

2011, 26(98) pp. 80-87

2011, 26(98) s. 80-87

The application of cryptography and steganography in the integration of seaport security subsystems

Zastosowanie kryptografii i steganografii w integracji podsystemów bezpieczeństwa informacyjnego portów morskich

Evgeny Ochin¹, Larisa Dobryakova², Zbigniew Pietrzykowski¹, Piotr Borkowski¹

¹ Maritime University of Szczecin, Institute of Marine Technology Akademia Morska w Szczecinie, Instytut Technologii Morskich 70-500 Szczecin, ul. Wały Chrobrego 1–2,

e-mail: e.ochin@am.szczecin.pl, z.pietrzykowski@am.szczecin.pl, p.borkowski@am.szczecin.pl ² West Pomeranian University of Technology, Faculty of Computer Science and Information Technology Zachodniopomorski Uniwersytet Technologiczny, Wydział Informatyki

71-210 Szczecin, ul. Żołnierska 49, e-mail: larisa555@gmail.com

Key words: seaport security, information systems, cryptography, steganography

Abstract

The integration of seaports security subsystems aims at a development of the complex connection of local seaport security subsystems into a uniform overall security system. This requires the use of wire and wireless telecommunication infrastructure of the seaport territory, port basin and ships attributed to that port. These authors consider the application of cryptography and steganography in integration of seaports security subsystems.

Słowa kluczowe: bezpieczeństwo portów morskich, systemy informacyjne, kryptografia, steganografia

Abstrakt

Integracja podsystemów bezpieczeństwa portu morskiego ma na celu opracowanie kompleksowego połączenia podsystemów lokalnych w jeden system globalny bezpieczeństwa. Wymaga to wykorzystania przewodowej i bezprzewodowej infrastruktury telekomunikacyjnej terenu portu, akwenu portowego oraz statków w porcie. W artykule rozpatruje się zastosowanie wybranych metod kryptografii i steganografii w integracji podsystemów bezpieczeństwa informacyjnego portów morskich.

Introduction

Traditionally understood, system integration consists in designing, construction, support and audit of serviceability of information infrastructure of an organization. Unfortunately, at present there is no **uniform standard international terminology** in the field of the system integration of security subsystems in organizations, although there exist standards of information security.

In 2006 the International Committee on Development of Information Security Standards (ISO/IEC JTC 1/SC 27/WG 1) made a decision to

consolidate all previous standards in the field of information security under one serial number ISO/IEC 27000 "Information technology. Security techniques. Code of practice for information security management". This standard determines requirements to control systems of information security, risk management, metrics and measurements. It also contains a manual on the introduction of ISO/IEC 27000, which provides:

 an overview of an introduction to the entire ISO/IEC 27000 family of Information Security Management Systems (ISMS) standards; a glossary of fundamental terms and definitions used throughout the ISO/IEC 27000 standards. Information security, like many technical subjects, evolves a complex range of terminology. Relatively, few authors take the trouble to define precisely what they mean, an approach which is unacceptable in the standardization as it potentially leads to confusion and devalues formal assessment and certification. As with ISO 9000 and ISO 14000, the base "000" standard is intended to address this.

Integration of seaport security subsystems

With reference to designing of seaports security systems the term "system integration" is understood as follows below.

The complex system integration of the seaport security subsystems is a development of complex decisions on linking local security seaport subsystems into a uniform global system of security based on the wire and wireless telecommunication infrastructure at the seaport territory and water area, and also onboard ships attributed to the port.

The integration of the diverse security seaport subsystems may be carried out with the use of existing information technologies [1]:

- Ethernet,
- TCP/IP,
- WiMAX Worldwide Interoperability for Microwave Access.

