Contribution to Securing Communications on VOIP

[1] Tahina Ezéchiel Rakotondraina, [2] Ndaohialy Manda-vy Ravonimanantsoa, [3]Andry Auguste Randriamitantsoa

[1, 2, 3] Department of Telecommunication, High School Polytechnic of Antananarivo
University of Antananarivo
Antananarivo, Ankatso BP 1500, Madagascar

Abstract

We contribute to the study of the security of voice in IP (Internet Protocol) network, which will become in the near future, a universal standard of voice and video networks Telecommunications. As with any phone call, it is a need to encrypt communication to respect the rights and privacy of each person. We implement the security of voice in IP packets and study material resource consumption on the establishment of this system. This is the major problem with this kind of technology that is currently experiencing various attacks threatening all communication systems.

Keywords: VOIP, Cryptography, AES, CPU, SRTP, TLS.

1. Introduction

VoIP is subject to various types of attacks namely capturing packets, eavesdropping communications and many others. Our contribution is to encrypt / decrypt packets (signaling and voice, SIP / RTP) passing the input / output of the network, as illustrated in Fig. 1.

Before any communication, the sender and receiver share a session key with the server. This key is exchanged over the network, in a SIP package "MESSAGE" type with the key exchange protocol of Diffie-Hellman, using a secure TLS (Transport Layer Secure) transport channel.

The session key used to encrypt and decrypt data using symmetric encryption algorithm such as "one time pad", that is to say, using different key for each session for each user, based on the cryptosystem AES (Advanced Encryption Standard).

The expected results will be the behavior of the server for normal communication and encrypted communication, according to the model proposed in Fig. 2.

2. Proposed Approach

As part of securing the voice in a VoIP network, our study is based on the following configuration:

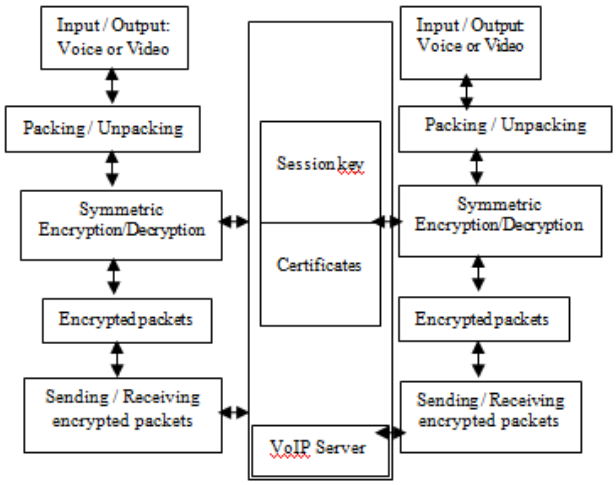

Fig. 1 Proposed Approach: Encryption Scheme Packages

The expected results will be the behavior of the server for normal communication and encrypted communication, according to the proposed model in Fig. 2.

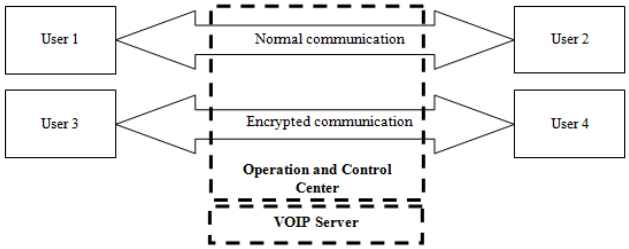

Fig. 2 Contrôle du trafic sur le serveur

3. Results and Interpretations

In our research, we used five computers: four computers for the clients and one for the server. The server configuration is as follows: the server is running on a PC (Personal Computer) Intel Pentium Core2Duo 3.2 Ghz, RAM 1 GB memory and a storage capacity of 10 GB The operating system is Linux with Version 6 of the Debian

distribution. The software used is: Asterisk 1.8 and softphones like X-Lite, Mizu Phone, Blink, PhonerLite, Ekiga and Twinkle. Throughout the simulation we used commercial network management system and as Wireshark, netstat, top.

