ANALYSIS OF INFORMATION SECURITY OF OBJECTS UNDER ATTACKS AND PROCESSED BY METHODS OF COMPRESSION

Dimitrina Polimirova-Nickolova, Eugene Nickolov

Abstract: In this paper a methodology for evaluation of information security of objects under attacks, processed by methods of compression, is represented. Two basic parameters for evaluation of information security of objects – TIME and SIZE – are chosen and the characteristics, which reflect on their evaluation, are analyzed and estimated. A co-efficient of information security of object is proposed as a mean of the coefficients of the parameter TIME and SIZE. From the simulation experiments which were carried out methods with the highest co-efficient of information security had been determined. Assessments and conclusions for future investigations are proposed.

Keywords: Information Security, File Objects, Information Attacks, Methods of Compression, Information Flows, Coefficient of Information Security

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

Introduction

The development of information systems and technologies extends the necessity of 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 an object of non-stop attacks according to their information security, which determines the significant necessity for investigation of methods and means for their protection.

A general strategy for protecting file objects could include applying compression methods to objects to achieve decrease in volume size of information flow.

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.

The Problem

The main aim of this paper is to make analysis of the information security of the file objects, found in TCP/IP environment, under information attacks, noting the influence of the compression methods.

The following tasks are set in reaching the aim:

1) to offer a methodology for evaluation of the information security of objects under attack and processed with a method of compression;

2) to set a co-efficient of information security of an object;

3) to find the methods of compression those reach the highest values of the co-efficient of information security.

For the aim of this paper the following work definitions are proposed [1], [2], [3]: 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; 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.

1. METHODOLOGY OF EVALUATION OF THE INFORMATION SECURITY.

The methodology for evaluation of the information security of an object supposed to attack and processed with a method of compression will meet the following limitations:

- only the potential sets of attacks, methods and objects will be analyzed. These sets are made by stagely reduction of the known at the moment of study information attacks, methods of compression and file objects by using of matrix transformations. The stages of reduction of the multitudes are described in [4];
- 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.

Upon determining [4] the real relationships between attacks, methods and objects, 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.

This paper is aimed at the possibility to evaluate the security (information security) of objects supposed to information attacks noting the influence of the methods of compression.

1.1 Setting the basic parameters for evaluating the information security.

The information security of an object can be determined as a quantitative value, which depends on several fundamental parameters, which can be represented as ratios of separate values before and after certain impact.

For the purposes of this paper considering the usage of standard users' requirements, not corporations' (governments') requirements it is enough to study and evaluate only the parameters *TIME* and *SIZE*, 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.

1.2. Determining the characteristics which influence over chosen parameters.

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):
  - o 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*;
  - o 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*.

1.3. Determining the evaluations of the characteristics, which have influence on the general valuation of the respective parameter.

Each characteristic is necessary to be evaluated with respect to the information security of an object under attack before and after applying a method of compression. To determine these evaluations is taken into consideration additional factors, which have influence on the evaluation of the respective characteristic. After that is necessary to examine each characteristic by providing simulation experiments, which will determine the relationship between the obtained after the examination result and the evaluation of the characteristic with respect to the information security of an object (for example: the increasing of the time of an attack to process an object, increases object's information security, which leads to higher valuation of this characteristic; the increasing of the size of the model for decompression decreases the possibility for better compression of the object, which leads to faster restoration in its original state, respectively to faster braking the protection mechanism of the object as a mean of method of compression, that means lower valuation of this characteristic with respect to the information security of this object). At the end the valuation (*V*) of the respective characteristic is determined.

1.4. Setting a weighted co-efficient for 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 [5], which consists of four basic stages: 1) determining the characteristics which have to be evaluated; 2) arranging the chosen characteristics in a matrix; 3) comparing each couple of characteristics by preliminarily selected measurement scales for evaluation; 4) determining the respective weights of the characteristics by consecution of mathematical operations.

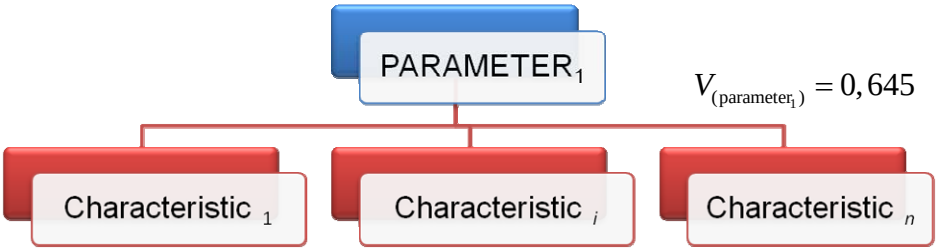
1.5. Estimating the general evaluation of the respective parameter.

