Global Journal of Computer Science and Technology
Network, Web & Security
Volume 12 Issue 12 Version 1.0 Year 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Secure Voip Call on Android Platform

By Saruchi Kukkar
Lovely Professional University

Abstract - In the Secure voice call, the human voice shall be digitized by the Android APIs and the VOIP packets will travel over the SIP layer. The digitization process also includes the encryption phase wherein secure call technique is used in order to generate unique keys every time a call handshake is done. During the Secure Call key exchange, the caller party sends a Secure Call hello packet. Once that packet is positively acknowledged by the recipient party the handshake happens successfully and the call packets get encrypted. Using Secure call, digitized voice data is transformed into cipher text form on third generation GSM data or GPRS servers in android platform which results in a better encrypted voice speed and clarity.

GJCST-E Classification: C.2.m

Strictly as per the compliance and regulations of:

Secure Voip Call on Android Platform

Saruchi Kukkar

Abstract - In the Secure voice call, the human voice shall be digitized by the Android APIs and the VOIP packets will travel over the SIP layer. The digitization process also includes the encryption phase wherein secure call technique is used in order to generate unique keys every time a call handshake is done. During the Secure Call key exchange, the caller party sends a Secure Call hello packet. Once that packet is positively acknowledged by the recipient party the handshake happens successfully and the call packets get encrypted.

Using Secure call, digitized voice data is transformed into cipher text form on third generation GSM data or GPRS servers in android platform which results in a better encrypted voice speed and clarity.

I. Introduction

VOIP works by converting analog voice signal into digitized data packets. The packets are sent out across the internet the same way as any other IP packets, using the internet's TCP/IP protocol The Internet is a notoriously insecure network. Anything send across internet can be easily snooped upon. This is of particular concern when highly confidential information, such as corporate data and credit card numbers, is transmitted across the Internet. Another related concern is that it can be difficult to know whether the person sending the information is really who he says is he.

Despite of the advantages of implementing VOIP there is a main drawback of using this technology that is the security issues. Since it will be connected to the Internet and use many of the same hardware and software components. VOIP becomes vulnerable to different types of attacks such as Man in the middle attack, Denial of service or Eavesdropping.

Several ways have been developed to solve these problems. At the heart of them is Encryption, it is technique of altering information so to anyone other than the intended recipient it will look like meaningless garble. When the recipient gets the information, it needs to be decrypted that is, turned back into the original message by the recipient, and only by the recipient. In the Encrypted IP voice call this digitized voice data is transformed into Ciphertext form using encryption techniques. Hence, the encrypted voice call is very secured as compared to VOIP.

II. Objectives

1) Users will be able to communicate effectively, speedily and most importantly, securely, there by enhancing the privacy and confidentiality of mobile communication.
2) Implementing voice encryption on third generation GSM data or GPRS servers which would in turn result in a better encrypted voice speed and clarity.
3) The configuration and usage of proxy server (SIP / Asterisk) through defining call routing and handset registration mechanisms.
4) It will enable the users to communicate with each other in an encrypted fashion

III. Research Design

Research design specifies the logical structure of a research project and the plan will be followed in its execution.

Suppose A want to communicate with B through secured voice communication. A and B must have android based mobile handsets with J2ME (proposed) application installed on it which is responsible for encrypted voice communication.

1. The mobile handsets need to be registered at SIP server.
2. When A calls B the application installed on mobile handsets will convert it into encrypted data.
3. The encrypted data will travel through GPRS channels.
4. The SIP server will route the call to the registered recipient B.
5. The application installed on B handset will perform the decryption process.

Author : Assistant Professor Lovely Professional University.
E-mail : ganpati.saruchi@gmail.com

