I T H E A

International Journal

INFORMATION THEORIES & APPLICATIONS

2009 Volume 16 Number 2

International Journal
INFORMATION THEORIES & APPLICATIONS
Volume 16 / 2009, Number 2

IJ ITA is official publisher of the scientific papers of the members of the ITHEA® International Scientific Society

IJ ITA welcomes scientific papers connected with any information theory or its application.

IJ ITA rules for preparing the manuscripts are compulsory.
The **rules for the papers** for IJ ITA as well as the **subscription fees** are given on *www.ithea.org* .
The camera-ready copy of the paper should be received by http://ij.ithea.org.
Responsibility for papers published in IJ ITA belongs to authors.

General Sponsor of IJ ITA is the **Consortium FOI Bulgaria** (www.foibg.com).

International Journal "INFORMATION THEORIES & APPLICATIONS" Vol.16, Number 2, 2009

Printed in Bulgaria

Edited by the **Institute of Information Theories and Applications FOI ITHEA®**, Bulgaria,
in collaboration with the V.M.Glushkov Institute of Cybernetics of NAS, Ukraine,
and the Institute of Mathematics and Informatics, BAS, Bulgaria.

Publisher: **ITHEA®**
Sofia, 1000, P.O.B. 775, Bulgaria. www.ithea.org, e-mail: info@foibg.com

ISSN 1310-0513 (printed) **ISSN 1313-0463 (online)** **ISSN 1313-0498 (CD/DVD)**

INVESTIGATION ON COMPRESSION METHODS USED AS A PROTECTION INSTRUMENT OF FILE OBJECTS

Dimitrina Polimirova, Eugene Nickolov

Abstract: This report examines important issues related to different ways to influence the information security of file objects, subjected to information attacks by the methods of compression. Accordingly, the report analyzes the relationships that may exist between selected set of known by the moment of exploration attacks, methods and objects.

A methodology for evaluation of information security of objects exposed to attacks is proposed. This methodology reports the impact of different methods of compression which can be applied to these objects. A coefficient of information security for each relation attack—method—object is created. It depends on two main parameters TIME and SIZE, which describe, respectively, the attack and the object. The parameters are presented as two separate relations variables before and after the impact of methods of compression.

Since one object can be processed by more than one method of compression, different criteria and methods are used for evaluating and selecting the best method of compression with respect to the information security of the investigated objects. An analysis of the obtained results is made. On this basis are made recommendations for choosing methods of compression with the lowest risk with respect to the information security of file objects, subjected to information attacks.

Keywords: Information Security, Information Attacks, Methods of Compression, File Objects, Co-efficient of Information Security, Risk Assessment.

ACM Classification Keywords: D.4.6 Security and Protection: information flow controls

1. Introduction

The development of information systems and technologies are increasingly expanding need for processing, transferring and saving of volume sizable information flows, which are in network TCP/IP environment. These information flows in the form of file objects, are subject of non-stop attacks according to their information security, which determines the significant necessity for research of methods and means for their protection.

A common strategy for the protection of the file objects could include applying of methods of compression to objects to achieve decrease in the size of information flow. In addition, the use of password with fixed minimum and maximum length can be used. The possibility for encryption of objects, which are preliminarily compressed and protected by password, can be included as the last stage of the strategy for protecting.

Within the framework of mentioned above possibilities for investigations can be estimated that is expediently to investigate this problem on separate stages.

For the purposes of this paper the following reservation can be made: it is enough to investigate only the influence of compression methods on objects exposed to one or more attacks, as the difference in their behavior before and after the attacks when standard and not corporate (government) requirements are used, is taken into consideration.

Since the 70-th of XX century the problem for security and protection of information flows has drawn developers' and constructors' attention in the area if information technology [5]. With the first malattack in the 60th of last century [39], a progress in the area of object protection is observed and requirements for information security of objects are increased. Later the problem for creation of maximum protection for information flows arisen.

This cause the necessity to conduct targeted research to clarify and successfully solving various tasks related to improving security in the processes of transferring, processing and storing of different types of information flows. Research on methods to enhance the information security of different types of file objects, became topical.

Information flows subjected to different attacks, are characterized with their large volume size. Different methods for compression were developed and their use became necessity in order to reduce their size. Compressing objects, however, may be used as a means of increasing their security.

2. The Problem

2.1. Actuality

The aim that can be placed within this paper is related to the investigation of publicly known by the moment of exploration information attacks, methods of compression and file objects.

The main hypothesis is linked with the ability to analyze and evaluate the effectiveness of methods of compression, applied as e means to protect these objects from attacks.

The approach for achieving the aim in accordance with the basic hypothesis is to use matrix transformations, applied on initially created base of relations between attacks, methods and objects.

Future analyses and investigations can be carried out in the direction of precise planning of the economic costs when customizing the security policy of different configurations of computers, systems and networks.

Investigation can be carried out also in cases of government computers, systems and networks, where encryption has a significant impact on information flow, especially when this process is applied to the already compressed objects.

2.2. The goal and main task

The investigations, which can be planned, have to be related to the analysis of the condition and perspective for development of known information attacks, methods of compression and file objects. Their scientific generalization in the form of three-way relation is necessary because only in their mutual relation the best analysis and thus the best decisions with respect to the effectiveness of methods of compression applied as a means to protection the file object from information attacks, can be achieved.

Main goal: research and analyze the change in the information security of file objects located in a TCP/IP environment, subject to information attacks, recording the impact of methods of compression.

Therefore, **the main tasks** resulting from the above defined purpose are as follows:

1) to propose a method for reducing *maximum* three-way relationships among certain attacks, methods and objects to *real* three-way relationships that can exist among them;
2) to propose a methodology for evaluation of information security of an object under attacks by recording the effect of the applied method of compression. Furthermore, using this methodology, the task is to define the methods of compression achieving the highest values of the coefficient of information security for each object for a respective attack, and for all objects for respective attacks;
3) to propose a procedure for selecting methods of compression with the lowest risk with regards to the coefficient of information security of the respective objects for all attacks;

4) to conduct experiments proving the accuracy of the approach that entails the use of matrix transformations applied to an initially created base of two-way relationships among attacks, methods and objects which are to be transformed into attack-method-object three-way relationships.

2.3. Work definitions

For the aim of this paper the following work definitions are proposed [6], [26],[35]: 1) as information security we will note the protection of the information in an object from a random or purposeful access aimed at reading, transferring (coping), modifying or destroying the information in it; 2) as file object we will note the whole interconnected data or program records, saved under one name (http://www.answers.com/file); 3) as information attack we will note an attack in connection with the content of the current information stream; 4) as method of compression we will note the procedure for data encoding aimed at shrinking their volume during the processes of transfer and storage; 5) as a data compression we will note transforming of input data into output codes. The decision for the correspondence *input data—output codes* is based on preliminarily selected model. In case of effective compression, the obtained flow of codes is smaller in volume than the input data, but even though the compression is not effective, the file object will have a better protection against different attacks, because the output data will be presented by codes.

During the investigation of the information security of file objects, they will be exposed to different information attacks. The attacks have been provisionally divided into malware and malattacks. In case of malware the direct participation of a user at the moment of the attack is missing, while in case of malattack the user's presence is required [30], [22].

When investigating the methods of compression, applied not only for reducing the object's size, but also for protecting them from information attacks, they will be divided in two main categories: lossless methods of compression and lossy methods of compression. Lossy methods of compression achieve better results with respect to the level of compression, but part of the information is removed [17]. In the group of lossless methods of compression are included those methods, which can guarantee the absolute repetition of output data with input data during the process *compression—decompression* [12].

Methods of compression can be applied over file objects represented by different file formats. Over 23000 file formats are known by the moment of exploration [37]. As file format we will note the way used for presenting the file information [23]. Different file formats for the different type of information, saved in file exist. The file objects are divided in two main categories: directly executable and indirectly executable. The directly executable objects can be used directly while indirectly executable objects need to be processed additionally to become directly usable.