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 $V_{(\text{parameter}_1)} = \sum_{i=1}^{n} \left(V_{(\text{charact.}_i)} . W_i \right)$ (Figure 1).



$V_{(\text{parameter}_1)} = 0,645$ From 0 to 1

$V_{(\text{charact.}_1)} = 0,4$ $V_{(\text{charact.}_i)} = 0,8$ $V_{(\text{charact.}_n)} = 0,5$ From 0 to 1

$W_{(\text{charact.}_1)} = 0,05$ $W_{(\text{charact.}_i)} = 0,5$ $W_{(\text{charact.}_n)} = 0,45$ $\sum_{i=1}^{n} W_i = 1$

Figure 1 Determining the evaluation of the parameter

2. DETERMINING THE CO-EFFICIENT OF INFORMATION SECURITY.

A co-efficient of information security 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.

2.1. Determining the co-efficient of information security of an object in regard to the evaluation of the parameter *TIME* ($K^{IS(T)}$).

The determination of $K^{IS(T)}$ proceeds over the following stages:

(1) for each relation attack—method—object is determined relatively valuation of the time ($RV_{(T)}$). It presents the number of increases of the value $V_{(T)}$ of an object after processing it with method of compression. The relatively valuation of the time can be represented as a ration of the *valuation-delta* ($\Delta V_{(T)}$) and *valuation-prim* ($V'_{(T)}$) for the security of the object with respect to the time (Formula 1):

$$RV_{(T)} = \frac{\Delta V_{(T)}}{V'_{(T)}} \qquad \text{Formula 1}$$

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

(2) for each object o_f is determined the highest value of relatively valuation of the time ($\max RV_{(T)}$), which presents the highest increase of $V_{(T)}$, achieved by this object in all triple relations;

(3) for each relation attack—method—object is determined the co-efficient of information security with respect to the parameter *TIME* ($K^{IS(T)}$). For each triple relation this co-efficient presents the part of maximum possible value of relatively valuation of the time, which the object is achieved (Formula 2):

$$K^{IS(T)} = \frac{RV_{(T)}}{\max RV_{(T)}} \qquad \text{Formula 2}$$

Graphically $K^{IS(T)}$ can be presented as (Expression 1):

$$K_z^{IS(T)} = f\left(a_i, m_j\right) \quad \text{for each } o_f \qquad \text{Expression 1}$$

where $a_i \in A_{pot}\{a_1, a_2, ..., a_i, ..., a_p\}$, $m_j \in M_{pot}\{m_1, m_2, ..., m_j, ..., m_q\}$, $o_f \in O_{pot}\{o_1, o_2, ..., o_f, ..., o_r\}$, and the index *z* is changing within the bounds of the formula a_p, m_q and o_r.

2.2. Determining the co-efficient of information security of an object in regard to the evaluation of the parameter *SIZE* ($K^{IS(S)}$).

The determination of $K^{IS(S)}$ proceeds over the following stages:

(1) for each relation attack—method—object is determined relatively valuation of the size ($RV_{(S)}$). It presents the number of increases of the value $V_{(S)}$ of an object after processing it with method of compression. The relatively valuation of the size can be represented as a ration of the *valuation-delta* ($\Delta V_{(S)}$) and *valuation-prim* ($V'_{(S)}$) for the security of the object with respect to the size (Formula 3):

$$RV_{(S)} = \frac{\Delta V_{(S)}}{V'_{(S)}} \qquad \text{Formula 3}$$

where $\Delta V_{(s)} = V''_{(s)} - V'_{(s)}$ like $V'_{(s)}$ is the determined valuation of information security of an object in regard to the size before applying the method of compression and $V''_{(S)}$ is the determined valuation of information security of an object in regard to the size after applying the method of compression;

(2) for each object o_f is determined the highest value of relatively valuation of the size ($\max RV_{(S)}$), which presents the highest increase of $V_{(S)}$, achieved by this object in all triple relations;

