Implementation of an Encryption Scheme for Voice Calls

Hazem M. El Bakry
Faculty of Computer Science
Mansoura University

Ali E. Taki El Deen
IEEE Senior Member
Alexandria University

Ahmed Hussein El Tengy
Dept. of Communication
Alexandria University

ABSTRACT
Voice calls is a popular way of communication between persons. Making voice call is cheap, fast and simple. Because of mobile networks attack or smartphones hackers, telephone conversations are vulnerable. This paper presents an encryption scheme for Voice Calls. It helps the user to encrypt the voice call before transmitting it on the mobile network. The idea of the proposed system is to encrypt voice calls without using any secure servers or any intermediate systems between mobile phone and the GSM network. The encryption process occurs before reaching to mobile phone. To maintain intensive security, an encryption algorithm based on RSA encryption is used. Moreover, it uses a public key known by all users and a private key which is a secret and restricted key to each user.

Keywords
Cryptography, RSA Encryption, Mobile System, Voice Call.

1. INTRODUCTION
Mobile communication devices have been common used recently, integrating multiple wireless networking technologies to support additional function [1]. Smartphones and Personal Digital Assistants (PDAs) give users mobile ability to use the internet, email, and many other applications, but smartphone protection hasn't maintained the same developments as computer security [2]. Technical security procedures, such as firewalls, antivirus, and encryption, are not usual on mobile phones, and mobile phone operating systems are not updated as often as those on personal computers. Since mobile phone calls are subjected to hacking, espionage, and eavesdropping, there should be a system that encrypt the phone call before transmitting, to provide security and safety [3].

The rest of the paper is as follows; The first section has already been introduced. section 2 is dedicated to illustrate the need for Securing Voice Communication, following is section 3 which introduces the Voice Over Internet Protocol (VOIP). After that, section 4 highlights the outcomes of Business VOIP and section 5 focuses on the encryption of Voice IP Calls. Moreover, illustration of GSM Voice Call Security is covered in section 6 and RSA Algorithm is briefed in Section 7. Section 8 presents the implementation of Encryption Scheme of Voice Calls. Section 9 formalizes the conclusion.

2. WHY THERE IS A NEED FOR SECURING VOICE COMMUNICATION?
Any voice communication is vulnerable by two risks. First one, when nearby person is listening to the conversation. The second one is, a person eavesdropping by interrupting the transmission of the call on the wires. The first risk can be avoided by being alerted during the communication but the second risk is beyond our control because, it is difficult to figure out [4].

Importance of securing voice communications plays an urgent need for our day to day life. The need for securing our voice communication can be performed by some steps [5]:

- Using an intermediate server has a software encrypts calls from two parties, but it is much cost and need hardware and not available in each place you can go.
- Using the code during the conversation by using code tables which change the word to another meaning, but this way is very old, hard to use, and not effective.
- Applying Voice Over Internet Protocol (VOIP) calls via some websites or applications needs an internet connection to establish the calls and it may not be fully secured.

3. VOICE OVER INTERNET PROTOCOL (VOIP)

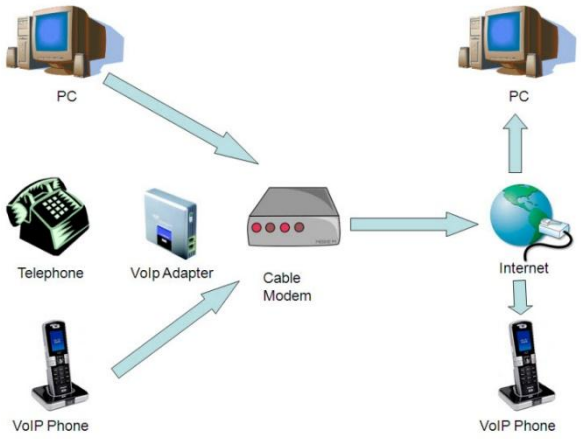

Fig.1 Illustration of making voice calls over internet protocols (VOIP)

a phone call via the Internet depend on VOIP because it uses TCP/IP for sending and for receiving the voice information. The VOIP converts the analog signal of the voice into compressed digitized data. The digitized data signal is broken up to packets. The packets are transmitted on the internet by using the internet TCP/IP protocol. The protocol combines the packets, delivers them, un-compresses them, and converts them back into original signal voice form. VOIP allows data and voice communications transmission on a single network, thus reduces the infrastructure costs. VOIP feature is that the phone calls via the Internet are free of charge as long as there is an Internet connection [6].