2.4. Short review of attacks, methods and objects

Information flows have been subject to various information attacks, and that has attracted the attention of scientists starting all the back in the 60s during the previous century [39]. Chris Rodgers has explored computer and network attacks in a TCP/IP environment featuring viruses, worms, Trojan horses and DoS attacks [25]. Daniel Klein has researched one of the most frequently used attacks for accessing systems or file objects – an attack through a password [16]. Marco de Vivo and David have examined the effect of various network attacks [19], [36]. In 2004, attacks on mobile phone become extremely popular, and those have been researched by Martin and Hsiao [20]. World organizations like CERT/CC, SANS and OIS research and analyze attacks and regularly publish related reports and bulletins.

Another group of scientists have been trying to find ways to reduce the size of the file objects by designing different methods of compression. For example, Cokus and Winkowski use methods of compression applicable to XML objects [3]. Butner, Iddan, Meron work on compressing images used in medicine and wireless

telecommunications which also have a higher rate of compression [2], [11]. Gilbert and Haffner have conducted studies in the field of compression of complex images and video both with and without a loss of information [8], [9].

3. Method for Reducing the Maximum Triple Relations Between Attacks, Methods and Objects to Real Triple Relations Between Them

3.1. Maximum triple relations between attacks, methods and objects

For achieving the tasks of the paper, the set of *maximum* number of attacks, methods and objects has to be determined.

The set of *maximum* number of attacks can be collected from the current information base of National Laboratory of Computer Virology of Bulgarian Academic of Sciences. It collects information for the information attacks, which were carried out to a separate personal and/or corporate computers, and/or networks, and/or systems at the moment of the investigation. This is a generalization of attacks, implemented in Bulgaria, Balkan Peninsula and south-east Europe.

Known methods of compression including lossless and lossy methods of compression, will be described.

The objects, included in the set of *maximum* number of objects are representative of different file formats. They belong to two main categories – directly executable and indirectly executable.

In the set of maximum number of attacks (A_{max}) are included 89 different attacks [38], divided in 33 main groups. 20 of these are in the category "Malicious software (Malware)" and 13 – in the category "Malicious attack (Malattack)".

59 methods of compression take part in the set of *maximum* number of methods of compression (M_{max}). They are divided in 9 groups: 5 of them belong to the category "Lossy methods of compression" [26] and 4 – to the category "Lossless methods of compression" [28].

42 file objects, representing over 23000 file formats are organized in 10 main groups. 7 of these belong to the category "Directly executable" and 3 – to the category "Indirectly executable". They form the set of *maximum* number of objects O_{max}.

For the purposes of the investigation, the current attacks will be denoted as a_i, where the index i changes from 1 to n (maximum number of known attacks), the current method of compression will be denoted as m_j, where the index j changes from 1 to k (maximum number of methods), and the current object will be denoted as o_f, where the index f changes from 1 to l (maximum number of objects).

3.2. Real triple relations between attacks, methods and objects

To turn out the unreal relations from the determined *maximum* sets, attacks, methods and objects have to be singled out by reducing. They will form the sets of *potential* attacks, methods and objects.

A group of experiments are carried out to determine the sets of *potential* numbers of attacks, methods and objects. The experiments have two stages: determination the *sets* of possible relations and determination the sets of *real* relations.

The first stage investigates the sets of *possible* relations which can exist between attack—object, method—object and attack—method. For each relation pair will be composed two matrixes. The first matrix will include the result of *expert* assessment for the corresponding relation. The second one will include the results from carried out *experiments* for the same relation.

The *expert* assessment will provide the possibility to exclude from the analysis the attacks, methods and objects about which: 1) there is no sufficient information; 2) the information is not public; 3) the information is rapidly changing; 4) there is not enough authentic hardware and software.

The expertly determined sets of relations will be put to a partial test by means of a number of planned simulative experiments. Thus the set of *possible* attacks, methods and objects will be singled out.

Determination of *possible* relations attack—object (Ω)

Let O_t be the set of file objects and A_t is a set of attacks that in a discrete moment of time t can gain access to the objects O. The elements of the set O_t and A_t are the apex of oriented graph G_t, determining the ability to access P to the object O in this way: the arc $A \xrightarrow{\rho} O$, where $\rho \subseteq P$ (as ρ will denote the different type of access: read, write, execute and delete), belongs to G_t then and then only when at the moment t the attack $a_i \in A_{max}$ accomplishes an access ρ to the object $o_f \in O_{max}$.

Let $\{G_t\}_{t=1}^{T}$ denote the set of states of the object from the point of view of the possibility for the attack A to obtain access to the object. $\Psi=\{G\}$ is the set of graphs for access of A to O. In the common case the sets of states in the relation attack—object (Φ), describing the successful/unsuccessful access of A to O, belong to the set Ψ.

The next stage is to determine the set $\Omega \subseteq \Phi \subseteq \Psi$, which includes those conditions, where the access of the attack $a_i \in A_{max}$ to the object $o_f \in O_{max}$ is possible.

Two matrices are composed to determine the set Ω: $Y_{(l,n)}$ and $E_{(l,n)}$. By the vertical of the matrices are included all attacks A_{max}, separated in n varieties $a_1, a_2, \ldots, a_i, \ldots, a_n$, $\bigcup_{i=1}^{n} a_i = A_{\max}$, $\bigcap_{i=1}^{n} a_i = \varnothing$. By the horizontal of the matrices are included all objects O_{max}, separated in l varieties $o_1, o_2, \ldots, o_f, \ldots, o_l$, $\bigcup_{f=1}^{l} o_f = O_{\max}$, $\bigcap_{f=1}^{l} o_f = \varnothing$. A research is conducted, where an attack a_i is trying to get access ρ to the object o_f, where ρ will present the different type of an access (read, write, execute and delete). Graphically this process can be illustrated in this way:

$$U_1 \longrightarrow a_i \xrightarrow{\rho} o_f$$

where U_1 is a user, who uses an attack $a_i \subseteq A_{max}$, to get access ρ to the object $o_f \subseteq O_{max}$, $i=1,2,\ldots,n$, $f=1,2,\ldots,l$.

In the matrix $Y_{(l,n)}$ for each cell the function of truth is produced [4] on the base of expert assessments: $J_x(K)\begin{cases}1, x \in K\\ 0, x \notin K\end{cases}$ for the attack and object: $J_a(a_1), J_a(a_2), \ldots, J_a(a_i), \ldots, J_a(a_n)$, $J_o(o_1), J_o(o_2), \ldots, J_o(o_f), \ldots, J_o(o_l)$. For each oriented graph $A \xrightarrow{\rho} O$ the result from the following logical expression $J_a(a_i) \wedge J_o(o_f)$ is filled out. If the obtained result is 1 (true) ($x=1$), then an attack $a_i \in A_{max}$ can get access to the object $o_f \in O_{max}$ ($A \xrightarrow{\rho} O$) and the relation can be investigated and analyzed. Otherwise with result 0 (false) ($x=0$), the attack $a_i \in A_{max}$ cannot get an access ρ to the object $o_f \in O_{max}$.and the relation drops off for further investigation.

From the obtained results for the relation attack—object the set of *expert* relations (*E*) can be singled out, which includes all attacks and objects the following logical expression is realized for: $J_a(a_i) \wedge J_o(o_f) = 1$.

In the second matrix $E_{(l,n)}$ for each cell a logical processing is made with result logical 0 or logical 1 by the so called function of truth $I_x(B)\begin{cases}1, x \in B \\ 0, x \notin B\end{cases}$ respectively for the attack and object: $I_a(a_1), I_a(a_2), \ldots, I_a(a_i), \ldots, I_a(a_n)$, $I_o(o_1), I_o(o_2), \ldots, I_o(o_f), \ldots, I_o(o_l)$ and in the corresponding cell of the matrix is filled out the result from the logical expression: $I_a(a_i) \wedge I_o(o_f)$ on the of the experiments, which were carried out. If the obtained result is 1 (possible) ($x=1$) then during the experiments the attack $a_i \in A_{max}$ had gotten an access to the object $o_f \in O_{max}$ ($A \xrightarrow{\rho} O$), otherwise with result 0 (impossible) ($x=0$), the attack's access is not accomplished.