(3) for each relation attack—method—object is determined the co-efficient of information security with respect to the parameter *SIZE* ($K^{IS(S)}$). For each triple relation this co-efficient presents the part of maximum possible value of relatively valuation of the size, which the object is achieved (Formula 4):

$$K^{IS(S)} = \frac{RV_{(S)}}{\max RV_{(S)}} \qquad \text{Formula 4}$$

Graphically $K^{IS(S)}$ can be presented as (Expression 2):

$$K_z^{IS(S)} = f\left(a_i, m_j\right) \quad \text{for each } o_f \qquad \text{Expression 2}$$

where $a_i \in A_{pot}\{a_1, a_2, ..., a_i, ..., a_p\}$, $m_j \in M_{pot}\{m_1, m_2, ..., m_j, ..., m_q\}$, $o_f \in O_{pot}\{o_1, o_2, ..., o_f, ..., o_r\}$, and the index *z* is changing within the bounds of the formula a_p, m_q and o_r.

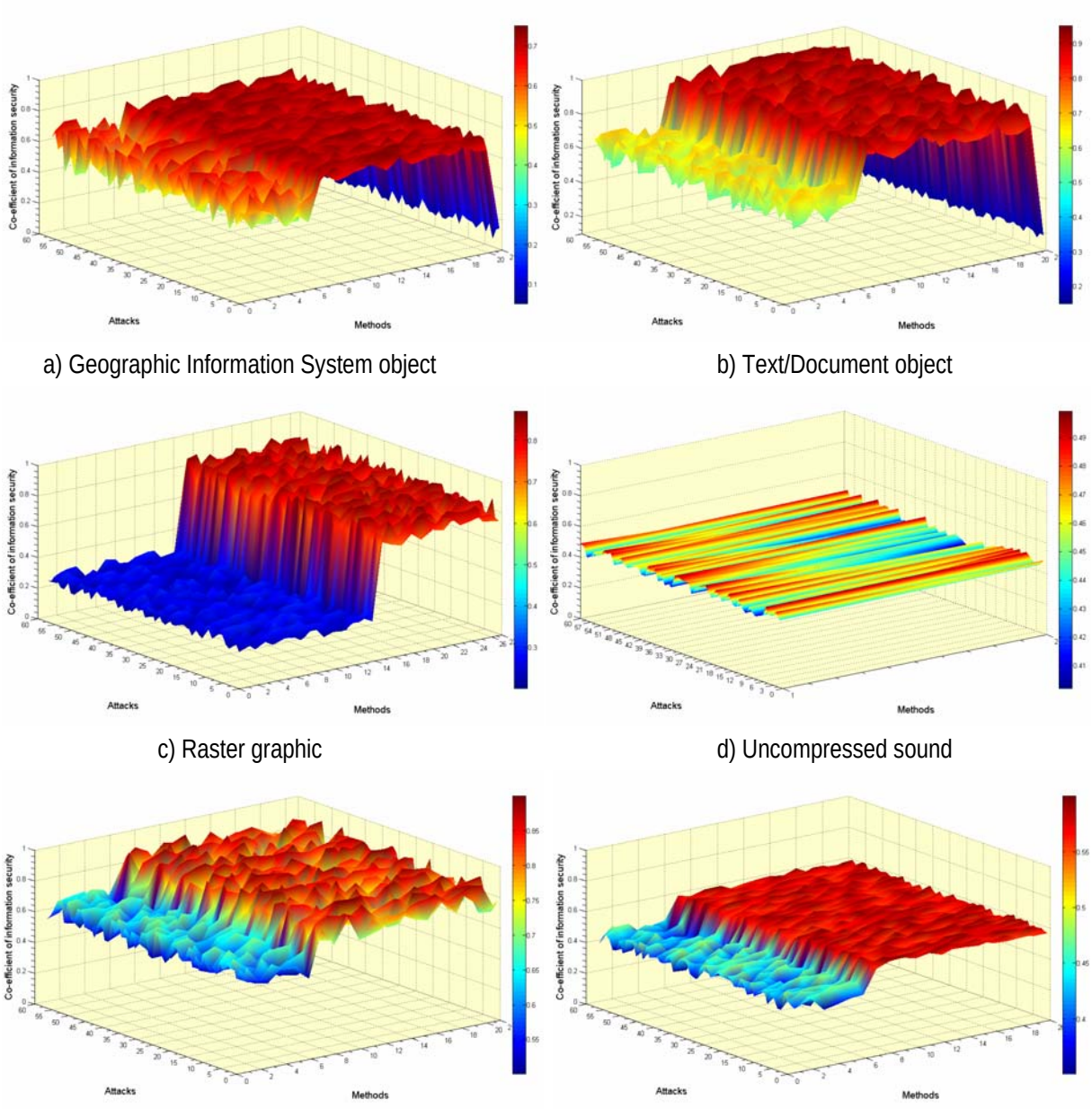
2.3 Determining the co-efficient of information security of an object (K^{IS}) as a mean of the co-efficients for evaluating the two parameters (*TIME* and *SIZE*).

