ANDROID DRIVEN SECURITY IN SIP BASED VoIP SYSTEMS USING ZRTP ON GPRS NETWORK

{Syed Abdul Mueed[1], Mohd. Salman[2], Rizwan Ali[3]} MTech. CS,
Ms. Shabina Ghafir[4] [Asst. Professor]

{[1]mueedsyed |[4]impmails4me}@gmail.com;
[2]salman.mohd@yahoo.com;
[3]rizu_ali_mca@yahoo.co.in;

Department of Information Technology
Jamia Hamdard University
Hamdard Nagar, New Delhi-110062

ABSTRACT: Voice has always been the poor cousin of data security[1]. In VoIP networks, most of the packets are transmitted without Encryption. Any unauthorized person can capture the packets with the use of packet sniffer and can obtain user information like user identity, SIP phone numbers and PINs required for identity theft. This report introduces an Android Based Application, which will enable the two parties to communicate securely but with an altogether different technology for call flow. Here, we digitize the voice (VoIP) and then transmit it using the GPRS data channel. The digitization process includes the encryption phase using ZRTP technique in order to generate unique keys every time a call handshake is done. Both the Android devices- wishing to communicate with each other using encrypted IP voice communication- must be registered in SIP server, a call Router/Director/Switcher. This study is conducted in a lab comprising an Asterisk base SIP Server, Two Android Devices with typical specifications, Wireshark tool for Encrypted traffic analysis, X-Lite Soft Phone Clients (for initiating and receiving calls) besides other tools.

KEYWORDS: VoIP, ZRTP, SIP, RTP, SRTP, Android, Encryption/Cryptography, GPRS, Wi-Fi, TCP/IP, 3G.

1. INTRODUCTION[2]:

The human folks have started to use mobile devices for important voice communication activities such as personal gossip, mobile commerce activities, credit card information transmission etc. The same is possible due to very high expansion happened in mobile communication technology. However, as mobile platforms advanced in popularity and store valuable information, intruders are also introducing their wicked efforts on these new gadgets. Like other medium of communication and commerce, mobile communication has not been spared of malicious attacks. The mobile industry has been hit hard by the illegal use of resources, the violation of privacy and access to confidential data. One major reason for this insecurity is due to the fact that these Tiny, Internet access-capable and intelligent devices are not designed with security aspect as a top priority. The security aspect in communication has become as important as uninterrupted communication. Voice calls travelling through voice channels using analog signals as carrier are highly vulnerable to snooping or

[1] [*Meakin- Cellcrypt's Vice- President of Marketing.*]

[2] [Taken from [12] with few amendments.]

eavesdropping. Our challenge is to develop an Android driven application that provides secure alternative to such an insecure and vulnerable mobile communication channel by employing encryption to VoIP systems on 3rd generation GSM data channels (GPRS).

2. EXISTING SYSTEMS:

This paper presents security alternative to VoIP systems using Android phones. Currently many VoIP applications exist for the various reasons and are widely used over the enterprise levels. For example, some VoIP applications are developed for the intranet based communications which are having the secure communication channels because they are not open for any kinds of attacks [13]. But some VoIP applications developed for mobile networks use the communication channels between the mobile users which are open in nature. Such a network is vulnerable for the various kinds of security threats. Hence such insecure communication channels are dangerous for the serious and important information leakage, data lost, hacking etc. In fact, VoIP systems offers multiple opportunities such as lower call fees, convergence of voice and data networks, simplification of deployment and greater integration with multiple applications that offer enhanced multimedia functionality. But on the contrary, VoIP also brings new challenges- among them- Security is perhaps the most compelling one [2]. VoIP systems face security threats such as Denial of Service; Interception or Eavesdropping; Masquerading or Impersonation; Spoofing; Identity and Service Theft; Call Integrity; Call Forwarding and Spam over IP.