The complex system integration of seaport security subsystems (SSS) will consist of the following stages [2, 3]:

- 1. The system integration of territory protection subsystems (TPS): acoustic TPS, vibration TPS, magnetic TPS, visual TPS;
- 2. The system integration of protection and fire signal subsystems of office buildings, ware-house etc.;
- 3. The designing system of visual observation outside the seaport territory and water area with a capability of long-time data storage;
- The system integration of water area protection subsystems (WAPS): acoustic WAPS, hydroacoustic WAPS, vibration WAPS, magnetic WAPS, visual WAPS, thermal video WAPS, radar WAPS;
- 5. The designing of information display system of protection subsystems to the uniform control station;
- 6. The designing of the personnel and motor transport access within the seaport territory;
- 7. The designing of ship access within seaport water area;

- The designing of multilevel differentiation of personnel access to rooms and network resources;
- 9. The system integration of seaport security subsystems considering:
 - integrated Physical / Logical Access,
 - authentication,
 - data integrity.
 - security of storage and data transfer.

The full-range consideration of all listed above stages of system integration of the seaports security subsystems within the framework of one article is impossible. While issues connected with the integration of subsystems mainly concern information technologies, the system security may be implemented principally by using methods and tools of cryptology, and refers to: authentication, data integrity, security of storage and data transfer (stage 9). In this article the principles of cryptology, especially cryptography and steganography and their application in the system integration of the seaports security subsystems is considered.

Cryptology in system integration

The cryptology (kryptos – secret, logos – science) deals with issues of information security of storage systems and data transfer. Cryptology embraces cryptography and cryptanalysis, as well as steganography and stegoanalysis (Fig. 1). Cryptography, the science of using mathematics to encrypt and decrypt data, enables storing sensitive information or transmit it across insecure networks (such as the Internet), so that it cannot be read by anyone except the intended recipient. Cryptanalysis is the science of analyzing and breaking secure communication **without knowledge of the keys**. Cryptanalysts are also called **attackers**.



Fig. 1. The basic areas of cryptology Rys. 1. Główne działy kryptologii

Selected cryptology methods and systems where investigated (examined) in view of their use (application) in integration of seaport security subsystems.

Symmetric-key encryption

In symmetric-key encryption, also called secretkey encryption or conventional cryptography, one key is used both for encryption and decryption. The key represents some chain of bits used for encryption / decoding of texts [4]. The addressee (for example, port or one of the ships) generates a private (confidential) key. The copy of this key is transferred to all potential senders of messages (for example, to all ships of the fleet), using confidential technologies of data transfer (Fig. 2).

The senders (the ships and/or seaport) cipher the information with the help of a private key (Fig. 3), transfer the addressee the ciphered information (to the port and/or to the ships), and CS deciphers the message with the help of the same confidential key (Fig. 4). The main shortcoming of this technology is the process of key confidential transfer to senders, i.e. key transfer requires the use of some cryptosystems.



Fig. 2. CS - Cryptographic System of the seaport or one of the ships

Rys. 2. System krytpograficzny portu morskiego lub jednego statku



Fig. 3. Encryption of the cleartext Rys. 3. Kodowanie tekstu wejściowego



Fig. 4. Decryption of the ciphertext Rys. 4. Rozszyfrowanie zakodowanego tekstu

Public-key cryptography (PKC)

In PKC the cryptographic system of a port generates two mathematically connected keys (Fig. 5), one of which the seaport declares as a public key and transfers this public key to all potential senders (the fleet ships), using open (unclassified) technologies of data transfer, and the other key receives the status of a private key and is stored in the place securely locked to avoid unauthorized access [4].

The seaport has generated 🔪 🔪	The seaport has transferred	
two keys: private 🖿 and public 🖛 🖊	the public key to the ships 🖭	- /

Fig. 5. The generation and transfer of keys Rys. 5. Generacja i przekazanie kluczy

The sender ciphers the information with the help of the public key (Fig. 6), which is accessible to all parties concerned, but only the addressee can decipher this message as only they have the private key (Fig. 7). Cryptographic PKC systems use irreversible or unilateral functions that possess the following property: at a preset value x it is rather simple to calculate value f(x); however, if y = f(x)there is no simple way of calculating the value x. That process is irreversible, where irreversibility is understood as practical impossibility to calculate the return value using modern computing means within a foreseeable interval of time.



