Zbigniew PIOTROWSKI, Jarosław WOJTUŃ, Jarosław OŚKA

Wojskowa Akademia Techniczna, Wydział Elektroniki

Hardware watermark token for VoIP telephony

Abstract. *The developed electronic device is a digital watermark token used to authenticate the subscriber in VoIP telephony. The device converts the signal in real-time, full-duplex, allowing simultaneous embedding of a watermark in the speech signal, as well as the extraction of the binary signature of a watermark on the receiving side of the Internet VoIP link. This paper presents a procedure for subscriber authentication in VoIP telephony and the structure of the hardware token, along with a functional diagram.*

Streszczenie. *Opracowane urządzenie elektroniczne stanowi token cyfrowego znaku wodnego wykorzystywanego do uwierzytelniania abonenta w telefonii internetowej VoIP. Urządzenie przetwarza sygnał w czasie rzeczywistym, w pełnym dupleksie, pozwalając na jednoczesne osadzanie znaku wodnego w sygnale mowy jak również ekstrakcję binarnej sygnatury znaku wodnego po stronie odbiorczej łącza internetowego VoIP. W artykule przedstawiono procedurę uwierzytelniania abonenta w telefonii VoIP oraz budowę sprzętowego tokena wraz ze schematem funkcjonalnym.* ***(Sprzętowy token znaku wodnego dla telefoni VoIP)***

Keywords: watermark token, digital watermark, subscriber authentication, VoIP telephony, OMAP-L137, hardware token
Słowa kluczowe: token znaku wodnego, cyfrowy znak wodny, uwierzytelnianie abonenta, telefonia VoIP, OMAP-L137, token sprzętowy

Introduction

Telecommunication systems require the operator to provide, among others: high-fidelity, quality and consistency of the processed signal, as well as clear identification of both interlocutors of a voice message. The presented system is an alternative to contemporary methods of subscriber authentication and is based on the addition of an additional signal to the channel used for voice communication, a so-called watermark that represents a binary signature of the subscriber (PIN). On the receiving side of the Internet connection set up for the VoIP session the subscriber's PIN is extracted from the received signal and the signature received compared with the one declared by the subscriber at the receiving side. Secret authentication provides additional security for voice calls in VoIP telephony. The system does not cause a delay as shown in [1] in the set up of a VoIP telephony network connection and is resistant to errors occurring during the transmission of RTP packets [2], and it does not require data encryption, for example, according to the proposed system [3].

Authentication of a subscriber over a VoIP link

Authentication is a process that consists of verifying the declared identity of a person, device, or service involved in the exchange of data. The definition of "authentication" is to be found in the cryptography standard ISO/IEC CD 9798-1 [4]. Impersonating (spoofing) someone else's identity is the primary means used by cyber-criminals to commit fraud in data communication networks. It is therefore reasonable to develop an identity verification system that would be one of the security components of a communication system [5][10]. Basically, the authentication process can be divided into factors used for the verification of identity. These factors can be classified into three categories:

- possession factor - authentication based on the person authenticated possessing an object;
- knowledge factor - authentication based on information shared between the authenticated and authenticating party;
- hereditary factor - authentication based on biometric features.

In accordance with [6] a strong authentication process set up as a multi-layer authentication process with two or more authentication factors makes it possible to minimise the likelihood of someone impersonating someone else's identity.

Currently literature on the subject describes only one electronic device (the Personal Trusted Terminal) that allows objective verification of the identity of a radio subscriber [7]. The creators of the above mentioned concept suggest [5] a possibility of using an objective method of identity verification in VoIP, GSM, PSTN networks. Objective verification of the identity of a subscriber can be accomplished through the use of mechanisms for hiding information on the basis of watermarking techniques.

