Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Voice Security in Virtual Private Network

Deep Shikha
Computer Science and Engineering
ITM University Sec 23-A Gurgaon, India

Abstract— The commercial deployment of VoIP inside a vitual private network leads to the employment of security mechanisms that can assure availability, reliability, confidentiality and integrity. The Session Initiation Protocol (SIP) is considered as the dominant signaling protocol for calls over the Internet. SIP, like other Internet protocols, is vulnerable to known Internet attacks with ZRTP encryption to provide voice security .

Keywords—SIP, ZRTP, VPN, VOIP, ANDROID, GPRS, WIRESHARK.

I. INTRODUCTION

Secured voice communication plays a very important role in our day to day lives. Any voice communication is threatened by two biggest risks. One is, when someone is listening to our conversation behind our shoulder. The other main dangerous risk is, someone listening to it over the wire at the time when it is getting transmitted .Hence there is emerging need to digitize voice data packets over SIP protocol using ZRTP as the encryption mechanism. Because of the advanced cryptographic techniques layered over robust protocols, this application makes VoIP calls, hard to intercept and decode thereby ensuring the integrity of the call .The commercial deployment of VoIP leads to the employment of security mechanisms that can assure availability, reliability, confidentiality and integrity. The Session Initiation Protocol (SIP) is considered as the dominant signalling protocol for calls over the Internet. SIP, like other Internet protocols, is vulnerable to known Internet attacks.

II. Voip

VoIP (voice over internet protocol) in the 1990s, a number of individuals in research environments, both in educational and corporate institutions, took a serious interest in carrying voice and video over IP networks, especially corporate intranets and the Internet. This technology is commonly referred to today as VoIP and is, in simple terms, the process of breaking up audio or video into small chunks, transmitting those chunks over an IP network, and reassembling those chunks at the far end so that two people can communicate using audio and video. This idea of VoIP is certainly not new, as there are research papers and patents dating back several decades and demonstrations of the concept given at various times over the years. VoIP took centre stage with the "information super highway" (or, the Internet) concept that was popularized by former Vice President Al Gore in the 1990s, as the Internet would make it possible to interconnect every home and every business with a packet-switched data network. Before Al Gore's effort to grow the Internet, the Internet was generally limited to use in academic environments, but the possibility of mass deployment of the Internet sparked this renewed interest in VoIP.

A. Why is VoIP Important?

One of the most important things to point out is that VoIP is not limited to voice communication. In fact, a number of efforts have been made to change this popular marketing term to better reflect the fact that VoIP means voice, video, and data conferencing. All such attempts have failed up to this point, but do understand that video telephony and real-time text communication (ToIP), for example, is definitely within the scope of the VoIP. VoIP is important because, for the first time in more than 100 years, there is an opportunity to bring about significant change in the way that people communicate. In addition to being able to use the telephones we have today to communicate in real-time, we also have the possibility of using pure IP-based phones, including desktop and wireless phones. We also have the ability to use videophones, much like those seen in science fiction movies. Rather than calling home to talk to the family, a person can call home to see the family. One of the more interesting aspects of VoIP is that we also have the ability to integrate a stand-alone telephone or videophone with the personal computer. One can use a computer entirely for voice and video communications (softphones), use a telephone for voice and the computer for video, or can simply use the computer in conjunction with a separate voice/video phone to provide data conferencing functions, like application sharing, electronic white boarding, and text chat. VoIP allows the ability to use a single high-speed Internet connection for all voice, video, and data communications. This idea is commonly referred to as convergence and is one of the primary drivers for corporate interest in the technology. The benefit of convergence should be fairly obvious: by using a single data network for all communications, it is possible to reduce the overall maintenance and deployment costs. The benefit for both home and corporate customers is that they now have the opportunity to choose from a much larger selection of service providers to provide voice and video communication services. Since the VoIP service provider can be located virtually

anywhere in the world, a person with Internet access is no longer geographically restricted in their selection of service providers and is certainly not bound to their Internet access provider.

III. Sip

SIP(Session Initiation Protocol) is a signalling protocol used to create, manage and terminate session in an IP based network. A session could be a simple two-way telephone call or it could be a collaborative multi-media conference session. This makes possible to implement services like voice-enriched e-commerce, web page click-to-dial or Instant Messaging with buddy lists in an IP based environment.

