APPLICATION OF METHODS OF MULTI-CRITERIA EVALUATION IN CHOOSING A METHOD OF COMPRESSION AS A MEANS OF HEIGHTENING THE INFORMATION SECURITY OF SYSTEM AND APPLIED OBJECTS

Dimitrina Polimirova, Eugene Nickolov, Cecko Nikolov

Abstract: In this paper is proposed a model for researching the capability to influence, by selected methods' groups of compression, to the co-efficient of information security of selected objects' groups, exposed to selected attacks' groups. With the help of methods for multi-criteria evaluation are chosen the methods' groups with the lowest risk with respect to the information security. Recommendations for future investigations are proposed.

Keywords: Attacks, Methods of Compression, Objects, Information Security, Methods for Multi-criteria Evaluation, Risk Assessment.

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

The Situation

In the modern society of advanced information technologies a great importance is attributed to different methods of compression of information flows. This is related not only to the growing requirements for reducing their volume, but also to the developing variety techniques for heightening their information security when they are exposed to different attacks.

In recent years, topic of theoretical and experimental researches will be different methods of compression, having for an object to reduce the volume of information flows in the processes of transfer, processing and storage [1].

Another current problem, with respect to information flows' investigations, is heightening their security in relation to different attacks. The successful solving of this problem can be reached by application of different methods of compression to achieve volume reduction of the object and heightening their information security.

The Problem

In [2] a number of experiments had conducted connected with the information security of the object under attack and processed by different methods of compression. Co-efficient of information security is determined and selection of methods with highest co-efficient values of for each object in relation to all attacks is made.

The nest stage is to choose the method with the lowest risk in respect to the co-efficient of information security in relation to the investigated attacks. What has become a priority problem is the set of seriously questions relating to theories, methodologies and practices applied in decision making in relation to implementing a specific safety policy in environment of risk and uncertainly under certain computer, system and network configuration.

The Experiment

The purpose of the current investigation is to propose a model for researching the capability to influence to the co-efficient of information security of objects by methods of compression.

The main purpose of the model is to rate the best alternatives or variants for the decision-maker by calculating multi-criteria problems [3].

The general formulation, the model is based on, is as follows. Let (*M*) is the set of elements (alternatives, real objects), which will be evaluated, compared and among which a selection will be made. All elements of *M* can be described by one set of characteristics (time, size etc.), which is the same for all elements of *M*. A vector of numerical values for characteristics is assigned for each element.

Posed tasks:

1) To design the basic parameters of the model.

In the model are included representatives of the attacks' groups ($a_i \in A_{pot}$), methods' groups ($m_j \in M_{pot}$) and objects' groups ($o_f \in O_{pot}$), which had been determined in [4] by means of matrix transformations, applied on initially build base of relations between maximum attacks' groups (A_{max}), methods' groups (M_{max}) and objects groups (O_{max}). Three representatives for each of the 8th methods' groups (from the set of M_{pot}) from totally 10 methods' groups (from the set of M_{max}) are chosen. Three representatives for each of the 18th attacks' groups (from the set of A_{pot}) from totally 33 attacks' groups (from the set of A_{max}) are included in the model. The methods and the attacks are investigated using three representatives for each of the 7 objects' groups (from the set of O_{pot}) from totally 10 objects' groups (from the set of O_{max}). The attacks' groups, methods' groups and objects' groups are shown in Tables 1a, 1b, 1c.

Table 1a List of attacks' groups

ATTACKS' GROUPS
I. Advertisements
V. Chat
VI. Criminal Investigations
VII. Cracking
VIII. Spying
X. Exploits
XIII. Scanners
XIV. Keyboard Modifiers
XVII. Computer Trojan Horses
XVIII. Computer Backdoors
XIX. Computer Worms
XX. Computer Viruses
XXI. Accessible information
XXIV. Content
XXV. Data Encapsulation
XXVII. Spoofing
XXXI. Social Engineering
XXXIII. Zombie Computers

Table 1b List of methods' groups

METHODS' GROUPS
I. Statistical lossless methods
II. Dictionary lossless methods
III. Image lossless methods
IV. Audio lossless methods
V. Other lossless methods
VI. Dictionary lossy methods
VII. Image lossy methods
X. Audio lossy methods

Table 1c List of objects' groups

OBJECTS' GROUPS
II. Scientific file formats
III. Data file formats
IV. Graphics
V. Sound
VII. Internet related
VIII. Binaries
X. Miscellaneous

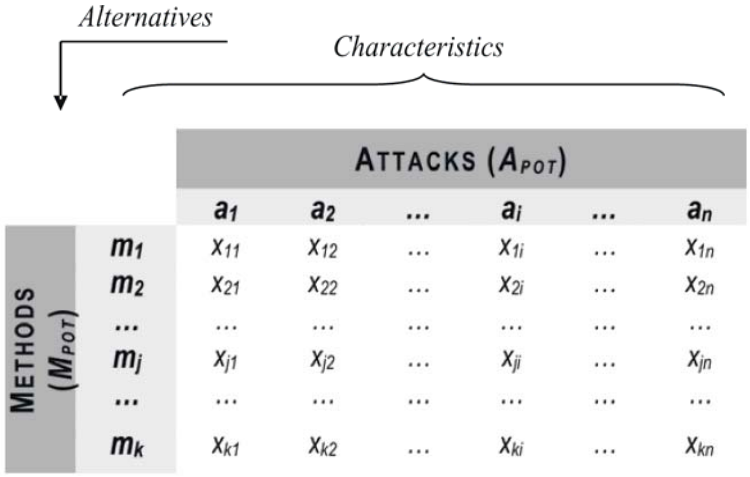
The model makes possible to assess the risk in relation to achieving higher co-efficient of information security when methods of compression are applied to different objects.