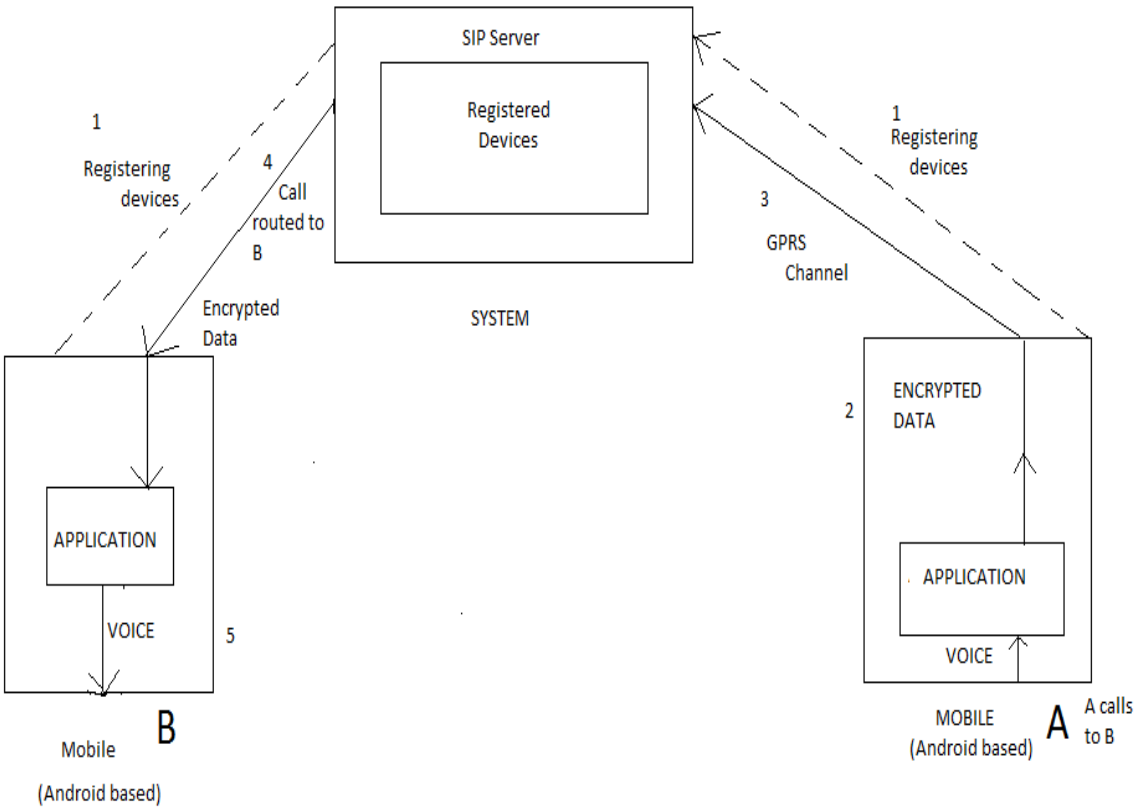

Figure 1 : Depicting the proposed system

Step1: Voice communication can occur in 2 ways namely: (a)Wi-Fi (without the SIM card in Android handsets)
(b)GPRS (with SIM card in Android handsets)
In the proposed work GPRS mode will be used

Step2: There would be 1 SIP server (Asterisk) and minimum 2 Android handsets. The handsets need to be registered at SIP server.

Step3: The SIP server of callcentric.com are used. SIP client is configured on both the Android handsets.

Step4: The Android application which will be developed needs to be installed on all the handsets which are registered in the SIP server and wish to communicate with each other using encrypted IP voice communication.

Step 5: The dialler will launch the Android application on his/her handset and dial the receiver's number. The dialling interface will be developed for the Android application. Once the call is made, the request will go the SIP server wherein the recipient's number will be checked and the call will be routed on its handset

Step 6: Once the recipient receives the call through the same Android application and the dialler starts the conversation, all the digitized voice data will first be encrypted on the dialler's handset by the application and then sent to the SIP server for routing to the recipient's handset. Logically, every handset will be assigned a numeric no. in the SIP server during configuration through which it will become identifiable.

Step7: The digitized voice data will travel in an encrypted fashion through the GPRS medium.

IV. Technical Workflow of The Application

1) The caller handset uses **Secure Call** application to initiate the VOIP call to the recipient.
2) When the call is made, the caller handset also sends the logical number of both caller and receiver via GPRS which is cross-verified at the call centric server for genuineness.
3) Once the genuineness of both the numbers is verified the analog voice signals are digitized using the SIP stack APIs which is PJSIP used in application. SIP stack APIs are a collection of packages and functions used for the transmission of voice over IP using SIP protocol.
4) Once the call is established successfully, the caller sends "Hello Packet" in order to exchange the secure key with the recipient. The caller sends the

"Hello Packets" a couple of times. When the recipient sends the acknowledgement for the hello packet, the secure key exchange is accomplished successfully. When the secure key is exchanges, the call packets become encrypted.

5) Before the call is connected, the sender and recipient parties have to register themselves with the call centric server in order to attain a logical number which is also added in the SIP client on Android in order to synchronize with the server so that the SIP account gets activated.
6) Once the SIP account is activated the SIP call session is established using SIP stack which is the collection of APIs and the encryption is performed using ZRTP. SIP stack is written in C language.
7) There are two different projects in the application. One project consists of the full SIP stack integration and the another deals with the Android interface design and the SIP client development.