SIP has been the choice for services related to Voice over IP (VoIP) in the recent past. It is a standard (RFC 3261) put forward by Internet Engineering Task Force (IETF). SIP is still growing and being modified to take into account all relevant features as the technology expands and evolves. But it should be noted that the job of SIP is limited to only the setup and control of sessions. The details of the data exchange within a session e.g. the encoding or codec related to an audio/video media is not controlled by SIP and is taken care of by other protocols.

SIP is limited to only the setup, modification and termination of sessions. It serves four major purposes

- SIP allows for the establishment of user location (i.e. translating from a user's name to their current network address).
- SIP provides for feature negotiation so that all of the participants in a session can agree on the features to be supported among them.
- SIP is a mechanism for call management - for example adding, dropping, or transferring participants.
- SIP allows for changing features of a session while it is in progress

SIP Commands

- *INVITE :* Invites a user to a call
- *ACK*: Acknowledgement is used to facilitate reliable message exchange for INVITEs.
- *BYE* : Terminates a connection between users
- *CANCEL*: Terminates a request, or search, for a user. It is used if a client sends an INVITE and then changes its decision to call the recipient.
- *OPTIONS*: Solicits information about a server's capabilities.
- *REGISTER* : Registers a user's current location
- *INFO* : Used for mid-session signalling

IV. ZRTP

It is described in the Internet Draft as a "key agreement protocol which performs Diffie-Hellman key exchange during call setup in-band in the Real-time Transport Protocol (RTP) media stream which has been established using some other signaling protocol such as Session Initiation Protocol (SIP). This generates a shared secret which is then used to generate keys and salt for a Secure RTP (SRTP) session." One of ZRTP's features is that it does not rely on SIP signaling for the key management, or on any servers at all. It supports opportunistic encryption by auto-sensing if the other VoIP client supports ZRTP. This protocol does not require prior shared secrets or rely on a Public key infrastructure (PKI) or on certification authorities, in fact ephemeral Diffie-Hellman keys are generated on each session establishment: this allows the complexity of creating and maintaining a trusted third-party to be bypassed. These keys contribute to the generation of the session secret, from which the session key and parameters for SRTP sessions are derived, along with previously shared secrets (if any): this gives protection against man-in-the-middle (MiTM) attacks, so long as the attacker was not present in the first session between the two endpoints. 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 communicating parties verbally cross-check a shared value displayed at both endpoints. If the values do not match, a man-in-the-middle attack is indicated. (In late 2006 the US NSA developed an experimental voice analysis and synthesis system to defeat this protection, but this class of attack is not believed to be a serious risk to the protocol's security).ZRTP can be used with any signalling protocol, including SIP, H.323, Jingle, and distributed hash table systems. ZRTP is independent of the signalling layer, because all its key negotiations occur via the RTP media stream. ZRTP/S, a ZRTP protocol extension, can run on any kind of legacy telephony networks including GSM, UMTS, ISDN, PSTN, SATCOM, UHF/VHF radio, because it is a narrow-band bitstream-oriented protocol and performs all key negotiations inside the bitstream between two endpoints.

V. Configuration

This application utilizes the configuration parameters of the SIP server. We have used the services of existing SIP servers in our application. Since the development and maintenance of SIP services is a costly affair, we took 3rd part services from callcentric.com. 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.

Dialler: 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, we have created different images of the numbers in the application and have used then as resources.

Then we worked on the Android event listeners in order to display the numbers on the screen when the user accesses those resources. We have also built a delete key through which the user will be able to delete the numbers if any incorrect numbers have been typed. After the user has typed the correct the numbers, 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. Else, once the call is connected, 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 we use ZRTP technique in order to generate unique keys every time a call handshake is done. During the ZRTP key exchange, the caller party sends a ZRTP hello packet. Once that packet is positively acknowledged by the recipient party the handshake happens successfully and the call packets get encrypted. 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 would 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. 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 ZRTP key exchange and we would be able to decode the VoIP packets and can listen to the conversation on a media player.

Technical Feasibility

Under the technical feasibility analysis, we evaluated below points:

Since the user had to talk using VoIP technology, we required a platform that could effectively make the use of VoIP technology in order to send the digitized voice over internet protocol. Hence, we decided to use smart phone technology in order to effectively convert the analog voice into digital because being an advanced technology, Android has got supportive APIs which made the task simpler.

