World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 5, No. 1, 6-10, 2015

Securing VoIP in SIP Mobile Network

Zaid Salah Munef
Master's Degree in Computer Science
Amman Arab University, Amman, Jordan

Alaa Hussein Al-Hamami.
Dean of Computer Sciences & Informatics College
Amman Arab University, Amman, Jordan

Abstract - Lately, the development and progress have become significant in the field of information technology, especially in the field of data transmission via internet. One kind of the data transfer is voice. This part of the development in the field of mobile devices, which is possibility supplying the device by internet service .These developments in the field of technology are concurring many problems, where it had a direct impact on this development and the turnout by the users.

In this paper, the model's implementation has done on a mobile device (Which is operating by (Android) system). The sound transfer process has been via the internet using the SIP server to authenticate and reliability the communication process between two parties, after that RSA algorithm (key size used 1024 bit) is using of increased the encryption keys strength and exchanged between the two parties and to ensure that the packet transmitted every time. (AES) algorithm used to encrypt the package, choosing this algorithm that is very effective, which is associated with the encryption speed. Key size used in the model with AES is (256 bit) to ensure the secured and speed of the proposed operation.

Keywords – VoIP; AES; RSA; SIP; UDP; TCP.

I. INTRODUCTION

The mobile is more than just device for making phone calls; it gives developments in hardware and software. Mobile phones use have been expanded such as send messages, check emails, process of shopping, banking service, store contacts, select map's, store important dates, camera service and other uses.

Part of the mostuseful is mobile Wireless Fidelity (Wi-Fi) that led to develop new services in domain transfer of media, including voice transfer known as Voice over Internet Protocol (VoIP).

VoIP service is providing very low-cost or semi-free voice calls. Through internet, and draws of attention many internet users. The VoIP services are generate from fixed sized packets. The size of VoIP packet is relatively small compared to other video or web packets, and the redundant header size of a VoIP packet is larger than the size of the payload including voice information [1].

VoIP is subjected to various types of attacks that called capturing packets, eavesdropping communications and many other types. For that transmissions of media need different factors like confidentiality, authentication, and integrity with replay protection to the media stream.

Additional, The development of voice transmission field generates many problems. The intruder problem considered from dangerous problem because the voice transferred might have important and sensitive information. Therefore the protection of data from misused is essential, and needed the encryption and decryption to provide the protection. So, the problems of intruders notes through eavesdropping or monitoring the data.

The VoIP is considered one types of voice transmission, so it needs to protect. Therefore, in this paper, the encryption is applied on the voice to produce the cipher voice and the decryption is applied to retrieve the original voice.

II. VOIP COMPONENTS

There are different elements of VoIP components, such as the following:

1. End-user Equipment

The end-user equipment is used to access the VoIP system to communicate with another end point.

2. VOIP Protocol

There are different types of VoIP protocols in network, but only the most commonly used ones are UDP, TCP, H.323 and SIP :-

2.1 User Datagram Protocol (UDP)

The UDP is defined to make available a datagram mode of packet communication between two devices in the networks. This protocol sent packet without wait any response from

second party. In this protocol, the delivery and the duplicate protection are not guaranteed, but it is processing errors that occur between transmitter and receiver by checksum field [2].

2.2 Transmission Control Protocol (TCP)

The TCP called a handshaking process, where establish a specific connection between source and destination. The transfer packet should be in sequence and does not send any packet before make sure the arrival of the prior packet, because the TCP packet depends on:-

Sequence number: each endpoint of a TCP connection establishes a starting sequence number for packets it sends from source.

Acknowledgement number: it is contained receive packet response from destination, if the response is positive then source sent the next packet. But the response is negative; the source resent the same packet [2].

Therefore, TCP will more time cost depends on network traffic condition than UDP to finish it. But the ensure safety arrival of packet in TCP is better than UDP.

2.3 H.323 Protocol

The H.323 makes it possible to create and deploy new services quickly and to take advantage of multimedia capabilities.

The H.323 is widely used within various internet real-time applications like NetMeeting and is widely deployed worldwide by service providers and enterprises for VoIP networks. The H.323 standard addresses call signaling, multimedia transport, and bandwidth control for point-to-point and multi-point conferences. Therefore the H.323's strength depends on data important [3].

2.4 Session Initiation Protocol (SIP)

The SIP is signaling /controlling protocol, for initiating, manipulating, managing and terminating interactive communication sessions between users, these sessions may include voice, video, instant messaging [4, 5].