Fig. 6. The ships cipher and send messages in the seaport with the help of the public key

Rys. 6. Statki szyfrują i wysyłają wiadomości do portu morskiego za pomocą klucza publicznego



Fig. 7. The seaport decodes and reads texts of messages with the help of the private key

Rys. 7. Port morski rozszyfrowuje i czyta teksty wiadomości za pomocą klucza prywatnego

To guarantee reliable protection of information, systems with the public key have to meet two obvious requirements:

- 1. Transformation of the initial text should be irreversible (Fig. 8) and its restoration on the basis of the public key should be impossible;
- 2. Definition of the private key on the basis of public key also should be impossible at the modern technological level. Thus, the exact bottom rating of complexity (quantity of operations) disclosing of the code is desirable.



Fig. 8. The irreversible transformations in cryptographic systems with a public key

Rys. 8. Nieodwracalne zmiany w systemach kryptograficznych z kluczem publicznym



Fig. 9. The basic applications of cryptographic systems with a public key $% \left({{{\rm{B}}_{{\rm{B}}}} \right)$

Rys. 9. Podstawowe aplikacje systemów kryptograficznych z kluczem publicznym

The encryption algorithms with a public key have received a wide circulation in modern information systems. So, the RSA algorithm became the actual world standard for open systems and is recommended by the International Consultative Committee for Telegraphy and Telephony. The PKCs are more labour-consuming than traditional cryptosystems. Therefore, in practice (Fig. 9) it is rational only to distribute the keys with the help of PKC as the volume of information is insignificant, and then with the help of symmetric cryptographic system to carry out an exchange of large-volume files.

The cryptographic RSA system

One of the most popular PKC systems is RSA [4], based on the fact that the finding of big simple numbers is carried out easily, but decomposition on a multiplier of two such numbers product is impracticable. It is possible to show that disclosing a RSA code is equivalent to such decomposition. Therefore, for any key length it is possible to identify the bottom rating of operations number for disclosing the code, and in view of productivity of modern computers to estimate the necessary time.

Now, the RSA algorithm is actively realized as independent cryptographic products, for example, in the sensational PGP program [5, 6], and as builtin units in popular applications, for example in browsers MS Internet Explorer and Netscape Communication.

The cryptographic system of Taher ElGamal

The ElGamal method represents the cryptographic system proposed in 1984 [4]. The ElGamal method underlies standards of the electronic digital signature in the USA and Russia. The given system is alternative to RSA and at an equal value of the key provides the same cryptographic resistance, however there is no general opinion concerning the preferability of this method. The ElGamal method is based on the discrete logarithm. If raising the number in a degree in a final field is easy enough, to restore the argument on value (that is to find the logarithm) is rather difficult. The algorithm of digital signature DSA developed by NIST and being part of the DSS standard is based on the method.

The cryptographic PGP system

The **PGP** (Pretty Good Privacy) allows to carry out encryption operations and the digital signature of data. Developed by Philipp Zimmerman [5, 6] in 1991, PGP represents a hybrid system, which includes an algorithm with the public key and the usual algorithm with a private key that gives high speed, characteristic for symmetric algorithms and essential convenience, characteristic for cryptography with the public key. From the point of view of the user PGP behaves as a system with the public key.

The PGP encryption is carried out as consistent hashing, compression of the data, encryption with a symmetric key, and encryption with a public key and each stage can be carried out by one of several supported algorithms. The symmetric encryption is made with one of five symmetric algorithms (AES, CAST5, TripleDES, IDEA, Twofish) on a session key. The session key is generated with the use of the cryptographic proof generator of random numbers. The session key is ciphered by the public key of the addressee using RSA or ElGamal algorithms (depending on the type of key of the addressee). Each public key corresponds to a login name or an e-mail address.

The PGP was initially developed for encryption of emails on the side of the client, but since 2002 it has also included the encryption of hard disks, files and folders, batch file transfer, protection of files and folders on network storehouses and now also encryption HTTP of searches and answers on the server side (mod openpgp) and the client (Enigform). Programs for the client side are incorporated into family PGP Desktop (includes PGP Desktop Mail, PGP Whole Disk Encryption and PGP NetShare).