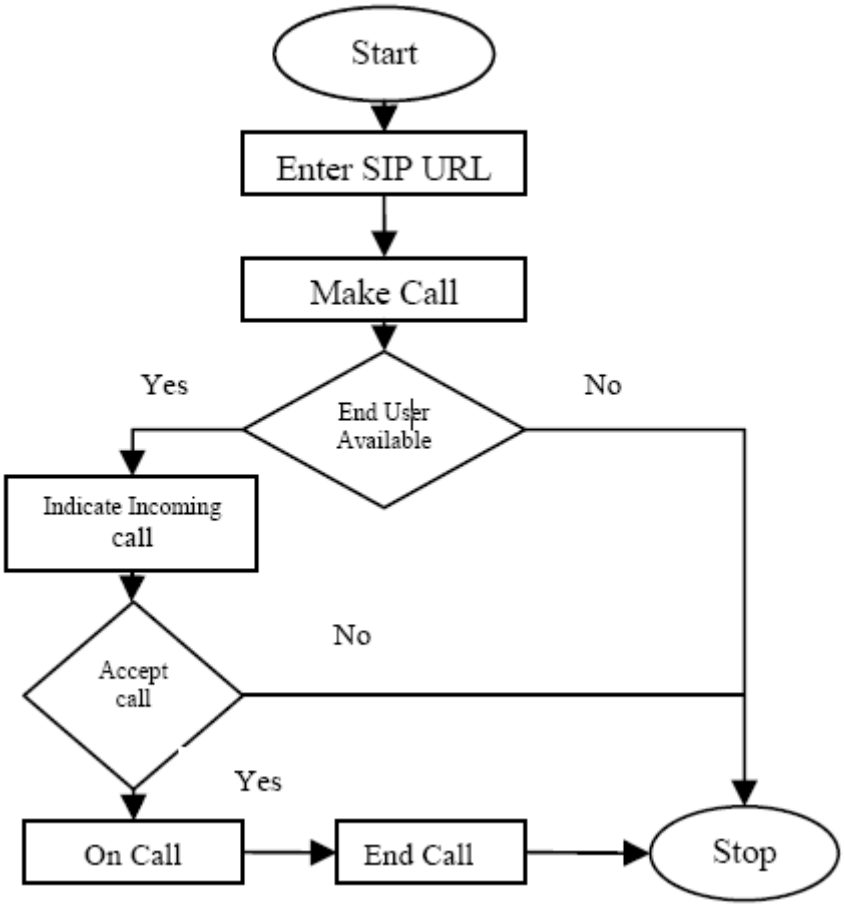

Fig. 2 : Workflow of application

This application shall work on both Wi-Fi and GPRS as the communication medium and requires that we have high-bandwidth network speed. 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 Secure Call key exchange and intruder would able to decode the VOIP packets and can listen to the conversation on a media player.

V. Significance

1) This can benefit the users to communicate with each other through digitized voice data which is free from any noise or interference in comparison to its analog variant and carries more clarity.
2) The best part of this communication will be it can be done from geographically any independent location.
3) It will enable the users to communicate with each other in an encrypted fashion which will enhance the security and confidentiality of the communication.
4) The most significant part is it support the newest generation of the mobile handset called SmartPhones which run on an advanced hardware and latest mobile operating system from Google called Android.

VI. Implementation

a) Secure Call application

The implementation of Secure Call application is done by developing several components and then joining them together. Every component signifies a specific functionality in the application.

i. *Configuration of SIP client*

This application utilizes the configuration parameters of the SIP server. Services of existing SIP servers are used. Since the development and maintenance of SIP services is a costly affair, so 3rd party services from Callcentric.com has taken.

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 it is 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.