Today, research is focussed on internet voice significantly with the intent to provide security to VoIP systems. Because majority of the VoIP traffic tends unencrypted and the reason being the lack of Standards [14]. As the VoIP technology has emerged, lots of competing-but not necessarily compatible- standards have been devised. However, this is starting to change e.g. Zfone is gaining the rapid popularity, and our paper uses ZRTP (a protocol used by Zfone) to encrypt VoIP traffic. [5] Providing security arrangements to such systems may affect the Quality of VoIP call such as induction of Jitter value, however is un-noticeable to the users.

3. RELATED WORK AND BACKGROUND:

3.1. Skype:

Although, it has nothing to do with SIP; however it is prudent to mention this section in the current article. After all, Skype is currently the most popular VoIP application [7] and provides for completely encrypted communication.

Skype makes wide use of cryptography to authenticate user and server identities, and to protect the content transmitted across the P2P network from disclosure by parties other than the peers. Skype uses only standard cryptographic primitives to meet its ends, which is a sound engineering approach. These primitives include the AES block cipher, the RSA public-key cryptosystem, the ISO 9796-2 signature padding scheme, the SHA-1 hash function, and the RC4 stream cipher. Skype uses a proprietary session-establishment protocol. The cryptographic purposes of this protocol are to protect against replay, to verify peer identity, and to allow the communicating peers to agree on a secret session key. The communicating peers then use their session key to achieve confidential communication during the lifetime of the session [3].

3.2. Androids:

[8]World is contracting with the growth of mobile phone technology and with the new technologies, new software and operating systems are required. Especially for smart phones, Mobile OS has greatly evolved from Palm OS in 1996 to Windows pocket PC in 2000 then to Blackberry OS and Android. One of the most widely used mobile OS these days is ANDROID. It is an open mobile platform that was developed by Google. It is based on Linux operating system and all of its applications are written in JAVA. Android phones typically come with several built-in applications and also supports third party programs. Developers can create programs for Android SDK software development kit using java and run through

Google's "Davlik" virtual machine which is optimised for mobile devices. After original release there have been number of updates in the original version of Android (Fig:1)

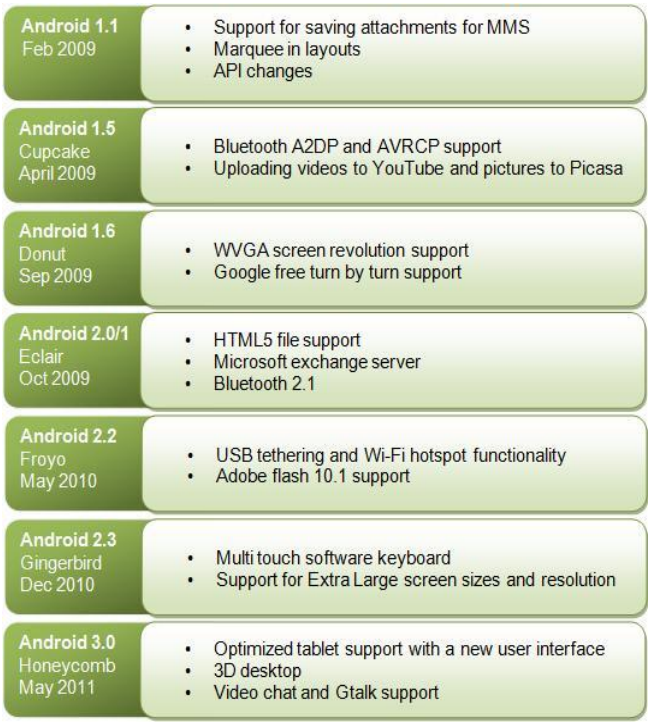

Fig. 1: Courtesy; engineersgarage.com

Another recent version called "Ice Cream Sandwich" announced on Oct 19, 2011 brought Honeycomb features to Smartphone's and added new features to it. However, our application would be compatible for version greater than 2.3 (GingerBread family) - which added SIP support -VoIP Calls *(Wikipedia).*

[3]CellCrypt has released Voice Encryption for different OS's including Androids recently.

