Identity management in VHF radio systems

Z. Piotrowski & P. Gajewski
Telecommunications Institute, Faculty of Electronics,
Military University of Technology, Poland

Abstract

For up-to-date commercial short-distance communication systems, e.g. RF systems of VHF bandwidth or WiFi wireless networks, the development of efficient and reliable algorithms and procedures for management of the radio network subscriber identity is becoming still more important and urgent need. The existing systems for that purpose are limited to checking of a simple authorization code against the tables for supervising the RF information. Identity of a radio network subscriber is verified on the basis of the rule that hidden messages and hidden responses are generated during the communication sessions. The concept of the centralized system for management of identities is based on the rule that a unique set of PIN numbers is assigned to each subscriber of the RF communication system. Each PIN number is repeatedly changed during a communication session in order to avoid the attack when a part of the signal including the PIN code is copied from the communication signal for further redistribution.
Keywords: VHF radio, hidden communication, hidden authorisation.

1 Introduction

Electronic identity understood as an unambiguous assignment of a digital ID to an individual person fulfils many important functions in contemporary telecommunications. Mechanisms of identification, authentication and authorization ensure the function of incontrovertibility of sent information and the use of abbreviation function mechanisms makes it possible also to verify the integrity of the received information. Safe data transmission through a telecommunication network requires the sent data to be provided with the following information: who sent it, who the addressee is; often, also confirmation is required of: who received the data and whether the received data


WIT Transactions on Modelling and Simulation, Vol 51, © 2011 WIT Press
www.witpress.com, ISSN 1743-355X (on-line)
doi:10.2495/CMEM110421

was modified during transmission. These are the most basic functions implemented as a standard in telecommunication systems; moreover, it is often demanded that the information be classified, i.e. inaccessible for third parties that are not authorized to receive it. Confidentiality functions are realized by means of encoding in accordance with the accepted cryptology standards.

However, there exist telecommunication systems of special purpose in which the above-described mechanisms are expanded by an additional function: the function of hidden transmission. A hidden transmission means hiding the fact of sending additional data through a telecommunication network by means of standard links, protocols and open transmission. Thus, the special-purpose telecommunication system may be one which uses a standard telecommunication network of a set architecture in order to carry out a hidden transmission.

Subscriber's identification involves recognizing the person by the system in accordance with the name declared by the subscriber, while authentication is the process of checking whether the declared subscriber name is coherent with the unique data assigned to the user and that stored by the system. Proper authentication takes place when the declared user name (so-called login) is coherent with the password assigned to it. The password depends on the adopted authentication scheme and may be the knowledge of the subscriber (password, personal data), the fact of possessing something (key, token, card), a characteristic biometric element (fingerprint, iris image, voice, anatomic face structure) or even a skill characteristic of a given subscriber (behavioral biometrics: handwriting, dynamics and manner of pressing keys). After a positive authentication process the subscriber is assigned rights to specific resources, i.e. so-called authorization.

2 Known authentication techniques and threats

According to Eric Diehl, head of an international group of experts from the Technicolor laboratory [1] which deals with the safety of multimedia material distribution, authentication is "*a hardware or software process whose aim is to determine an impossible-to-forge identification manner of two conversation or transaction actors. From this process it stands that the actors confirm and authenticate one another's identity using techniques of passwords, exchange of confidential information or digital signature*."

Authentication may be multi-stage (expanded) or hierarchical which takes into account authorization levels. A classic example may be the scenario of authenticating an internet banking customer in which losing a one-time password for a transaction realization does not lead to the loss of previously acquired resources, e.g. preview of bank account, history of operations. Here, multi-stage authentication involves using two or more identification attributes, e.g. a password and a token, or a password and a biometrics feature (fingerprint reader). The problem of losing electronic identity (identity fraud) is one of the most frequent causes for infringing safety in existing telecommunication systems. What main threats may be identified to the loss of electronic identity? Javelin's report [2] introduces several definitions of identity loss which provide

an insight into the existing threats. They include *data breach*, i.e. an unauthorized revealing of information that compromises the safety, privacy and integrity of user identification data; *identity fraud*, i.e. unauthorized use of part of personal data for financial gain (it may be done without identity theft – familiarization with data, randomly generated credit card numbers); *identity theft*, i.e. unauthorized access to personal data; *Man-in-the-Middle (MTM)* defined as unauthorized access to personal information in which the perpetrator is able to decipher, modify and embed information between two parties during a session without their knowledge; *Synthetic Identity Fraud* denoting a fictional identity created in order to deceive an organization, e.g. identity generated using real social insurance numbers and various first and last names. Of course, there are many other definitions and notions related to electronic identity loss. Electronic identity theft is the most common internet offence and losses suffered as a result of an improper distribution and protection of electronic identity are huge.