There are many applications use VOIP such as skype, 3CX, Google Hangout, line, wechat, and Cool Dialer.
VOIP uses many protocols, for example H.323, Media Gateway Control Protocol (MGCP), Session Initiation Protocol (SIP), H.248 (Megaco), Real-time Transport Protocol (RTP), RTP Control Protocol (RTCP), Secure Real-time Transport Protocol (SRTP), Session Description Protocol (SDP), Inter-Asterisk eXchange (IAX), Jingle XMPP VOIP extensions, and Skype protocol [7].

4. OUTCOMES OF BUSINESS VOIP

The top outcomes of business VOIP include [8]:

- Lower calling costs 55% of current or potential VOIP users said that cost was the main reason for using or considering the service, as said by a survey conducted by Better Buys for Business. Many business VOIP plans allow unlimited local and international calling.
- Greater management outcome by establishing a telephone system network on the company's computers manages users' phones easily. Adding or moving extensions will require a simple change in software systems configuration, rather than a hectic re-wiring process.
- Enhancing mobility business VOIP employees helps to make and receive calls while being out of the office by using computer software that try to be like their physical telephone. Many systems also have call routing features. These features automatically forwards calls to users' mobile or home phones.
- Advanced features Since being software-based, many business VOIP systems include powerful calling features which enhance users' productivity. common features as displaying name directory, call records, multiple folders for organizing voice mails, and ability for integration with PCs that allows users to call a number directly from a web browser or address book on a client.
- Integration with other software VOIP systems can also increase productivity by integrating with other useful software applications. For instance, software tools can allow businesses to keep better track of phone activity to increase the efficiency of their call centers.

5. ENCRYPTING VOICE IP CALLS

VOIP converts voice as analog signal into digitized data then compresses it. The voice as digitized signal is divided or broken up into packets. The packets are delivered across the internet by using the TCP/IP protocol. Anything sent across the internet can easily be interfered. This raises a concern, especially when the information is confidential, like credit card numbers or corporate data. Another concern is to clearly identify the data sender and recipient [9].

Several ways have been developed to resolve these problems, including encryption, change in information software from one to another. Even if received by someone else it will look strange and has no meaning. before the recipient receives the information, the decryption converts the message back to its original format [10].

6. GSM VOICE CALL SECURITY

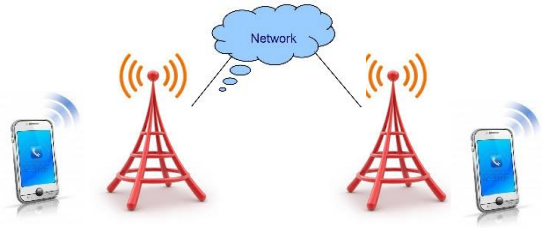

Fig.2 Diagram for GSM Voice Call Security.

GSM system guarantees the confidentiality of the user's data as well as traffic signals within the network. The encrypting algorithms used in GSM ensures traffic confidentiality. Although applied only for the wireless channels. Voice traffic is transmitted across the networks in the form of PCM speech which is possible be unauthorized access to GSM-to-GSM or GSM-to-PSTN conversations. Furthermore, only operator of the network controls the encryption process on the GSM speech channel and it is optional and not by the end user. Maybe some users prefer to control the encryption of their communications. To ensure the security of communications the speech signal should be encrypted before entering the communications system.

GSM utilizes different encryption algorithms for security purposes. Such as A5/1, A5/2, and A5/3 ciphers, which are used for transmitting the signal over the air. The strongest of these algorithms is A5/1 which was developed and applied in the United States and Europe; while the weakest algorithm is A5/2 which is used in other countries. A ciphertext-only attack is able to break A5/2, in addition, the rainbow table attack could crack A5/1[11].

