Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 9, September 2015, pg.261 – 269

RESEARCH ARTICLE

Design and Implementation Encrypted Call Application on Android System

Kadhim H.K.Alibraheemi[1], Wafaa A.A. Alrekaby[2]

[1]Department of CS, Education College for pure science, Thi-Qar University, Iraq

[2]Department of CS, Education College for pure science, Thi-Qar University, Iraq

[1]Email: alshemkhy@gmail.com

[2]Email: wafaali8055@yahoo.com

Abstract: Cellular phones are being used to discuss sensitive information, whether personal, commercial or medical. The main challenge in cellular phones is security threats like eavesdropping within calls made by attackers. Private calls over the Internet are exposed to many communication attacks which led to the development of new applications added to the Android systems. These (so called) apps are used for protection of voice communications. Problems of being attacked could be solved by using encryption algorithms, protection protocols or development Hardware, all of them can be added to the mobile protection technique. The proposed application which is called Wafaa in this research is to develop the application using VoIP protocol to transmit voice over the Internet, and use SRTP protocol that provides strong encryption based on AES encryption algorithm and ZRTP protocol for key exchange.

Key words: Call encryption, Security algorithm, Android application, Communication protocols.

1. INTRODUCTION

The institute of Electrical and Electronics Engineers (IEEE) 802.11is interested in mobile devices and the added security of these devices and their own private networks security issues [1]. They have developed a lot of mobile phone specifications and added three basic services for the conservation of these devices and the protection of information in circulation. There are identity communication devices authentication, protection of confidential information, and control access to resources that authorized devices. Therefore Smart Phones have become portable of the most important means for the transmission of information and communication between the communities. This information can be extremely sensitive, it is either business information, political information or intelligence information .These was developed within the community so it became necessary to provide protection for this type of information. Protection applications in the mobile phone may not be sufficient to secure this confidential information therefore it was necessary for the provision of other applications like special system Android to protect the information. depending on how information is transferred, whether a message , through a voice call or through the email or information of all kinds as well, whether voice, video, or a message .There are ways to protect information and greet these methods where information is encrypted using a well known encryption algorithms . So our work in this research is on the implementation of the application added to the Android platform for the purpose of protecting voice communication transmitted via the Internet using a technique called Voice over Internet Protocol (VoIP) and a set of Internet protocols, which protect communications.

1.1. Problem Statement:

Mobile devices became the most commonly used devices for transferring important and sensitive information, whether political information, medical or economic. It has become necessary to protect this information and add security applications to mobile devices for the purpose of protection and to maintain the confidentiality of information and protect it from attacks.

1.2. Problem Discussion:

Cellular phones have become commonly used to discuss topics like Sensitive business and personal information. However, there is little concern for the security of these calls, but it can be important for certain people. So it became necessary to use Encrypted telephone calls because it was a solution to this problem. This required an Internet connection to transmit voice. In this paper, we propose an application running on Phone calls to encrypt calls. We can add it to your smart phone and specifically on the Android operating system. The proposed structure uses VoIP to transmit voice and convert it from an analog signal to a digital. Depending on Real Time Transport Protocol (RTP) that transmit digital packets in the form of packets over the network lines and the Secure Real Time Transport Protocol (SRTP) to add protection These packages use an algorithm Advance Encryption Standard (AES) and Zimmermann Real-time Transport Protocol (ZRTP) which is used to generate a special key for each call. The tools used in this research includes Integrated Development Environment (IDE) it is Software application that provides comprehensive facilities to computer programmers for software development such Eclipse, and some of development kits such as Java Development Kit (JDK) is a set of tools used for creating and manipulating Java code. Also the required tools include java that converts your java files into byte code, and Software Development Kit (SDK) that enables developers to create applications for the Android platform.