SIP is used to setup IP based multimedia services such as audio and video streaming, instant messaging, and other real-time communication across commonly used packet networks. The SIP is mediator between two parties and it is transfer data between two clients, so opens many opportunities for several attacks such as registration hijacking, impersonating a proxy and Denial of Services (DoS). SIP is includeda parameters (Confidentiality, Integrity, Authentication, Privacy, and Availability), it contains the sensitive information like the user name and the location of the user, andestablished call between two parties, the conversation should be protected and the information [4, 5].

3. Security Methods of VoIP

There are different types of VoIP security through encryption algorithm, but only used in this thesis the most commonly ones are AES and RSA:-

***3.1** Advanced Encryption Standard (AES) Algorithm*

The AES is use to provide security for sensitive data, and it is based on Substitution and Transposition methods. The AES is used in many password-protected documents and wireless communications such as wireless sensor networks, and also in top secret government files, for which it was first built.

In such situation, AES encryption will be done for each block separately. So, the sensitive part of the algorithm is the secret key. Therefore should are motivated to do some processing to give more security to this key [6, 7].

***3.2** Rivest-Shamir-Adleman (RSA) Algorithm*

The RSA algorithm is one of the most popular public-key encryption and it is kind of asymmetric encryption methods. It is can be used both for encryption and signature. In additional that, VoIP networks are growing very fast, so a larger volume of VoIP traffic is expected and this will significantly increase the cost of supporting security voice by RSA computations.

The RSA algorithm can depend in a secured data by increasing the corresponding keys sizes in order to cope with the improvement of processors speeds that the attackers might use to attack this algorithm [8, 9].

Therefore in this case, the proposed model is using RSA and AES to reduce the intruder attacks and problems of get data during the process of transportation, as discussed in statement of problem.

III. RELATED WORK

Recently, there have been many researches who presented suitable transfer method in the VoIP field, which is representing the protocol for transmitting voice data using the internet.

Several techniques and algorithms have been presented to improve the quality of VoIP transmission, but these techniques have been focused on one side of the transmissionaspects, such as security, quality or speed [10, 11, 12].

In this paper, attempted to handle all the important aspects of the VoIP field and this has been achieved through focusing on two important points:-

- The first point: - the transmission VoIP process occurred through SIP server, who works as a monitoring on the communication session between two parties (sender and receiver).
- The second point: - providing transmission security by depending on the characteristics of two algorithms (RSA and AES).

IV. PROPOSED SOLUTION

This paper is focused on two main points:

- The modelproposes and generates method to reduce the threats during transfer operation. This model should be secured and without drawing any attention to the intruders.

- The security algorithm will depend on two characteristics AES algorithm (high speed and reasonable security) and RSA algorithm (Strong Security and reasonable speed).This is using the advantages of AES speed with RSA security to produce an algorithm that called AR2SS (AES & RSA Speed and Security).

The model includes three procedures (Noted all step above work together and the chart illustrate working of every step):-

1. SIP Server procedure: this procedure's function is to make a connection between two parties, it is elaborate when receiving extension request and check it if available or not, then open session will depend on available or not (sender and receiver).
2. Sender procedure: this procedure's function is to encrypt the audio in the sender side, and then sends it to the receiver. Which is working after the extension is available.
3. Receiver procedure: this procedure's function is to receive the encryption audio from sender, and then decrypts it in the receiver side. Which elaborating after the SIP server is opening session.

V. USED ALGORITHMS

There are many algorithms used in this thesis for providing suitable security in transmission voice, these algorithms are divided into three procedures and each procedure includes many steps to execute a specific function.

1. Major algorithm

This part is used to transmit audio between the sender and the receiver, in addition to third-party in safely form, as following:

// Input: audio.
Output: audio. //
Step1: Call (SIP-Server algorithm).
Step2: Call (AR2SS-Encrypt Algorithm).
Step3: Send encrypt packet
Step4: Call (AR2SS-Decrypt Algorithm).
Step5: Return (audio).

2. SIP-Server Flowchart

This part is used to receive the required extension from the sender, then make sure this extension is available case or not. Based on the case, the server decides to open the session or not,as following:

// Input: desired extension.
Output: give permission or not. //
Step1: Step1: IF (New Register ==True) Then
Step2: X ← register include all extension
Step3: Else
Step4: Y ← desired extension from sender
Step5: If (Y == True in X) Then
Step6: Z ←give permission and open session between parties
Step7: ELSE
Step8: Z ← not permission to open session
Step9: End If
Step10: Return (Z)

3. AR2SS-Encrypt Algorithm

This part is used to open the session with the SIP server, also make sure the second party existing or not. After that, the sender is encrypting the audio then sent it to the recipient side, as following:

// Input: original audio.
Output: encrypted audio with index of encrypted key//
Step1: IF (in-call == New Call)
Step2: Connect with SIP server
Step3: Generate (10 Keys) from IP-Sender
Step4: Send desired extension to the SIP as (Ext# receiver @ IP address sip server)
Step5: Receive IP-Receiver from SIP server
Step6: Generate (10 Keys) from IP- Receiver
Step7: Start connection between parties
Step8: X ← Rand (Key)
Step9:X1 ← encrypt by RSA(X)
Step10: Send (X1) to the receiver
Step11: IF (Flag == False) Then
Step12: Flag ← True
Step13: ELSE
Step14: Flag ← False
Step15: END IF
Step16: IF (Flag ==True)
Step17: J ← 2
Step18: ELSE
Step19: J ← 1
Step20: END IF
Step21: END IF
Step22: Record from MIC by Stream Thread
Step23: While (in-call == True)
Step24: For I=J: 2:10 // by using key receiver
Step25: X2 ← 8096 byte (data)
Step26: X3 ← Encrypt by AES_{Keyi} [X2] //X3: data encrypted
Step27: X4 ← Encrypt by AES_{KeyX_1} [index Key_i] //X4: index key encrypted
Step28: Send (X4,X3) to the second party by Audio Streamer Send Sound to port (50505).
Step29: IF(in-call== True) Then
Step30: Continue

Step31: ELSE
Step32: Break
Step33: END IF
Step34: END FOR
Step35: END While
Return (X3,X4)

4. AR2SS-Decrypt Algorithm

This part is used to receive encrypted data from the sender, then decrypt this data and combine it,

// Input: encrypted audio with index of encrypted key.
Output: original audio //
Step1: R← Received (X1) from sender
Step2: R1← RSA (R)
Step3: While (in-call == True)
Step4: Received (X3) and (X4) from sender by Audio Receiver from port (50505).
Step5: R2← X3 //R2: encrypted data
Step6: R3← decrypt by $AES_{Key\ R1}$ [indexKey_{X4}] //R3: index key
Step7: R4← decrypt by $AES_{Key\ R3}$ [R2] //R4: data decrypted
Step8: R5← combine (R5,R4) //R5:result data
Step9: Listen (R5)
Step10: END While
Return (X5)

VI. Experiment

This part is explaining the results which were obtained through the implementation of the program on PC (CPU 3120 GHz, RAM 8 GB) with Samsung mobile device. This type is (i9300), which CPU 1GHz and RAM 8 GB with also a router of 108 megabyteper second the speed of transmitting data. The experiments are clarified in each one a different key were used more than the other one with similar packet or the opposite:

- In the 1st experiment (key size 128 bit &packet size 20000 byte) obtained a high speed but unacceptable security is in data transfer.
- In the 2nd experiment (key size 192 bit &packet size 20000 byte) obtained unacceptable security and unacceptable speed is in data transfer.
- In the 3rd experiments (key size 256 bit &packet size 20000 byte) obtained acceptable speed and security is in data transfer.
- In the 4th experiment (key size 256 bit &packet size 10000 byte) got insufficient security one time and insufficient speed on the other time.
- In the 5th experiment (key size 256 bit &packet size 40000 byte) obtained a high security but unacceptable speed is in data transfer.

In addition to the table mentioned above, noted the average time between the encryption and decryption process is 2.25 - 4.75 millisecond. It is depending on quality of service (Internet), with a service users' numbers, which used the fixed packet size (20000) byte and changed key size (128,192 and 256) bit, as shown in Figure 1.

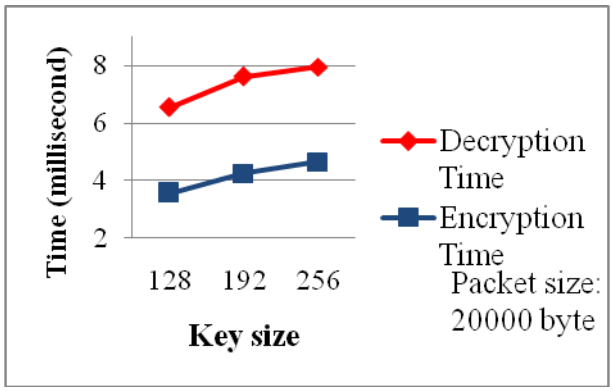

Figure 1. The results show for the effects of the key size on the Encryption & Decryption average time.

While is using the fixed key size (256) bit and changed packet size (10000, 20000 and 40000) byte, as shown in Figure 2.