The proposed method involves sending additional information through the VoIP link in a secret manner along with the speech signal. This additional information, an individual PIN number assigned to the subscriber, is embedded in the form of a watermark in a manner that is imperceptible in the speech signal. As a result of the above operation we obtain a signal as follows:

$$X^{*} = X + K(X, PIN) \quad (1)$$

where:
X – original signal, here the speech signal;
$K()$ – function forming the watermark signal;
X^{*} – watermarked signal

A diagram of the watermark encoder is shown in Figure 1.

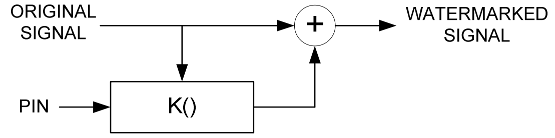

Fig. 1. Block diagram of the watermark encoder

At the receiving side extraction of the watermark signal is performed in order to obtain the subscriber's PIN. This PIN is then compared against a database that contains subscriber data and PIN numbers assigned to them. In case both PINs match (the one received and the one stored in the database) the subscriber's authentication is positive. A diagram of the watermark decoder is shown in Figure 2

$$PIN^{*} = D(X^{*}) \quad (2)$$

where:
$D()$ – function extracting the watermark signal;

(3) $$\mathrm{STATUS}=\begin{cases} AUTH\ OK,\ \text{if}\ PIN = PIN^* \\ NO\ AUTH,\ \text{if}\ PIN \neq PIN^* \end{cases}$$

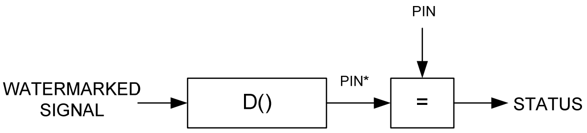

Fig. 2. Diagram of the watermark decoder

The procedures for embedding and extracting the watermark are implemented in the hardware watermark token. The subscriber authentication mechanism operates in end-to-end mode. Verification of the identity of subscribers is done without interfering with existing SIP, H.323 signalling protocols. Moreover, such a solution has the feature that it is independent of the IP telephony system operator and there is no need to modify the existing telecommunications network infrastructure. Figure 3 shows a schematic of the verification of identity of subscribers in end-to-end mode using the designed watermark token.

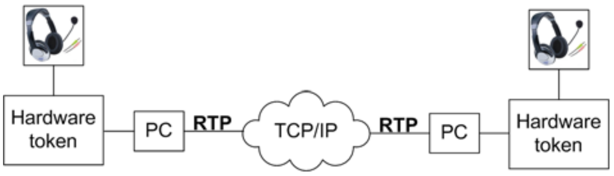

Fig. 3 VoIP subscriber authentication diagram

In order to confirm his or her identity, the user of the token must enter their signature in person, this stems from the need to provide protection against the possibility of the terminal being used by a third person. The user receiving a call will be, after the time it takes for the watermark to be extracted, informed by the system of the outcome of the verification.

Another problem, one not covered in this article, is the safe distribution of signatures within the system.

Hardware of the digital watermark token

The device's architecture is based on a modern DSP processor from Texas Instruments. During the development work 5 units were constructed, with each new edition having a PCB with a more compact architecture, offering more features and boasting greater attention to detail. The final version of the PCB will be presented later in this paper.

The end user receives the device enclosed in an aluminium housing from HAMMOND with the dimensions of 100mm x 20mm x 50mm. The token is shown in Figure 4.

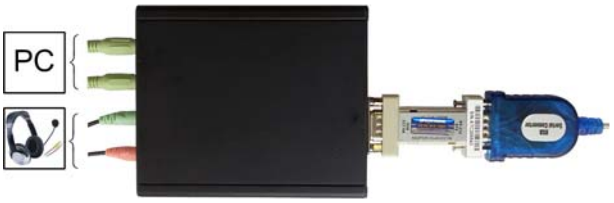

Fig. 4. Hardware watermark token

The watermark token is equipped with the following interfaces:

- USB or RS232 interface for communication with a PC;
- 3.5 mm minijack connector to connect to a headset (microphone + headphones).
- 3.5 mm minijack connector to connect to the audio path of the PC.