Encryption of dataflows

Modern IT uses technologies, which require the transmission of particularly large volumes of information. This problem arose comparatively recently with the appearance of multimedia facilities and networks with high bandwidth, providing multimedia communications. Because voice transmission, graphics and video information in many cases require confidentiality, there is a problem of encoding enormous information arrays. For interactive teleconference systems, conducting audio and/or visual communications, such encoding must be carried out in real time and be transparent for users.

The continuous message (dataflow)	The dataflow coder with a public key 🖦	The ciphered dataflow
--------------------------------------	--	-----------------------

Fig. 10. The seaport with the help of a public key codes the dataflow and sends it to ships $% \left(\frac{1}{2} \right) = 0$

Rys. 10. Port morski za pomocą publicznego klucza koduje potok danych i wysyła go do statków



Fig. 11. The ship with the help of a private key decodes the dataflow $% \left({{{\rm{D}}_{{\rm{B}}}} \right)$

Rys. 11. Statek za pomocą klucza prywatnego rozszyfrowuje potok danych

Stream encoding is most widespread (Fig. 10). In the systems with stream encoding the PKC does not wait till a transferrable message ends, and at once carries out its encoding and transmission. The example of stream encryption standard is RC4.

Another method of stream encoding is the encoding of blocks: the fixed volume of information (block) accumulates, and then, transformed by a cryptographic method, is passed in a communication channel.

Electronic digital signature

A major benefit of public key cryptography [4] is that it provides a method for employing electronic digital signatures (EDS). Digital signatures enable the recipient of information to verify the authenticity of the information origin, and also verify that the information is intact. Thus, public key digital signatures provide authentication and data integrity. A digital signature also provides non-repudiation, which means that it prevents the sender from claiming that he or she did not actually send the information. These features are every bit as fundamental to cryptography as privacy, if not more.

As a rule, the EDS scheme includes in itself the algorithm of generation of user's key pairs, function of calculation, and also function of signature verification. The calculation function of signature on the basis of document and private key actually calculates a signature, but the function of signature verification checks whether this signature and the public key correspond to the document.

The sender codes a message by the private key (Fig. 12).



Fig. 12. The seaport ciphers the message with the help of the private key

Rys. 12. Port morski szyfrowuje wiadomość za pomocą klucza prywatnego

Using the public key a recipient can decipher a message and make sure that it was ciphered indeed by the proprietor of the private key (Fig. 13). In all its versions PGP supports the certificates of the public keys and easily recognizes a substitution or random errors of transmission. However, it is sufficiently difficult to create a certificate protected from modification, because only the integrity of certificate is here guaranteed after its creation.



Fig. 13. The ship reads the message with the help of the public key

Rys. 13. Statek odczytuje wiadomość za pomocą klucza publicznego

Besides, users must also check that the public key in a certificate indeed belongs to the sender. From the first versions there are PGP products which include in itself the internal scheme of the certificates verification, named web of trust. The set pair "name of user – public key" can be signed by the third person, certifying accordance of the key and proprietor.

It is necessary to understand the difference between an electronic digital signature and the message code authenticity, in spite of the similarity of their tasks (assuring the document integrity and impossibility of refusal from authorship). EDS algorithms belong to the class of asymmetric algorithms, while the codes of authenticity are calculated on symmetric charts.

Steganography

Steganography is a science of such organization of hidden data communication at which the fact of data communication disappears. This makes it different from cryptography, which hides the meaning of a message, but does not hide the message itself. In computer steganography two main file types exist: the stego-message (the secret message) and the container -a file which is used for concealment in it of the stego-message. The initial state of the container without hidden information is a container-original, and the final one, when it already contains a stego-message is a container-result. Images, sound, video files are frequently used as container-original files. Embedding of the stego--message in the image is accompanied by some distortions, but the character of distortions should be minimal. The viewer should not notice deterioration of the container-original data.