On the base of the obtained results the set of *experimental* relations (*B*) can be singled out, which include all attacks and objects, for which is completed the following condition: $I_a(a_i) \wedge I_o(o_f) = 1$.

Crossing the set *B* with *E* the set of possible relations attack—object (Ω) can be singled out, where $\Omega = \left[I_a(a_i) \wedge I_o(o_f)\right] \wedge \left[J_a(a_i) \wedge J_o(o_f)\right] = 1$.

From the set Φ will be picked out the set of *possible* relations attack—object $\Omega=\{\Omega_i\}$, where *i* has one of the value from 1 to *T*, which covers those conditions of the object toward the attack, which will take a part in determination of the sets of *real* relations.

By analogy the other sets of possible relations method—object (Ξ) and attack—method (Θ) are determined. Figure 1, 2, 3, 4, 5, 6, 7, 8, and 9 are graphically presented the obtained result for the sets of *expert* relations (in red), the sets of *experimental* relations (in blue) and the sets of *possible* relations (in green).

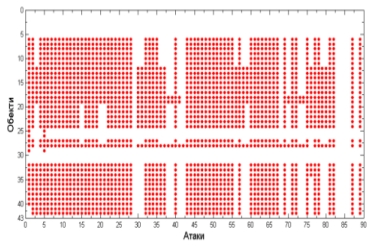

Figure 1 Set of *expert* relation attack—object (*E*)

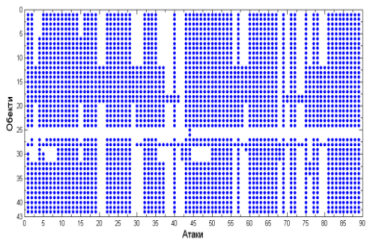

Figure 2 Set of *experimental* relation attack—object (*B*)

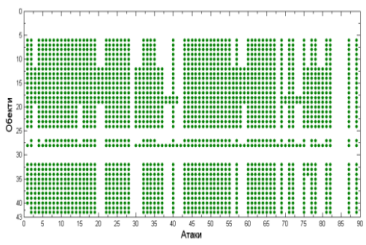

Figure 3 Set of *possible* relation attack—object (Ω)

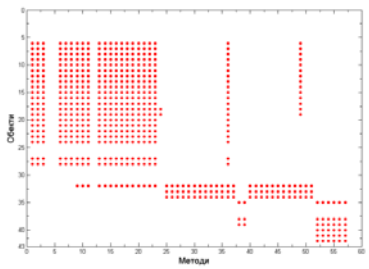

Figure 4 Set of *expert* relation method—object (*P*)

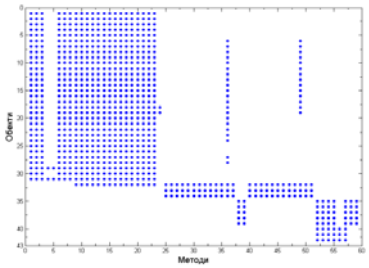

Figure 5 Set of *experimental* relation method—object (*C*)

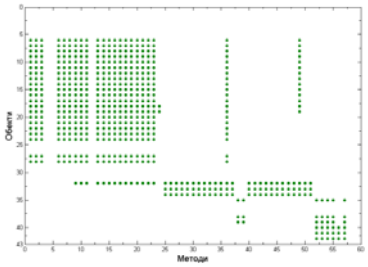

Figure 6 Set of *possible* relation method—object (Ξ)

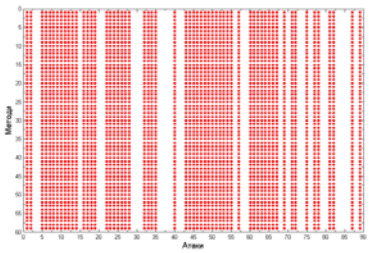

Figure 7 Set of *expert* relation attack—method (*Y*)

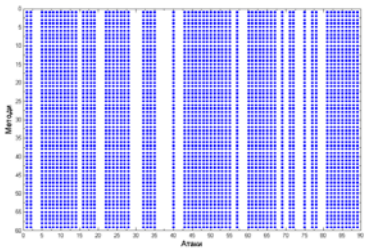

Figure 8 Set of *experimental* relation attack—method (*D*)

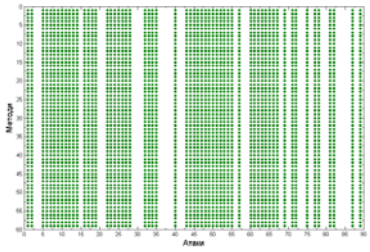

Figure 9 Set of *possible* relation attack—method (Θ)

The next stage of reducing the attacks, methods and objects includes investigation of the relations Ω—Ξ, Ω—Θ и Θ—Ξ.

Let the elements of the set Ω and Ξ form a totality of elements $\alpha \subseteq \mathrm{A}$ then and then only, when for the elements $\omega_z \subseteq \Omega$ and $\xi_h \subseteq \Xi$ the following logical expression is realized for (Expression 1):

$$\mathrm{A} = \left\{\left[I_a(a_i) \wedge I_o(o_f)\right] \wedge \left[J_a(a_i) \wedge J_o(o_f)\right]\right\} \wedge \left\{\left[I_m(m_j) \wedge I_o(o_f)\right] \wedge \left[J_m(m_j)\right] \wedge J_o(o_f)\right\} = \\ = \Omega \wedge \Xi = 1 \qquad \text{Expression 1}$$

The elements of the set Ω and Θ form a totality of elements $\beta \subseteq \mathrm{B}$ then and then only, when for the elements $\omega_z \subseteq \Omega$ and $\theta_c \subseteq \Theta$ the following logical expression is realized for (Expression 2):

$$\mathrm{B} = \left\{\left[I_a(a_i) \wedge I_o(o_f)\right] \wedge \left[J_a(a_i) \wedge J_o(o_f)\right]\right\} \wedge \left\{\left[I_a(a_i) \wedge I_m(m_j)\right] \wedge \left[J_a(a_i)\right] \wedge J_m(m_j)\right\} = \\ = \Omega \wedge \Theta = 1 \qquad \text{Expression 2}$$

The elements of the set Ξ and Θ form a totality of elements $\gamma \subseteq \Gamma$ then and then only, when for the elements $\xi_h \subseteq \Xi$ and $\theta_c \subseteq \Theta$ the following logical expression is realized for (Expression 3):

$$\Gamma = \left\{\left[I_m(m_j) \wedge I_o(o_f)\right] \wedge \left[J_m(m_j) \wedge J_o(o_f)\right]\right\} \wedge \left\{\left[I_a(a_i) \wedge I_m(m_j)\right] \wedge \left[J_a(a_i)\right] \wedge J_m(m_j)\right\} = \\ = \Xi \wedge \Theta = 1 \qquad \text{Expression 3}$$

The set of *real* relations between attacks, methods and objects is $\mathrm{X} = \mathrm{A} \bigcap \mathrm{B} \bigcap \Gamma$ or (Expression 4):

$$\mathrm{X} = (\Omega \wedge \Xi) \wedge (\Omega \wedge \Theta) \wedge (\Xi \wedge \Theta) = \mathrm{A} \wedge \mathrm{B} \wedge \Gamma = 1 \qquad \text{Expression 4}$$

Using the Matlab™ 33811 *real* three-way relations attacks—methods—objects from total 220 542 *maximum* three-way relations are determined.

