International Journal of Computer Networks and Communications Security

VOL. 2, NO. 9, SEPTEMBER 2014, 292–297
Available online at: www.ijcncs.org
ISSN 2308-9830

Smuggling VOIP Watermarks Using Intended Corrupted Packets

Mazen Mohamed Flaifl[1], Sherif Radwan Belal[2], Ismail Abdel Ghafar Ismail[3], Ashraf Diaa El-Din Elbayomy[4], Mohamed Zaki Abdel Megeed[5]

[1, 2] Military Technical Collage, Department of Computer Engineering

[3] Arab Academy for Science and Technology

[4] Azhar University, Department of Computer Engineering

[5] Military Technical Collage, Department of Communications

E-mail: [1]mazen.ali.f@gmail.com, [2]belal_sherif@yahoo.com, [3]ismail.ghafar@aast.edu, [4]adiaa@afmic.com, [5]mzaki.azhar@gmail.com

ABSTRACT

Designing and embedding a watermark for VoIP is the main goal of this paper, A new model is introduced and characterized by high robustness, high security and must be non-perceptual. The watermarking model is suitable for real-time service and supports the needs of embedding the watermark into the traffic of VoIP and its extraction additionally this model offers authentication and integrity. The model based on digital watermarking and steganography. Another factor was taken in consideration; the amount of data used and its influence on the voice quality of service. the model is implemented using C# code for both embedding and extracting the watermarking spite of the intended cheating mechanisms that might complicate the send/receive conditions. In addition, the model performance has confirmed its robustness and quality of service.

Keywords: *IP Telephony / VoIP Security, Digital Watermarking, Steganography.*

1 INTRODUCTION

In TCP/IP networks VoIP, which is a real-time service, uses RTP (Real-Time Protocol) with UDP (User Datagram Protocol) for transport of digital streams. Currently there is one control protocol for RTP and it is RTCP (Real-Time Control Protocol)[1].

Steganography and Digital Watermarking are Information Hiding sub disciplines. The general difference between those two techniques is that steganography aim is to keep the subsistence of the information secret and in watermarking making it undetectable. However, the most important applications for our purposes are: the possibility of generating and embedding the watermark to achieve authentication and integrity including exchanging additional information. The watermark that will be used in, proposed here, authentication and integrity solution must possess certain parameters, like: robustness, security, transparency, complexity, capacity, verification and invertiblity.

Some security issues can face the VoIP environment such as identifying VoIP participants and call altering which raise the need for a model to make a trusted relationship in the VoIP environment.

We propose a new model that introduces the using of watermark to secure the VoIP communications and identifying the VoIP participants at all stages of the call by generating a unique watermark for each user depending on user's private data and exploring different ways of smuggling the generated watermark inside the VoIP traffic on messaging stage.

The paper is organized as follows. In section 2, the related work discussed while in section 3 the model for VoIP watermarking described. Next, we give details about watermark generation in section 4 and we explained the formation of a covert channel in section 5. Finally, the model is implemented at section 6 and the paper conclusion at section 7.

2 RELATED WORK

We can get advantage of using the digital watermarking to offer authentication and integrity for IP Telephony through two possible scenarios, in which:

I. Securing the audio stream

II. Securing both audio and signaling protocols

In the case of using digital watermark in securing signaling messages, we still have a disjunction set of the security mechanisms for securing the audio stream and a signaling protocol thus there are no benefits [2]. Working algorithms for securing the media stream presented in [3], [4] and [5]. This work wants to combine two phases of VoIP call to achieve securing VoIP with low impact on the voice quality of service. Applications of the VoIP covert channels differ as they can pose a threat to the network communication or used to improve the functioning of VoIP [6] (e.g. security [7] or quality of service [8]). That is why we will focus on the second scenario: the simultaneous authentication and integrity protection of audio and signaling messages.

Three flavors of network steganography designed, all of which manipulate IP. The three methods developed are Lost Audio Packet Steganography, or LACK; Hidden Communication System for Corrupted Networks (HICCUPS); and Protocol Steganography for VoIP application. As their names imply, these techniques exploit lost packets, corrupted packets, and hidden or unused data fields in the VoIP transmission protocol. LACK hides information in packet delays, HICCUPS disguises information as natural "distortion" or noise, and Protocol Steganography hides information in unused data fields [9].