3.1 First case: Normal Communication

In this first simulation we study the case of a basic communication, which is adopted by 80% of users of VoIP. In this context, we will successively:

- The characteristics of a SIP signaling packet
- The diagram exchanges
- The server behavior

```
INVITE sip:1000@192.168.100.10 SIP/2.0
Via:                              SIP/2.0/UDP
192.168.100.12:64312;branch=z9hG4bK-
d87543-093f6c046629653c-1--d87543-;rport
Max-Forwards: 70
Contact: <sip:1001@192.168.100.12:64312>
To: "1000"<sip:1000@192.168.100.10>
From:
"1001"<sip:1001@192.168.100.10>;tag=4721
7725
Call-ID:
5e4d7067a23bc602MjllNzM5NmI2YjdlOGI4YWIy
MGRhYWJjZGUxYzc3MzI.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS,
BYE, REFER, NOTIFY, MESSAGE, SUBSCRIBE,
INFO
Content-Type: application/sdp
c=IN IP4 192.168.100.12
t=0 0
m=audio 52970 RTP/AVP 107 119 0 98 8 3
101
a=alt:1    4    :    EAan+ijN    moQBg2NH
192.168.100.12 52970
a=alt:2    3    :    7RRe5NLd    zmXw9Ga6
192.168.100.130 52970
```

Fig. 3 Excerpt from a normal SIP INVITE packet types

We note a description of basic session with no security system. The proof is that using the utility wireshark packet capture, we can obtain and decode RTP packets, which are responsible for the transport of voice, and so we can clearly hear the discussions.

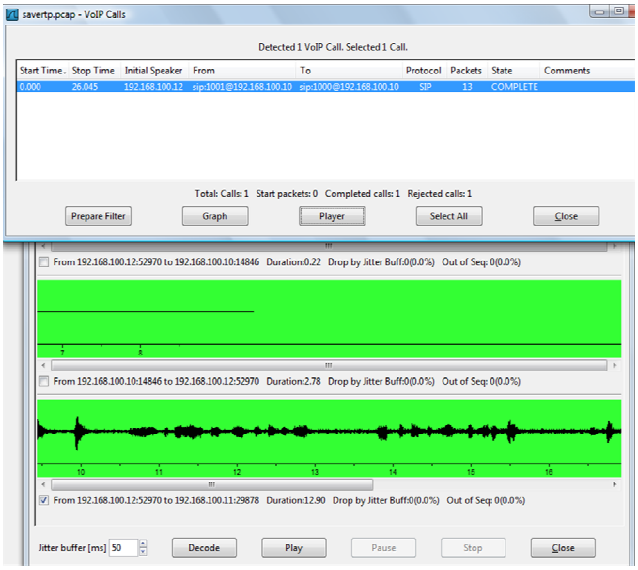

Fig. 4 Spectre de la voix Capturée

Fig. 4 shows that the voice passes through the network in clear form. Thus, any person located in the network is able to listen to the communication.

Table 1 gives a summary of the behavior of the server during this communication. It should be noted that these values represent the peaks during all communication.

Table 1 : Récapitulatif du comportement du serveur

CPU1	CPU2	RAM	Band width
6.0%	8.7%	22.2%	64Kbps

As we saw in the first case above, the VoIP basic infrastructure based on SIP / RTP offer no privacy on voice flows data. These flows can be intercepted and decoded by anyone who can sniff a point in the path taken by the RTP packets.

The problem is actually quite different. Indeed, problems arise when it is necessary to quantify: some conversations actually intended to remain confidential, hence the need for encryption.

3.2 Second case: Encrypted Communication

SRTP (Secured RTP) protocol has been developed to provide an encryption function of RTP protocol and ensure the confidentiality of communications. This protocol is based on the AES encryption, using stream cipher technical. The implementation of SRTP processing the encryption and decryption of the packet (voice) stream with the same key, the parameters is exchanged by the terminal when establishing communication.

In our study key exchange is done through SIP messages over a secure TLS channel which in turn uses the RSA cryptosystem for the creation of the certificate and key negotiation session.

Compared to the normal communication, we can see different descriptions. First, we notice some changes in the SIP packet. Indeed, the following lines have been added:

```
SIP/2.0 200 OK
Via:SIP/2.0/UDP
192.168.100.130:5060;branch=z9hG4bK005b05659b
6fe2118e9229e502929237;rport=5060;received=19
2.168.100.12
From:                                    "2001"
<sip:2001@192.168.100.10>;tag=2779306622
To:
<sip:2000@192.168.100.10>;tag=80a32b129b6fe21
1a858c129a9a643ba
.
.
.
t=0 0
m=audio 5062 SRTP/SAVP 8 0 2 3 97 110 111 9
101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=crypto:1              AES_CM_128_HMAC_SHA1_80
Inline:bu3FBm9vGSJGr6eMl4fCy8oZLcJerFn5tg5kMv
A
a=ssrc:3671974514
a=sendrecv
```

Fig. 5 Extrait d'une description d'un paquet SIP sécurisé

Specifications highlighted in Fig.5 give the protocols and security adopted. Moreover, the decoding of SRTP packets analyzed shows a fully encrypted communication. In this context, these spectra represent streams audio related to noise.