As we had to initiate a secure communication, we technically evaluated several cryptographic algorithms which could fortify the user and make him/her feel secured that the communication which is happening over data channels of GSM is secured and cannot be easily eavesdropped or intercepted. Therefore to enforce this measure, we planned to use the most secured protocol that could make the call very secured at a dynamic level. And hence, the ZRTP technique which we used empowers the users to have a dynamic secured key negotiation every time a new call session is created. We planned to use this technique as it covers several cryptic algorithms and is a combinational implementation that triggers a unique secure key exchange between the handsets thereby making the digitized call packets secure. Furthermore, we also had to analyze the most suitable protocol that could support the advanced encryption and at the same time, also deliver the encrypted VoIP packets over the internet protocol effectively and efficiently. For this purpose, as per our technical feasibility, we concluded to use SIP or Session Initiation Protocol, which envelops over the TCP/IP protocol and enables the user in secured VoIP communication using smart phone, Android technology.Hence, keeping the above points into consideration, we can say that the technical feasibility evaluation of this application was positive which enabled us to initiate a secure VoIP communication using advanced Android technology, protocol and encryption technique.

Behavioural Feasibility

Under this feasibility analysis, we analyzed the working behaviour of this application in different situations.We evaluated that after this application is successfully developed will the secure-key exchange happen between the 2 Android phones or SIP clients under all circumstances. We noticed that, in order to make the key exchange happen, it is essential that the SIP accounts of both the users in the Android handsets should be active and synchronized with the 3rd party SIP server which we are using in this application. As this synchronization requires a basic resource, i.e. internet, the phones must

have high-speed GPRS connection in them. In the absence of which, the SIP accounts will not be registered and the call might not happen. But the best part is, even if GPRS connectivity is unavailable, the phone might connect to any possible Wi-Fi network or hot spot or may be a home group even to access synchronize the SIP accounts and since it is possible virtually every time, it makes our application behaviourally feasible.

Also, we evaluated whether the encryption technique and SIP protocol would be available everywhere. We henceforth concluded that that since SIP protocol envelopes over TCP/IP and TCP/IP is a protocol used in global standards and since, ZRTP technique also works on the SIP protocol, it makes our application behaviourally feasible because the technologies and platforms that we are using in it are globally available.