The receiver gets a packet and checks it for errors using the packet's checksum. Normally, if the checksum is wrong, the computer discards that packet. However, if a terminal has the right steganography program installed, it will not discard these intentionally wrong checksums instead, it will know these are the data packets to scan for steganograms [9].

3 THE PROPOSED MODEL FOR VOIP WATERMARKING

The proposed model of VoIP watermarking will apply the general watermarking model on the VoIP traffic adding some features to the model for achieving the goal of this paper. A watermark generation algorithm introduced and new techniques for smuggling the watermark into the traffic are used including the reverse action to extract the generated watermark and the original VoIP traffic.

Figure1 illustrates the general watermarking model. The data stream (original data) and the watermark are the inputs of the watermark embedding process, which is responsible for merging the original data with the watermark producing watermarked data stream. The communication channel carries the watermarked data stream to the other side, which makes invertible process on the watermarked data stream called watermark extraction to produce the original watermark and the original data or watermarked data as needed.

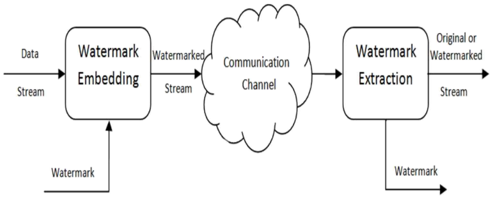

Fig. 1. General Watermarking Model

The proposed model designed to work on signaling and messaging phases of the VoIP calls providing host-to-host security. At the signaling phase the VoIP user that request to make a call referred later by "sender", initiate the VoIP call by preparing his data and send it to another user referred later by "receiver" through SIP. Following the proposed model, both the sender and the receiver should do further action that is keeping the sender's data to create a corresponding secure hash values and store these values at their buffers for future use. Moreover, the sender and the receiver should exchange data about the way of hash value creation and information about the watermark.

Figure 2 illustrates the block diagram of the proposed model for VoIP watermarking which described in five stages. First stage, the sender side generates watermark by producing a secured values from user voice stream, random key and the signaling massage (user identifier (ID), signal time stamp (ST) and selective signaling parameters (SPA)). Second stage, the sender embeds the generated watermark into the voice stream to produce a watermarked voice stream that passes from the sender to the receiver via a communication channel (data network). Third stage at the receiver side, the watermark extractor module processes the watermarked voice stream to detach the watermark from the voice stream. The fourth stage, watermark regeneration uses the voice stream, same random key and the signaling messages to produce the watermark as the first stage.

Last stage is comparing the extracted watermark with the regenerated one to take a decision depending on the comparison that clarifies the trust of the sender voice stream. In addition, some data exchange happens between the VoIP sender and receiver.

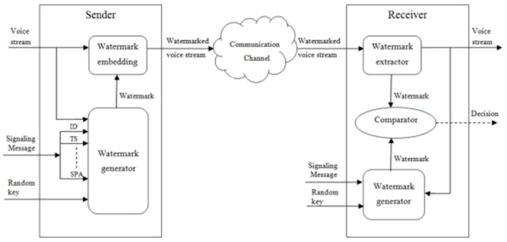

Fig. 2. Proposed Model Block Diagram

All the previous stages reversed to start at the receiver side in order to offer a trust relationship inside the VoIP environment between the VoIP participants.

4 WATERMARK GENERATION

The proposed solution introduce a way for generating the watermark by applying HMAC algorithm to produce secure hash values for a chosen data of the VoIP traffic and enforcing all created hash values into XOR function to produce the VoIP watermark using random key.

Figure 3 presents the watermark generator in more details; containing a functional blocks, inputs and outputs. The watermark generator receives the voice stream, signaling messages and random key to construct a watermark achieving authentication and integrity.

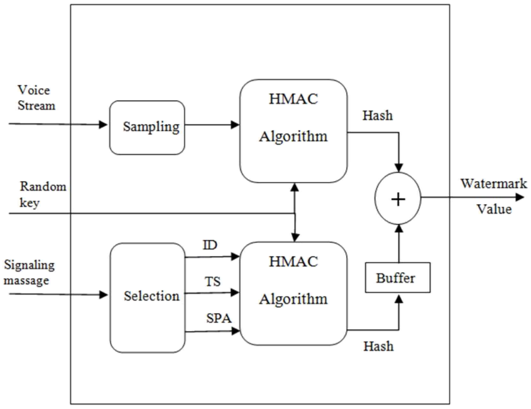

Fig. 3. Watermark Generator Block Diagram

The voice stream is in the form of RTP packets where the RTP header contains payload type, sequence number and time-stamp; the payload data of the RTP packet carries the digitized voice.

