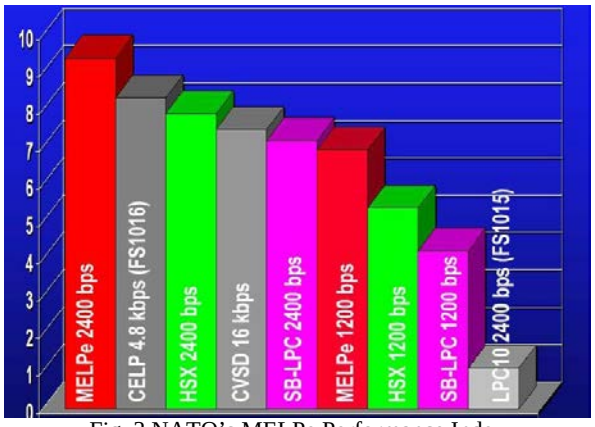

Fig. 3 NATO's MELPe Performance Index

One of the greatest benefits of the MELPe is that it shares the same bit format as MELP, and hence can interoperate with existing MELP system and delivers better quality at both ends. MELPe provides better performance and quality than older military standards, especially in noisy environments such as army vehicle, battlefield and aircraft.

B. Multiple Encryption for Securing Voice

Voice encryption is the process of converting sound signals or voice into a secure form. It provides high security for voice communication. There is the possibility of information theft during the conversation through insecure communication medium such as telephone, mobile and IP phone etc. Voice encryption can resolve this problem and enables to establish secure communication between sender and receiver. In modern technology, mostly secure voice systems are using multiple encryption technique for secure communication without losing its quality and clarity. In this process, voice information is secured through multilayer security by number of encryptions using various advance and complex encryption algorithms.

Fig. 4 Multiple Encryption of Voice Communication

Multiple encryption ensures high safety of voice information over insecure wireless network. It offers telecommunication security that gives protection against eavesdropping and information theft for various forms of voice communication between 3G, GSM, 2.5 and IP network. In modern age, mostly secure voice devices are implementing the concept of multiple encryption and using 256 bit AES encryption algorithm which is the most advanced encryption technique for voice communication and more advanced than the DES standard.

For secure voice communication multiple encryption provides the various benefits, which are follows as:

(a) High level security through number of encryption with different encryption keys for each session using Asymmetric Public key cryptography and Diffie-Hellman Key exchange algorithm.
(b) End-to-end secure data and voice communication over GSM network.
(c) Maintaining voice quality and clarity.
(d) Efficient implementation of encryption algorithms for minimum impact on battery life.

Many IT companies are providing highly advanced voice encryption devices such as Snapshield, Snapfone, Snapgate and Snapmaster, which have the capabilities of voice encryption. These voice encryption devices are trusted by government offices or organizations, private enterprises and individuals.

III. SECUREGSM: AN IMPLEMENTATION OF SECURE VOICE COMMUNICATION

The techniques of secure voice communication are implemented successfully to provide reliable voice communication over wireless media. SecureGSM is one popular application in the market, which provides a secure voice communication over wireless network.

SecureGSM products encrypt the phone call in both directions, end-to-end, to Military Grade encryption standards and beyond. On connection between parties, SecureGSM products use strict verification procedures to ensure the

identity of calling parties, backed up by widely endorsed encryption technologies.

SecureGSM In-Confidence is next generation product designed to deliver SecureGSM's famous triple-layer encryption to secure Voice over IP (VoIP) communications. In-Confidence is the only dedicated multi-party conferencing product with triple layer encryption capabilities available on the market today [5].

This product is very popular for secure voice communication due to its advance features of voice security and encryptions. It includes various advanced features as:

*SecureGSM™ *In-Confidence* features robust, triple cipher (3 x 256 bit), cascading encryption based on AES, Twofish and Serpent ciphers. Any one of these encryption algorithms is considered unbreakable by today's standards and the triple layer ensures that encrypted data is future proof.

*If any one of the encryption algorithms is broken, or found flawed in the future, it is not possible to obtain data to decrypt or compromise the remaining layers or chains.

*Robust, high performance, asymmetric key generation engine. Private and public keys are generated per session and subsequently destroyed (unrecoverable) upon termination of call.

*Calling party identity verification procedures as protection from "man in the middle" attack and comprehensive procedures to ensure keys or foreign data have not been injected or substituted by a third party.

Triple ECDH - Elliptic Curves Diffie-Hellman (3 x 571 bit) Public Key Infrastructure.

*Unique Party Authentication Module.