After determining of the co-efficients $K^{IS(T)}$ and $K^{IS(S)}$, for each object can be composed co-efficient of information security. The co-efficient of information security of an object (K^{IS}) can be determined as a mean of co-efficients for valuation of parameters *TIME* and *SIZE* (Formula 5):

$$K_z^{IS} = \frac{1}{n}\sum_{p=1}^{n} K^{IS(p)} \qquad \text{Formula 5}$$

where $K^{IS(p)}$ is the co-efficient of information security of an object in regard to a given parameter *p*, *n* is the number of investigated parameters in regard to information security of an object and *z* is changing within the bounds of the formula a_p, m_q and o_r.

Graphic interpretation for determined values of the K^{IS} for most frequently used file objects is shown on Figure 2a), b), c), d), e), f).



a) Geographic Information System object

b) Text/Document object

c) Raster graphic

d) Uncompressed sound

e) Dynamic web page

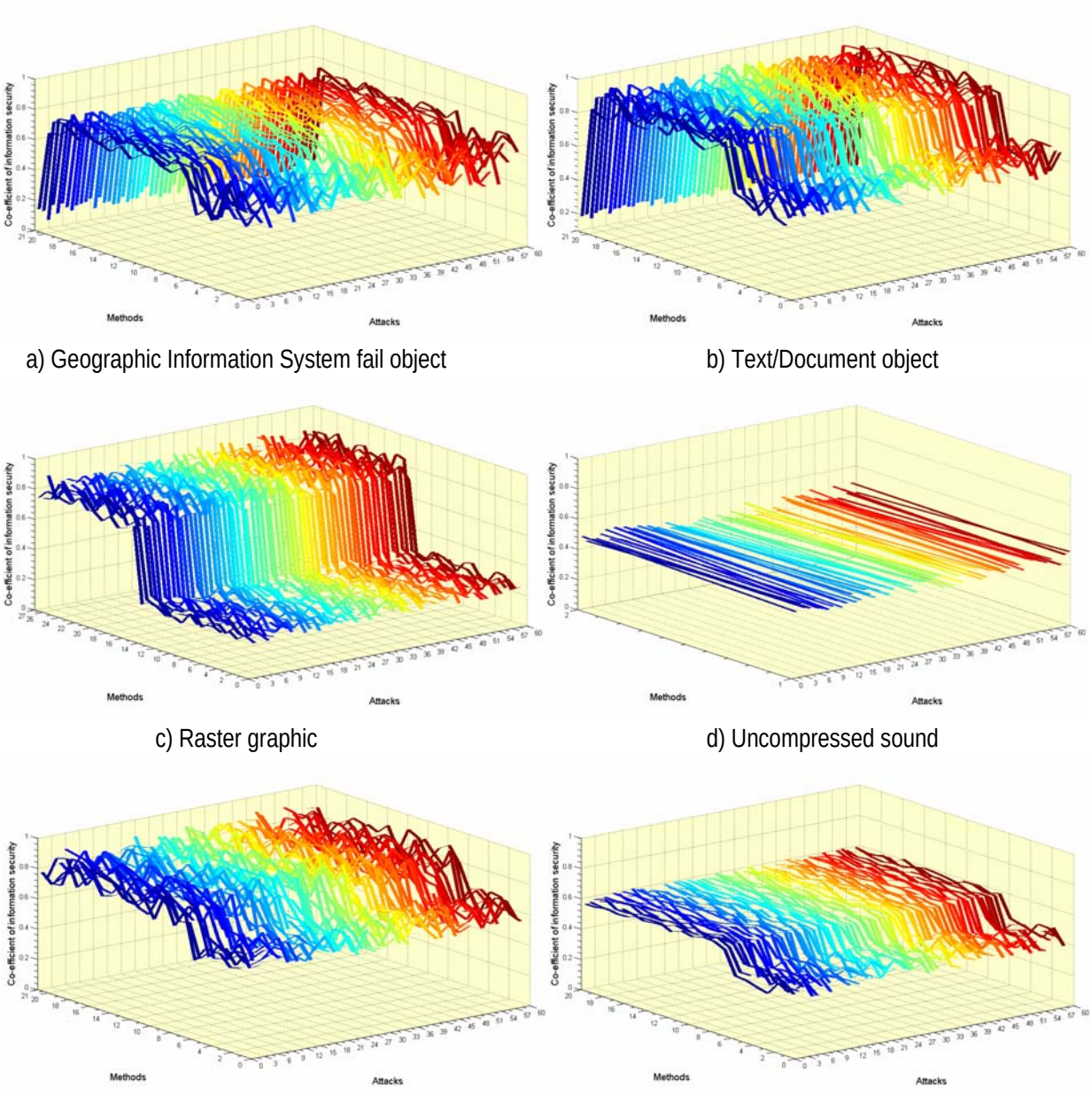
f) Source code

Figure 2 Graphic interpretation for determined values of the co-efficient of information security for different file objects

3. METHODS WITH THE HIGHEST VALUES OF THE CO-EFFICIENT OF INFORMATION SECURITY.

3.1. Determining the methods with the highest values of the co-efficient of information security for each object for the given attack.

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 fig 3a), 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.



a) Geographic Information System fail object

b) Text/Document object

c) Raster graphic

d) Uncompressed sound

e) Dynamic web page

f) Source code

Figure 3 Distribution of the co-efficient for informational security for given object and attack, when a given method of compression is applied

3.2. Determining the methods with the highest values of the co-efficient of information security for all objects in regard to given attacks.

Thus for each object can be set up a group of methods of compression, reaching the highest values of K^{IS} with respect to all attacks on which the object can be exposed.

Derived from this particular scientific work the results are the basis for further research in connection with the opportunity to determine the method of compression, which will have the lowest risk in regard to the information security for the given object and attacks, for which it can be applied.

Assessments

1) Parameters used for determining *TIME* and *SIZE* are sufficient for researching information security of objects and computer systems and networks for consumer, not governmental (corporate) needs.

2) Evaluation in regard to the selected objects, which were processed with methods of compression, is positive and the allowances do not affect the derived result.