The sampling function receives the RTP packets to choose samples used in the watermark generation, then, passes the elected packets to the HMAC algorithm to create a hash value for each packet using secret key.

The signaling message consist of the call setup and control, in the form of SIP and SDP protocols containing message type and call agreement parameters between sender and receiver.

The selection function selects user unique identifier (ID), time-stamp of the signal packet (TS) and selective signaling parameters (SPA), passes these selections to the HMAC algorithm to create a hash value using random key, this hash value is stored in a buffer waiting for the RTP packet hash value. Then, the two hash values are XORed to generate the watermark.

5 FORMING A COVERT CHANNEL

The RTP protocol works at the VoIP environment as a messaging stage, RTP packet consist of header and payload, the header describe the packet and the payload content while the payload carries the digitized voice. The RTP header has the payload type (PT) identifier; this field identifies the format of the RTP payload and determines its interpretation by the application. An RTP source may change the payload type during a session. A receiver must ignore packets with payload types that it does not understand. [RFC 3550]

The intentional corruption achieved by changing the content of the payload; in this case, the VoIP environment does not recognize the corruption and the system will process the packet payload passing the output to the audio device resulting a voice distortion. Thus, another action have to be done to mark the intentionally corrupted packet, changing the value of the PT header field can fulfill this need in which this packets can be recognized by the VoIP environment to drop these packets and avoid sending them to the audio device.

The intended corrupted packets used in smuggling the watermark. Packets intentionally corrupted by choosing undefined or unused value for PT field. This action used twice with two different values, one is used to determine that the payload content is used in the watermark generation, which is important information for the receiver, and the other packet used as a covert channel by embedding the watermark value inside the packet payload. For the complexity of the detection, the watermark data inserted in different parts inside the payload, the information of the exact places inside the payload that contain the watermark data is sent to the receiver side.

Figure 4 illustrate the watermark embedding process and the use of RTP packets as a covert channel. There are two main functions; first is the embedding of the watermark data inside the RTP packet, and in order to make the receiver recognize the intended corrupted packet, the second function needed to mark the packet as corrupted one.

The watermark extractor at the receiver side receives the watermarked stream to fetch the marked RTP packets to perform one of two actions depending of the marked packet received. If the packet marked as used in watermark generation, the extractor remove the packet mark to be used in watermark regeneration. The other action, when the packet is marked as watermark carrier then the watermark extractor takes out the watermark from this packet.

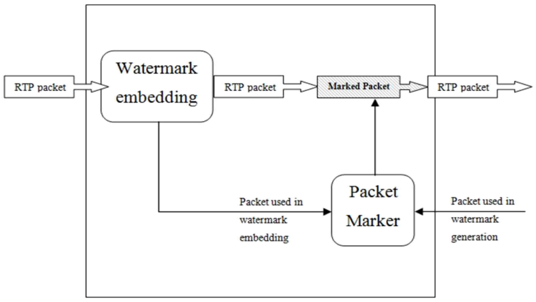

Fig. 4. Embedding Block Diagram

Figure 5 illustrate the watermark extractor flow chart starting by receiving the RTP packet to check it is marked or not, if the packet is not marked then receive the next packet, else if marked then check the type of marked packet. If the packet is marked as data packed then send it to the watermark regenerator block to create the watermark and set data flag value true.

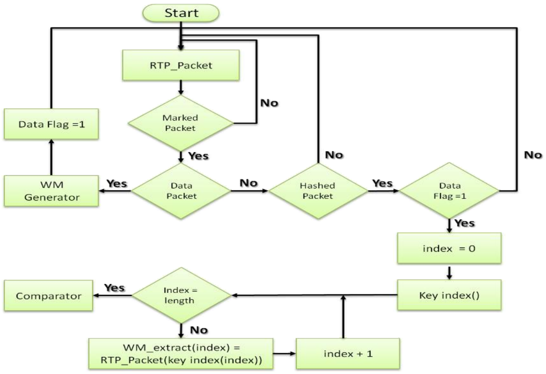

Fig. 5. Extractor Flow Chart

6 IMPLEMENTATION

Experimental scenario for the proposed VoIP solution is built using C# as a programming language, the solution follow the VoIP standards uses SIP and SDP as signaling protocols and RTP as media transmission protocol. SIP, SDP and RTP built as classes. The solution implements a class "Globals" that define:

- SDP_Hash as a secure hash value of the sender's data created at the VoIP signaling phase
- SDP_Hash_Calc as a secure hash value of the data received at the VoIP signaling phase
- RTP_Hash as a secure hash value of the sender's data created at the VoIP media transport phase
- RTP_Hash_Calc as a secure hash value of the data received at the VoIP media transport phase
- Watermark as a sender's watermark value to be smuggled inside the traffic
- Watermark_Rx as a watermark value extracted from the received traffic to be smuggled inside the traffic
- Watermark_Calc as a sender's watermark value calculated at the receiver side
- Hashing as a function for calculating a secure hash value using the secret key
- Generate_Watermark as a function for generating the watermark
- Generate_Index as a function to generate a random index used to define the place where the watermark is smuggled inside the RTP packets

A valid SIP request formulated by a user (sender) must contain the following header fields: To, From, CSeq, Call-ID, Max-Forwards, and Via; all of these header fields are mandatory in all SIP requests. These six header fields are the fundamental building blocks of a SIP message class, as they jointly provide for most of the critical message routing services including the addressing of messages, the routing of responses, limiting message propagation, ordering of messages, and the unique identification of transactions. These header fields are in addition to the mandatory request line, which contains the method, Request-URI, and SIP version. The SIP_Stack class provides a function to create the appropriate request using these header fields. The proposed solution enforces the sender to buffer Call-ID and From-header-field, used later in the watermark generation process.

During call setup, communication details negotiated between the endpoints using Session Description Protocol (SDP), which contains fields for the codec used, caller's name, etc. The sender sends SIP INVITE request containing SDP info for the session, which forwarded to the receiver, possibly via a proxy server. Eventually, the receiver will send an "OK" message back containing the call preferences in SDP format. Then the sender will respond with an "ACK". SIP provides for the ACK to contain SDP instead of the INVITE, so that an INVITE may be, seen without protocol specific information. After the "ACK" received, the conversation may commence along the RTP / RTCP ports previously agreed.

The proposed solution describe the SDP as a set of classes to generate SDP packet which is a part of the SIP stack, SDP_Message class illustrate the creation of session description data which used to identify the sender, which the solution employs this user identity as a part of the sender watermark. The sender creates an object named "SdpOffer" as an instance of the basic class "SDP_Message" which contains MediaDescriptions property that describes media type and media attributes. The media type currently defined media as "audio". The sender initializes the main properties of SdpOffer such as Version, Origin, SessionName and SDP_Time with the appropriate data.

The sender then convert the SdpOffer concatenated with the buffered SIP header fields to binary data, this data is applied to Hash-based Message Authentication Code (HMAC) algorithm to produce secure hash value "SDP_Hash" using a random key and store this value to be used later in the watermark generation.

At the media transport phase, the sender construct RTP packets by preparing the packet header data containing Payload Type (PT) which will be used by the solution in the smuggling of watermark, the digitized voice is the packet payload. The sender select digitized voice sample from the RTP packet payload, and apply hash function on the chosen digitized voice sample to create a secure hash value using a random key. Subsequently the solution has two secure hash values, one created to identify the user data at the signaling phase SDP_Hash and the other value associated with the user voice RTP_Hash.

A watermark generation function implemented to use the previously created secure hash values to produce the sender watermark; the same function used at the receiver side to regenerate the sender's watermark using the same parameters.

The proposed solution has introduced intended corrupted packet as a cheating technique for watermark smuggling inside the VoIP traffic. Packets intentionally corrupted by choosing undefined or unused value for PT field. Intended corrupted packet used as a covert channel to embedded the watermark value. The watermark value embedded in different parts inside the payload using Generate_Index function from Globals class, the information of the exact places inside the payload that contain the watermark data sent to the receiver side.

The model performance illustrated by figures 6 and 7. Figure 6 presents chart shows the delay variation of the packets (Delta) measured in milliseconds (ms), for VoIP traffic. The chart shows time measured in milliseconds (ms). There are two lines on the chart. The red line represents delta of VoIP watermarked traffic using corrupted packets as covert channel. The blue line represents non-watermarked VoIP traffic. The chart demonstrates that watermarked and non-watermarked traffic have similar Delta behavior according to network.