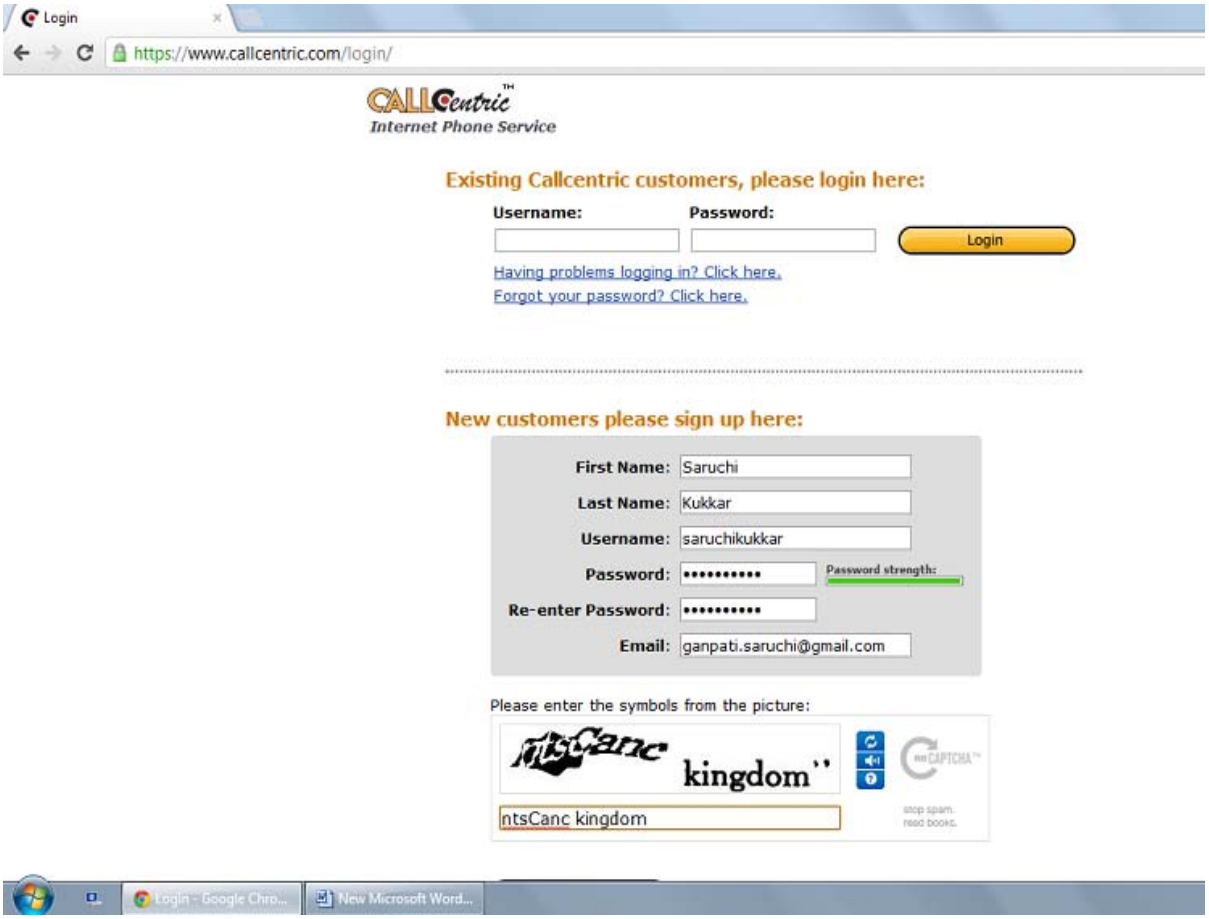

Fig. 3 : SIP Account Configuration

In the SIP account configuration, as in Fig. 3 the generic details are mentioned after which the user shall be assigned a logical number which would essentially be the telephone number of the device.

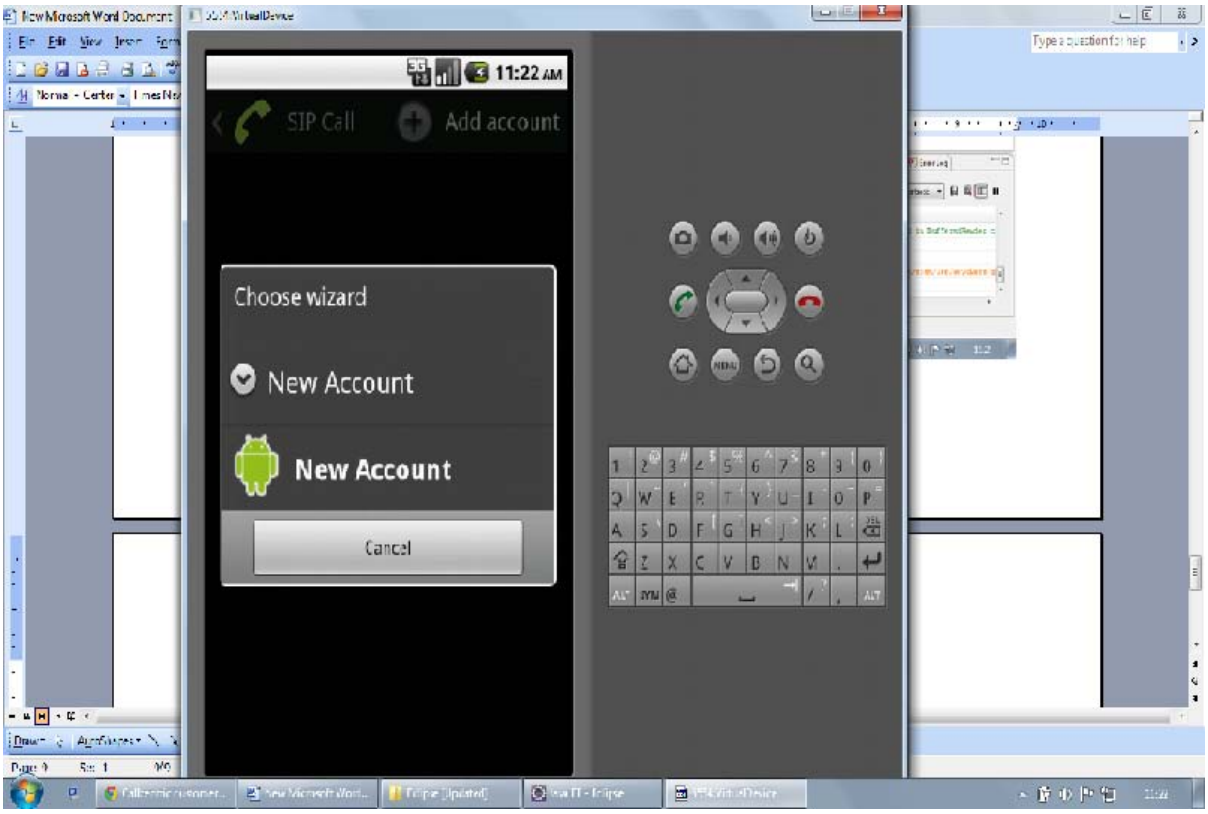

Fig. 4 : Activate the SIP account in the Secure Call application

Activate the logical number (SIP account) assigned by SIP server of Callcentric.com as shown in Fig. 4 by Creating the New Account in Secure Call application.