CellCrypt[3] releases Voice Encryption Application for Android *(pcworld.com):* The Company Cellcrypt released an application for mobile phones running Android that allows for end-to-end encrypted calls *(CellCrypt, june14, 2011).*

The product, CellCrypt Mobile, is a software-only application that is downloaded to an Android device. To make an encrypted call, the caller and recipient both must have the software installed, although they can use different OS's, such as Symbian, Android or BlackBerry. Cellcrypt Mobile is essentially a VOIP (voice over IP) application that uses either Wi-Fi or an operator's data channel on GPRS, EDGE, 3G or satellite networks to transmit voice. The software uses public key cryptography. This application uses two algorithms for every cryptographic process, for a voice call, it first uses RC4 256-bit to encrypt; then encrypts it again using AES 256-bit.

4. PROPOSED SYSTEM:

Keeping the security concern in VoIP systems into consideration, we ought to develop an Android application which will enable users to communicate securely. Most significantly, we use an altogether different technology for call flow. Generally, voice calls travel using GSM

[3] [CellCrypt is a US based company providing encryption on Smartphone's.]

technology careered on analog signals. In our project, we digitize the voice and then transmit it using the GSM network but not using voice channel, instead we use GSM data channels or more precisely, the GPRS channel for same. Here, the communication application is developed for the voice communication over IP on 3G- Network which uses the mechanism of encryption on the digitized packets. An SIP or Asterisk server- a 3rd party server is needed for virtual routing between two Android handsets. It is basically a call router/director and is needed for device registration mechanisms so that two end-systems are identifiable to each other.
The efficiency of this application intensifies with the fact that we would be using third generation GSM networks or 3G for same which are fast, reliable and make our encrypted voice communication highly fast and efficient.

4.1 Encryption Mechanism:

4.1.1 ZRTP (Zimmermann RTP):

ZRTP developed by Phil Zimmermann provides confidentiality, authentication and integrity between two end devices communicating over voice over IP. This protocol has been published by IETF as RFC 6189 to enable interoperability of SIP/ZRTP end points from different vendors. ZRTP utilizes the Diffie-Hellman key exchange [4] mechanism to derive a common key between two communicating parties. The protocol assumes that key exchange occurs after the signaling has taken place [e.g. SIP (Session Initiation Protocol)]. ZRTP is an extension of RTP, therefore ZRTP packets are embedded in RTP packets and because RTP endpoints ignore unknown extensions- the protocol is backward compatible [2]. These extensions are ignored by an endpoint unless it supports ZRTP. During this phase, both parties exchange information about whether they support ZRTP or not[4]. If both ends of a session support ZRTP, a Diffie-Hellman key exchange is performed to agree on session key. After a successful handshake process between two end points, RTP packet streams are encrypted as Secure RTP (SRTP). Thus, Diffie-Hellman solves the problem of how to agree on the key between two end systems, hence providing more security.

How Good is ZRTP? ZRTP is a new protocol to negotiate the cryptographic keys for encrypting the call. It has some nice cryptographic features lacking in other approaches to VoIP encryption [15].

- Although it uses a public Key algorithm, it avoids the use of PKI (public key Infrastructure). In fact, it does not use persistent public keys at all; instead it uses an ephemeral Diffie-Hellman with hash commitment and allows the detection of Man-in-The-Middle attack (MiTM) by displaying a SAS for the users to verbally compare over the phone.
- It has PERFECT FORWARD SECRECY, meaning the keys are destroyed at the end of the call, which precludes retroactively compromising the call by future disclosure of key material.
- It does not rely on the SIP signalling for the key management and on the SIP servers at all. It performs its key agreement and key management in a purely peer-peer manner over the RTP packet stream.
- It supports OPPORTUNISTIC ENCRYPTION by auto-sensing if the other VoIP client supports ZRTP.
- The design is more secure, simpler, more appropriate and more elegant than other protocols under consideration by Internet Engineering Task Force working groups [16].