According to the aforementioned Javelin's report and the Spendonlife service [3], in 2008 the United States of America recorded a loss of $31 billion on account of various forms of identity loss, whereas total losses in the world amount to $221 billion. In USA, 26% of identity theft cases involved an unauthorized takeover of credit card numbers and purchases of material goods made by third parties based on those numbers; 18% was theft of public utility services (gas, electricity) involving assigning a given service to a person residing outside their area of permanent residence; 17% was banking fraud (change of account assets, theft of access codes for ATM systems); 12% involved theft of social security numbers, e.g. in order to obtain employment; 5% included loan fraud (applying for a loan on someone else's behalf, e.g. assigning a social security number to other personal data); 9% was fraud related to taxes, driver's license, etc.; 13% involved other types of identity theft. In 2008, 10 million people in the US alone have become victims of identity theft, i.e. 22% more than in 2007. In the same year (2007) 1.6 million households in USA experienced theft which was unrelated to credit card losses, but instead - to breaches of bank accounts or debit card accounts. Moreover, 38 to 48% of people notice the theft of their electronic identity within 3 months, while 9 to 18% does not notice this fact for 4 or more years.

The seriousness and scale of electronic identity loss was noted also in recent years by decision-making authorities in the European Union, including the European Commission. One of the many initiatives aimed at solving the problems with assigning and distributing electronic identity is the pilot program STORK [4] (***S****ecure iden****T****ity cr****O****ss bo****R****ders lin****K****ed*) which pertains to a cross-border recognition of existing national electronic identity systems (eID), thus allowing for obtaining access to public services in member states. Several dozen million people in EU use national eID identity cards when accessing services related to social insurance, filling in tax returns and other services. Thus, the project is related to electronic identity management (eIDM) through a system which is a federation of already existing systems. This is a fundamental difference in comparison to other projects realized by EU regarding identity,

e.g. FIDS, PRIME, PRIMELIFE, PICOS, SWIFT, SWEB where attention was paid more to attempts at standardizing marked off, centralized systems. The European Commission argues that eIDM is a foundation stone in the implementation of a full scope of eGovernment services for citizens, as well as for businesses in the entire European Union [5]. It should also be mentioned that a number of interesting initiatives were created thus far which, according to their creators, are aimed at facilitating the determination of a person's identity in order to provide them with access to specific resources. One such initiative is Identity 2.0 [6]; its creator, Dick Hardt aims at co-creating and supporting an OpenID architecture [7] (architecture of dispersed authentication and distribution of identity in the Internet). The idea of the proposed mechanism is simple: instead of remembering countless numbers of login-password pairs for different internet services, it is enough that the user creates an account on an OpenID server of their choice. Wanting to log in on any internet service, the user will be redirected to an OpenID server by providing his/her OpenID ID in the form of a URL address. The OpenID server authorizes the logging-in operation. An organization supporting this technology was created under the name OpenID Europe [8].

According to Elbirt [9], the recommended measures of electronic identity protection include personal data protection (social insurance numbers, last name (including family name), date of birth, previous residence address, driver's license number). Consultations are also recommended in institutions dedicated to protecting personal data in order to familiarize oneself with forms of illegal obtaining of personal data by third parties and with recommendations pertaining to revealing one's personal data. Another protection measure is to retain information confidentiality (separating personal data from business data, restricting and not revealing data to other people or businesses, and in the case of data loss – immediate alarming and reporting the fact of data loss). In order to minimize the risk of an unauthorized leak of personal data, tracking carried out transactions is recommended, e.g. payments with credit cards by periodic printouts of statements. Moreover, it is advisable to properly store personal information by encrypting files and a periodic change of passwords. Furthermore, it is advisable to destroy old documents, printouts from bank accounts using shredders. In the case of electronic documents the disposal should occur by means of special computer programs which irretrievably delete a document from the computer's memory.

3 Hidden authentication

The need to introduce effective authentication procedures is especially noticeable in military heterogenic systems which offer speech transmission services. A complex solution to the problem of authentication is called for especially by short-term prototyping and implementation of new systems in accordance with the COTS (*commercial, off-the shelf*) rule. The use of the network's multi-service character in the concept of *Next Generation Networks* (NGN) may lead to a new approach to designing innovative and effective solutions in subscriber authentication.