7. RSA ALGORITHM

RSA algorithm is designed by Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman. As an asymmetric cryptography. RSA generates a public key and private key, the public key is known for everybody and it can be used in encrypting the messages while the private key is secret and restricted to the user. The public and private keys can be generated by this way [12]:

- Choosing a random large number p and q
- $n = pq$, (n is the modulus for the private and the public keys)
- $\emptyset(n) = (p-1)(q-1)$
- Choosing an integer (e) so that as $1 < e < \emptyset(n)$, and e is coprime to $\emptyset(n)$, (e) is released as the public key exponent)
- Find d such that $1=d.e \bmod \emptyset(n)$, (d) is defined as the private key exponent).
- Public key is (e, n).
- Private key is (d, n).
- The encryption of $m = m^e \bmod n$
- The decryption of $c = c^d \bmod n$

Advantages of RSA algorithm:

- RSA is a powerful and widely used.
- It is more secure than that of DES and others
- It has a Resistance from external attacks
- More accurate

Applications of RSA:

- RSA is widely used for securing the message communications through encryption and decryption.
- digital signature uses RSA algorithm.
- key distribution uses RSA algorithm.
- in e-commerce and remote banking use RSA algorithm.

8. IMPLEMENTATION OF AN ENCRYPTION SCHEME FOR VOICE CALLS

As shown in Figure 3, the concept is securing the voice call in its journey from the sender device to the receiver one which is simply described as 2 reverse processes. The first process receives the voice call from the microphone in its analogue nature, then transfers it to digital form using an analogue to digital converter circuit. The outcome then is treated by an encryption circuit. After that it is sent to a digital to analogue converter circuit to turn it to the analogue form again to be compatible with the mobile GSM network. Upon receiving the voice by the receiver device, the second process starts as the voice is changed from the analogue form to the digital one using an analogue to digital converter circuit. The digital outcome is then treated by a decryption circuit. After that it is converted back to its analogue nature by a digital to analogue converter circuit to be compatible with the speakers in the receiver device as an audible sound.

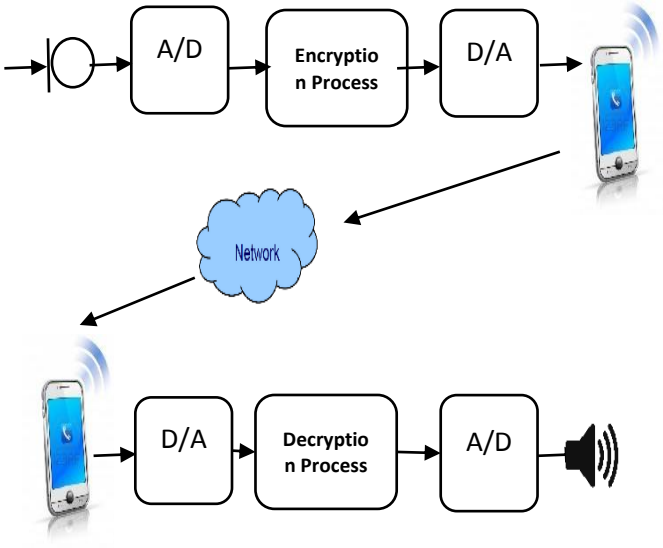

Fig. 3 Transmitting and receiving GSM calls after encrypting and decryptingFig.1 Illustration

