JOURNAL OF SCIENCE OF THE MILITARY ACADEMY OF LAND FORCES

Volume 49 Number 4(186) 2017

DOI: 10.5604/01.3001.0010.7228 (

SELECTED PROBLEMS OF SECURITY OF INFORMATION CONFIDENTIALITY IN CYBERSPACE

Leszek WOLANIUK*

* *Faculty of Security Studies, General Tadeusz Kosciuszko Military Academy of Land Forces*
e-mail: leszek.wolaniuk@awl.edu.pll

Received on 23th May; accepted after revision in November 2016

Summary:

Information confidentiality is the one of the cornerstones of IT security, which is defined and described in ISO/IEC 27000 standard. Contemporary practices of disclosing information to unauthorized persons and systems are the reason for difficulties in this concept implementation. At every step we encounter situations where information is extracted or obtained illegally from different sources. The main purpose of this paper is to present the issue of information confidentiality protection in cyberspace, as a complex, full of contradictions problem of techno-social character. The role of information confidentiality in functioning of a society, organization and individual has been described. The most important information confidentiality threats have been characterized and the description of a number of incidents illustrating those threats has been quoted. Contemporary security threats have been presented as well as selected methods of information confidentiality protection transmitted in ICT networks. The characteristics of protection systems of information confidentiality have been analyzed, with special attention paid to their functionality and vulnerability to existing threats. The concept of protecting the confidentiality of information transmitted on the Internet based on the use of cryptography and steganography has been presented.

Keywords:

information confidentiality, cyberspace security, ICT security

INTRODUCTION

According to the Judeo-Christian tradition, violation of information confidentiality was the first and greatest crime committed by people, the crime called the original sin in the Old Testament. In the symbolic description in Genesis the first humans – Adam and

Eve violated the restriction on the access to the information set about themselves and their surrounding world and were thus expelled from Paradise. They lost trust of their God, his favor and many attributes that they had been originally endowed with [12].

Regardless of the views resulting from the above description, there should be no doubt that protecting information from unauthorized persons' access constitutes one of the pillars of our civilization. It is all the more important due to the fact that at the current stage of its development, we are the so-called information society, in which information is the pivotal good that is under protection.

We learn about the consequences of effective confidentiality protection or its loss from the human history, chasing the course of many conflicts as well as other key events. Julius Caesar would have probably lost his life sooner if not for effective protection of his letters to Cicero with the use of a cipher, nowadays called the Caesar cipher. The Russians could have won the Battle of Warsaw in 1920 if one of the Polish Military Staff officers Lt. Jan Kowalewski had not broken the cipher used by them to send radio commands to subordinate troops. It resulted in the loss of confidentiality of this information by revealing its content, thus informing the Polish Headquarters about the weaknesses and intentions of the Red Army, which in consequence led to "the Miracle on the Vistula" [5].

The issue of information confidentiality protection is not and has never been treated unambiguously. When this question is considered in the context of an individual, its right to privacy as well as in terms of security of groups of people, including states, requirements for systems protecting against unauthorized access to information are very high. However, when criminals, terrorists or agents of hostile states use the same confidentiality tools, the whole issue is completely different.

Today information confidentiality defined in the 27000 standard as *"property based on the fact that information is not shared or disclosed to unauthorized persons, subjects or processes"* [8]refers primarily to information stored, sent, processed and presented with the use of ICT systems and networks. That is why the issue of determining rules of information confidentiality security in the global computer network, or the Internet, otherwise known as cyberspace, is the key problem of today's world, its quintessence.

1. CONFIDENTIALITY IN CYBERSPACE

Cyberspace is a common information platform of the information society. The platform's operation is of key significance for the society's functioning. In such the socio-economic system, information is an important immaterial good, equivalent or even more valuable than material goods. Due to this interpretation of the role of information in the modern society, it is worthwhile asking about the meaning of information confidentiality in this context. Its violation is unequivocal with unauthorized access to information, i.e. unauthorized acquisition. It is similar to the theft in the material world with the difference that the legal holder still owns a copy and often does not know that it has been stolen. This undoubtedly results from a lack of awareness about characteristics of information and rules applicable in the world of information systems. An additional problem is the way of communication through cyberspace. Ac-