One known method of steganography [7, 8] which uses multimedia files is the substitution of Least Significant Bits (LSB) of the container by the corresponding stego-message in coordinate area of the container or in the field of its spectrum.

Requirements for stego-systems:

- Stego-transformations must bring minimal distortions into the container;
- Stego-system should be constructed in such a way that only the owner of stego-key can read a stego-container message built in and to be aware of the fact of hidden message existence;
- The high reserve in the passing of a message and the indomitability of the secret message at possible distortions of the container, including cases of evil intent.

As meeting all requirements is impossible, depending on the purpose of using steganography, separate requirements are satisfied. If confidential information transfer is to be done, then protecting the fact from being discovered is a priority, and in the case when information about copyright is inserted, it is important to protect the information from changes or elimination.

Steganography in system integration

In steganography there are two areas of application:

• steganography can be used for hiding transmission, storage and treatment of confidential information, intended for the further receipt by a number of persons. In that case the purpose is to prevent detecting a message by third parties;

- steganography can be used for the identification of copyright on multimedia files:
 - Watermarking. Digital watermarks are used for securing copyrights or property rights on digital representations, pictures or other creative works;
 - Fingerprinting. Inside a multimedia file a unique identifier is inserted as a determiner of the copy owner. This identifier allows to copy-protect that multimedia file or software and prevent distribution without license;
 - Captioning. Storing the diversely presented information in one piece on purpose.

The human sense organs are not able to reliably distinguish insignificant changes in files thus modified. According to the principle of hiding information, the methods of computer steganography are mainly divided as follows:

- methods of direct insertion: surplus informative environment is used in spatial (for an image) or temporal (for a sound) area and consists in embedding bits of secret report in an unimportant part of the container;
- spectral methods: to hide information, these methods use spectral presentations of environment elements of the environment which information is built into;
- methods based on text properties;
- methods using the features of computer formats: these methods are simple in realization and frequently do not require special software. The simplicity of realization turns around the simplicity of discovery; however, these methods can be used when malefactors do not suspect the presence of hidden information.

Messages can be hidden in all types of files: text, graphic, voice, video, in headings of network protocols and others [9].

Least Significant Bits

One known method of steganography using multimedia files is the substitution of Least Significant Bits (LSB) of the container by the corresponding stego-message. The frequency of these methods results from their simplicity and ability to hide sufficiently large volumes of information in relatively small files.

The methods of partial replacement of the Least Significant Bits include: method of pseudocasual interval, method of pseudocasual transposition, method of the sectional hiding. In these methods message bits are built selectively, not in every file bit, in accordance with the rules described in the relevant algorithm.

The group of message-building algorithms to be worked out for audio and image files on the basis of LSB modification make use of principles of rank filtering, such as [7, 8]: algorithms on the basis of median filtering, of double rank filtering and of triple rank filtering. The basic element of stegomessage introduction is the rank filter of the least significant bits of the container, allowing to modify the container LSBs and, simultaneously, build a message. The distinctive feature of these methods is that the message introduction is accompanied by an insignificant distortion of the container and that such distortions of the container are possible without inserting stego-message bits in it.

To work out the method of partial LSB replacement with the use of a pair of containers we need the method of message building in multimedia data based on two containers LSB analysis, methods on the basis of additional bit bringing in multimedia data. The advantage of such methods is their big resistance to unauthorized reading by third parties.

Discrete Cosine Transform

There are a few methods of image presentation in the spectral area, using as the container Discrete Cosine Transform (DCT), Discrete Fourier Transform, Discrete Wavelet Transform (DWT) and some others [10]. Similar transformations can be applied to separate parts of an image, or to the whole image. The most widespread method of hiding confidential information in the area of frequency is the relative replacement of DCT coefficient values: an image is divided into blocks, with a DCT applied to each. Each block is intended for hiding one bit of data. The equally common method of replacement of DWT coefficients is based on the modification of defined values of coefficients in the matrix of high-frequencies of the image.