The aim of this paper is to show an alternative for current solutions on verifying electronic identity and its distribution in telecommunication networks, using the technique of information hiding. The paper presents exemplary scenarios of authenticating in a VHF radio link with the use of a hidden transmission of additional information. Results are presented of tests and experiments on two algorithms of watermarking speech signals which enable the embedding of additional information (the personal ID of the user) in the call (original) signal, as well as the extraction of this additional information from the received signal. The personal identification number (PIN) is represented by a digital watermark with a determined *data payload* which is inaudible in the presence of an original call signal. One of the audio watermarking methods is called *Drift Correction Method* (DCM) [10] which has unique parameters in terms of the obtained data payload and robustness against degrading factors and which is offered together with the described new, one-stage psychoacoustic correction system as a basis of a new authentication standard in radio systems and internet telecommunications. A patent was obtained in the Patent Office of the Republic of Poland [11] for the method of one-stage psychoacoustic correction. Because of the confirmed generated high data payload of the watermark, the drift correction method opens up a path for carrying out not only hidden, but also confidential acoustic transmissions. Watermark *data payloads* higher than 128 bits enable the use of known methods for encrypting binary strings with a determined cryptographic power before they are embedded into the original signal in the form of a watermark. Thus, the use of a hidden and confidential transmission significantly increases the safety of the carried out transmission for especially important transmissions, e.g. radio transmissions.

4 Experimental results

In order to realize the procedure of subscriber authentication in telecommunication links, a decision has been made to use one of the known authentication models which involve transmitting a binary signature to subscribers who exchange correspondence between themselves. However, it must be noted that the authentication model has been supplemented by a hidden signature sent through a watermark added to the call signal, which constitutes its significant modification. This chapter presents the results of experiments related to subscriber authentication with the use of an information hiding technique for a radio VHF link. The link uses the drift correction modulation as a method of embedding a watermark in the original signal. Moreover, results were discussed from the carried out experiments.

A supplementation to the carried out experiment is a test of the hardware encoder and decoder of the watermark – a Personal Trusted Terminal (PTT) with an algorithm based on the phase angle scanner method that uses a detector of spectral line amplitude instead of a detector of phase angle mistuning values. A description of the method using the detector of spectral line amplitude, as well as a description of the hardware encoder and decoder of the watermark may be found in [12] and [13–17].

Aim: To check the robustness of the watermark embedded in an acoustic signal by a hardware encoder against a transmission in a VHF link.

Description of experiment: a signal with an embedded watermark was decoded; a hardware encoder and decoder were used which are based on the method of forming and detecting a spectral line amplitude [12]. The watermarked signal was sent through an ultrashort wave link (VHF) with the use of Radmor (TRC 9200) military radio stations. Transmission parameters: sending and receiving frequency 30MHz (simplex work), F3E modulation in an HLG working mode of the radio station at a determined frequency. A speech signal was transmitted in *real time* for a watermark data payload P=15 [b] and with a duration of the transmitted signal t=30 [s]. As a result of the experiment's realization, a chart was obtained of the effectiveness of decoding the correspondent's signature. The diagram of the VHF link was presented in Figure 1.

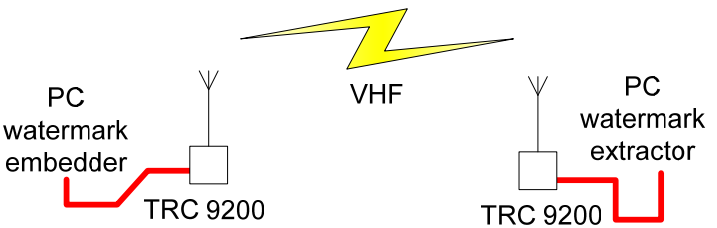

Figure 1: Scheme of the realized VHF radio link with the use of watermark encoder and decoder.

In experiment the software encoder of the watermark embedded the watermark signal into the speech signal in real time. In the application, the WM binary signature denoted the PIN number of the radio correspondent. At the receiving side of the radio link the watermark decoder compared the decoded PIN with the PIN declared in the on the receiving side. In the case of a coherence of both PIN numbers: the decoded with the declared one, the device displayed information about authenticating the radio correspondent. Tests were carried out which involved transmitting and decoding the PIN number in a radio link for 10 radio correspondents with assigned PIN values. Each correspondent read out a fragment of a radio telegram for 30 seconds with a pressed switch (radio station work mode on transmitting). Each radio correspondent was authenticated three times in sessions with numbers 1-5. Only in the case of two radio correspondents was an erroneously decoded PIN obtained in one in five sessions. In the case of the remaining eight radio correspondents, a positive authentication was obtained in each of the five sessions. Thus, the authentication effectiveness in this experiment equalled 96%. An effectiveness of 100% will be required from a professional, commercial authentication system.