cess to the Internet is usually obtained using individual IT resources in a way that gives a sense of intimacy and discretion. Cyberspace users, with their eyes fixed on computer and smartphone screens, often separated from the outside world, relying solely on themselves, have a false sense of security and exclusiveness of their communication. Unfortunately, this picture is misleading. From the point of view of technical solutions used in the Internet, in reality the web communication is more like talking to someone in a restaurant full of guests instead of meeting in a secluded place. Actually, given the nuances of commonly used network solutions, such communication would better reflect a situation where in a crowded restaurant we are talking to someone sitting several tables away through a chain of guests occupying tables between us and the addressee of our messages. Intermediaries pass on the information, providing it sequentially along the route to one another. This is how it is done in computer networks with packet communication and the Internet is such a network! The only difference is that intermediaries exchanging our information are not people but computer devices. When we communicate with any other cyberspace user, we do this by using public communication links and a sequence of intermediary network devices located somewhere in the world. We never know for sure who controls their operation at a given moment and where exactly the intermediaries who pass on our messages are located.

Obviously, referring to the comparison with communication in a public place, the undoubted loss of information confidentiality can be avoided and instead of passing by the "mouth-to-mouth method", information with written information rolled up into a ball can be used. Only will it protect us from meddlesome intermediaries of the transmission process?

The situation regarding cyberspace communication is additionally complicated by the fact that it takes place very quickly, without unnecessary delays, using communication interfaces that do not convey most details about the course of the communication process. This gives the Internet users a feeling of mono processability and directness of communication. While accessing network resources most of them have no idea about how many and what processes are implemented by intermediary devices, which results in loss of control over the whole process.

The information society, using all available tools, intensifies production of knowledge and its application. The mainstream of information society's life is in cyberspace. Its image is a reflection of the situation in the world, interpersonal relationships, people's views, emotions, issues and problems. Unfortunately, even a brief moment on any information portal is enough to see that this image is not positive. Cyberspace is at war. Individuals and organizations constantly strive to acquire as many information resources as possible, gain an edge over opponents, destroy them and control the highest possible amount of resources in cyberspace. At least for now, this concerns primarily information resources. However, activity in the virtual world has a major impact on the contemporary real world, as humanity is increasingly dependent on computer technology. It is estimated that the activity of cybercriminals brings the world economy from $375 billion to $575 billion of annual losses. It is worth mentioning that at the

same time it is unknown how many of these losses are a result of not fully legal activity of organizations from various states that conduct business activities on the Internet.

1.1. Threats and incidents related to information confidentiality security

Due to the fact that information is the most desirable good in contemporary world, there is a continuous war in cyberspace to get as much of this good as possible. The times of courtesy principles of discretion have long faded into oblivion. Today, everyone, from criminals, public benefit organizations to state authorities, use every means to illegally obtain information in cyberspace. To understand the scope of the problem, it is worthwhile to familiarize with the facts.

The Internet technique of transmitting information through intermediaries attracts numerous people willing to do this. Companies such as Google, Twitter, Facebook and many others offer their intermediary services in the process of Internet users communication for free. In return they only require "trifles" in the form of personal data of communication platforms users. To comply with the formalities, they conclude agreements with the users containing rules of disposing these data. These agreements are intended to create the image of these intermediaries as reliable, discrete and friendly providers of communication services. Unfortunately, this image is misleading. Terms of service are so extensive and twisted that even lawyers are not able to wade through their nuances effectively. In addition, service providers always give themselves the right to freely change the rules. As part of these terms, they often give themselves the right to full disposal of information entrusted to them by Internet users, who constantly affirm it by obediently clicking on the box next to *"I accept the terms of use"*. In fact, it can be stated that in such a case there is no problem of violating information confidentiality because the service provider is no longer unauthorized to access the information, as the recipient has granted this authorization to him. Unfortunately, this is not so easy. These companies' "charitable" activity in the form of connecting people is only a fraction of the scope of their operations. The main part of the process involves sharing information about us with others. This sharing is the source of colossal profits of our intermediaries. No one asks anymore what the payers for data sets are going to do with them. These transactions are not fully legal anyway, thus the parties to them do not ask one another unnecessary questions. Encouraged by impunity of such practices, some operators of communication platforms go even further and offer their clients services based on their surveillance. Facebook can be an example of such activity, as in 2014 it introduced a service allowing to remotely turn on the camera or microphone of a user's smartphone at any moment in order to explore his or her music or movie preferences [14]. The most interesting thing is that many users of this social network have agreed to it. The problem is, however, that they never really know who and why watches or eavesdrops on them.