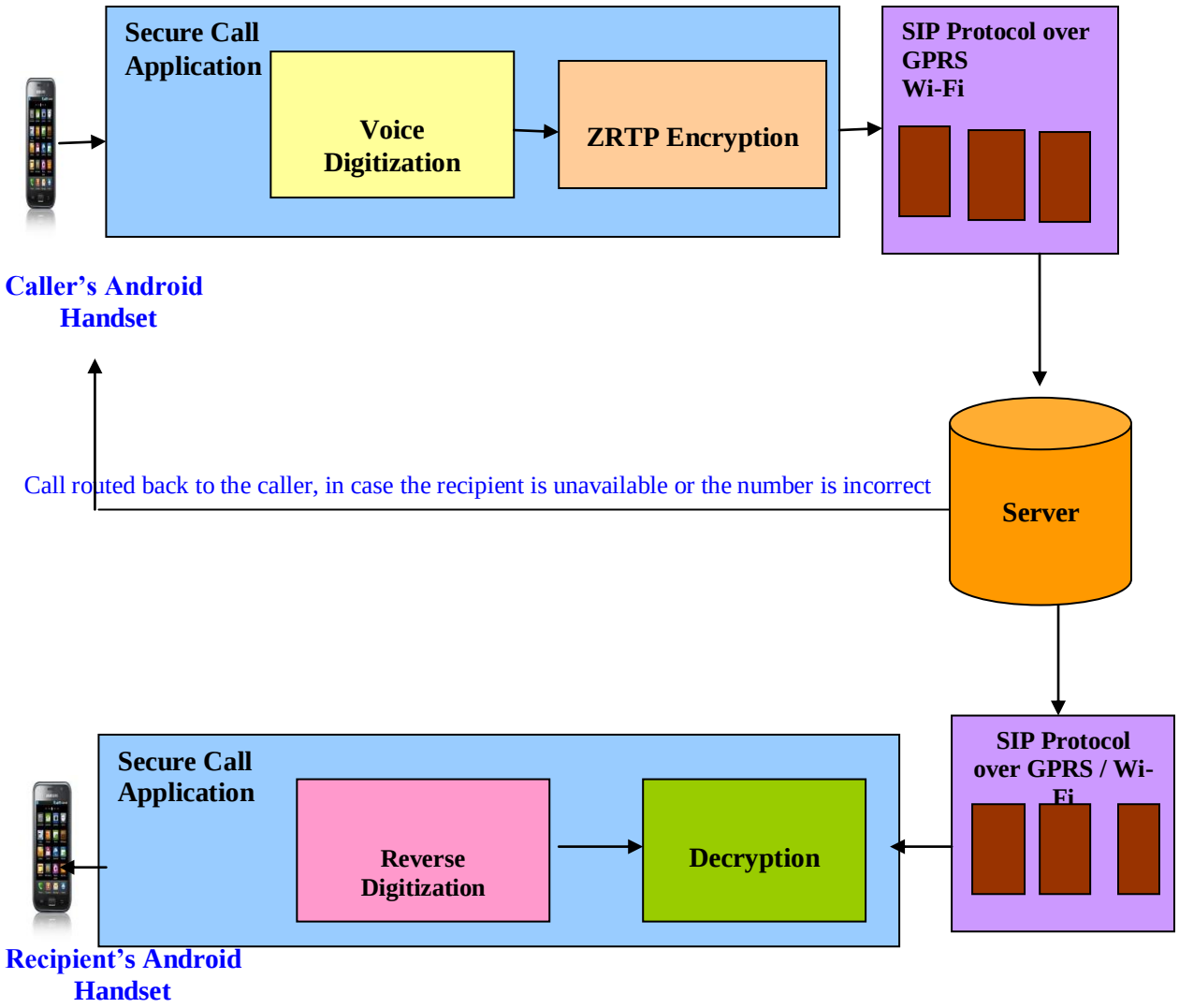

Fig. 1 Encryption /Decryption process during calling.

VI. Result of Simulation

Simulation is performed on Wire shark which is a free and open-source packet analyser. It is used for network troubleshooting, analysis, software communications protocol development, and education. Originally named **Ethereal**, in May 2006 the project was renamed Wire shark due to trademark issues. Decoding / Decrypting the digitized VoIP call packets. As we can see, since first call is encrypted, there are no voice call pitches visible, only a straight line because it is an encrypted call and could not be decoded whereas in the quadrant below it, voice graph is visible because, we could actually intercept, decode and listen to that voice conversation which occurred between the 2 SIP clients, caller and recipient.