When connected to a computer, the device is seen as a standard headset. This makes it possible to connect to another person using any voice messaging software, for example Skype. The result of the authentication is visualised using an application written in Microsoft Visual C#. A user-friendly interface and standardised connectors mean that the prototype of the device can also be used by a person that does not have high technical qualifications.

The design process of the hardware layer of the device started with the choice of the OMAP-L137 [8] processor and the TLV320AIC3106 audio codec [9] co-operating with the aforementioned processor. The OMAP-L137 C6-Integra™ processor is a modern dual-core processor designed for low power consumption applications. Its structure features a ARM926EJ-S™ core, a C674x core and virtually all modern peripherals. Peripherals used in our project include: USB Host, USB Device, MMCSD (Multimedia Card Secure Digital) interface, UART, SPI, I2S, I2C. The processor requires external SDRAM memory and non-volatile FLASH memory in order to function. The processor and the audio codec have been connected using the I2S interface used for two-way digital audio signal transmission. The audio codec system has in its structure a complete analogue line that makes it possible to plug in a microphone and headphones without the use of external active systems. In order to enable the FULL DUPLEX mode, the left and right channel signals were split and directed in two opposite directions. This means that the left channel of the codec is used for the embedding of the watermark, while the right channel for the detection of the received watermark. Connection to a PC using the audio path and a communication interface, such as USB or RS232, is not a trivial task. This is due to the ground loop phenomenon which occurs and is characterised by a specific hum, which leads to a deterioration of the quality of the audio signal. One way to counteract this phenomenon is to use specialised systems for galvanic isolation of signal and audio grounds. One such system is Analog Devices' ADuM3160.

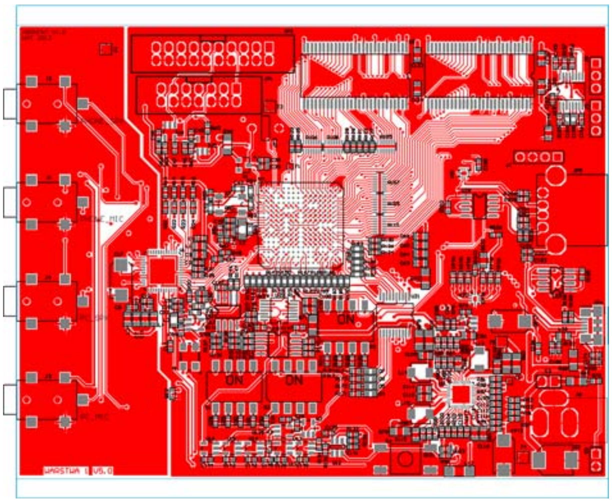

Fig. 5. PCB diagram

The most significant challenge facing a designer of such a system is to write a driver that will optimally use the computing power of the DSP for processing a real-time algorithm. The solution employed in this project is to use the operating system DSP/BIOS drivers, which significantly reduce the embedding time of the algorithm. In DSP/BIOS access to data sent and received from the audio codec is provided using a universal SIO (serial input-output) driver. Optimal and stable operation of the driver was achieved when using 256 samples per frame and 4 auxiliary buffers. The entire application for the DSP was written in C. The processor was programmed using the CCSv4 (Code Composer Studio) integrated development environment and the XDS510 USB debugger from Spectrum Digital.

The PCB was designed in ALTIUM Designer and made at Techno Service in Gdańsk. Due to the need to use a processor in a BGA256 housing with a pitch of 1 mm and 0.5 mm diameter ball, it was necessary to create a 4-layer board, gold-plated, and include decoupling capacitors mounted in the 0402 housing. A PCB diagram and a photo of the final version are shown in Figures 5 and 6.