The set of *potential* number of attacks (A_{pot}) is expressed as real attacks (received from the *real* relations) in relation to the maximum number of attacks (A_{max}). The real attacks are expert and experimental estimated for the corresponding object/objects with respect to the corresponding method/methods and described with the technique of matrix transformation. The set of *potential* number of attacks A_{pot} can be denoted as $A_{pot} = \{a_1, a_2, ..., a_i, ..., a_p\}$, where *p* is the index the potential attacks alter for, where $p \le n$ (Expression 5).

$$A_{pot} = \bigcup_{i=1}^{p} a_i, \qquad a_i \subseteq \mathrm{X} \qquad \text{Expression 5}$$

The set of *potential* number of methods (M_{pot}) is expressed as real methods (received from the *real* relations) in relation to the maximum number of methods (M_{max}). The real methods are expert and experimental estimated for

the corresponding object/objects with respect to the corresponding attack/attacks and described with the technique of matrix transformation. The set of *potential* number of methods M_{pot} can be denoted as $M_{pot} = \{m_1, m_2, ..., m_j, ..., m_q\}$, where q is the index the potential methods alter for, where $q \leq k$ (Expression 6).

$$M_{pot} = \bigcup_{j=1}^{q} m_j, \quad m_j \subseteq \mathrm{X} \qquad \text{Expression 6}$$

The set of *potential* number of objects (O_{pot}) is expressed as real objects (received from the *real* relations) in relation to the maximum number of objects (O_{max}). The real methods are expert and experimental estimated for the corresponding attack/attacks with respect to the corresponding method/methods and described with the technique of matrix transformation. The set of *potential* number of objects O_{pot} can be denoted as $O_{pot} = \{o_1, o_2, ..., o_f, ..., o_r\}$, where r is the index the potential objects alter for, where $r \leq l$ (Expression 7).

$$O_{pot} = \bigcup_{f=1}^{r} o_f, \quad o_f \subseteq \mathrm{X} \qquad \text{Expression 7}$$

4. Methodic for Evaluation of the Information Security of an Object, Exposed to Attacks with Considering the Influence of Methods of Compression

4.1. Information security and its evaluation about file object

The methodology for evaluation of the information security of an object will meet the following limitations:

- only the potential sets of attacks, methods and objects will be analyzed;
- the experiments are conducted at standard users', non-corporations' (governments') requirements;
- in order to simplify the computations the lossy methods of compression are except;
- in conducting the experiments for determining the co-efficient of information security, the objects used have equal or similar starting size (1 MB).

Studies and analysis can be made in the following three directions:

- evaluation of the *success of the attack*, made on an object processed with a method of compression;
- evaluation of the *protection by method of compression*, applied on an object, exposed to an attack;
- evaluation of the *security of an object* exposed to an attack and processed by a method of compression.

From the mentioned above three directions in this paper will pay attention only to the evaluation of the security (information security) of objects, exposed to information attacks noting the influence of the methods of compression.

The information security of an object can be determined as a quantitative value, which depends on several fundamental parameters. For the purposes of this paper only the parameters *TIME* and *SIZE* will be studied and analyzed by marking the difference in the objects behavior before and after applying the method of compression.

The parameter *TIME* (*T*) reflects the evaluation of time for attack at an object BEFORE and AFTER the influence of the method of compression. The parameter *SIZE* (*S*) reflects the evaluation of the size of an object BEFORE and AFTER its processing with a method of compression.

After determining the main parameters, which will be analyzed and evaluated with regard to the information security of an object, is necessary to determine the basic characteristics, which have influence on the evaluation of the main parameters.

The basic characteristics, which have influence on the evaluation of the parameters BEFORE applying a method of compression to the object, are:

- for the evaluation of the parameter *TIME* the following characteristics can be taken into consideration: *time for examination* and *time for processing*;
- for the evaluation of the parameter *SIZE* will pointed characteristics depending of the category to which file objects belong to. Two basic categories are: DIRECTLY USED (these are objects, which have to be used directly) and NON-DIRECTLY USED (these are objects, requiring secondary processing to become directly used):
- the characteristics, which have influence on the evaluation of the parameter *SIZE* for objects belonging to DIRECTLY USED category, are: *characters' size, image's size, video's and audio's size* and *official information's size*;
- the characteristics, which have influence on the evaluation of the parameter *SIZE* for objects belonging to NON-DIRECTLY USED category, are: *resolution of the image*, *bit depth, official information's size* (for representatives of the group "graphical objects"); *sample size*, *sample rate*, *official information's size* (for representatives of the group "music and sound").

The basic characteristics, which have influence on the evaluation of the parameters AFTER applying a method of compression to the object, are:

- for the evaluation of the parameter *TIME* the characteristic *time for restoration* is added to these, mentioned above before applying a method of compression to an object;
- for the evaluation of the parameter *SIZE* are specified characteristics, depending of the method of compression applied over the object:
- when *statistical methods* of compression are applied, the characteristics (in addition to these mentioned above for DIRECTLY USED objects), which have influence on the evaluation, are: *entropy of the message*, *information redundancy*, *level of compression*, *bits of information after compression*, *size of the model for decompression*;
- when *dictionary methods* of compression are applied, the characteristics (in addition to these mentioned above for DIRECTLY USED objects), which have influence on the evaluation, are: *size of the dictionary*, *entropy of the message*, *information redundancy, level of compression*;
- when *image methods* of compression are applied the characteristics (in addition to these mentioned above for NON-DIRECTLY USED graphical objects), which have influence on the evaluation, are: *average number of pixel repetitions, average number of sequenced pixels*, *level of compression*;
- when *audio methods* of compression are applied the characteristics (in addition to these mentioned above for NON-DIRECTLY USED objects from the group "sound and music"), which have influence on the evaluation, are: *level of sample size*, *level of sample rate*, *average number of sequenced zero samples, level of compression*.

Each characteristic is defined evaluation (*V*) with respect to the information security of an object subjected to attack BEFORE and AFTER applying a method of compression. To establish these evaluations is taken into consideration additional factors affecting the evaluation of the respective characteristic. Then each characteristic is examined by conducting experiments. Thus, the relationship between the result obtained after the examination

and evaluation of the characteristic with respect to the information security of an object, is determined. At the end the valuation (*V*) of the respective characteristic is determined.

The next stage is to determine the weighted co-efficient of each characteristic. The weighted co-efficient (*W*) determine the level of influence which each valuation of the respective characteristic have influence on the general evaluation of the parameter to which it belongs to. For determining the weighted co-efficient of the characteristic is used the AHP (Analytic Hierarchy Process) method [10], [33], which consists of four basic stages: 1) determining the characteristics which have to be evaluated; 2) arranging the chosen characteristics in a AHP matrix; 3) comparing each couple of characteristics by preliminarily selected bipolar measurement scales for evaluation; 4) determining the respective weights of the characteristics by consecution of mathematical operations.

The estimating of the general evaluation of the parameter consists of the following stages: 1) determining the evaluation of the characteristics, which have influence on the basic evaluation of the selected parameter $V_{(\text{charact.}_n)} = [0 \div 1]$, where *n* is the number of the characteristics; 2) setting the weighted co-efficient of each characteristic $W_{(\text{charact.}_n)}$, like $\sum_{i=1}^{n} W_i = 1$; 3) determining the evaluation of the parameter as $V_{(\text{parameter}_1)} = \sum_{i=1}^{n} \left(V_{(\text{charact.}_i)} . W_i \right)$.

4.2. Determination of the coefficient of information security

A co-efficient of information security (K^{IS}) is compounded to analyze the information security of the objects. It is presented as a variable, formed from the examined above parameters *TIME* and *SIZE*, reflecting the condition of the object before and after applying methods of compression.

The co-efficient of information security of an object reflects the total estimation of the parameters TIME and SIZE for each set of real relations between attack (a_i), methods (m_j) and object (o_f), where $a_i \in A_{pot}$, $m_j \in M_{pot}$, $o_f \in O_{pot}$.