[5]Muhammad Tayyab Ashraf in his paper *"ZRTP: A New Approach to Secure VoIP Calls"* concludes that ZRTP security method is best choice to protect the RTP traffic between the sender and receiver. Because its implementation is very easy and it is independent of the network devices used between end devices- i.e. we don't have a central key server. The key exchange is done by the software at both endpoints (the recipient's and caller's applications). Since

[4] [The exchanged information may also include information about Hash, Cipher, and Short authentication string (SAS)].

there's no human interface into the keys, the key server can't be compromised as there is no key server. Additionally ZRTP, an application layer protocol isn't limited to number of calls. This study shows that ZRTP is more suitable security method for securing VoIP media stream due to efficient utilization of bandwidth.

[4]Another study which describes the weakness and strength of each possible security to VoIP systems, verifies that ZRTP[5] is a best tool for VoIP encryption on 3G (broadband) for traffic travelling.

ZRTP application layer protocol doesn't rely on Public key infrastructure (PKI) that makes it efficient, instead ZRTP transmits shared secret keys over RTP stream and generates a unique secret for every call i.e. ZRTP shared secret is different for every call. Although, part of the shared secret is cached between calls, a new one is compute for every new call based on that same cached value. If a Man-in-the-Middle attack is attempted on the cached shared secret, the fact that SAS[6] is read aloud suffices to prevent it because the read aloud values will be totally different from the first call on. Even in those cases where the Man-in-the-Middle attack occurs at the first session and the callers did not check their SAS, the moment they do check their SAS the moment they will find out that the man-in-the-middle attack actually happened at the first session. The following figure[7] displays the communication between two end devices with ZRTP:

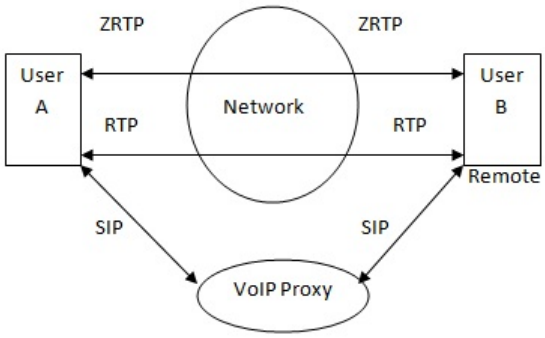

Fig. 2: Communication using ZRTP/RTP

RTP and SIP:

The Real Time Transport Protocol (RTP) is used for the real time transportation of data. In case of VoIP, it is used to transmit voice. It is standardized by IETF in RFC 3550. When it comes to signaling protocols (e.g. SDP and SIP), RTP is the protocol used for data transmission. Combining SIP and RTP protocols, we can then establish a VoIP call between two peers (2 Android Handsets in present case).

SRTP [18]:

This protocol is used to encrypt the low level voice packets, but can't be used until both the parties have agreed on what keys to use for SRTP encryption. The SRTP protocol (RFC 3711) says nothing about how session keys are negotiated. Here, ZRTP is the protocol that the two parties use to negotiate the SRTP session key. E.g. Zfone[8] uses the SRTP, but uses ZRTP first to negotiate the session key.

Secure Internet Voice Call:

When security is added to a VoIP system, the quality of VoIP call is affected. Our application uses ZRTP technique as already specified. The encryption of packets could be successfully shown through their decoding using a packet sniffing tool in which we shall sniff the VoIP packets on an IP address by connecting the Android device via Wi-Fi on a shared network which has a public IP address. After sniffing the packets, we will decode them in order to hear the voice. The packet sniffing can't occur in the GPRS network as we don't have access point to can the packets.

[5] [Renaming Zfone with ZRTP]
[6] [(SAS is an innovative method of authentication employed by ZRTP generated during the Diffie-Hellman key exchange)]
[7] [Taken from[5], with minor changes]

[8] Zfone is a VoIP phone encryption software used to implement ZRTP on end devices.

4.2 GPRS:

GPRS is a packet based communication service for mobile devices that allows data to be sent and received across a mobile telephone network. It is an overlay of GSM, an open mobile platform that was developed by Google.

