Non Repudiation of Voice Over Ip Project: Security

Student National Polytechnic Institute:

Yango Alexander Colmenares

A20342669

December 2014
i. Abstract

- This project tries to demonstrate a method for non-repudiation services for SIP conversations.
- Non-repudiation is a method to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message.
- Non-repudiation could be apply to oral contract agreement for voice calls that use RTP.
ii. Table of Contents

i. Abstract.................................................................................................................. 2
ii. Table of contents.................................................................................................... 3

1. Introduction............................................................................................................. 4
2. Project description.................................................................................................. 5
   2.1 Goal..................................................................................................................... 5
   2.2 Milestones.......................................................................................................... 5
   2.3 Requirements.................................................................................................... 5
3. Logical architecture............................................................................................... 6
5. Issues..................................................................................................................... 9
   5.1 Documented fixed issues................................................................................... 10
   5.2 Documented unfixed issues........................................................................... 10
6. Conclusions.......................................................................................................... 11
7. References............................................................................................................ 12
1. Introduction

The latest successful example for the ever ongoing convergence of information technologies is internet based telephony, transporting voice over the internet protocol (VoIP). Analysts estimate a rate of growth in a range of 20% to 45% per annual, expecting that VoIP will carry more the fifty percent of business voice traffic (UK) in a few years [1].

The success of VoIP will not be limited to cable networks, convergent speech and data transmission will affect next generation mobile networks as well. The new technology raises, however, some security issues. For eavesdropping traditional, switched analogue or digital phone calls, an attacker has to get physical access to the transport medium. Digital networks are generally more amenable to attacks.

This holds already for ISDN and to a yet greater extent for IP networks. Efforts to add security features to VoIP products are generally insufficient, though proposals exist for privacy protection. Secure VoIP protocols, using cryptographic protection of a call, would even be at an advantage compared to traditional telephony systems. Protocols like SRTP can provide end-to-end security to phone calls, making them independent from the security of the transport medium and the communication provider [2]. This can also be beneficial in view of the high security requirements for wireless phones.
2. Project description

2.1 Goal

- To demonstrate the method described in the paper, “Security and non-repudiation for voice-over-ip conversations”, Published by Cristian Hett, Nicolai Kuntze, and Andreas U. Schmidt, Fraunhofer-Institue for Secure Information Technology SIT Darmstadt, Germany.


2.2 Milestones

- Understand the process of Non-Repudiation described in the paper.
- Emulate the process described in the paper.
- Create a data structure according to the description in the paper.
- Put values into the data structure using Wireshark traces of RTP conversation.

2.3 Requirements

In order to reproduce the documented system, the following elements are necessary:

- Server Matlab R2014b
- Wireshark Sip Codec G711
- Data structure for the storage of the data for two calls
- Magic Jack Softphone
- Cryptograms RSA and CRC-32

3. Logical architecture
Below is the logical architecture of VoIP:

![WebConf architecture](image)

**Figure 1: WebConf architecture.**

The implementation of the singing scenario is based on the SIP/RTP protocol, but the method could also be applied to other protocols like the Inter-Asterisk-protocol IAX [16] or the well established H.323. The signing protocol extends SIP/RTP [17] in a compatible way to transport signatures and acknowledgments of signatures. Instead of modifying a particular type of (soft-)phone, we chose to implement this as a proxy that intercepts the SIP call signalling and also the RTP audio (and video) streams. A strength of the technique is that it does not modify or in any way delay the transported audio stream. Instead signatures are transported sparely and separately from the audio stream.
4. Physical Architecture Process Security

The following ladder diagrams extracted from the WebRTC project site clearly describe the client behavior when it sets up a call (Figure 2), receives a call (Figure 3) or hang up (Figure 4).

Protection of the integrity of voice conversations. Protecting a (recorded, digital) voice conversation from falsification and tampering with is different from protecting the integrity of other digital data due to the relevance of the temporal context. In particular, packet ordering and loss have to be considered properly, and a creation time must be assigned to each conversation.

![Ladder Diagrams](image)

Figure 2: WebRTC calling.