The determination of K^{IS} for each relation attack—method—object proceeds over the following stages:

1) determining the co-efficient of information security for evaluation of the parameter TIME and SIZE;

To determine the co-efficient of information security of an object with respect to the parameter *TIME* ($RV_{(T)}$) and *SIZE* ($RV_{(S)}$), relatively valuation of the parameter TIME and SIZE is determined. It presents the number of increases of the value $V_{(T)}$ and $V_{(S)}$ of an object after processing it with method of compression. $RV_{(T)}$ and $RV_{(S)}$ can be represented as a ration of the *valuation-delta* ($\Delta V_{(T)}$ respectively $\Delta V_{(S)}$) and *valuation-prim* ($V'_{(T)}$ respectively $V'_{(S)}$) for the security of the object with respect to the time (Formula 1 and 2):

$$RV^{(T)} = \frac{\Delta V_{(T)}}{V'_{(T)}} \tag{1}$$

$$RV^{(S)} = \frac{\Delta V_{(S)}}{V'_{(S)}} \tag{2}$$

where $\Delta V_{(T)} = V''_{(T)} - V'_{(T)}$, $\Delta V_{(S)} = V''_{(S)} - V'_{(S)}$ like $V'_{(T)}$ and $V'_{(S)}$ is the determined valuation of information security of an object in regard to the time BEFORE applying the method of compression and $V''_{(T)}$ and $V''_{(S)}$ is the determined valuation of information security of an object in regard to the time AFTER applying the method of compression;

Thus for each set of real relations between attacks, methods and objects a relatively valuation of the object with respect to the parameters TIME and SIZE is determined.

For the parameters *TIME* and *SIZE* is formed a coefficient of the information security ($K^{IS(p)}$) for evaluation of the parameter (p) as (Formula 3):

$$K^{IS(p)} = \frac{RV_{(p)}}{\max RV_{(p)}} \tag{3}$$

where: $RV_{(p)} = \frac{V''_{(p)} - V'_{(p)}}{V'_{(p)}}$ is the average value of the parameter, which show with how many times is increased the value of the corresponding parameter after the application of a method of compression on an object; $V'_{(p)}$ is the value of the information security of the object corresponding to the parameter before the application of method of compression; $V''_{(p)}$ is the value of the information security of the object corresponding to the parameter after its treatment with method of compression; max$RV_{(p)}$ is the maximum average value corresponding to the parameter, achieved from the same object in one of the others *real* relations, in which it takes part.

The coefficient of the information security of an object (K^{IS}) can be represented as average value of the coefficients of evaluation of the parameters (Formula 4):

$$K_z^{IS} = \frac{1}{n}\sum_{p=1}^{n} K^{IS(p)} \tag{4}$$

where $K^{IS(p)}$ represents a coefficient of the information security of an object corresponding to a given parameter, n is the number of tested parameters corresponding to the information security of an object, and z varies in the boundaries of the multiplication of a_p, m_q and o_r.

On Figure 10 a), b), c), d), e), f) is shown graphical interpretation of the obtained values of K^{IS} for some of the most commonly used objects.

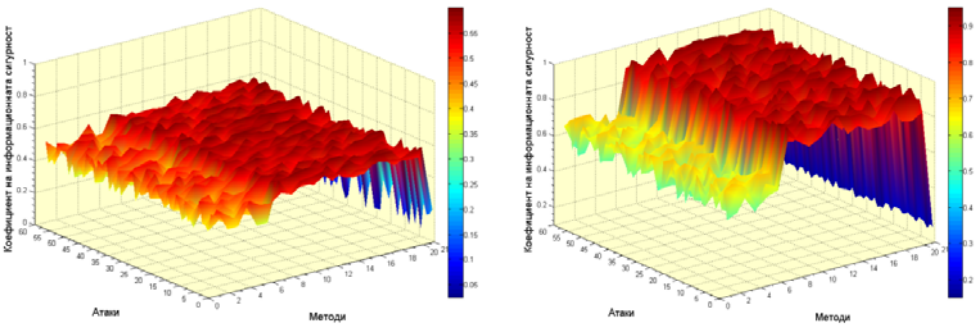

Figure 10 a) Geographic Information System object **Figure 10** b) Text/Document object

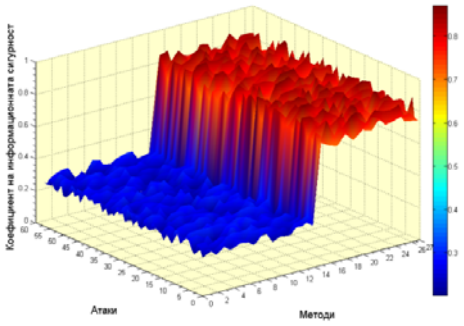

Figure 10 c) Raster graphic

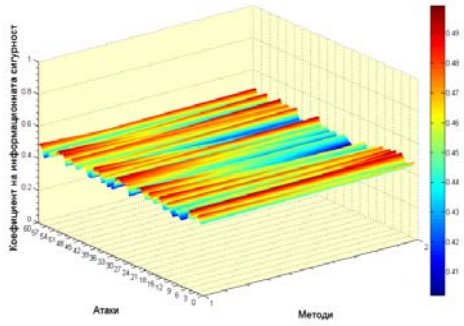

Figure 10 d) Uncompressed sound

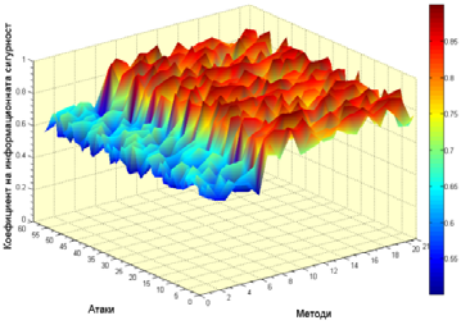

Figure 10 e) Dynamic web page

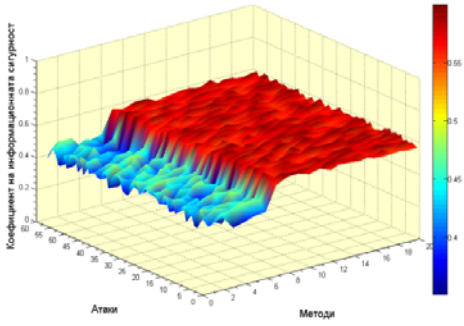

Figure 10 f) Source code

Figure 10 Graphic interpretations for determined values of the co-efficient of information security for different file objects

After determining K^{IS} for each object we can determine which is the method with the highest value of K^{IS} for the given object and attack. On Figure 11 a), b), c), d), e), f) we can see a graphical presentation of the change in the co-efficient of information security for given objects in regard to given attacks, determined after applying the given methods for compression.