The methods of hiding information are widespread in texts, in their linguistic, syntactic and semantic layers. In the linguistic method a message is built by manipulating the character spacing. The methods of changing punctuation, structure and style of a text belong to the syntactic methods of text steganography. Semantic methods use the ambiguity of grammatical form, for example, two synonyms determine the values of hidden bits and use them in the text in accordance with the bits of the built in message. A quantitative evaluation of firmness of the steganography system of defense against external influence is an intricate problem, and in practice is usually implemented by methods of system analysis, mathematical simulation or experimental research.

As a rule, professionally developed stego-system provides the model of defense, which solves two basic tasks: hiding the fact that there is protected information and blocking of unauthorized access to information, carried out by electing the proper method of hiding the information. Preliminary cryptographic defense (encoding) of the hidden information can be as an additional level of defense.

Stegoanalysis

Along with direct formulation of reports typical of steganography, there is **stegoanalysis**, which encompasses methods for finding out whether hidden information has been embedded into a transferrable message or not.

Methods of stegoanalysis are divided into universal and private (applied only to a separate steganographic algorithm). Most stegoanalysis methods make use of a mathematical model of the container and search for anomalies characteristic for the inserted message. There is a number of methods based on different mathematical models of the process of steganography. As a rule, stegoanalysis gives probabilistic results (probability of the presence of a hidden message in a container), and only sometimes the exact answer. After some of the hidden information is extracted from the file containing it (if it is necessary) its further decoding may be successful.

Modern steganographic systems include cryptographic subsystems by submitting by itself the most powerful instrument of concealment and defense (Fig. 14).



Fig. 14. A modern steganographic system includes cryptographic subsystems

Rys. 14. Współczesny system steganograficzny zawierający podsystemy kryptograficzne

Conclusions

The comprehensive system integration of seaport security subsystems is an intricate problem. It requires the linking of local seaport security subsystems in the single global seaport security, preceded by comprehensive analysis of existing methods of cryptology. The choice of a particular system must meet formal criteria of optimization. Unfortunately, standard methods of estimating the cryptographic and steganographic system efficiency are not available. Our claim in the conclusion is that the modern designing of such systems is rather an art than formal procedure of engineering design.

References

- 1. OCHIN E., GUCMA L., GUCMA M.: Magneto-Acoustic Seaports Security Systems: State of the Art. Scientific Journals Maritime University of Szczecin, 2011.
- 2. Rbtec Electronic Security Systems, http://rbtec.com.
- 3. Centrum Techniki Morskiej, http://www.ctm.gdynia.pl.
- 4. SCHNEIER B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C. Second Edition, 2008.
- 5. How PGP works, http://www.pgpi.org/doc/pgpintro.
- 6. PGP Corporation, http://www.pgp.com.

- DOBRYAKOVA L., OCHIN E.: Wbudowanie Cyfrowych Znaków Wodnych (CZW) w dane medialne na podstawie filtracji typu mediana. Materiały VI Konferencji Międzynarodowej "Analiza, prognozowanie i sterowanie w systemach skomplikowanych", Sankt-Petersburg, Rosja, 2005, 223–236.
- DOBRYAKOVA L., OCHIN E.: Architektura procesorów filtracji medianowych w systemach sterowania o dużej szybkości działania i o wysokiej niezawodności. Materiały konferencyjne Konferencji Międzynarodowej "Elektrodynamika techniczna, wrzesień, Kijów", Ukraina, 2005, 69–70.
- DOBRYAKOVA L., OCHIN E.: Przegląd metod i algorytmów steganografii komputerowej. Rocznik Informatyki Stosowanej Wydziału Informatyki Politechniki Szczecińskiej, No. 9, Szczecin, Polska, 2005, 115–122.
- DOBRYAKOVA L., OCHIN E.: The 2D-steganography method in the spatial-frequency area. 14th International Conference on Advanced Computer Systems, 15–17 październik, Międzyzdroje, Polska, 2008, 378–381.

Recenzent: prof. dr inż. Jerzy Sołdek Zachodniopomorski Uniwersytet Technologiczny w Szczecinie