In addition to the loss of confidentiality of our information as a result of extortion or light-heartedness in cyberspace, it leads to a great number of incidents related to permanent surveillance with the use of specialized software. There is no guise of legality here. Secret services of many countries, without any embarrassment, regularly intercept all information transmitted in ICT networks [4], from time to time raising

alarms on fraudulent Internet surveillance practices. It is worth noting here that this wiretapping does not only concern citizens of states in question, but also other countries, which in many cases of detecting such practices should result in serious diplomatic sanctions. However, that does not happen. Sanctions, not just diplomatic ones, are imposed on others who carry out such activities [3]. States agencies have received such extensive powers after 2001 that they often do not bother to choose the goals of their activity. They simply invigilate everyone and register almost everything and when they find something interesting from an operational point of view, they use it. In turn, state institutions dealing with surveillance or combatting such practices are often victims of attacks on the security of information confidentiality. It is worth to mention the 2012 incident when a hacker group called LulzSec conducted a mass wiretapping of information sent via the Internet by employees and associates of the FBI [2].

These cases could be cited endlessly. The multitude of these incidents, however, raises the question about the reasons and possible measures of confidentiality protection used in cyberspace.

2. TOOLS OF PROTECTING CONFIDENTIALITY OF INTERNET COMMUNICATION

The development of computer technology, including the Internet, is often seen as the cause of problems related to protection of confidentiality and privacy in today's world. However, the same modern technology provides a number of tools allowing for solving them. Together with its development, many rules, standards, hints of the "best practice" type or technical solutions have been developed, which should effectively help deal with the task of protecting information from unauthorized access. There are many solutions available out of many physical, organizational and technical methods of protecting information confidentiality. However, there is always the issue of possibility of using the available solutions and their effectiveness. An unequivocal conclusion about the effectiveness of individual methods can be drawn from the literature of the subject. The picture of the situation leaves no illusion: any solution to the problem of information confidentiality based on the key role of man in the process of this protection is ineffective because it is man who is almost always the weakest link in a security system. The applied system solutions using physical or organizational methods sooner or later turn out to be solutions that only serve to improve the well being of a person interested in confidentiality protection, creating the impression that he or she is safe. Technical methods operate independently from the will and intention of man. Simple, tested, properly designed and implemented ones eliminate the possibility of interference in the process of information confidentiality protection so effectively that they prove to be undoubtedly better than the best of organizational practices or solutions of physical nature.

The most effective technical solutions for the protection of information confidentiality were have been the tools developed by specialists in the field of cryptography and steganography.

Cryptographic tools dedicated to this protection are ciphers, which serve to change the form of information in such a way that even the author himself is not able to read the

content of a message. The knowledge of how to restore information to its original form is an element of authorization to ascertain its content.

In the case of steganographic solutions, where confidential information is hidden in other information, the knowledge of where the secret message is and how to retrieve it is a decisive factor for the authorization to read restricted content.

2.1. Ciphers

Ciphers are an inherent and frequently the only component of systems for protection of confidentiality in the cyberspace. They are such an important element of our world that even the United Nations in the report of one of its special employees, David Kaye, stated that due to the mass use of unethical practices violating the right to privacy by states, the use of encryption to protect information confidentiality should be an indispensable right of every human [9].

Unfortunately, many states constantly limit the use of encryption in private communication by introducing regulations according to which the application of such techniques is subject to similar restrictions as the use of firearms or other types of lethal weaponry. In addition, many countries impose export restrictions that take into account all activities related to the exchange of technical ideas from the field of cryptography. From time to time, initiatives are also taken in some countries to control the level of security of ciphers used by citizens. This is accomplished, for example, by limiting the size of cryptographic keys to such length that makes it possible to crack the cipher using specialized hardware and software, or enforcing the policy of depositing decryption keys in government agendas, or using only such ciphers that could easily be broken by specialists acting on the order of state authorities.