In our project, we propose to implement it on GPRS (3G) but this application shall work on Wi-Fi as well. The release of 3rd Generation network technology standardizing TCP/IP on mobile systems, promises to permit strong & end to end security, which functions only over IP networks [12]. Wi-Fi requires no SIM cards in handsets; however, GPRS requires SIM cards on both the Android handsets.

5. RESEARCH METHODOLOGY:

5.1. Motivation: The main use case is covering "Sensitive" but unclassified information and probably 95 percent of conversations in the government are of a sensitive but unclassified nature. Most likely all of those sensitive but unclassified conversations are made in the clear. Because cell phones are vulnerable to interception, not just by traditional mechanisms of countries or well-funded criminals, but there is an emerging threat from hackers who have developed equipment that can intercept voice calls for as little as $1,500[11]. It used to be hundreds of thousands of dollars – but now everyone can get a hold of it and so the risk of it happening has gone up.

High profile users such as Defence Officials, Executives, Celebrities, Dignitaries and others don't wish to be snooped on, as the VoIP communication available is highly vulnerable to 3rd party eavesdropping or intrusion [16]. Advanced facilities and features in Mobile Operating System Technologies especially Smartphone's supporting vast and diversified applications *(Smartphone encryption application helps sensitive information get more secure: Meakin from CellCrypt)* and 3rd Generation Technologies (3G) has made it possible to deliver voice fast and securely between two End-Systems. Taking this assumption into consideration, we wish to develop this application for Mobile Communication.

5.2 Design: The Design process specifies the logical overflow of the execution steps in the research and development project. The flow chart of the proposed system is given in the fig. 3 following.

The proposed system will have the following principles and regulations:

- The lab consists of one Asterisk based SIP server with at least 2 Android supporting devices.
- SIP server acts as a call Router/Director to forward calls between Android devices and will always be on the network.

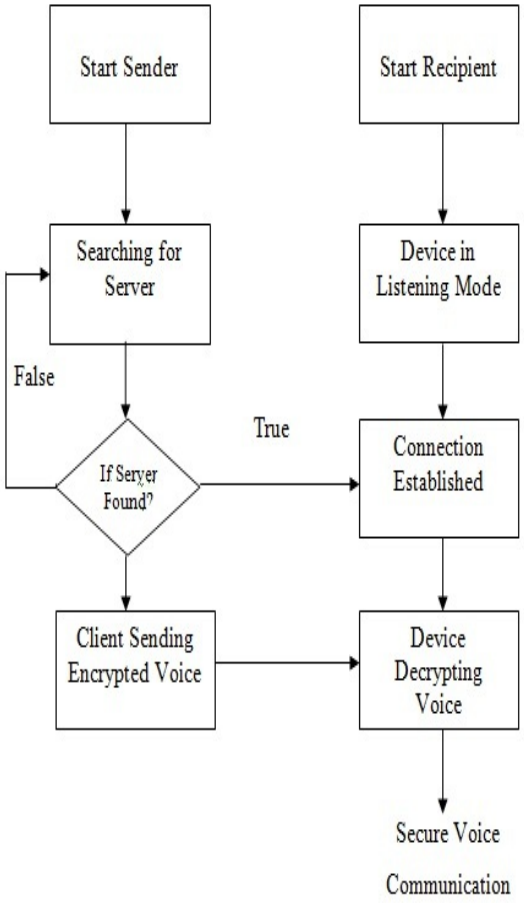

Fig3: Flow of the Proposed System

- SIP configuration includes registering both Android devices with it, so that the

devices become identifiable to each other before connection is established.