3) In regard to the methods of compression we used the assessment is positive and the above mentioned experiments can be used and tailored to other methods of compression.

4) We can conclude, looking at the experiments, that with the decreasing size of an object after compression, time needed for an attack to complete its work over the object will increase.

5) As with the co-efficient of information security the best results were obtained from data objects, processed with dictionary methods of compression, and the worst results were obtained with the graphics objects processed with statistical methods of compression.

6) From all 59 methods of compression, 13 of them gave us the highest value of the co-efficient of information security of the object. They are from the group of dictionary methods and image methods of compression.

Bibliography

[1] Elena Ferrari, Bhavani M. Thuraisingham, *Web and Information Security*, IRM Press, 2006, ISBN: 1-59140-589-0, p. 215

[2] http://www.answers.com/file

[3] David Salomon, *Data Compression: The Complete Reference*, Springer, 2006, ISBN: 1846286026, p.1-9

[4] Polimirova, D., Nickolov, E., Nikolov, C., *Investigating The Relations Of Attacks, Methods And Objects In Regard To Information Security In Network TCP/IP Environment*, International Journal "Information Theories & Applications", vol. 1 / 2007, Number 1, ISSN 1313-0455, p. 85-92

[5] Hubert Hasenauer, *Sustainable Forest Management: Growth Models for Europe*, Springer 2006, ISBN: 9783540260981 p.267-269

Authors' Information

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

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

ICT SECURITY MANAGEMENT

Jeanne Schreurs, Rachel Moreau

Abstract: Security becomes more and more important and companies are aware that it has become a management problem. It's critical to know what are the critical resources and processes of the company and their weaknesses. A security audit can be a handy solution. We have developed BEVA, a method to critically analyse the company and to uncover the weak spots in the security system. BEVA results in security scores for each security factor and also in a general security score. The goal is to increase the security score Ss to a postulated level by focusing on the critical security factors, those with a low security score.

Keywords: Security, Scan, Audit

Introduction

As a consequence of the fast integration of technologies as Internet, Intranet, Extranet, Voice over IP and e-commerce, companies ICT-infrastructure will move to more openness to the outside world and as a consequence