As one can suppose, such ideas have never aroused overwhelming enthusiasm among citizens and sometimes they have even encountered strong opposition. One of such actions was the design and make of a private cryptography package called PGP (*Pretty Good Privacy)* available on the Internet in 1993. This was the period of validity of extremely restrictive rules on the export of cryptographic solutions and therefore a 3-year-long federal investigation was conducted against the author of this software Phil Zimmermann, alleging that he had violated the federal law restricting arms trade, which led to mass protests of the Internet community and the author's emigration to Switzerland. Finally, after a number of different reorganizational actions and many attempts to discredit the PGP as a tool for protecting confidentiality and influencing the level of such protection, the package remained available for web surfers in both a commercial and free version, only offering the possibility of individual cryptographic protection of email and single files. It can now be obtained on the Internet under the name PGP or GPG. Despite many attempts to discredit it [1], the package is simple to use and considered one of the best tools for encrypting individual files and email content.

At present, only those types of tools that have a widely accepted recommendation of the expert community in the field of cryptology are used for confidentiality security in cyberspace. Currently, various solutions use mainly the AES algorithm, which since 2001 and the announcement of the global competition results has been the standard

of symmetric encryption in the world. Its resistance to breaking is, for the time being, unquestionable.

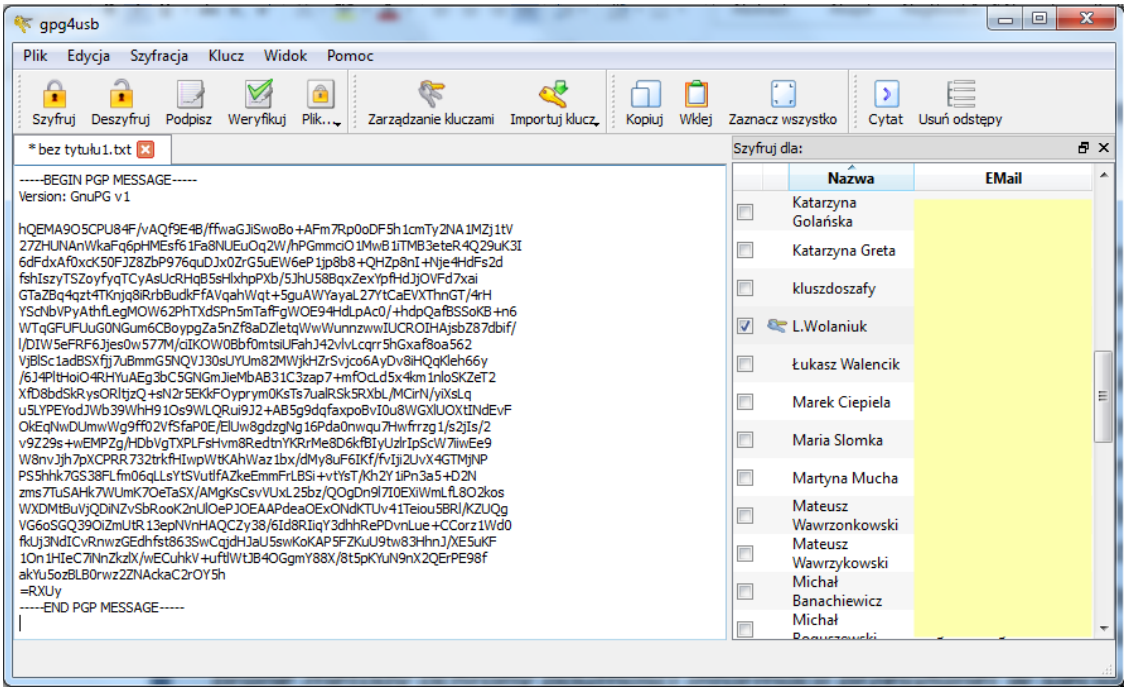

Fig. 1. The example of a text encrypted using GPG. The encrypted text is a summary of the article

Source: own elaboration

The RSA is the most popular encryption algorithm with a public key. This cipher was designed in 1977 and so far, despite its age, it has been used as a key component of many cryptographic systems. However, it is accompanied by the need for constant adaptation of the applied cryptographic keys to the present state of the art, as the effectiveness of its security is time-limited and related to the current level of research on solving the problem of product distribution of prime numbers. Moreover, it is anticipated that once quantum computers are put into use, every public-key encryption could be cracked within a few seconds. For this very reason, the development of this direction of research on encryption has been abandoned, as the US National Security Agency has clearly confirmed, declaring its intention to construct a quantum computer capable of breaking every cipher used to protect the confidentiality of Internet communication [10,13].