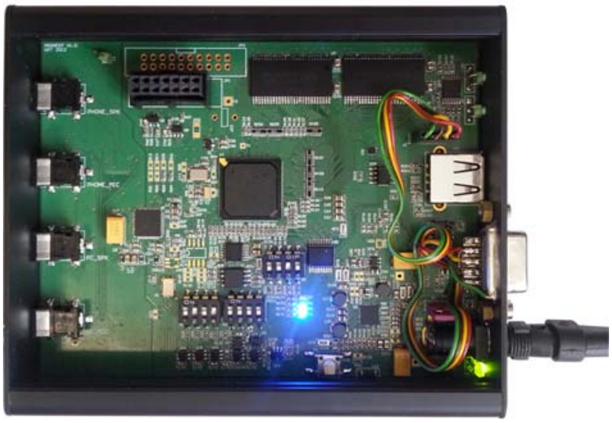

Fig. 6. Photo of the PCB

Summary

This paper presents an objective method of subscriber identity verification over a VoIP link using a hardware watermark token. The proposed solution allows for robust subscriber authentication using two factors - the possession factor, having a watermark token, and the knowledge factor consisting of information regarding the binary watermark signature used in a particular session shared between users. The device has been tested using an IM program and two tokens in a dedicated VoIP session. The result of the experiment was a high 100% efficiency of subscriber authentication for 100 attempts of extraction and comparison of the binary watermark signature while maintaining transparency of the watermark signal embedded in the speech signal.

Scientific work funded from assets for science for the years 2010-2012 by the Ministry of National Defense DNiSW/U/5/BN/1.14/2010/779

REFERENCES

[1] Matić V., Leb A., Mitić D., Dukić M.: Estimation of post dialling delay in telephone networks, *Przegląd Elektrotechniczny*, vol. 88, no. 5B/2012, 154-156

[2] Lebl A., Mitić D., Markov Z.: Calculation of signalling RTP packet error probability in internet, *Przegląd Elektrotechniczny*, vol. 87, no. 10/2011, 364-368

[3] Karpinski M, Aleksander M, Litawa G, Karpinskyi V The security of data transmission over telecommunication networks based on advanced data encryption methods *Przegląd Elektrotechniczny*, vol. 85, no. 4/2009, 19-21

[4] ISO/IEC CD 9798-1:2010 Information technology - Security techniques - Entity authentication - Part 1: General

[5] Piotrowski Z., Gajewski P.: Voice spoofing as an impersonation attack and the way of protection, *Journal of Information Assurance and Security,* vol. 2 (2007) 223-225

[6] Committee on National Security Systems *National Information Assurance (IA) Glossary*, CNSS Instruction no. 4009, 2010

[7] Gajewski P., Nowosielski L., Piotrowski Z., Zagoździński L.: Handset with hidden authorization function, *European DSP Education & Research Symposium EDERS 2008*, Proceedings ISBN: 978-0-9552047-3-9, (2008), 201-205

[8] Dokumentacja techniczna procesora: http://www.ti.com/lit/ds/symlink/omap-l137.pdf

[9] Dokumentacja techniczna kodeka audio: http://www.ti.com/lit/ds/symlink/tlv320aic3106.pdf

[10]Drgas Sz., Dąbrowski A., Zamorski D., Automatyczne rozpoznawanie mówcy z wykorzystaniem różnych jąder opartych na cechach prozodycznych połączonych z cechami spektralnym, *Przegląd Elektrotechniczny*, vol. 2012, no. 6/2012, 51-54

***Autorzy**: dr inż. Zbigniew Piotrowski, E-mail: zpiotrowski@wat.edu.pl, mgr inż. Jarosław Wojtuń E-mail: jwojtun@wat.edu.pl, mgr inż. Jarosław Ośka, E-mail: jaroslaw.oska@wat.edu.pl, Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Telekomunikacji, ul. Kaliskiego 2, 00-908 Warszawa 49.*