1.3 OBJECTIVES:

The main objectives of this application are:

1. To provide applications available in government departments for the purpose of conducting a secure communication
2. Protecting the confidentiality of information
3. Protection of contacts from being changed by using a protocol that verifies that the packets sent is the same as the received packets
4. Contact protection from eavesdropping.
5. Authenticating the identity of communicating devices

2. CALL ENCRYPTION ANALYSIS

This application is an encrypted VoIP client designed with the mobile environment. In any call, there are generally four participating entities:

1. The initiator client. This is typically the device of the user who is initiating a call to another user.
2. The responder client. This is typically the device of the user who is receiving a call from another user.
3. The master server: responsible for *signaling* and *authentication*. These can be located in trusted locations and given isolated access to the Wafaa user database and signaling interfaces.
4. The relay server: provide the lowest-latency path for a call. Since all *authentication* and *signaling* are delegated to a master server, the relay servers don't need to be as highly trusted. The Server is responsible for the following:

1. **Signaling**: The Server receives call setup requests from initiators and signals responders that they are receiving an incoming call.
2. **Authentication**: The Server provides a server-trusted level of authentication that initiators and responders are who they claim to be when setting up calls, making it non-trivial to spoof calls. The call has the following steps:

1. A caller contacts a master server, and signals that they would like to establish a call with a responder.
2. The responder receives an encrypted signal, connects to the master server, and indicates that it has received the call signal.
3. If the responder chooses to answer the call; it is relayed through the closest available relay server.

3. CALL SIGNALING

In Voice over Internet Protocol, voice communication is carried out using the Internet Protocol (IP). The voice signal is first separated into frames, which are then stored in data packets, they are sent out across the internet the same way as any other IP packets. Then they are transported over IP network using voice communication protocol. Currently, the majority of VoIP systems use either one of two standards; the ITU standard H.323 and the IETF standard SIP, while a few still use proprietary protocols like SCCP [2].VoIP requires a means for prospective communications partners to find each other and to signal to the other party their desire to communicate. This functionality is referred to as Call Signaling. The need for signaling functionality distinguishes Internet telephony from other Internet multimedia services such as broadcast and media-on demand services. VoIP, when used for synchronous voice or multimedia communication between two or more parties, uses signaling that creates and manages calls [3]. The caller can define a call as a named association between applications that is explicitly set up and torn down. Examples of calls are two-party phone calls, a multimedia conference or a multi-player game. A call may encompass a number of connections, where a connection is a logical relationship between a pair of end systems in a call. For example, a non-bridged three party audio only call will have three connections, creating a full mesh among the participants. A media stream or session is the flow of a single type of media among a set of users. This flow can either be uncast (in which case it is between two users), or multicast (more than two users). A media session is associated with one or more connections. In the three party call examples, if the media is distributed using uncast, there will be one audio session per connection. If the audio is distributed via multicast, there will be one audio session associated with all three connections. It is not required that calls have media streams associated with them, but this is likely to be the common case. Internet telephony signaling may encompass a number of functions: name translation and user location involves the mapping between names of different levels of abstraction, feature negotiation allows a group of end systems to agree on what media to exchange and their respective parameters such as encoding, call participant management for participants to invite others on an existing call or terminate connections with them, feature changes that make it possible to adjust the composition of media sessions during the course of a call, either because the participants require additional or reduced functionality or because of constraints imposed or removed by the addition or removal of call participants [4].

3.1. VoIP Signaling Protocols

There are a signaling protocols used in this application but this section will explain the Session Initiation Protocol (SIP). SIP it is an application layer control protocol for creating, modifying and terminating sessions with one or more participants. The architecture of SIP is similar to that of HTTP [5]. Requests are generated by the client and sent to the server. The server processes the requests and then sends a response to the client. A request and the responses for that request make a transaction. SIP has INVITE and ACK messages which define the process of opening a reliable channel over which call control messages may be passed. SIP makes minimal assumptions about the underlying transport protocol. This protocol itself provides reliability and does not depend on TCP for reliability. SIP depends on the Session Description Protocol (SDP) to describe the details of the call (i.e., audio, video, a shared application, codec type, size of packets, etc.). SIP uses a Universal Resource Locator (URI) to identify a logical destination, not an IP address. The address could be a nickname, an email address (e.g., sip:chintanv@mit.edu), or a telephone number. SIP supports session descriptions that allow participants to agree on a set of compatible media types. It also supports user mobility by proxy and redirecting requests to the user's current location. The services that SIP provides include:

1. User Location: determination of the end system to be used for communication
2. Call Setup: ringing and establishing call parameters at both called and calling party
3. User Availability: determination of the willingness of the called party to engage in communications
4. User Capabilities: determination of the media and media parameters to be used
5. Call handling: the transfer and termination [5].