In modern software packages using ciphers the so-called hybrid encryption is most commonly applied, which is based on creating encrypted information packets that is a public-key encrypted information consisting of the main information cryptogram obtained with the use of a symmetric cipher and symmetric cipher key. In order to decrypt such information, one must first use a private key associated with a public key used to encrypt a packet, separate the two pieces of gained information and then decrypt the cryptogram with the information using a symmetric encryption key. Obvious-

ly, these operations are performed programmatically, without participation of the user whose only task is to use the asymmetric method keys (public key cipher).

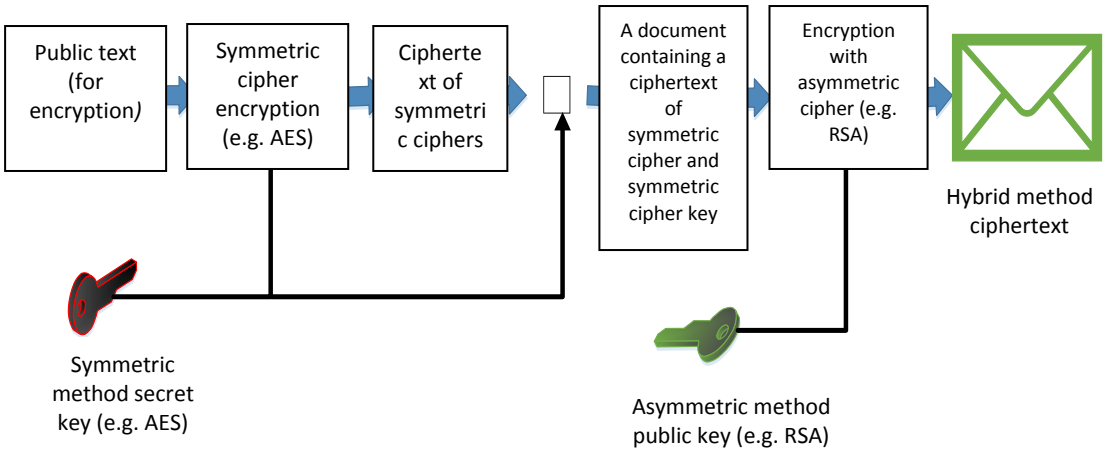

Fig. 2. The scheme of the hybrid encryption method.

Source: Own study

The problem with such encryption packages is the automation of generating the symmetric method key. Unfortunately, there is no guarantee that the applied asymmetric method key is so unique that it cannot be easily discovered. In addition, the way of generating asymmetric method keys also sometimes does not meet the security requirements. Some software developers use weak pseudorandom number generators, results of which are easily predicted or they simply apply key sets created earlier on and stored in the database. These practices significantly reduce the level of information confidentiality protection, creating grounds for suspicion of the inclusion of the so-called "backdoors" in ciphertexts, allowing unauthorized decryption of a message.

2.1.1. Cipher security

According to the Kerckoffs' principle, security of a cipher should only depend on hiding the cryptographic key and not on hiding the algorithm of its operation. During the World War II the Germans learned the accuracy of this rule, not knowing that the Poles had discovered the principle of the Enigma encryption and decryption machine (the cipher algorithm and its weak points), for the rest of the War they were convinced that confidentiality of their reports was effectively protected using this tool. Failure to consider this principle was not exclusively a German domain. At the end of the 1980s, one of the most famous cryptographers of the modern world, co-author of the RSA Ron Rivest, developed a new the algorithm of a new cipher named RC4 (used until today to, for example, protect confidentiality of WiFi networks). The cipher algorithm was not publicly disclosed to the expert environment for the purpose of analysis, but without undue delay, relying solely on the author's recommendation and the authority of the invention's author, it was directed to implementation in order to protect the confidentiality of information on the Internet. Author's heartedness was quickly punished. In 1994, an anonymous person published the cipher algorithm on the Internet, pointing out its weaknesses, which caused a shock and led to a dismay of many experts and us-

ers to panic due to the loss of confidence in the privacy tool, for example, in encrypted connections using the Netscape Navigator web browser or many other commercial products related to electronic banking. The cipher algorithm was most likely reproduced through the programmatic implementation of the RC4 using the reverse engineering method. The published cipher algorithm was called ARCFOUR, which clearly suggested the connection with the RC4. The cryptanalysts from the whole world conducted a public analysis of the "secret" cipher and found much vulnerability to breaking, which has ultimately discredited some of its implementations [14] [7].