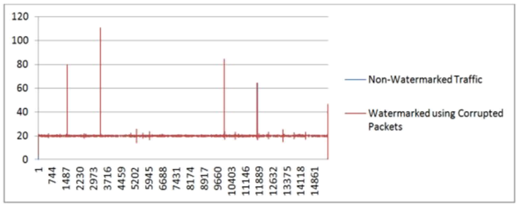

Fig. 6. Packets Delay Variations of Non-watermarked and Watermarked VoIP traffic

The chart also shows that the difference between watermarked and non-watermarked traffic is very small and the Delta values work around 20 ms. This trend supports the theory that the value 20 ms is the average delay of the traffic packets. During the conversations, the Delta value slightly differs in the two graphs. These results would seem to contradict the idea that watermarked traffic has low impact on the voice delay.

Lastly, the results indicate that at some points the delta values increase for the watermarked or the non-watermarked traffic. However, this could be due to network congestion.

Figure 7 presents chart shows the difference between the delay variations of the two VoIP traffic illustrated in figure 6.

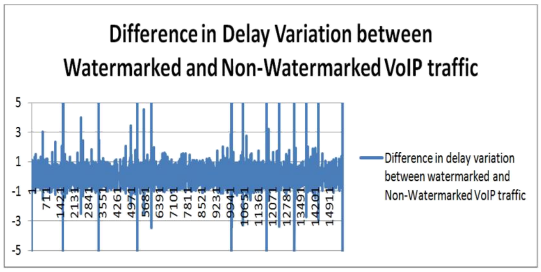

Fig. 7. Difference in Delay Variations between Non-watermarked and Watermarked VoIP traffic

The chart demonstrates that the difference between the delay variation Delta of watermarked and non-watermarked traffic is very small which the VoIP users cannot recognize. The chart also shows that the difference between watermarked and non-watermarked Delta is very small and values varies between 5 and -5 in most of the time.

7 CONCLUSION

This paper proposes an effective security model for VoIP communications. The exploits two information hiding techniques:

I. Steganography to create a covert channel.

II. Smuggling to by-pass the underling watermarks as corrupted packets.

For the used watermark, the paper illustrates both the embedding and extracting techniques at the sending and receiving nodes, respectively. In addition, the intended corruption technique that depends on checking the sequence number of the packet header is pointed out. The performance of the proposed model has indicated its applicability for VoIP security purpose because of its high robustness, infinitesimal overhead, limited delay and maintaining the voice quality.

5 REFERENCES

[1] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson: RTP: A Transport Protocol for Real-Time Applications, IETF, RFC 3550, July 2003.

[2] W. Mazurczyk, Z. Kotulski: New VoIP Traffic Security Scheme with Digital Watermarking, Lecture Notes in Computer Science Volume 4166, 2006, pp 170-181.

[3] M. Steinebach, F. Siebenhaar, C. Neubauer, R. Ackermann, U. Roedig, J. Dittmann: Intrusion Detection Systems for IP Telephony Networks, Real time intrusion detection symposium, Estoril, Portugal (2002).

[4] S. Yuan, S. Huss: Audio Watermarking Algorithm for Real-time Speech Integrity and Authentication, International Multimedia Conference Proceedings of the 2004 Multimedia and security workshop on Multimedia and security, Magdeburg, Germany (2004) 220 - 226

[5] T. Mizrahi, E. Borenstein, G. Leifman, Y. Cassuto, M. Lustig, S. Mizrachi, N. Peleg: Real-Time Implementation for Digital Watermarking in Audio Signals Using Perceptual Masking, 3rd European DSP Education and Research Conference, ESIEE, Noisy Le Grand, Paris (2000).

[6] W. Mazurczyk, K. Szczypiorski: Steganography of VoIP Streams, Lecture Notes in Computer Science Volume 5332, 2008, pp 1001-1018

[7] W.Mazurczyk, Z. Kotulski,: New Security and Control Protocol for VoIP Based on Steganography and Digital Watermarking. In Proc. of: IBIZA 2006, Kazimierz Dolny, Poland (2006)

[8] W.Mazurczyk, Z. Kotulsk: New VoIP Traffic Security Scheme with Digital Watermarking. In Proc. of: SafeComp 2006, Springer-Verlag, Lecture Notes in Computer Science 4166, 170-181, (2006)

[9] J. Lubacz, W. Mazurczyk, K. Szczypiorski: Vice Over IP : The VoIP Steganography Threat , IEEE Spectrum, 29-Jan-2010.