3.2. Supporting Protocols

SIP works in conjunction with

1. Session Description Protocol (SDP)

SDP is a format used to describe multimedia session parameters for the purpose of session declaration, session arraignment, and others. A multimedia *session* is a set of multimedia senders and receivers and the data packet flowing between them; a single session may consist of multiple media streams. A session declaration consists of a session level description (details that apply to all media streams) and optionally, several media-level descriptions. Since SDP is diametrically a format specification, it is independent on the transport layer and may be conceived by SIP [6].

2. Real-time Transport Protocol (RTP)

RTP, Real-time Transport Protocol, is an application level protocol that is intended for delivery of delay sensitive content, such as audio and video, through different networks. The purpose of RTP is to facilitate delivery, monitoring, reconstruction, mixing and synchronization of data streams. Although RTP does not provide quality of service on IP networks, its mixers can be used to facilitate multimedia delivery on a wide range of link types and speeds. RTP is designed to use both unicast and multicast transport protocols. Even though RTP is a relatively new protocol, it is widely used by applications like Real Network's RealPlayer, Apple's QuickTime and Microsoft's NetMeeting. Some of the common applications of RTP are audio and video streaming media services and video conferences. As RTP is usually used trough Internet, the network should be considered as

insecure. Although many media streams are publicly available, video conference usually requires confidentiality. In many situations it would be preferable if the user could authenticate the originator and ensure the integrity of media streams [7].

3.3. Encryption Protocols

When some agents want to communicate with a media stream (for example voice or video), the RTP is used. This protocol does not provide encryption. So it is necessary to use Secure RTP (SRTP) to secure the communication. In order for this to work, the agents need to agree on key material and ZRTP provides them with a procedure to perform this task it is a key agreement protocol, which relies on a Diffie-Hellman exchange to generate SRTP session parameters, providing confidentiality and protecting against Man-in-the-Middle attacks even without a public key infrastructure or endpoint certificates.

3.3.1. Key Exchange

ZRTP "Z" is a reference to its inventor, Zimmermann; "RTP" stands for Real-time Transport Protocol. Unlike session initiation and description, the key exchange is a fundamental security mechanism. Therefore, we describe the key exchange protocols specific to VoIP in more details. It is essential to understand what security guarantees they provide, because, a mismatch between the expectations of the transport-layer protocol and the security properties actually ensured with the key exchange. ZRTP describes an extension header for Real time Transport Protocol (RTP) to establish a session key for SRTP sessions using authenticated Diffie-Hellman key [8]. The main distinguishing feature of ZRTP is that it does not require prior shared secrets or the existence of a separate Public-Key Infrastructure (PKI). This is an important consideration as it eliminates the need for a trusted certificate server. Since Diffie-Hellman (DH) key exchange is malleable and does not provide protection against man-in-the-middle attacks, ZRTP uses a Short Authentication String (SAS), which is essentially a cryptographic hash of two Diffie-Hellman values, for key confirmation. The communicating parties confirm the established key verbally over the phone, by looking at their respective phone displays and reading the displayed SAS values to each other. After that, they rely on key chaining: the shared Diffie-Hellman secrets cached from the previous sessions are used to authenticate the current session. [9].During the run of the protocol two agents exchange messages involves they are initiator and the responder.