Fortunately, the rules currently in force in the world exclude the repetition of situations described above. However, the Kerckoffs' principle still continues to operate and unambiguously identifies the person responsible for the cipher security – it is the user of the cipher, disposer of the component authorizing him or her to read the encrypted message. The security of encrypted communication depends on the user's commitment and ingenuity in the scope of secret cryptographic key protection. However, it is worth to consider how and what, if at all, influence the user has on this level of protection. Many processes related to protection of communication confidentiality in cyberspace are implemented automatically, without any involvement, control or even knowledge of the user of these processes. It therefore has no real impact on the security of hiding the key of the used cipher, which is decided on by the designer of cryptographic software. In addition, in many implementations in which the user could have an impact on, for example, the quality of the key used for encryption, operational-functional issues often lead to weakening of confidentiality protection offered by the cipher. For example, in some applications, when a user decides the value of a cryptographic key, he / she is not required to provide a random value for the full-length key, which would guarantee the effective protection of the given cipher, but only a key no longer than the nominal length specified for that cipher. In the situation when a user creates a simple key (in applications called a password for simplicity) that is shorter than required for the used cipher the software itself complements it to a full-length with a sequence which can be discovered from the content of an encryption program. This way, an attacker already knows a part of an encryption key and he or she only needs to discover the missing element. Given the fact that the system searching for passwords that is currently offered on the Internet using the method of systematic search of the collection of all potential values makes it possible to check even 300 million passwords per second [11], most cryptographic keys less than 10 characters-long and consisting of letters and digits can be discovered in a relatively short time. For example, for keys consisting of 8 lowercase Latin characters and digits (24 letters and 10 digits), the total number of possible values is 34^8 = 1785793904896, which constitutes, for instance, 6000 machine cycles, which is about 1.5 hour of work of the aforementioned system. Assuming that the machine will not have to check all possible variants of the sequence to identify a password, finding the missing part of the key will take less than an hour!

2.2. Steganography

Steganography is an art of hiding secret information in other information. The essence of its operation is to prevent a receiver unauthorized to learn the content of a message from guessing that there is additional information placed in a normally looking information message. It has been used for centuries to protect confidentiality of messages through the use of specially crafted ink, paper placement of text tags or, as during the Cold War, the use of microprint.

Together with the development of computer technology it turned out that digitally transmitted text or multimedia data often contains many excess or unused elements that can prove helpful in hiding other information. In digital technology a secret message can be hidden in a text document, picture, sound file or a movie file. On the Internet one may sometimes find portals equipped with discussion forums where for users that are not logged in the content is not fully accessible by hiding it using a white font on a white background. Text information in images is hidden in a slightly different way. Single bits of color of consecutive dots (pixels) are used, which constitute a picture. Due to the fact that modern graphic messages use mostly displays that distinguish millions of shades of colors, the use of a single bit of one pixel can result in at most a color shift of this bit by a code value of 1, which in practice is unnoticeable to a casual observer. Considering the fact that an average image today is made up of millions of pixels, it can be easily calculated that many pages of text can be hidden in it. For example, in a typical 13-million-pixel holiday photo, where each color of every bit is encoded with a value of $0 – 2^{24}$ (16777216 – average number of colors in modern digital images), over one million 8-byte characters can be hidden!

Fig. 3. The example of stenography using messages. Image files are the same size. The text of the summary of the article is hidden on the right one

Source: own elaboration

The condition for maintaining the confidentiality security of a steganographic message is hiding the fact of placing implicit content in a particular picture or sound file. It is practically impossible to determine which of them contains hidden information since a large amount of data of this kind of data is present in cyberspace. If the information

intended to be hidden is additionally encrypted beforehand, violation of confidentiality of a message is practically impossible.

There are free and commercial steganographic tools available on the web. The most popular ones are *Steghide*, *SteganographX Plus*, *Courier* or *Hide'N'Send*. Many of them have built-in encryption mechanisms for messages before they are hidden in a carrier that most often consists of pictures, though, for example, *Steghide* allows for hiding information in *jpg* image files and *wav* sound files.