Fig. 5 : Configuring SIP account in device

Android user will configure the SIP account in the device by mentioning the logical number, password and account name and registering the account as depicted in Fig. 5

Account name- Saruchi

Logical number-17772438110 (provided by SIP server of Callcentric.com)

Server- callcentric.com

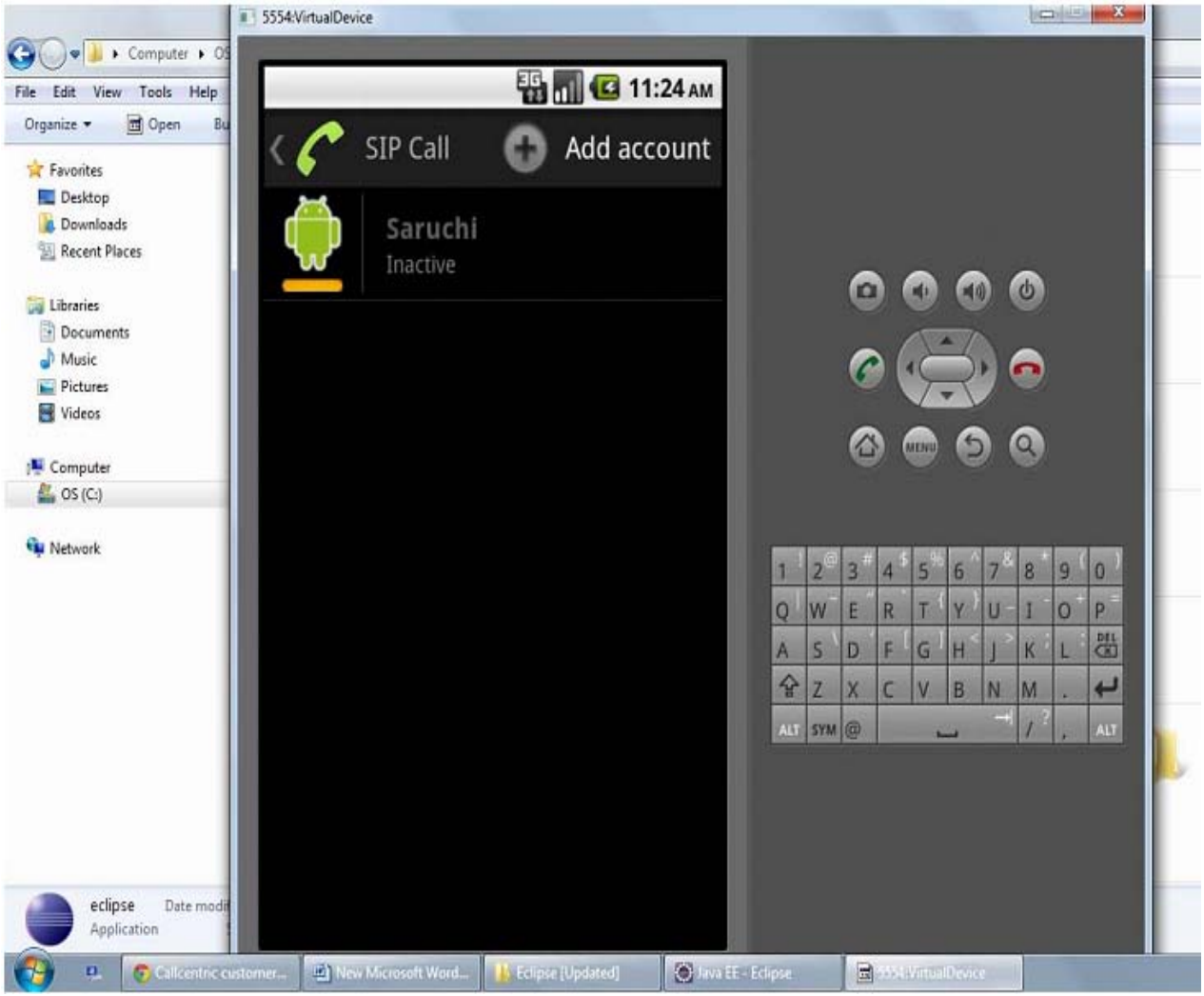

Fig. 6 : Android SIP Client

Android SIP client named Saruchi and Logical no. 17772438110 has been created. Tap the icon to make it Active as shown in Fig.6. Once the account is active, the VOIP calls shall be made and received from that account only.

ii. *Dialler Application*

In this component, once the SIP account is registered, the user will be able to dial the number of another Android SIP user through a custom-made touch-pad. In order to develop the custom touch-pad, different images of the numbers have created in the application and have used then as resources.