3.3.2. Secure Real Time Protocol (SRTP)

The SRTP protocol is merely a secure audio/video profile for RTP that offers confidentiality, integrity and authentication for video and audio streams. The secure profile is designed to exist between the RTP application and underlying transport layers. Media packets moving down through RTP stack are intercepted and secured, into SRTP packets, before being passed to the transport layer. Conversely, SRTP packets moving up the stack are unprotected, into RTP packets, the purpose of SRTP is to ensure confidentiality [10] one of the goals of SRTP is to ensure the confidentiality of the media session, and this is done using encryption. Two ciphers to be used to encrypt SRTP payloads, AES and the "Null" cipher. Other ciphers can be implemented, but they must be described in a standards track. The Null cipher performs no encryption; AES is a symmetric block cipher. Plaintext is encrypted by blocks to produce a ciphertext based on a given key, the same key is used to encrypt and decrypt the blocks. The decryption process is the opposite of the encryption process; the ciphertext goes through the block cipher which produces the plaintext using the key [10] integrity: Both the origin integrity (authenticity) and the data integrity are secured by a keyed hash function (HMAC-SHA114). Hash based Message Authentication Code (HMAC) uses a cryptographic hash function (in our case SHA1) and a secret key to produce Message Authentication Code (MAC) for a given message. And authenticity of RTP payloads, hence addressing the security needs for real-time multimedia applications. This is achieved through a framework that allows for the upgrade to new cryptographic algorithms, while maintaining a minimal overhead [11].In SRTP, a cryptographic context refers to the cryptographic state information maintained by the sender and receiver for the media stream. This includes the master key, session keys, and identifiers for encryption and message authentication algorithms, lifetime of session keys, and a Rollover Counter (ROC).The default encryption algorithm is the Advanced Encryption Standard in either counter mode as shown figure 1.The encryption process consists of two steps:

1. The system is supplied with one or more master keys via a non-RTP-based key exchange protocol, from which ephemeral session keys are derived. Each session key is an example of a pseudorandom function, redrawn after a certain number of packets had been sent, with the master key, packet index and key derivation rate as inputs.
2. The packet is encrypted via the generation of a key stream based on the packet index and the salting and session keys, followed by computation of the bitwise XOR of that key stream with the payload section of the RTP packet.

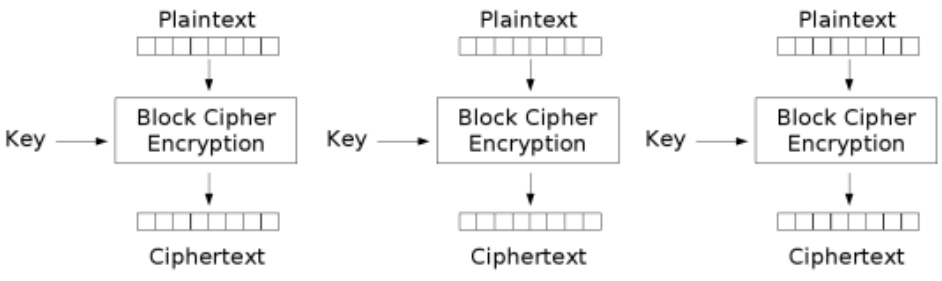

Fig .1 AES Algorithm

4. APPLICATION IMPLEMENTATION REQUIREMENTS

To implement Waffa application we need the following requirments:

1. Android Platform 4.3 or later
2. Install the integrated development enviroment(ECLIPSE), version: luna service release 2 (4.4.2)
3. Java Development Kit (JDK)
4. Software Development Kit (SDK)

5. APPLICATION SCREEN SHOTS

In this section we will display some of screen shots for different causes

Application installation: The proposed application is installed on Android OS mobile devices. After installation the mobile number is needed and the country codes as shown in figure 2, when choosing a country and mobile number, the user will be send a code to verify that it is the user personal phone as shown in the screen shot at figure3.

Figure 2**:** Country Code

Internet verification*:* To continue within the registration, the user must have internet connection. If internet connection is available and the mobile number is correct the user will continue with the registration, as show in figure 4, otherwise will receive connectivity error as shown at the screen shot figure 5.