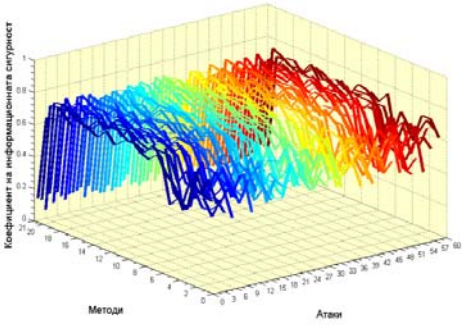

Figure 11 a) Geographic Information System fail object

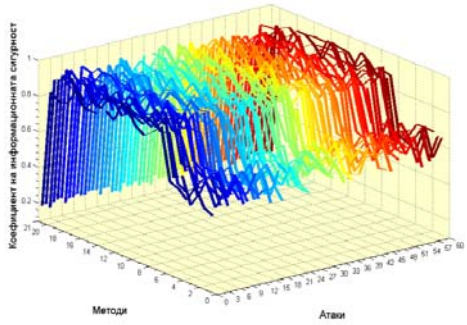

Figure 11 b) Text/Document object

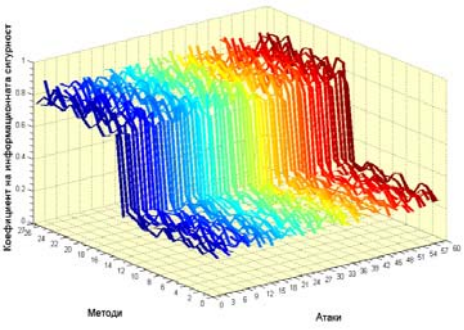

Figure 11 c) Raster graphic

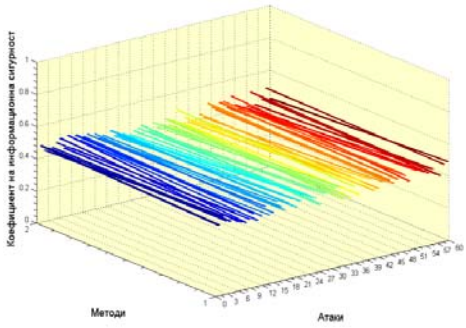

Figure 11 d) Uncompressed sound

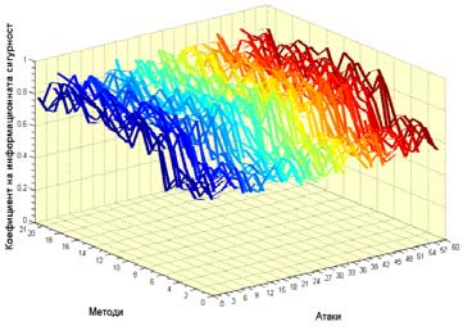

Figure 11 e) Dynamic web page

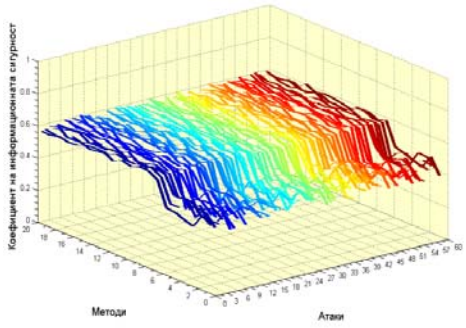

Figure 11 f) Source code

Figure 11 Distribution of the co-efficient for informational security for given object and attack, when a given method of compression is applied

In practice though, one object can be subjected of several attacks simultaneously. For each objects can be formed a group of methods, achieving highest values of K^{IS} towards all attacks, to which it might be exposed. They are used to define the methods with lowest risk for compression in relation to the information security of the objects.

5. Selecting Procedure for Methods of Compression with Lowest Risk with Respect to the Coefficient of Information Security

5.1. Model for choosing of alternatives

The considered model is related to the examination of the possibility to influence on information security of objects, exposed to attacks by methods of compression. The final goal of the model is to choose the best alternatives (variants) for the decision making person by calculation several problems for multi-criteria evaluation [31]. Finally for each object a method of compression will be chosen which will reduce to the lowest risk with respect to the information security of selected object towards to all attacks to which the object can be exposed.

Stage one from the construction of the model is connected with the definition of the objects which will be explored and the different alternatives, compiling of the different compression methods, which can be applied to the corresponding object.

Stage two is connected with the selection of the different characteristics/situations compiling of the different attacks, which can attack the corresponding compressed object.

Stage three is connected with definition of the weight of the different characteristics/situations, e.g. to define for each attack the possibility to attack the chosen compressed object.

On stage four with the help of chosen criteria and methods for selection of alternatives is made a selection of a alternative with lowest risk (compression method), and the rest alternatives are sorted in descending order in relation to the information security of the object.

The last stage five from the construction of the model is connected with the selection of the best alternative (compression method) for each object, which is with lowest risk in relation to the information security of the object in question towards all attacks, to which it can be exposed.

In the model are included attacks ($a_i \in A_{pot}$), methods ($m_j \in M_{pot}$) and objects ($o_f \in O_{pot}$), which had been determined by means of matrix transformations, applied on initially build base of relations between maximum number of attacks (A_{max}), methods (M_{max}) and objects (O_{max}). After dropping out the sets of *real* relations, where lossy methods of compression take part, are analyzed 60 attacks (from the set of A_{pot}) from total 89 attacks (from the set of A_{max}), 36 methods (from the set of M_{pot}) from total 59 methods (from the set of M_{max}). The methods and the attacks are investigated on 27 objects (from the set of O_{pot}) from total 42 objects (from the set of O_{max}).

During description of the model, the following terms will be used:

Risk – when we speak of risk we will have in mind the risk of achieving a lower value of K^{IS} of the object when applying a method of compression as means of protection from different attacks;

Profit – the profit of application of the method of compression on an object is connected with the achievement of higher value of K^{IS}.

5.2. Choosing of evaluation criteria

It is necessary to systematize the available information to realize this model. For that purpose a matrix $B_{(q,p)}$ is built, which includes the most efficient methods for one object (which are the different alternatives for decision-maker) and the attacks, which can access to these objects processed by these methods (which are the set of characteristics). The vector of numerical values for characteristics, which is assigned for each element, is the co-efficient of information security (K_{INF}). The matrix $B_{(q,p)}$ is built for each object from the set of *potential* number of objects.

The best variant for decision-maker can be determined with the help of the matrix and different methods for the game theory [14] and multi-criteria evaluation methods [27]. This variant includes the method of compression with the lowest risk with respect to the co-efficient of information security of the object, which is chosen by the decision-maker in connection to investigating attacks.

Under lowest risk alternative we assume the compression method, which best satisfies the execution of the target of the model, namely to achieve the best information security of the object towards all attacks through application of a compression method.

For the finding of alternative with lowest risk are used the following criteria from game theory:

- Maximum of the mathematical expectation for the profit (E_a);

- Minimum of the mathematical expectation for the risk (E_r);
- Criteria of Laplace for the profit (L_a);
- Criteria of Laplace fir the risk (L_r);
- Criteria of Wald (*WA*);
- Criteria of Savage (*SA*);
- Criteria of pessimism-optimism (*H*);
- Criteria of pessimism-optimism of risk (*F*).

The methods of compression can be sorted according level of preference with the help of the following two methods for multi-criteria evaluation (multi-criteria evaluation methods):

- Method of the linear combination of formal criteria (S_j);
- Method of maximum guaranteed result (t_j).

Both methods are based on the same model.

Maximum of the mathematical expectation for the profit (Ea)

Maximum of the mathematical expectation for the profit (E_a) can be determined as (Formula 5) [13]:

$$E_a = \max_j \overline{b_j} \tag{5}$$

where $\overline{b_j} = \sum_{i=1}^{p} \lambda_i b_{ji}$, p is the number of attacks, b_{ji} is a component of the matrix $B_{(q,p)}$, λ_i is the weight co-efficient and it represents the possibility of one in preliminary chosen attack to get access to one object from preliminary chosen set of objects. The vector components $\vec{\lambda} = \left(\lambda_1, \lambda_2, ..., \lambda_i, ..., \lambda_p\right)$ are real non-negative numbers and represents weight for decision-making. The following limitation $\sum_{i=1}^{p} \lambda_i = 1$ has to be observed.

Minimum of the mathematical expectation for the risk (Er)

Minimum of the mathematical expectation for the risk (E_r) can be determined as (Formula 6):

$$E_r = \min_j \overline{r_j} \tag{6}$$

where:

$$\overline{r_j} = \sum_{i=1}^{p} \lambda_i r_{ji},$$

$$r_{ji} = \beta_i - b_{ji}\,,\ \beta_i = \max_j b_{ji}\,.$$

By analogy a variant of these both methods for multi-criteria evaluation can be examined when the values of weighted co-efficient are equal. For more detailed analysis can be assumed that the weighted co-efficient (λ) cannot always be known. In that case can be made the assumption that all values of λ are equal (Laplace principle).

Criteria of Laplace for the profit (La)

Criteria of Laplace [18] for the profit (L_a) can be determined as (Formula 7):

$$L_a = \max_j \overline{b_j}^L \tag{7}$$

where $\overline{b_j}^L$ is the average value of the profit in cases when the weights co-efficient are equal: $\overline{b_j}^L = \sum_{i=1}^{p} \lambda_i^L b_{ji} = p^{-1} \sum_{i=1}^{p} b_{ji}$, where p is the number of the situations (attacks).