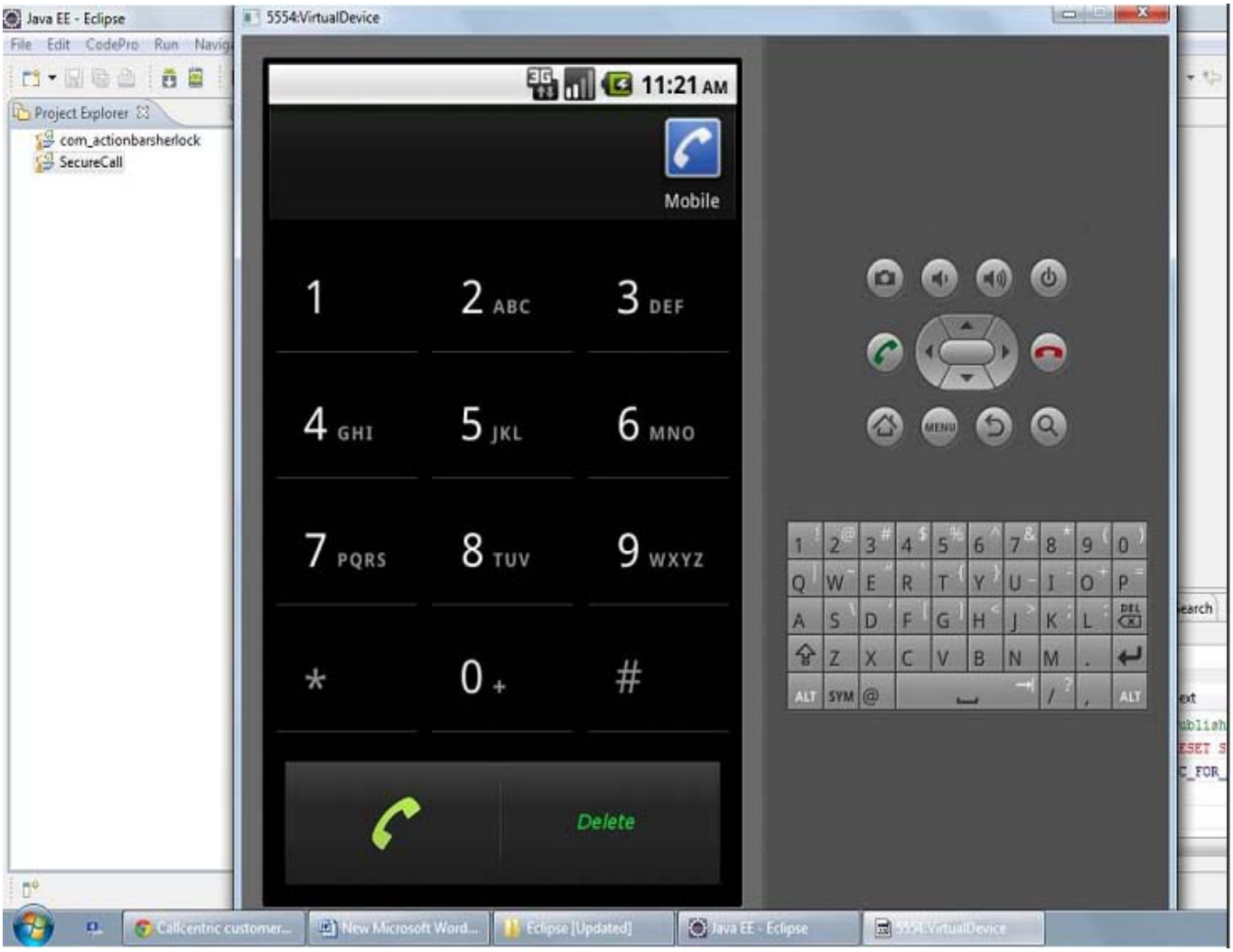

Fig. 7: Dialler Application

Then work is done on the Android event listeners in order to display the numbers on the screen when the user accesses those resources. There is a delete key through which the user will be able to delete the numbers if any incorrect numbers have been typed.