Figure 3: Registration Screen

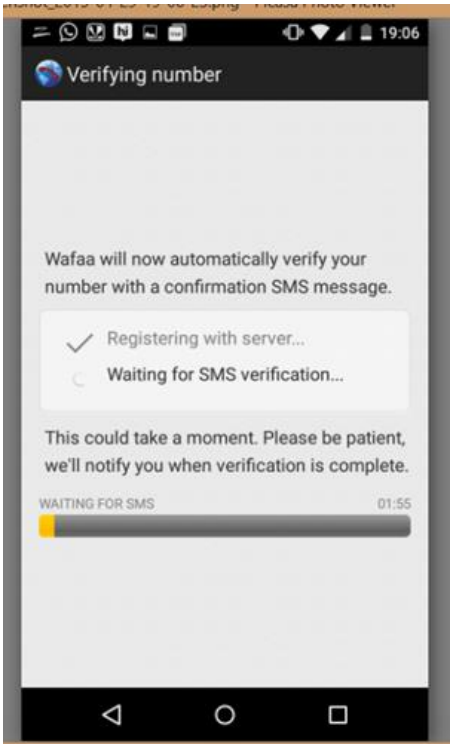

Figure 4: Verifying number

Figure 5: Connectivity error

Making calls: After verifying the setup of the proposed application in order to make encrypt call, contacts will appear on the screen as shown in figure 6 and figure 7. The screen shot is similar to any typical contact list but in this application it consist of only contacts that are authorized to use Wafaa application .After dialing the number and the receiver is connected to the internet, the dialing screen shot will appear as shown in figure 8. After the call is made and the receiver responds to the call, their name and phone number will appear on the screen as shown in figure 9.