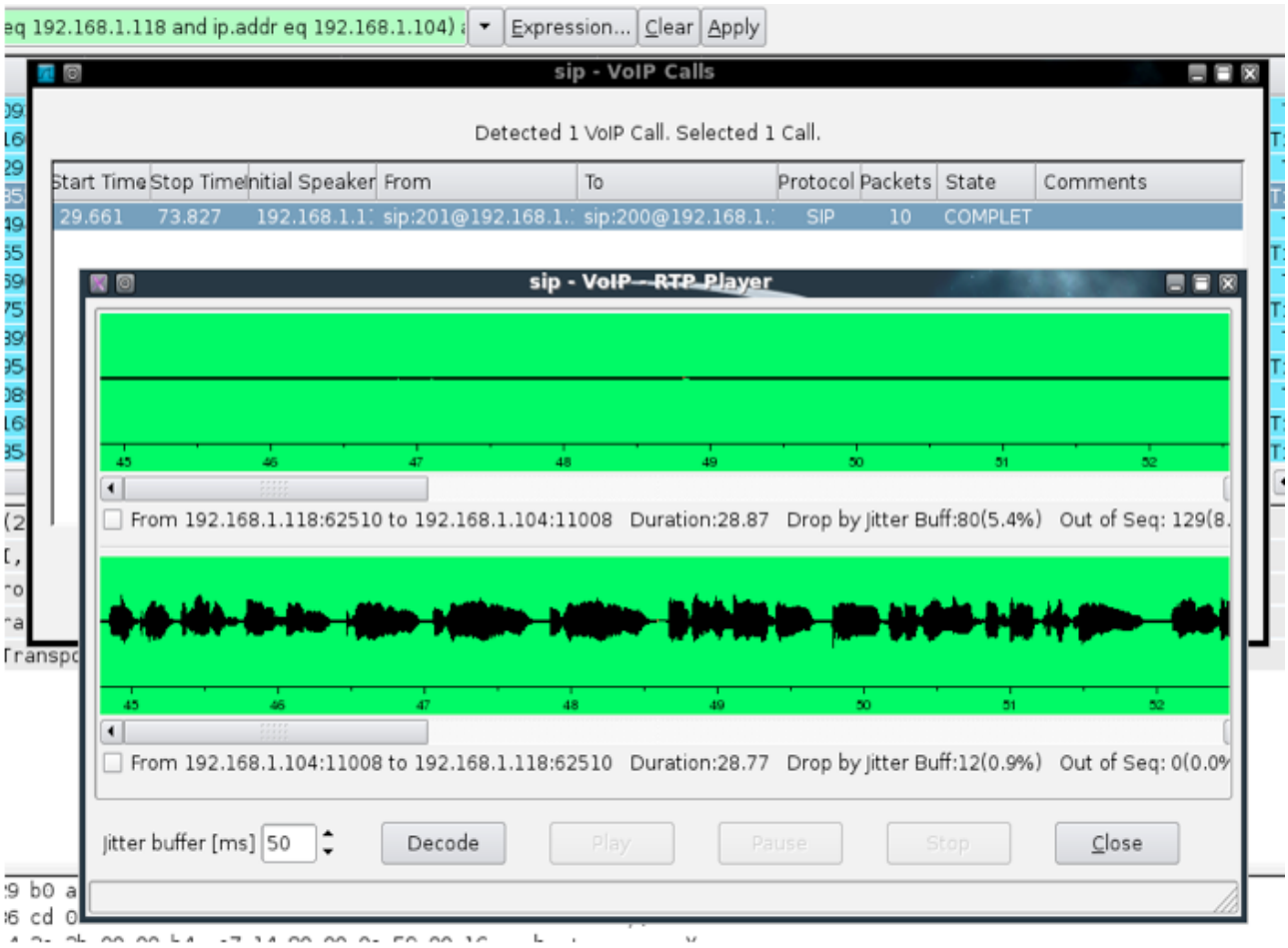

Fig 2 Sniffing VoIP Packets in the established call session between the caller and recipient Android SIP client phones

A. ADVANTAGES

- The fact that we are using smart phone technology for the communication purposes makes this application all the more robust and safe to use.
- As we are delivering the digitized call packets over VoIP using SIP protocol, it makes the calls secure, fast and reliable to use.
- All the communication is encrypted using ZRTP technique. We know that ZRTP technology is a latest combinational or hybrid implementation of certain cryptographic algorithms which not only encrypts the call data but also makes it hard to break or decrypt.
- The fact that encryption mechanism in our application is triggered dynamically between the two Android SIP clients who are using our application makes it very powerful, stable and reliable

B. FUTURE SCOPE

Although we attempted to develop this application as complete in all respects, there still exists a scope of further improvement as mentioned below:

- We can further strengthen this application to include secured video calls.
- Another enhancement as a future scope could be call conferencing under which multiple parties having SIP accounts can talk to each other at the same time.
- We can also enhance this application to initiate or receive voice-based GSM calls so that it is not just restricted to the VoIP domain but also the voice domain

VII. CONCLUSION

This application would help the users to have a secured communication in a digitized manner effectively as it will enable the users to know whether the call is secured or unsecured because the best part of this application would be, during call duration, the users would automatically come to know about the security aspect of the call as, in secured calls, the negotiated key would highlight and in unsecured calls, it will not. The digitized voice data packets over SIP protocol using ZRTP as the encryption mechanism makes VoIP calls, hard to intercept and decode thereby ensuring the integrity of the call.

ACKNOWLEDGMENT

I would like to give my sincere thanks to my guide Mrs Kusum grewal for helping me in successfully completing this research work. I deem it my previlige to have her as my guide and having her continuous encouragement n support.

REFERENCES

[1] . Rosenberg, H.Schulzrinne, G. Camarillo, A, Johnston, J. Peterson, R. Sparks, M. Handley and E. Schooler, "SIP: Session Initiation Protocol", RFC3261, June 2002.

[2] U-T, Geneva, Switzerland, ITU-T G.711.1 - Wideband embedded extension for G.711 pulse code modulation, Mar. 2008.

[3] . Baugher, D. McGrew, M. Naslund, E. Carrara, K. Norrman. The Secure Real-time Transport Protocol (SRTP). RFC 3711. 2004.

[4] . Pylarinos, S.Louvros, K.IoannouA.Garmpis and S.Kotsopoulos, "Traffic analysis in GSM/GPRS networks using voice pre-emption priority,"World Scientific and Engineering Academy and Society, pp.120-123, 2005.

[5] Lucas, etc. [author], Xielin, etc. [translate]. Firewall policy and VPNconfiguration [M].Chongqing: China Waterpower Press, 2008.