Therefore, we depart from the basic security aspects of VoIP communication and view conversations on a transactional level between caller and callee. The top-level category of protection targets that we consider is non-repudiation of conversations. Three tasks of ascending complexity are addressed in the present work:

1) Protection of the integrity of voice conversations. Protecting a (recorded, digital) voice conversation from falsification and tampering with is different from protecting the integrity of other digital data due to the relevance of the temporal context. In particular, packet ordering and loss have to be considered properly, and a creation time must be assigned to each conversation.
2) Authentication of speakers. An initial authentication of caller and called together with the inherent biometric authenticity of voice is the basic approach to this problem. While it could be resolved in principle solely on the transport layer, it is advantageous to combine it with the methods of 1) to obtain proof that a (recorded) conversation was carried out completely from the authenticated devices. It has to be noted that each authentication of a speaker requires trust in the devices used by the communication parties.

3) Electronic signatures over voice conversations. Building on 1) and 2) it is possible to achieve, for voice conversations, the level of non-repudiation provided by electronic signatures over digital documents, i.e., an expression of will. For this, the aforementioned tasks must be complemented by a proof of possession of a trustworthy signature token and device, and the intention to sign.

We present theoretical and technological concepts for each of the tasks 1) – 3) and describe their realization in a demonstration environment. The existing VoIP infrastructures are largely unaffected by our concepts through a seamless and efficient integration in the SIP [9] and RTP protocols. On the other hand, the three tasks pose increasing technical requirements on the part of the involved devices.
5. Issues

5.1 Documented fixed issues

The main scenario of this paper is shown in Figure 1 and is a bidirectional interactive conversation between two parties A and B. A wants to sign the conversation and release it to B as a declaration of his will, i.e., a commitment in the sense of a signed offer. In effect, A wants or is required to make sure that the conversation between A and B provides non-repudiation, in any case he expresses the explicit will to make non-reputable statements or stipulations in the call. For that, A possesses a digital certificate for a signature public/private key pair. B and any third party to whom the signed conversation is presented as evidence, are assumed to be able to verify the certificate of A and any data signed with the associated private key, i.e., we assume a PKI structure in the background. A signs the complete call including both channels comprising everything that B says. B stores the signed conversation in a secure archive of his choosing. B can later proof to third parties or court that the call happened and had the claimed contents. If B fails to store the conversation in an archive or deletes it, A can deny that the call ever happened. Cohesion is ensured by the used protocol and procedure, so that the full bidirectional interactive dialogue is continuously signed.

As part of the implementation, the ability to record and archive a conversation on the part of B had to be developed. While the main scenario requires changes to the terminal equipment on both sides for signing and interchange of signed data, we were also able to apply similar methods to a pure archiving scenario [13]: A component VSec, implanting the integrity of the archived conversation, could be placed anywhere in the way from A to B as long as any part of the communications was carried out over SIP/RTP. Thus the archive functionality can be added to the corporate VoIP telephone system, into the devices used by A and B or integrated in any other point which has access to all exchanged packages of the communication. Using this, party B can source out the archive from VSec.

The communication between the component VSec which listens and intercepts the conversations and the archive itself is secured. These methods are applicable in the present scenario, and are particularly interesting considering the limited storage space of mobile phones.
5.2 Documented unfixed issues

Behavior disabling the stream
When a moderator disables or enables the stream of a different user, the application registers the resource that belongs to the other user with the connection ID (CID) of the moderator. It produces a wrong behavior that eliminates the resources of the user when the moderator closes its session. This discovered issue affects all WebConf versions.

The fastest way to fix this design error would be to let the moderator notify the user and let the user to enable or disable his own stream. A different approach would be the increasing of server functionalities letting the moderators to update some resource fields without changing the connection ID.

An extension to this concept is that both parties could sign the conversation. This is sensible in the form of parallel signatures, i.e., each party signs their own utterances and what the other party said and both parties archive it. This slight variation provides mutual non-repudiation.

The signing scenario is implemented in a flexible demonstrator placed as a proxy between the internet and the soft-phone or VoIP hardware phone of party A and between the internet and the phone of party B. The demonstrator manages certificates and signing of the voice data and also archives the conversation if used by party B. The proxies shown in Figure 1 are an implementation detail as our demonstrator does not integrate with a specific VoIP client directly, but is located on the same computer or in the same network and can be used with any SIP phone.
6. Conclusions

This project has a great potential and can be oriented to fit many needs in educational, business and personal areas.

Security project is open to collaboration. You can receive information or join it contacting Professor Carol Davids (davids@iit.edu) or Yango Colmenares (yangocolmenares@gmail.com).
7. References

[1] Yango Colmenares final report:

    Fraunhofer-Institute for Secure Information Technology SIT


[8] C. Hoene, H. Karl, and A. Wolisz: A perceptual quality model for adaptive

    Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261

     2000 IEEE 59-65