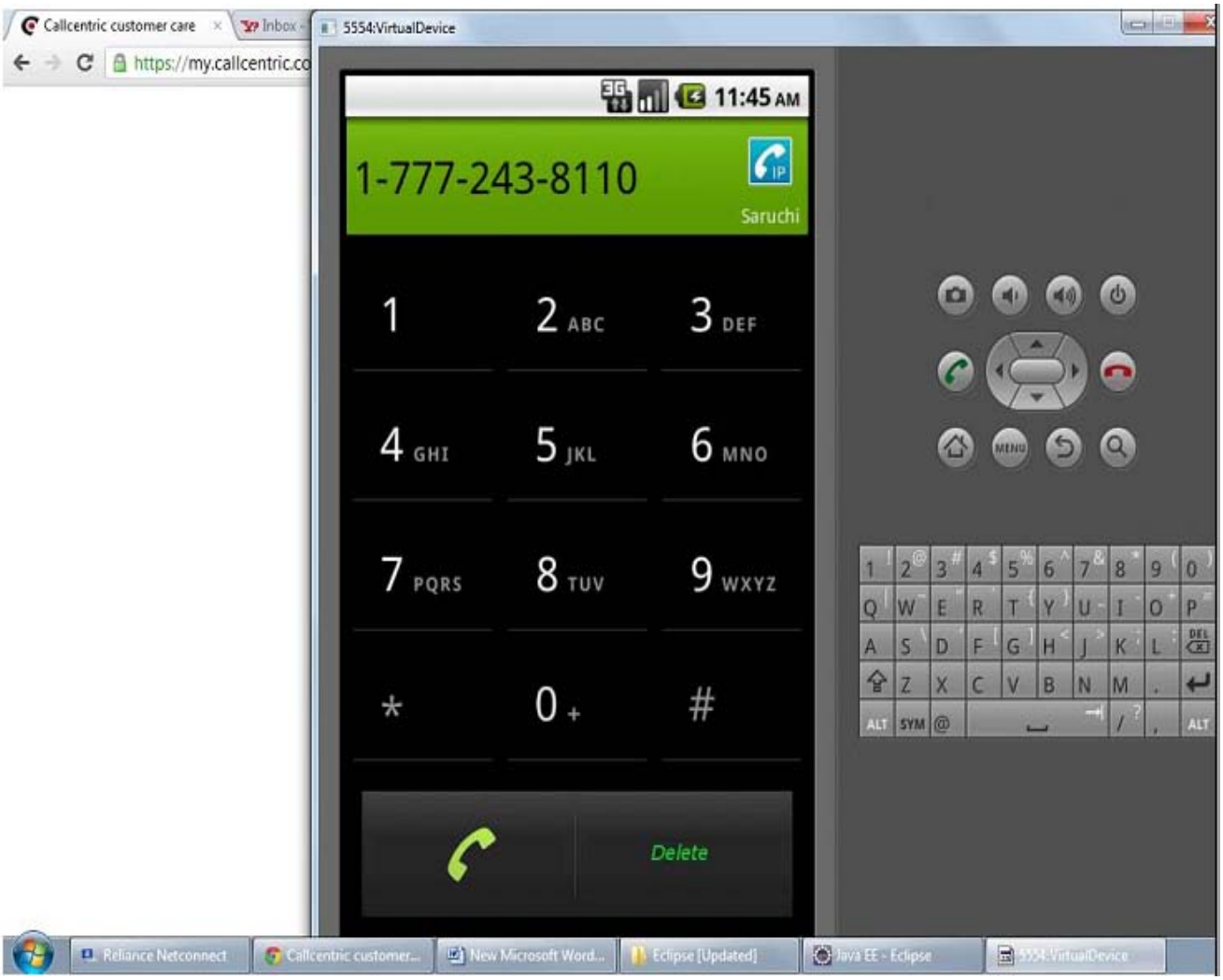

Fig. 8: Initiating a Call

After the user has typed the correct numbers as in Fig. 8 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 call centric server.

iii. *Digitization of Voice Call*

When the call is connected, the human voice shall be digitized by the Android APIs and the VOIP packets will travel over the SIP layer. Once the genuineness of both the numbers is verified the analog voice signals are digitized using the SIP stack APIs which is PJSIP used in our application. SIP stack APIs are a collection of packages and functions used for the transmission of voice over IP using SIP protocol

iv. *Encryption Phase*

The digitization process also includes the encryption phase wherein we use secure call technique in order to generate unique keys every time a call handshake is done. During the Secure Call key exchange, the caller party sends a Secure Call hello packet. Once that packet is positively acknowledged by the recipient party the handshake happens successfully and the call packets get encrypted.

i. The Secure Call protocol does not rely on a public key infrastructure or on certification authorities, In fact ephimeral Diffie-Hellman keys are generated on each session establishment: this allows to bypass the complexity of creating and maintaining a complex third trusted party.

ii. These keys will contribute to the generation of the session key and parameters for SRTP sessions, along with previously shared secrets: this gives protection against Man-in-the-Middle attacks, assuming the attacker was not present in the first session between the two endpoints.

iii. To ensure that the attacker is indeed not present in the first session (when no shared secrets exist), the Short Authentication String method is used: the two endpoint compare a value by reading it aloud. In case the two values match, then no Man-in-the-Middle attack has been performed.

iv. Key agreement procedure on a Diffie- Hellman exchange and on cached secrets established in

preceding sessions (if any): this creates a new shared secret, from which all key material can be derived by means of one-way functions.

v. Keying material is destroyed at the end of each session, thus this protocol offers perfect forward secrecy.

v. *Demonstration*

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, try to decode them in order to hear the voice. The packet sniffing cannot occur in the GPRS network because we do not have an access point to can the packets.

vi. *Installing Application on Android Phones*

1. Enable USB debugging, Stay Awake, and Allow mock locations on both the Android phones on which application has to be installed.
2. Connect Android phone to Laptop via USB cable.
3. Open the android application in Eclipse IDE. Run it as Android application. Once the application get installed on the Android phone , the dialler interface will appear on the Android phones.
4. Configuring Account on SIP client:- Open the application on the Android phones, Configure SIP account by entering Account name, User, Server name provided by Call centric.
5. Activate the SIP account. It will get activated via GPRS. Now SIP client is configured.
6. This application shall work on GPRS as the communication medium and requires high-bandwidth network speed.