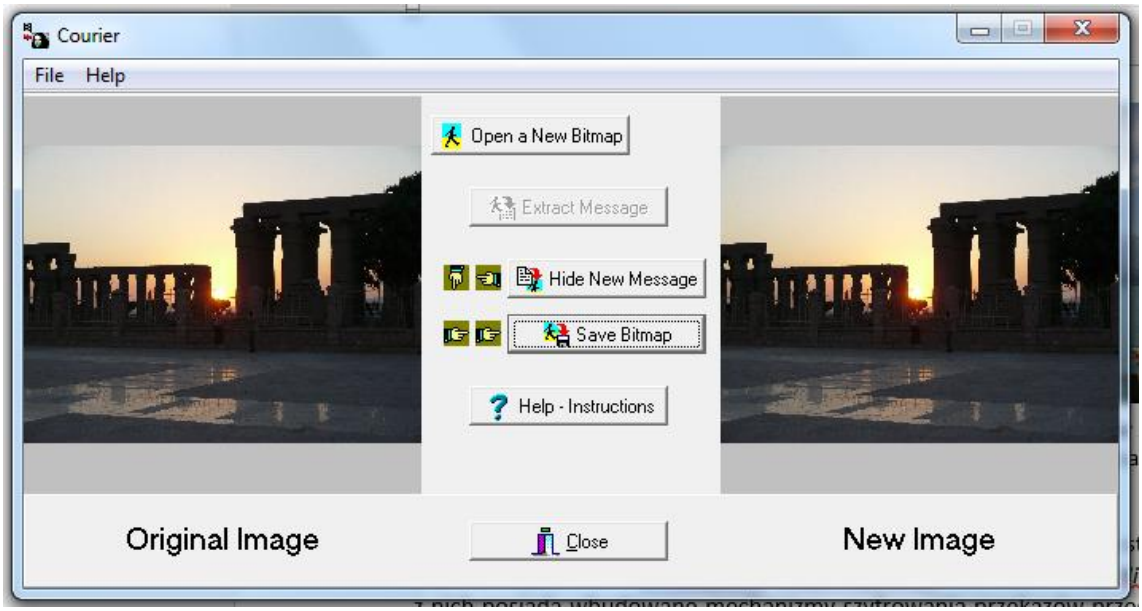

Fig. 4. The main panel of the Courier program

Source: own elaboration

Although there are also tools available on the Internet that are meant to detect hidden steganographic messages (e.g. *Stegdetect*) [11], they have a very low rate of effectiveness since their operation is based on knowledge of algorithms of steganographic tools' operation, not having enough data to detect anomalies in multimedia files. Taking into account the limit connected to the need to check all multimediafiles it is easy to observe that using steganography is a quite effective way to protect the confidentiality of digital messages.

CONCLUSIONS

The day-to-day practice proves that the majority of system safeguards for information confidentiality cannot be relied on, as they do not work properly or do not work at all. In addition, in legislative solutions, slowly but systematically, there is an increasing systemic tendency of limiting the right to information confidentiality for everyone both in cyberspace and beyond it. The justification for these changes is an increase in the level of security of the society through the control of ICT networks that are massively exploited by criminal and terrorist groups. Citizen surveillance schemes are set up without introducing at the same time unequivocal sanction regulations related to abuses in

this area. This leads to a situation where officers of services responsible for state security can with no limitations abuse the confidentiality of citizens' information without considering the views of the interested parties or courts [6]. An interesting aspect of this problem is also that the regulations allowing for the breach of information confidentiality by various services lack restrictions on the use of individual protection against such infringements. This creates an unequivocal image of the world in which, referring to the right to self-defense, care should be taken to protect the information confidentiality on an individual basis.

When we intend to send a letter in the real world, we carefully glue the envelope in order to prevent accidental disclosure of the content to unauthorized persons. We do not believe the notion resulting from the universally applicable law that protects our correspondence from unauthorized access. It would also be naive to believe that if we insufficiently secured an envelope with our letter the institution responsible for sending or delivering it would repair it on our behalf. The same logic should apply when transmitting information in cyberspace. When sending any information, such as an email or text message, via the Internet we should ensure that its confidentiality is safeguarded. It should not be expected that a telecom operator or systemic mechanisms of information security built into a browser, computer networks or data exchange servers will do it for us. Individual confidentiality protection packages should be a basic element of every Internet user's equipment. It seems that such packages, in the form of dedicated software enabling a personalized approach to the issue of confidentiality protection, can obligatorily equip every user of cyberspace. a good option would be popularization of solutions based on the combination of cryptography and steganography. While in the case of cryptography, there is virtually no choice and one should rely on the use of tested and standard symmetric cryptography solutions (e.g. AES) or public-key cryptography (e.g. RSA), in relation to steganography the possibility to choose carriers to hide information should be greatly expanded and modified. There should be solutions available allowing to hide information messages in any kinds of data or information processes, without embedding in them information about the type of hiding algorithm used. The user is to decide what security measure to apply in order to protect the information transmitted. It seems that in the case of these systems all-mechanisms related to full automation of the process must also be avoided, as there is a risk of losing control over the process due to the implicit nature of many operations implemented in it. It is up to the individual concern to choose whether he or she only needs cryptographic protection or a combination of many methods of confidentiality protection. He or she should initiate the security process, select security measures and specify how they should be used. However, a minimum of knowledge and skills is required. As in many other areas, without deep reflection on the problem, mastering several skills in the field of security measures implementation and the awareness of the rules of ICT security works, the problem of interfering with confidentiality communication in cyberspace will still grow.