Criteria of Laplace fir the risk (Lr)

Criteria of Laplace fir the risk (L_r) can be determined as (Formula 8):

$$L_r = \min_j \overline{r_j}^L \tag{8}$$

where $\overline{r_j}^L$ is the average value of the risk in cases when the weights co-efficient are equal: $\overline{r_j}^L = \sum_{i=1}^{p} \lambda_i^L r_{ji} = p^{-1} \sum_{i=1}^{p} r_{ji}$, where p is the number of the situations (attacks).

Criteria of Wald (WA)

This is criterion of pessimism. Its calculation is necessary because the aim of the model is to select this variant which is with maximum profit and minimum risk. The Wald criterion (*WA*) is called maximin (criterion of pessimism) [21] and it selects for optimal this strategy which responds to (Formula 9):

$$WA = \max_j \alpha_j \tag{9}$$

where:

$$\alpha_j = \min_i b_{ji}$$.

Criteria of Savage (SA)

This criterion also works with the risk and it is criterion of pessimism too. Criteria of Savage (*SA*) [15] selects for optimal this strategy, where the risk value is minimal in cases of the more unfavorable situation. The optimal strategy can be fined as (Formula 10):

$$SA = \min_j \gamma_j \tag{10}$$

where:

$$\gamma_j = \max_i r_{ji}.$$

Criteria of pessimism-optimism (H)

Under existing circumstances a pessimistic position of the decision making person can be chosen in other cases – optimistic. The criterion uses the matrix $B_{(q,p)}$. The number θ, which is a measure for the pessimism of the decision making person. The number can be between 0 and 1. When θ=1, then we have situation of extreme pessimism. When θ=0, this criterion become criterion of extreme optimism. Criterion of Hurwicz (*H*) [29], [32] recommends selecting this alternative, which (Formula 11):

$$H = \max_j h_j \tag{11}$$

where:

$$h_j = \theta\alpha_j + (1-\theta)\max_j b_{ji}.$$

The criterion is calculated in the model when θ=0, θ=0,5 and θ=1.

Criteria of pessimism-optimism of risk (F)

Criteria of pessimism-optimism of risk (*F*) [24] can be defined as (Formula 12):

$$F = \min_j f_j \tag{12}$$

where $f_j = \theta \max_i r_{ji} + (1-\theta)\min_i r_{ji}$.

The criterion is calculated in the model when θ=0, θ=0,5 and θ=1.

The next stage of the model is related with the estimation of the decision. Therefore two main methods for multi-criteria evaluation are used: Method of the linear combination of formal criteria and Method of maximum guaranteed result. Both methods use the matrix ($B_{(q,p)}$), whose elements are normalized in matrix $C_{(q,p)}$ (Formula 13) [1].

$$c_{ji} = \frac{b_{ji}}{\beta_i} = \frac{b_{ji}}{\max_j b_{ji}} \tag{13}$$

Method of the linear combination of formal criteria (Sj)

The matrix with normalized values $C_{(q,p)}$ is used [7]. It uses the vector $\vec{\lambda} = \left(\lambda_1, \lambda_2, ..., \lambda_i, ..., \lambda_p\right)$ as an input parameter.

The calculating is:

(1) For each alternative (methods' group) is assigned the number S_j where (Formula 14):

$$S_j = \sum_{i=1}^{p} \lambda_i c_{ji} \tag{14}$$

(2) The alternatives are sorted in ascending order by the number S_j, i.e. on the first place is the alternative with the maximum value of S_j, if there are several such an alternatives, their order in the list is arbitrary. Alternatives with lower values of S_j, follow, etc.

By analogy a variant of this both method can be examined when the values of weighted co-efficient (λ) are equal (Laplace). In this case (Formula 15):

$$S_j^L = \sum_{i=1}^{p} \lambda_i^L c_{ji} = p^{-1} \sum_{i=1}^{p} c_{ji} \tag{15}$$

Method of maximum guaranteed result (tj)

The matrix with normalized values $C_{(q,p)}$ [7], [34] is used. It uses the vector $\vec{\lambda} = \left(\lambda_1, \lambda_2, ..., \lambda_i, ..., \lambda_p\right)$ as an input parameter too, for which the following limitation $\sum_{i=1}^{p} \lambda_i = 1$ has to be observed for.

The calculating is:

(1) For each alternative (method of compression) is assigned the number t_j where (Formula 16):

$$t_j = \min_i \left(\lambda_i c_{ji}\right) = \min\left(\lambda_1.c_{j1}, \lambda_2.c_{j2}, ..., \lambda_i.c_{ji}, ..., \lambda_p.c_{qp}\right) \tag{16}$$

(2) The alternatives are sorted in ascending order by the number t_j.

In case when the values of weighted co-efficient (λ) are equal (Laplace) (Formula 17):

$$t_j^L = \min_i \left(\lambda_i^L c_{ji}\right) \tag{17}$$

5.3. Procedure of choosing an alternative

These methods for multi-criteria evaluation are applied for each matrix (i.e. for each objects' group). Thus, for each object we can choose an alternative (method) we give preference to, with respect to the co-efficient of information security to all attacks.

6. Experiments Proving the Reliability of the Approach

The methods used for conducting of the experiments include the use of corresponding hardware and software instruments, which is connected with matrixes, matrix transformations, methods for evaluation of the risk, multi-criteria valuation, multi-criteria choice and other.

For the software realization is used the program system for scientific studies of the company "*The MathWorks*" which includes the *family фамилията Matlab® and Simulink®* – widely used software for analytical transformations, numerical calculations and graphical presentation of obtained results.

The used for the experiments apparatuses includes two server configurations each with two work stations. The first server configuration (in conjunction with two work stations) is used for investigation of "attacking behavior". The other server configuration (in conjunction with two work stations) is used for investigation of "protecting behavior". Each couple work stations are used accordingly for "managing station" and "standard station".

7. Assessments and Conclusion

7.1. With respect to the sets of attacks, methods and objects:

The selected number of maximum attacks (89 numbers), methods (59 numbers) and objects (42 numbers) is enough for determination of the sets of *potential* number of attacks, methods and objects.

After conducted expert evaluations and experiments can be summarized that:

- from total 3738 relations attack—objects, *expert* evaluated 2231 relations, *experimental* verified are 2861 relations and 2188 *possible* relations attack—object are formed;
- from total 2478 relations method—objects, *expert* evaluated 588 relations, *experimental* verified are 845 relations and 585 *possible* relations method—object are formed;
- from total 5251 relations attack—method, *expert* evaluated 3540 relations, *experimental* verified are 3835 relations and 3540 *possible* relations method—object are formed.

From total 220542 *maximum* triple relations, 33811 *real* triple relations attack—method--object are determined.

The number of attacks, methods and objects from the set of *potential* number of attacks, methods and objects, which take a part in the investigations are as follows: A_{pot}=60 numbers, M_{pot}=53 numbers and O_{pot}=30 numbers.

1) The chosen methodology for analyzing the relations attack-method-object by means of matrix transformations is effective and operative, and it contains the necessary potential for new deep analyses in this and another related areas.
2) The results give a possibility of specific planning of safety procedures and safety policies for the different computers, systems and networks configurations. Conditions are created for precise planning of economic expenses, connected with a specific safety policy with a specific configuration of computer, system and network.

7.2. With respect to the information security of object:

1) The selected for the investigation parameters TIME and SIZE are enough to investigate the information security not only of objects, but also of computer systems and networks when standard and not corporate (government) requirements are used.
2) The evaluation with respect to the chosen objects, which will be processed by methods of compression, is positive and suppositions don't influence on the obtained results. The evaluation with respect to the

chosen methods of compression is also positive and the conducted experiments can be generalized for other methods of compression, which don't take part in the investigation.

3) Based on the conducted experiments, we can make the conclusion that reducing the object's size after compression leads to increasing the time required by an attack to get an access to an object.

With respect to K^{IS} the best results are shown with objects from the group of **data file objects**, processed with a method of compression belonging to the group of *dictionary* methods of compression. The worst results are shown with objects from the group of **binary file objects** and **graphic file objects**, processed with a method of compression belonging to the group of *statistical* methods of compression.