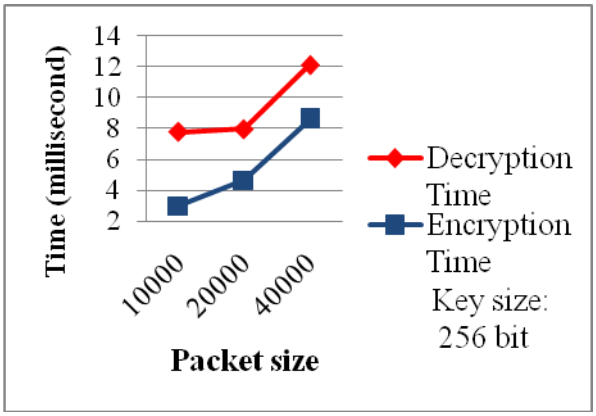

Figure 2. The results show for the effects of the packet size on the Encryption & Decryption average time.

Consequently a key size of 256 bit and packet of 20000 bytes was selected as a proposed solution for acceptable security and speed, where the packet contains the data that the receiver can listen to the audio without delay. In addition, having enough time to decrypt the following packets and listen to it. Based on must take into account the effect of quality and service, as well as the number of users. Where affect the speed of transport directly.

VII. Conclusion& Future Work

The voice transmission processis providing in secured way by using two algorithms RSA, AES through advantages of each algorithm, the characteristics of AES algorithm is declared as high speed and reasonable security. In addition, a characteristic of RSA algorithm is declared as strong security and reasonable speed.

The model implemented multi experiments in three procedures: SIP server procedure, sender procedure and receiver procedure which executing through a call between two phones. The model obtained many results that shown in chapter four, and declared difference of time for encryption and decryption processes.

The time difference is depending on the packet size from sender to receiver, with comparing the encryption and decryption processing time that declared possibility data encryption in suitable time. Results of experiments showed that the sent 20016 byte to each sender packet size, which is including 16 byte for key. It will be receiving 20000 bytes, and the total time between the encryption and decryption process for each packet is 2-5millisecond. It is depending on quality of service (Internet), with how to use a service in case of increasing number of user. But this difference is not effect on transfer voice.Future works, applied this program on other Mobile operating systems and send messages on live chat programs with video calls. It can use other techniques of exchanging key such as Diffi-Hellman exchange key algorithm, and the user can connect toglobal network rather than local network.

REFERENCES

[1] Jung J., Y., Kang, H., S., Lee, J., R., (2013). Performance evaluation of packet aggregation scheme for VoIP service in wireless multi-hop network. Ad Hoc Networks.

[2] Forouzan, A., B., (2006). Data Communications & Networking (sie). Tata McGraw-Hill Education.

[3] Malhotra, S., and Kaur, P., (2011). Comparison of Call Signaling Protocols for Ad-hoc Networks. International Journal of Computer Applications, Vol. 27, No.10.

[4] Voznak, M.,and Rozhon, J., (2013). Approach to stress tests in SIP environment based on marginal analysis. Telecommunication System.

[5] Kaur, J., and Singh, K., P., (2013). Comparative Study of Speech Encryption Algorithms Using Mobile Applications. International Journal of Computer Trends and Technology (IJCTT), Vol. 4, Issue 7.

[6] Cho, J., Soekamtoputra, S., Choi, K., and Moon, J., (2013). Power dissipation and area comparison of 512-bit and 1024-bit key AES. Computers and Mathematics with Applications.

[7] Pradhan, C., and Bisoi, A., K., (2013). Chaotic Variations of AES Algorithm. International Journal of Chaos, Control, Modeling and Simulation, Vol.2, No.2..

[8] Naqi, Wei, W., Zhang, J., Wang, W., Zhao, J., Li, J., Shen, P., Yin, X., Xiao, X., and Hu, J., (2013). Analysis and Research of the RSA Algorithm, Information Technology Journal.

[9] Kumar, S., Narasimham Ch, and Setty, P., (2013). Small Secret Exponent Attack on Multiprime RSA. International Journal of Soft Computing and Engineering, Vol. 3, Issue. 2.

[10] Lazzez, A., (2013). VoIP Technology: Security Issues Analysis. arXiv preprint arXiv:1312.2225.

[11] Son, B., Nahm, E., and Kim, H., (2013). VoIP encryption module for securing privacy. Multimedia tools and applications Vol. 63 No.1, page. 181-193.

[12] Singh, H., P., Singh, S., Singh, J., and Khan, S., A., (2014). VoIP: State of art for global connectivity—A critical review. Journal of Network and Computer Applications, Vol.37, page 365-379.

AUTHORS PROFILE

Prof. Dr. Alaa Hussein Al-hamami, Dean of College of Computer Sciences and Informatics, Prof. of Database Security, Amman Arab University, Jordan.

Mr. Zaid Salah Munef received the BSc degree in Computer Network Systems from Applied Science University, Jordan in 2010, and the MSc in Computer Science from Amman Arab University, Jordan in 2015.