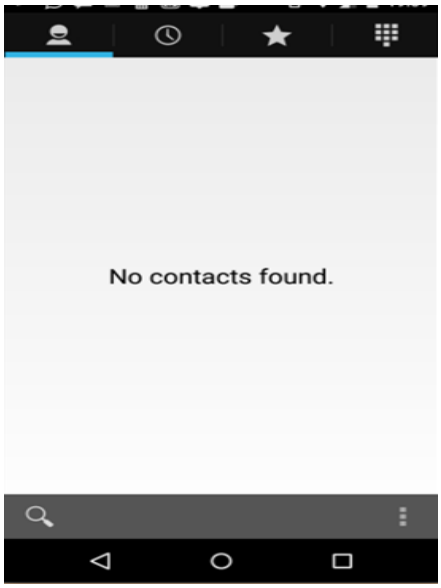

Figure 6: Contact list

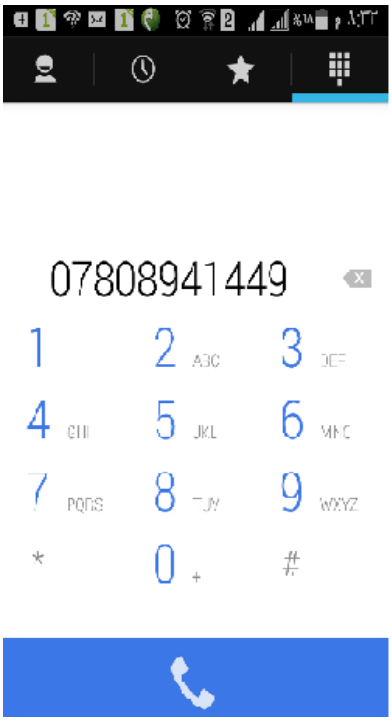

Figure 7: Contact screen

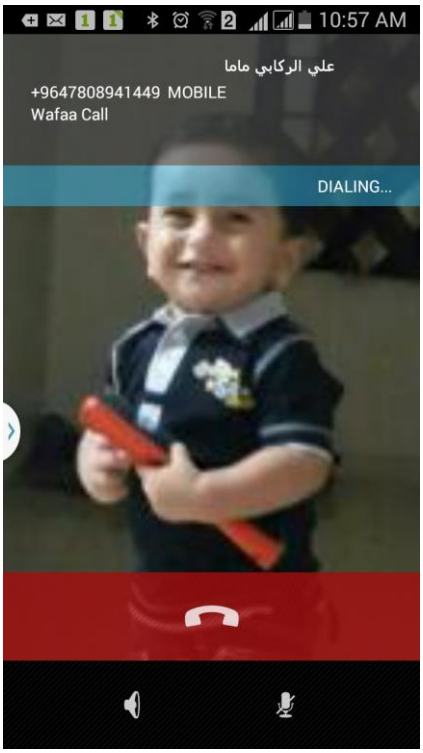

Fig .8 Dialing screen

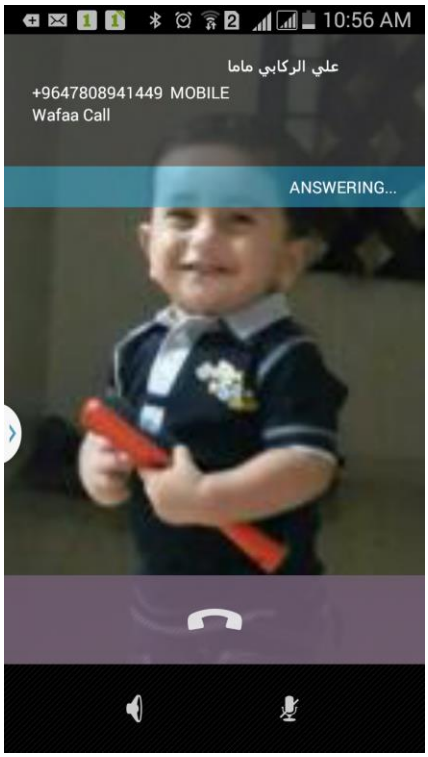

Fig.9 Answering screen

6. CONCLUSIONS

Android operating system is considered as a flexible environment and scalable by adding applications to it and making updates to existing applications. These provide security in addition to the protection for communications or messages through the protocols or protection means .The VoIP Protocol is a basic protocol to transmit Voice over the Internet as the environment protocol itself provides the ability to protect the audio or video with the support of some of the protocols required. This Protocol is used for the purpose of protecting the voice, RTP which is important and basic protocol that transmits the audio in the form of packets across the Web and SRTP protocol which protects such transfers packets of the AES encryption algorithm. This is one of the strong encryption algorithms because the key length is equal to the length of the packet is encrypted and is generating a random key and thus the attacker is given an opportunity that is too weak to get .Therefore voice communications became protected and eavesdropper cannot understand conversation being made.

7. REFERENCES

[1] Sheila Frankel, etl," Establishing Wireless Robust Security Networks**:** A Guide to IEEE 802.11i, Recommendations of the National Institute of Standards and Technology", NIST, Technology Administration, U.S. Department of Commerce, special publication 800-97, Feb. 2007.

[2] Saruchi Kukkar, "Secure Voip Call on Android Platform", Global Journal of Computer Science and Technology Network, Web & Security Volume 12 Issue 12 Version 1.0, 2012.

[3] Prateek Gupta, etl, "Security Analysis of Voice-over-IP Protocols", The University of Texas at Austin, IEEE Computer Society, 2012 IEEE 25th Computer Security Foundations Symposium.

[4] J. Rosenberg, etl, "SIP: Session Initiation Protocol". IETF RFC 3261, June 2002.

[5] T. Dierks and C. Allen, "The TLS Protocol Version 1.0", IETF RFC 2246, January 1999.

[6] The Government of the Hong Kong Special Administrative Region, "VOICE OVER IP SECURITY", (http://www.infosec.gov.hk/english/technical/files/voice.pdf), February 2008

[7] Ville Hallivuori," Real-time Transport Protocol (RTP) security", Helsinki University of Technology, HUT TML 2000.

[8] Riccardo Bresciani , Andrew Butterfield," ProVerif Analysis of the ZRTP Protocol", International Journal for Infonomics (IJI), Volume 3, Issue 3, September 2010

[9] G.Aghila, D.Chandirasekaran," An Analysis of VoIP Secure Key Exchange Protocols against Man-in-the-Middle Attack", India, International Journal of Computer Applications (0975 – 8887), 2011.

[10] Jean Baptiste fuzzier," key management protocols for secured real time multimedia session with SRTP", Jean-baptiste.fuzier@grenoble-inp.org, IK2554 – Practical Voice Over IP,15\10\2010..

[11] Bradley Clayton, etl" Integrating Secure RTP Into the Open Source VOIP PBX Asterisk", Computer Science Department Rhodes University, Grahamstown, 2006.