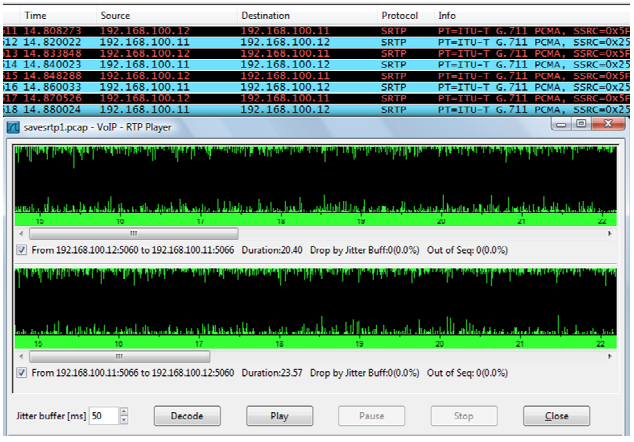

Fig. 6 Spectrum of an encrypted voice

Fig. 6 shows that the communication is encrypted and SRTP protocol is used.

For the behavior of the server we have the following summary table:

Table 2 : Comportement du serveur pour une communication crypter

CPU1	CPU2	RAM	Band width
6.1%	5.9%	23.8%	73Kbps

4. Conclusion

Based on our analysis, we find a slight difference between normal communication and encrypted communication. These differences lie in the fact that encrypted communication consumes a lot more resources that the implementation of the encryption module, both the secure transport of cryptographic keys on the packets in the Asterisk server requires adding a process where the need for additional resource.

It is clear that the module data encryption in VoIP is not yet fully implemented in the server, since the use of a real-time requires a minimum treatment period of service. The results showed that we can properly secure the data to the risk of a maximum use of resources such as CPU and memory, the server and increased the latency of the system.

Acknowledgments

Authors thank the Laboratory of the Department of Telecommunication at the Ecole Superieure Polytechnique d'Antananarivo (ESPA) University of Antananarivo, Madagascar for its Sponsor, financial and technical supports.

References

[1] P. Montoro, E. Casilari, "A comparative study of VoIP Standards with Asterisk", Forth international conference On Digital telecommunication, 2009.

[2] J. V. Meggelen, J. Smith, and L.Madsen, Asterisk - The Future of Telephony, 2nd ed., O'Reilly Media, Inc.,2007.

[3] H. N. Elmahdy and P. Muller, "The Impact of Packet Size and Packet Dropping Probability on Bit Loss of VoIP Networks", International Journal on Computer Network and Internet Research, Vol. 8(II), 2008, pp. 25-29.

[4] D. Endler, and M. Collier, Voice Over IP Security Secrets & Solutions, McGraw-Hill/Osborne, 2007.

[5] T. Wallingford, VoIP Hacks Tips and Tools for Internet Telephony, O'Reilly, 2005.

[6] P. Thermos, and A. Takanen, Securing VoIP networks threats, vulnerabilities, and counter measures, Wesley, 2007.
[7] D. Kuhn, J. Walsh, and S. Fries, Security Considerations for Voice Over IP Systems, US National Institute of Standards and Technology, 2005).

Tahina Ezéchiel Rakotondraina was born in Antsirabe, Madagascar on 1984. He received his M.S. degrees in Information Theory and Cryptography in 2010 at University of Antananarivo (Madagascar). He works as a Teacher assistant. He received his Ph.D. in Information Theory and Cryptography at High School Polytechnic of Antananarivo in 2013. His currents research interests include Cryptography, multimedia, Information Hiding, VOIP. He is an author of four papers published in international journal and a PCM member of AIRCC.

Ndaohialy Manda-Vy Ravonimanantsoa received his Engineer Diploma in computer science from 2008 at ENI (University of Fianarantsoa, Madagascar) and his M.Sc. from 2009 at Ecole Superieure Polytechnique d'Antananarivo (ESPA) University of Antananarivo, Madagascar. Currently he is working for ESPA and he had a PhD in Computer Science in 2013. His research interests include VoIP, Asterisk server, SIP Protocol and computer science.

Andry Auguste Randriamitantsoa received his Engineer Diploma in Telecommunication from 2009 at Ecole Supérieure Polytechnique d'Antananarivo (ESPA) University of Antananarivo, Madagascar and his M.Sc. from 2009 at ESPA. Currently he is working for ESPA and he had a PhD in Automatic and Computer Science in 2013. His research interests include Automatic, robust command, computer science.