- The communication will occur through 3G network (GPRS). The internet speed has to be good to ensure speedy delivery of encrypted IP packets (this is important because at the start of the call it takes a second or two to negotiate the cryptographic keys [17], further the induction of jitter values could incur some delay as well).
- The voice application developed needs to be installed on both the android devices for the communication session to take place.
- A logical number will be assigned to every device by the SIP server during configuration. Once the sender will dial the number, the Android APIs will initiate a call to the SIP recipient registered on the server. If the call is made to an invalid recipient, it will be handled by the IVR of the server. Else once the call is connected, the human voice will be digitized by the Android APIs and the VoIP packets will travel over the SIP server.
- The digitization process also includes the encryption phase, where in we use ZRTP technique in order to generate unique keys every time a call handshake is made. During the ZRTP key exchange, the caller party sends a ZRTP Hello Packet[9]. Once that packet is positively acknowledged by the recipient party, the handshake happens successfully and the call packets get encrypted.
- The digitized voice (VoIP) will travel through GPRS in an encrypted fashion. The android application will enable the recipient to enjoy the DYNAMIC DECRYPTION i.e. to say, it will be users will to listen to the original decrypted voice, else it may be some un-interpretable voice delivered.
- The secured communication can only occur dynamically if the sender and recipient devices are equipped with this application. Otherwise, the call would be insecure which essentially means that there would not be any ZRTP key exchange and we would be able to decode the VoIP packets and can listen to the conversation on a media player.
- SIP or Asterisk server is a 3rd party (freeware) server which is mainly needed for virtual routing. It has got virtual PSTN etc.

The following figure (Fig. 4) depicts the proposed system:

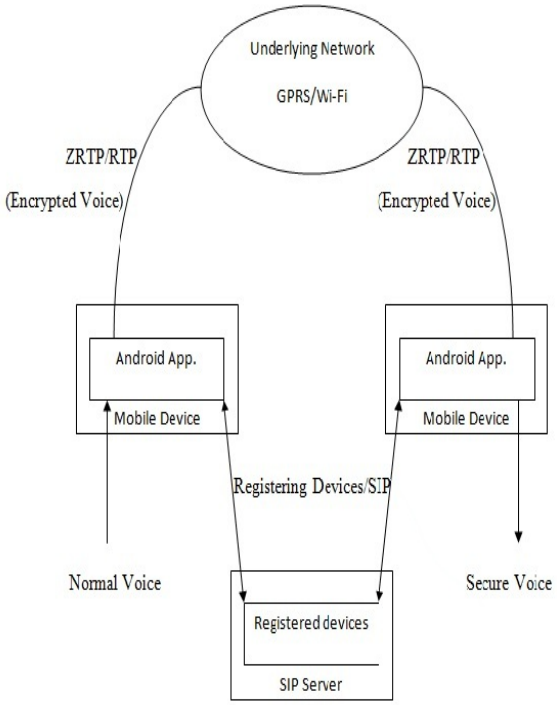

Fig. 4: Proposed Model

5.3 IMPLEMENTATIONAL TOOL'S:

This Research based application implements security in VoIP systems using ZRTP Encryption technique. The lab comprises of Asterisk Based SIP server, X-Lite Soft phone clients, Android Phones and Wireshark analyzer tool for traffic analysis. The following gives the description used:

5.3.1 Android 4.1 SDK (at API Level 15): This SDK was developed by Google and is based on

[9] [10]The purpose of the Hello Packet is to confirm that end point supports the protocol and to see, what algorithms the two end points have in common.

Linux operating system with all of its applications written in advanced java. It also includes collection of specification and technologies used for developing applications for the devices which have limited processing power in storage capabilities like Mobile Phones, Wireless Devices and Pagers. Common concepts from Java used in this application development include:

- Android Event Handling
- Inheritance
- Multithreaded Programming
- Simple Java Beans
- Java Collections Framework (Data Structures, Array List)

SIP based VoIP: The platform includes a SIP protocol stack and framework API (at level 15) that lets developers build internet telephony applications. Using the API, applications can offer voice calling features without having to manage sessions, transport-level communication, or audio- these are handled transparently by the platform's SIP API and services.

5.3.2 Configuration of SIP Client: This application utilizes the configuration parameters of the SIP server. Additionally, as most of the SIP servers are Linux-based, configuring the SIP server also requires assignment of the dynamic IP address to the Linux server which requires high-end network configuration on Linux. And even if we are successful in that configuration, it is practically infeasible to achieve good call clarity and speed because the servers need a high bandwidth internet speed which is only applicable if we take 3rd party services.
In the SIP account configuration, we mention the generic details after which the user shall be assigned a logical number which would essentially be the telephone number of the device. In order to activate this number in the application, the Android user will configure the SIP account in the device by mentioning the logical number, password and account name and registering the account. Once the account is registered, the VoIP calls shall be made and received from that account only.