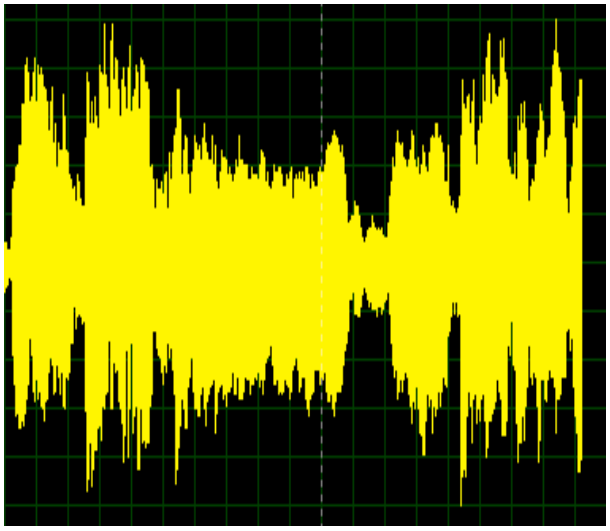

Fig 4 Analog Audio signal before encryption

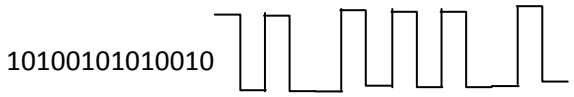

Fig.5 Digital Audio signal after encryption

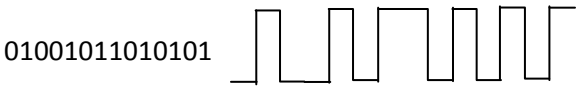

Fig 6 Digital Audio signal after encryption

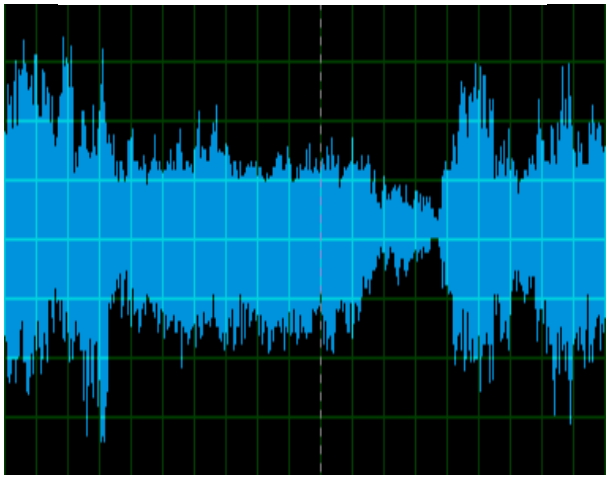

Fig.7 Analog Audio signal after encryption

9. CONCLUSION

In this paper, the need of encrypting important voice calls has been clarified, Because of mobile networks attack, the GSM networks are not secure. Thus, the paper has described a designed circuit that solved this problem. The main idea is encrypting the voice before sending it to the phone device and in the other side decrypting the voice after receiving it by the phone and obtain a clear voice by an external speaker. The circuit has converted the voice received from the microphone from analog to digital format, then encrypted it, and finally

converted it from digital to analog format, and sent it to the transmitter (phone) to transmit it to the GSM network. On the other side, the receiver (phone) has received the analog encrypted signal. This signal then has passed to the circuit that converted it from analog to digital format, and then decrypted it. The final step is to convert the form of decrypting digital signal to analog, and produced audible sound by speakers again. By this way securing telephone calls from eavesdropping and intruders has been achieved.

10. REFERENCES

[1] Chin, E., Felt, A. P., Greenwood, K., and Wagner, D. "Analyzing Inter-Application Communication in Android". In Proc. of the Annual International Conference on Mobile Systems, Applications, and Services (2011).

[2] Marko Hassinen, "SafeSMS - End-to-End Encryption for SMS Messages", *IEEE International Conference on Telecommunications*, 2008, 359-365.

[3] S. Jahan, M. M. Hussain,M. R.Amin and S. H. Shah Newaz, "A Proposal for Enhancing the Security System of Short Message Service in GSM", IEEE International Conference on Anti-counterfeiting Security and Identification, 2008, 235-240.

[4] Nichols, Randall K. & Lekkas, Panos. "Speech cryptology". Wireless Security: Models, Threats, and Solutions. New York: McGraw-Hill 2002.

[5] C. K. LaDue, V. V. Sapozhnykov, and K. S. Fienberg. A data modem for GSM voice channel. IEEE Transactions on Vehicular Technology, 57(4):2205–2218, July 2008.

[6] Mehta, P.; Udani, S., "Voice over IP", IEEE Potentials, Vol.: 20 Issue: 4, Oct.-Nov. 2001.

[7] Lydia Uys, "Voice over internet protocol (VoIP) as a communications tool in South African business", African Journal of Business Management Vol.3 (3), pp. 089-094, March 2009.

[8] A.A. Ojugo, R.E. Yoro, A.O, Eboka., "Implementation Issues of VoIP to Enhance Rural Telephony in Nigeria", Journal of Emerging Trends in Computing and Information Sciences, Vol. 4, No. 2 Feb 2013.

[9] Saruchi Kukkar, "Encrypted IP Voice Call Communication on Android through Sip Server on 3G GPRS" International Journal of Engineering and Technology Volume 2 No. 2, February, 2012.

[10] Ferguson, N., Schneier, B. and Kohno, "Cryptography Engineering: Design Principles and Practical Applications", T. Indianapolis: Wiley Publishing, Inc. 2010.

[11] N.N. Katugampala, "Real Time Data Transmission Over Gsm Voice Channel for Secure Voice & Data Applications", Exploring the Technical Challenges in Secure GSM and WLAN, 2004. The 2nd IEE (Ref. No. 2004/10660).

[12] Arfan Shaikh, "Audio Steganography And Security Using Cryptography", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 2, February 2014.