REFERENCES

1. Angwin J., The World's Email Encryption Software Relies on One Guy, Who is Going Broke, [online] [access: 15.11.2016]. Available on the Internet: www.propublica.org.
2. Arizona Police Confirm 2nd Hack on Officers' Email, [online] [access: 15.11.2016]. Available on the Internet: http://www.foxnews.com /tech/2011/06/29/.
3. Documents Reveal NSA and GCHQ Efforts to Destroy Assange And Track Wikileaks Supporters – TRNN Transcript, [online] [access: 20.11.2016]. Available on the Internet: http://michaelratnerpresente.com.
4. Edward Snowden: Leaks that exposed US spy programme, [online] [access: 20.11.2016]. Available on the Internet: http://www.bbc.com/ news/world-us-canada-23123964.
5. [online] [access: 25.11.2016]. Available on the Internet: http://www.polskieradio.pl /39/156/Artykul/256306,Cud-nad-Wisla-czyli-Bitwa-Warszawska.
6. [online] [access: 15.11.2016]. Available on the Internet: http://www.rp.pl/Dane-osobowe/304089959-Panoptykon-sluzby-czesciej-siegaja-po-dane-internetowe-rzadziej-po-telefoniczne.html.
7. [online] [access: 15.11.2016]. Available on the Internet: http://www.wikiwand.com /en/RC4.
8. International standard ISO/IEC 27000. Information technology — Security techniques — Information security management systems - Overview and vocabulary, 3rd edition, 2014 p. 2.
9. [online] [access: 15.11.2016]. Available on the Internet: www.ohchr.org/Documents/Issues/Opinion/.../MLRC.doc, 2015.
10. NSA 'developing code-cracking quantum computer', [online] [access: 15.11.2016]. Available on the Internet: http://www.bbc.com/news/technology-25588605.
11. Pejas M., Techniki ukrywania informacji w danych cyfrowych i narzędzia je wykrywające, *Przegląd bezpieczeństwa wewnętrznego. Technika, technologia i bezpieczeństwo informatyczne*, no. 1/09, p. 105-114
12. Praca zbiorowa, *Biblia Tysiąclecia - Pismo Święte Starego i Nowego Testamentu*, wydawnictwo Pallottinum, 2014, rozdział: Księga Rodzaju
13. The NSA Has Quantum Fever, [online] [access: 15.11.2016]. Available on the Internet: http://motherboard.vice.com/read/the-nsa-has-quantum-feve.
14. Wobst R,. *Kryptologia*. *Budowa i łamanie zabezpieczeń*, Wydawnictwo: RM, 2002. s.218

BIOGRAPHICAL NOTE

WOLANIUK Leszek - Lt. Col. (ret.) DSc. Eng. Assistant Professor in the Institute of Safety Engineering at the General Tadeusz Kosciuszko Military Academy of Land Forces in

Wroclaw. He is a graduate of the Department of Cybernetics at the Military Academy of Technology in Warsaw. He defended his doctoral dissertation at the Faculty of Electronics at the Wroclaw University of Technology. He specializes in information security and cryptology.

HOW TO CITE THIS PAPER

Wolaniuk L., (2017) – Selected problems of security of information confidentiality in cyberspace. *Zeszyty Naukowe Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki Journal of Science of the gen. Tadeusz Kosciuszko Military Academy of Land Forces*, 49 (4), p. 194-207, DOI: 10.5604/01.3001.0010.7228