4.1 Personal trusted terminal features

The aim of the device is to transmit a Personal Identification Number (PIN) through a telecommunication link in the form of a binary signature assigned to a given subscriber. The binary signature (PIN) is represented by a watermark signal which is sent together with the speech signal and which is inaudible in its presence. At the receiving side of the link, the watermark is decoded and the obtained binary signature is compared with the one that is stored in the database of the handset. In the case of a coherence of the received signature with the declared one, the caller is authorized during the realized connection. Then the LCD of the handset displays a suitable message. If only one of the interlocutors has a handset with the function of hidden authorization, conducting a conversation is possible like in a standard phone; however, the user of a handset with an authorization function receives a warning message regarding the lack of authorization due to no watermarked signal. The system is intended to work with military battlefield VHF radio stations. The system has advanced mechanisms of reducing resulting frequency mistuning and psychoacoustic correction. Using a standard handset without an authorization function the user is never sure whether he is speaking to the dedicated caller, even despite his recognizable features: the tone of the voice, intonation, timbre, base frequency, formant frequency distribution, etc. This happens because of the possibility of applying an artificial voice synthesis technique or changing the voice features of a third person during conversation. This is even more possible because the quality of the radio link is low and we do not always know precisely the voice of our interlocutor; thus, a change of the caller's identity is facilitated.

The basic task of the worked out handset is especially to ensure a safe exchange of messages between the authenticated subscribers in a radio link without openly using cryptography mechanisms. Third persons impersonating the identity of a given interlocutor are not informed about the process and result of the authentication; thus, the conversation with the unauthorized interlocutor may be continued without revealing important messages or it may be finished.

5 Conclusions

The presented authentication VHF system does not interfere with the telecommunication infrastructure of currently functioning radio systems. The lack of a special handset with a hidden authorization function does not, in any way, prevent the realization of a connection provided the correspondent has a regular handset. An attempt to discover a realized connection with a watermark sent in the background of the call signal is made more difficult because of the inaudibility of the watermark and the necessity to analyze the speech signal in terms of a hidden message in all call tracks realized at a given moment, e.g. during telecommunication rush hour. The digital watermark is perceptually transparent and inaudible on the host signal's presence and is robust against intentional and unintentional attacks. The developed system allows for transmission together with the speech signal a watermark signal with dedicated

data payload. Watermark signal represents PIN assigned to the specific subscriber using encryption based on a single-use key so that the PIN number is changing during each call session.

Acknowledgement

This paper has been co-financed from science funds granted within the years 2010-2012 as a research project of the Ministry of Science and Higher Education of the Republic of Poland No. 0181/R/T00/2010/12

References

[1] http://eric-diehl.com
[2] Javelin Strategy & Research, "2009 Identity Fraud Survey Report", Feb. 2009, www.javelinstrategy.com
[3] http://www.spendonlife.com/guide/2009-identity-theft-statistics
[4] http://www.eid-stork.eu/
[5] http://ec.europa.eu/information_society/activities/egovernment/policy
[6] http://identity20.com
[7] http://openid.net
[8] www.openideurope.eu
[9] A.J. Elbirt, *Who Are You? How to Protect Against Identity Theft,* IEEE Technology and Society Magazine, vol. 24, Issue 2, 2005, p. 5-8
[10] Z. Piotrowski, Drift Correction Modulation scheme for digital audio watermarking. Proceedings 2010 Second International conference on Multimedia Information Networking and Security MINES 2010, Nanjing, China, 4-6 November 2010, ISBN: 978-0-7695-4258-4, IEEE Computer Society, Conference Publishing Services (CPS), pp. 392-397
[11] Z. Piotrowski, Gajewski P., European Patent Application no. 09151967.8 (EP 2 085 964 A2), "*Method and apparatus for subscriber authorization and audio message integrity verification*". European Patent Office
[12] Gajewski P., Łopatka J., Piotrowski Z., *A New method of frequency offset correction using coherent averaging*, Journal of Telecommunications And Information Technology, 1/2005, National Institute of Telecommunications, ISSN 1509-4553, Warsaw 2005
[13] Piotrowski Z., Effectiveness of the frequency offset computation procedure, Elektronika, nr 3/2010, s.76-79, Wydawnictwo Sigma-NOT, 2010
[14] Piotrowski Z., Zagoździński L., Gajewski P., Nowosielski L.: *Handset with hidden authorization function*, European DSP Education & Research Symposium EDERS 2008, Proceedings, pp.201-205, Published by Texas Instruments, ISBN: 978-0-9552047-3-9
[15] Piotrowski Z., Nowosielski L., Zagoździński L., Gajewski P.: *Electromagnetic Compatibility of the Military Handset with Hidden Authorization Function Based on MIL-STD-461D Results*, Progress In Electromagnetics Research Symposium PIERS 2008 Cambridge

Proceedings, pp.103-107, Published by The Electromagnetics Academy, ISBN: 978-1-934142-06-6, ISSN: 1559-9450

[16] Z. Piotrowski, The National Network-Centric System and its components in the age of information warfare, Safety and Security Engineering III, WIT Press 2009, pp. 301-309, ISBN: 978-1-84564-193-1

[17] Z. Piotrowski, K. Sawicki, M. Bednarczyk, and P. Gajewski, *New Hidden and Secure Data Transmission Method Proposal for Military IEEE 802.11 Network* Conference Proceedings, The 6th International Conference in Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP 2010, Darmstadt Germany