Fro total 53 numbers methods from the set of *potential* numbers of methods, 20 achive the highest values of K^{IS} of the object. They are from the group of: *dictionary* methods of compression, *image* mathods of compression and *audio* methods of compression.

7.3. With respect to the procedure for methods of compression with lowest risk

1) The main task of risk management is risk optimization, i.e. to find the moment where the risk and attaining higher level of information security when methods of compression are applied on objects are compensate each other.
2) Independently from the made expenses, the risk assessment shows that the application of methods of compression to a great extent heightens the information security of objects under attacks.
3) The conducted experiments shows that the lowest risk with respect to the information security is obtained for objects from the groups **scientific file objects** and **data file objects**, exposed to attacks when methods of compression from the group of *dictionary* methods of compression are applied.

7.4. With respect to the experiments:

The program systems for scientific investigations *"The MathWorks"* can be successfully applied when determining the sets of real relations between attacks, methods and objects, obtained by using matrix transformations and reducing by stages the sets of *maximum* relations. Thus, from total 220542 *maximum* relations attacks—methods—objects are determined 33811 *real* relations, which are investigated with respect to the information security of objects.

With respect to the number of the elements of the sets of *expert* relations attack—object, methods—object and attack—method, can be concluded that they are accordingly 2231 from total 3738, 588 from total 2478 and 3540 from total 5251.

Bibliography

Barley, M., Kasabov, N., *Intelligent Agents And Multi-Agent Systems: 7th Pacific Rim International Workshop on Multi-Agent Systems*, Springer (2005), ISBN 3540253408, p. 154

Butner, S, Ghodoussi, M., Transforming a Surgical Robot for Human Telesurgery, IEEE Trans. on Robotics and Automation, vol. 19, iss. 5, Oct. 2003, pp. 818 – 824

Cokus, M., Winkowski, D., XML Sizing and Compression Study For Military Wireless Data, Proceedings of XML Conference & Exposition 2002, Baltimore Convention Center, Baltimore, MD, USA, December 8-13, 2002

Damm, W., Josko, B., Pnueli, A., Votintseva, A., A Discrete-Time UML Semantics for Concurrency and Communication in Safety-Critical Applications, Science of Computer Programming, Vol. 55, 1-3/2005

David Dittrich. The DoS Project's "trinoo" Distributed Denial of Service Attack Tool (1999) (http://staff.washington.edu/dittrich/misc/trinoo.analysis)

Denning, D., A lattice model of secure information flow, Communications of the ACM, v. 19 n. 5, May 1976, pp. 236-243

Ferrari, E., Thuraisingham, B., Web And Information Security, IRM Press (2006), ISBN: 1591405890

FILExt – The File Extension Source (http://www.filext.com/)

Galotti, K., Making Decisions That Matter: How People Face Important Life Choices, Lawrence Erlbaum Associates (2002), ISBN 080583396X, p. 58

Gilbert, J., Brodersen, R., A lossless 2-D image compression technique for synthetic discrete-tone images, Data Compression Conference, 1998. DCC apos; 98. Proceedings Volume , Issue , 30 Mar-1 Apr 1998, pp. 359–368

Haffner, P., LeCun, Y., Bottou, L., Howard, P., Vincent, P., Riemers, B., Color documents on the Web with DjVu, Proc. IEEE Int. Conf. Image Processing, Kobe, Japan, Oct. 1999

Hasenauer, H., Sustainable Forest Management: Growth Models for Europe, Springer (2006), pp. 267-269

Iddan, G., Meron G, Glukhovsky A, Swain P, Wireless Capsule Endoscopy, Nature, vol. 405, 25 May 2000

Istepanian, R., Pattichis, C., Laxminarayan, S., M-Health: Emerging Mobile Health Systems, Springer (2006), ISBN 0387265589, p. 282

Karlin, S., Mathematical Methods and Theory in Games, Programming, and Economics, Courier Dover Publications (2003), ISBN 0486495272, pp. 179-182

Keeping, E., Introduction to Statistical Inference, Courier Dover Publications (1995), ISBN 0486685020, pp. 151-173

Kerzner, H., Project Management: a systems approach to planning, scheduling, and controlling, John Wiley and Sons (2003), ISBN 0471225770, p. 659

Klein, D., Foiling the Cracker: A Survey of, and Improvements to, Password Security, In UNIX Security Workshop II, August 1990

Koohang A., Harman, K., Learning Objects and Instructional Design, Informing Science (2006), ISBN-13: 978-8392233770, p. 180

Kundisch, D., New Strategies for Financial Services Firms: The Life-Cycle-Solution Approach, Springer (2003), ISBN 379080066X, pp. 148-149

Marco de Vivo, Gabriela O. de Vivo, Germinal Isern. Internet Security Attacks at the Basic Levels. ACM SIGOPS Operating Systems Review, 32(2):4–15, (1998)

Martin, T., Hsiao, M., Ha, D., Krishnaswami, J., Denial-of-Service Attacks on Battery-powered Mobile Computers, Proceedings of the Second IEEE International Conference on Pervasive Computing and Communications (PerCom'04), (2004), ISBN 0769520901, pp. 309-318

Nielsen, T., Zhang, N., Symbolic and Quantitative Approaches to Reasoning With Uncertainty, 7th European conference ECSQARU 2003 Aalborg, Denmark, July 2003 Proceedings, Springer (2003), ISBN 3540404945, pp. 3-4

Radhamani, G., Rao, R., Web Services Security and E-business, Global (2007), ISBN-13: 978-1599041681, p. 115, p. 25

Reilly, E., Concise Encyclopedia of Computer Science, John Wiley and Sons (2004), ISBN 0470090952, p. 388

Ricci, P., Environmental and Health Risk Assessment and Management: Principles and Practices, Springer (2006), ISBN 1402037759, p. 54

Rodgers, C., Threats to TCP/IP Network Security. (2001)

Salomon, D., Data Compression: The Complete reference, Springer (2004), ISBN 0387406972, p. 868

Sandblom, C.-L., Eiselt, H., Decision Analysis, Location Models, and Scheduling Problems, Springer (2004), ISBN 3540403388, pp. 19-150

Sayood, K., Lossless Compression Handbook, Elsevier (2003), ISBN 0126208611, pp. 229-234, pp. 273-273, pp. 301-310

Schniederjans, A., Information Technology Investment: Decision-making Methodology, World Scientific (2004), ISBN 9812386955, p. 244, p. 249

Shaw, W., Cybersecurity for SCADA Systems, PennWell Corp. (2006), ISBN-13: 978-1593700683, p. 194

Straffin, P., Game Theory and Strategy, The Mathematical Association of America (1996), ISBN 0883856379, pp. 7-22, pp. 56-62

Vigna, G., Jonsson, E., Kruegel, C., Recent Advances in Intrusion Detection: 6th International Symposium, RAID 2003, Pittsburgh, PA, USA, September 2003, Proceedings, Springer (2003), ISBN 3540408789, p. 146

Vinze, A., Chen, H., Raghu, T., Zeng, D., Ramesh, R., National Security, Elsevier (2007), ISBN 0444519963, p. 69

Попчев, И., Метев, Б., Христов, Ч., Маркова, Л. Диалогова система за многокритериална оценка и избор, Печатница на Издателството на БАН (1985), 3-5 стр., 8-12 стр.

Стенли, Т., Компресиране на данни, Интерфейс България, (1998)

http://ncs.nlcv.bas.bg/index_en.htm

http://www.sptimes.com/Hackers/history.hacking.html

Authors' Information

Dimitrina Polimirova, PhD, Research Associate, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Part-time lecturer at New Bulgarian University, Phone: +359-2-9733398, E-mail: polimira@nlcv.bas.bg

Eugene Nickolov, Prof., DSc, PhD, Eng, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Regular lecturer at New Bulgarian University, Phone: +359-2-9733398, E-mail: eugene@nlcv.bas.bg