5.3.3 WireShark: Wireshark is a free and open-source packet analyzer for analyzing encrypted VoIP traffic flowing through GPRS. Wireshark application is installed on a separate computer in order to capture the voice and signalling traffic passing through the network. Using this packet sniffing tool, we can successfully show the encryption of VoIP packets through their decoding by connecting the android device via Wi-Fi on a shared network which has a public IP address.

5.3.4 X-Lite Soft Phone: X-Lite soft phone clients have been configured on a computer for initiating and receiving the calls.

5.3.5 Android Device Specification: At least two Android Handsets needed with some typical specifications. It must be from Gingerbread family i.e. version>=2.3 with Processor frequency greater than 1GHZ and with RAM of at least of 512 MB size. If we install our client application on the version < 2.3, a non-secure call will happen. The secured and non-secured call would be shown mentioned on the Android Phone handsets.

5.3.6 Other Specifications: High speed GPRS connection in both the handsets; USB Data Card that provides Public IP[10] to the system, a Wireless Router (not ADSL).

6. COCLUSION:

We can safely conclude that VoIP systems are prone to security issues. This report attempts one of the Android based solution by employing ZRTP Encryption technique using SIP Proxy servers. Using this procedure, users can communicate securely, reliably but on 3G networks as it will ensure faster packet delivery.

[10] [Public IP is the one, that is ping-able from the outside system on Network]

REFERENCES:

[1]. J.Bilien: Agreement for Secure Voice over IP. Master's thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, Dec 2003.

[2]. Samuel Sotillo: Zfone; A New Approach for Securing VoIP Communication; ICTN 4040 Spring 2006.

[3]. CellCrypt Encrypts voice calls on Smatphone's :http://www.cellcrypt.com/

[4]. Synopsis of Security Threats and Implements in SIP-Based VoIP Systems: Canadian Journal on Network and Information Security Vol. 1, No. 5, July 2010

[5].Muhammd Tayyab Ashraf: ZRTP; A New Approach to Secure VoIP Calls (Canadian Journal on Network and Information Security Vol. 1, No. 6, August 2010).

[6]. William Stallings (2006), Cryptography & Network Security, Principles and Practices - Pearson Education.

[7]. SKYPE SECURITY EVALUATION; Tom Berson Anagram Laboratories 18 October 2005.

[8]. What-is-Android:
http://developer.android.com/guide/basics/

[9]. Security in SIP-Based Networks from Cisco Systems.

[10]. P.zimmerman from Zfone Project, A. Johnston, Ed. Avaya, J. Callas PGP Corporation, july 2009.

[11]. Interview with Meakin: http://mil-embedded.com/articles/smartphone-meakin-of-marketing-cellcrypt-inc/

[12]. Wireless Security, Challenges and solutions: http://www.peterindia.net/WirelessSecurity.html

[13]. Secure voice Communication over Wi-Fi area Network: GANPAT UNIVERSITY JOURNAL OF ENGINEERING & TECHNOLOGY, VOL.-1, ISSUE-1, JAN-JUN-2011

[14]. VoIP traffic Encryption Tools: http://searchunifiedcommunications.techtarget.com/tip/VoIP-traffic-encryption-tools

[15]. WHY IS ZRTP BETER? http://zfone.com/faq.html#better

[16]. VoIP EAVESDROPPING: Hardening N/W security to contain VoIP Risks; http://searchsecurity.techtarget.com/tip/VoIP-eavesdropping-Hardening-network-security-to-contain-VoIP-risks

[17]. DOES ZRTP SLOW DOWN THE VoIP CALL? http://zfone.com/faq.html#backdoor

[18]. ISN'T SRTP GOOD ENOUGH, WHY ZRTP? http://zfone.com/faq.html#srtp