Fig. 5 (a) SecureGSM Dialing

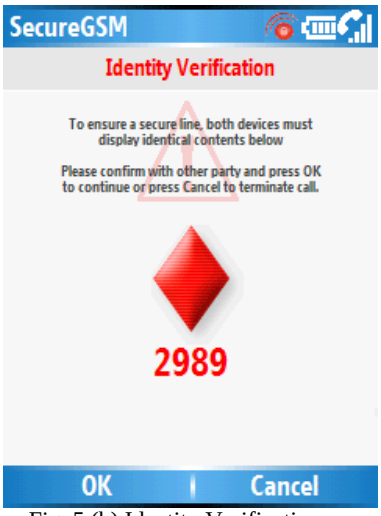

Fig. 5 (b) Identity Verification

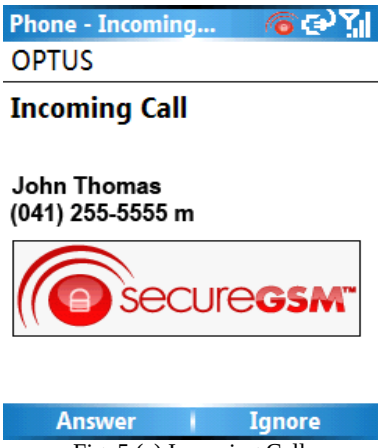

Fig. 5 (c) Incoming Call

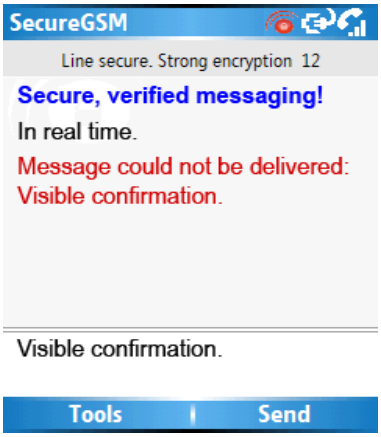

Fig. 5 (d) Confirmation Message

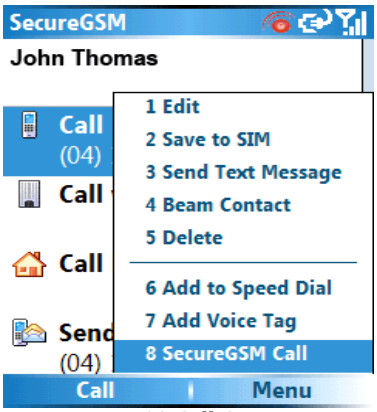

Fig. 5 (e) Call Option

Fig. 5 (f) Secured Call Incoming

Fig. 5 SecureGSM for Secure Voice Communication

During installation, signature files correspondent to each of the program files, along with list of all files that belong to a SecureGSM product installation are placed in the installation folder. The signature files contain verification checksums of each file required to be verified. If the product or a component of the product is modified, corrupted or does not belong to that particular installation, its checksum will be different from what was recorded in its signature file. SecureGSM products stop phone tapping and interception by using unbreakable encryption and offer unparalleled ease of use.

IV. Conclusion

Many users incorrectly assume that commonly available communications methods offer a sufficient amount of protection against malicious interception. It has been proven, time and time again that built in protection mechanisms available in public telephony are easily compromised. Interception equipment for phone tapping (especially over-the-air mobile phone interception) is readily available. Internet telephony (VoIP) is well known to be easily interceptable and thus presents a further challenge where information must be kept private. The demand of voice security is increasing day by day due to maintain the confidentiality of secret information during voice communication over insecure network. It is proved that multiple encryption is making important role to secure voice communication without losing voice quality and clarity. It is widely used to enhance the security of voice communication enormously in comparison of simple voice encryption over wireless network.

References

[1] D. P. Agrawal and Q-A. Zeng, Introduction to Wireless and Mobile Systems (2nd Edition, published by Thomson, April 2005) ISBN 978-0-534-49303-5

[2] The SIGSALY Story, by Patrick D. Weadon, National Security Agency/Central Security Service

[3] R. Barbieri, D. Bruschi, and E. Rosti, "Voice over IPsec: Analysis and Solutions," Proc. 18th Ann. Computer Security Applications Conf., IEEE CS Press, 2002, pp. 261–270.

[4] Weblink: http://www. compandent. com/products_ melpe.htm# MELPeDemo (An implemented security standard)

[5] Web Article "SecureGSM™ *In-Confidence* Next generation encrypted voice, messaging and conference"

Himanshu Gupta is associated with academics and research activities since last seven years. He is presently working as a Senior Faculty Member in Amity Institute of Information Technology, Amity University, Noida, India.

Himanshu Gupta is having specialization in Network Security & Cryptography. He is having prestigious membership in various reputed technical and research organizations such as CSTA (USA), Computer Society of India (India), TIFR (India), IACSIT (Singapore), UNESCO (Paris) and IEEE Computer Society (USA). He has successfully completed a patent titled as "A Technique & Device for Multiphase Encryption" under the domain area of Network Security & Cryptography in the field of Information Technology.

Himanshu Gupta has attended many National and International Seminars, Workshops & Conferences and presented many research papers in the field of Information Technology. He has visited many countries as Malaysia, Singapore, Bangkok and Cambodia for the academic and research purpose. He has been delivered many technical sessions in the field of "Network Security & Cryptography" in various reputed universities and research organizations as an invited speaker.

Dr. Vinod Kumar is associated with teaching and research activities since last 30 years. He is presently working as Professor, Department of Computer Science and Dean, Faculty of Technology, Gurukul Kangri University, Haridwar since last 13 years .

Dr. Vinod Kumar has been Founder Head of the Computer Science Department, Founder Dean, Faculty of Technology and Founder Directorl, College of Engineering and Technology, at GKU Haridwar. Fifteen researchers have already got the degree of Ph.D awarded under his guidance and Eight are pursuing research for their Ph.D.

Dr. Vinod Kumar has published about 75 research papers in various national/ international journal/conferences of repute. He is a member of IEEE, USA and Association of Computing Machinery (ACM), USA. Also, He is a Senior Life Member of Computer Society of India, Life Member System Society of India, Life Member, International Goodwill Society and Life Member of Ramanujan Mathematical Society. He has been Chairman of Haridwar Chapter of Computer Society of India.