References Références Referencias

1. Angelos D. Keromytis, (2011), "A Comprehensive Survey of Voice over IP Security Research" , IEEE
2. Nor Shahniza,Kamal Bashah, Tore Jonvik & Do van Thanh (2010), "A Mobile Service Architecture for improving Availability and Continuity", IEEE
3. Lu Tian, Nicolas Dailly, Qiao Qiao, Jihua Lu1, Jiannan Zhang, Jing Guo and Ji'ao Zhang (2010), "Study of SIP Protocol Through VOIP Solution of Asterisk", IEEE.
4. Chan Yeob Yeun and Salman Mohammed Al-Marzouqi (2009), "Practical Implementations for Securing VOIP Enabled Mobile Devices", Third International Conference on Network and System Security – IEEE.
5. Chung-Hsin Liu and Chun-Lin Lo (2009), "The study of the SIP for the VOIP", Fifth International Joint Conference on INC, IMS and IDC
6. Liancheng Shan and Ning Jiang (2009), "Research on Security Mechanisms of SIP-based VOIP System", Ninth International Conference on Hybrid Intelligent Systems-IEEE.
7. Mohammed A Qadeer, Robin Kasana and Sarvat Sayeed (2009), "Encrypted Voice Calls with IP enabled Wireless Phones over GSM/ CDMA/ WiFi Networks", International Conference on Computer Engineering and Technology
8. Pablo Montoro and Eduardo Casilari (2009), "A Comparative Study of VOIP Standards with Asterisk", Fourth International Conference on Digital Telecommunications- IEEE.
9. Zourzouvillys, T. Rescorla, (2009) "An Introduction to Standards-Based VOIP: SIP, RTP, and Friends", Internet Computing, IEEE.
10. Ahmad Ali Habeeb, Mohammed A Qadeer, and Shamshir Ahmad (2007), "Voice Communication over GGSN/SGSN", IEEE
11. P. Thermos and A. Takanen (2007), " Securing VOIP Networks: Threats, Vulnerabilities, and Countermeasures", Addison-Wesley Professional USA.
12. Tuneesh Lella and Riccardo(2007), "Privacy Of Encrypted Voice-Over-IP", IEEE.
13. D.R. Kuhn, T.J. Walsh, and S. Fries (2005), "Security Considerations for Voice Over IP Systems", National Institute of Standards and Technology-Gaithersburg, MD USA.
14. T.Abbasi, S.Prasad, N.Seddigh, and I.Lambadaris (2005), "A Comparative study of the SIP and IAX VOIP protocols", Proc.of Canadian Conference on Electrical and Computer Engineering
15. Chia-Hui Wang, Mei-Wen Li, and Wanjiun Lian (2003), "A Distributed Key-Changing Mechanism for Secure Voice Over IP (VOIP) Service", IEEE.
16. Q. Shen (2003), "Performance of VOIP over GPRS," Advanced Information Networking and Applications 17th International Conference,
17. Goode, AT&T Labs and Weston (2002), "Voice over Internet protocol (VOIP)", IEEE.
18. J.Rosenberg, H.Schulzrinne, G.Camarillo, A.Johnston, J.Peterson, and R.Sparks, M.Handley, E.Schooler (2002), "SIP: Session Initiation Protocol", Internet Engineering Task Force (IETF).
19. Kalden R, Meirick, and MeyerM (2002), "Wireless Internet access based on GPRS", IEEE.
20. Si DF, Long Q, Han XH and Zou W (2002), "Security mechanisms for SIP-based multimedia communication infrastructure," IEEE Conf. on Comm, Circuits and Systems (ICCCAS)
21. Phone Lin, Yi-Bing Lin(2001), "Channel allocation for GPRS", IEEE
22. J.McNair, I. F. Akyildiz and M. Bender (2000), "An Intersystem Handoff Technique for IMT-2000 Systems", Proc. IEEE INFOCOM.
23. J.F. DiMarzio (2009), Android A programmers guide", McGraw Hill

24. Theodere D. Rappaport (2008),"Wireless and mobile Communication", Education", New Delhi.
25. Stallings W (2007),"Network Security and Cryptography, Pearson Education", New Delhi.
26. Van Meggelen J., Smith J., Madsen L. (2007), "Asterisk: The Future of Telephony", O'Reilly Media.
27. Emmanuel Seurre, Patrick Savelli, Pierre-Jean Pietri(2003), "GPRS for mobile Internet", Artech House.
28. Regis J. Bates (2002), "General Packet Radio Services" , Tata McGraw Hill
29. http://www.asterisk.org/
30. http://www.callcentric.com/
31. http://www.developer.android.com/
32. http://www.ibm.com/developerworks/opensource/library/os-android-devel
33. http://www.openhandsetalliance.com/
34. http://www.wireshark.org.

This page is intentionally left blank