2) To build the main database.

It is necessary to systematize the available information to realize this model. For that purpose a matrix $B_{(k,n)}$ is built, which includes the most efficient methods for one objects' group (which are the different alternatives for decision-maker) and the attacks' groups, which can access to these objects' groups processed by these methods' groups (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 $B_{(k,n)}$ is built for each of 7th objects' group. On Table 2 is shown a model of this matrix.

In the database of the matrices are included the average values of the obtained coefficients of information security when 24 representatives of the 8th methods' groups are applied to 21 representatives of the 7th objects' groups, exposed to 54 representatives of the 18th attacks' groups.

Table 2 A matrix structure, including co-efficient of information security, obtained when methods' groups are applied to one objects' group, exposed to the corresponding attacks' groups.



		ATTACKS (A_{POT})					
		a_1	a_2	...	a_i	...	a_n
METHODS (M_{POT})	m_1	x_{11}	x_{12}	...	x_{1i}	...	x_{1n}
	m_2	x_{21}	x_{22}	...	x_{2i}	...	x_{2n}
	...	...	...	...	...	...	...
	m_j	x_{j1}	x_{j2}	...	x_{ji}	...	x_{jn}
	...	...	...	...	...	...	...
	m_k	x_{k1}	x_{k2}	...	x_{ki}	...	x_{kn}

To simplify the visualization in Table 3 are shown the average values of the co-efficient of information security, obtained from all 7 matrices.

Table 3 Matrix with average values of obtained coefficient of information security when methods' groups are applied to one objects' group, exposed to the corresponding attacks' groups.

		ATTACKS' GROUPS								
		I	V	VI	VII	VIII	X	XIII	XIV	XVII
		=1=	=2=	=3=	=4=	=5=	=6=	=7=	=8=	=9=
METHODS' GROUPS	I			2,5	3,3	3,62	2,43	3,63		2,76
	II			3,86	4,62	5,26	2,42	5,28		4,13
	III	6,05	6,16	5,36	6,19	6,17		6,22	5,33	5,39
	IV			3,75	4,67	4,68		4,69		4,22
	V			2,76	3,79	3,79	2,06	3,8		3,33
	VI	25,87	25,93	25,17	25,96	25,95		25,97		25,21
	VII	17,53	17,6	16,82	17,62	17,61		17,64		16,87
	X			7,2	8,11	8,12		8,13		7,7
		ATTACKS' GROUPS								
		XVIII	XIX	XX	XXI	XXIV	XXV	XXVII	XXXI	XXXIII
		=10=	=11=	=12=	=13=	=14=	=15=	=16=	=17=	=18=
METHODS' GROUPS	I	2,81	2,72	2,45	2,64	3,32	3,17	4,16	2,54	3,33
	II	4,19	4,09	3,79	4,01	4,64	4,52	6,33	3,9	4,65
	III	5,42	5,36	5,3	5,36		5,86	6,19	5,3	6,25
	IV	4,19	4,19	3,97	4,03		4,51	4,67	3,91	4,69
	V	3,37	3,23	2,92	3,18	3,79	3,7	5,52	3,03	3,8
	VI	25,25	25,17	25,06	25,17		25,73	25,96	25,06	25,99
	VII	16,9	16,82	16,73	16,82		17,38	17,62	16,73	17,66
	X	7,67	7,67	7,45	7,5		7,98	8,11	7,38	8,13

3) To determine methods for evaluation.

The best variant for decision-maker can be determined with the help of the matrix and different methods for multi-criteria evaluation. 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. To find these variants, the following methods for multi-criteria evaluation are used: method of linear

combination of formal criteria and method of maximum guaranteed result. Both methods are based on the same model.

To calculate such a problem according to these methods for multi-criteria evaluation, a transformation, cold normalization (c_{kn}), has to be accomplished for the matrix $B_{(k,n)}$. This means that the maximum value for the column a_i has to be found, where we write 1, and the rest are filled up as the current value of K_{INF} is divided on the maximum value of K_{INF}. The obtained normalized results are filled in matrix $C_{(k,n)}$, which has the same structure as matrix $B_{(k,n)}$ and is part of input data for the model, realizing methods for multi-criteria evaluation and chose of elements from M_{pot} (Table 4).

Table 4 A matrix structure with normalized values

Alternatives ↓ / *Characteristics* →

		ATTACKS (A_{POT})					
		a_1	a_2	...	a_i	...	a_n
METHODS (M_{POT})	m_1	c_{11}	c_{12}	...	c_{1i}	...	c_{1n}
	m_2	c_{21}	c_{22}	...	c_{2i}	...	c_{2n}
	...	...	...	...	...	...	...
	m_j	c_{j1}	c_{j2}	...	c_{ji}	...	c_{jn}
	...	...	...	...	...	...	...
	m_k	c_{k1}	c_{k2}	...	c_{ki}	...	c_{kn}
	$\max_n$	max_1	max_2	...	max_i	...	max_n

To simplify the visualization in Table 5 are shown the average values of the normalized coefficients of information security, obtained from all 7 matrices.

Table 5a Matrix with average values of normalized coefficients of information security (left part).

		ATTACKS' GROUPS								
		I	V	VI	VII	VIII	X	XIII	XIV	XVII
		=1=	=2=	=3=	=4=	=5=	=6=	=7=	=8=	=9=
METHODS' GROUPS	I			0,1	0,13	0,14	1	0,14		0,11
	II			0,15	0,18	0,20	0,99	0,2		0,16
	III	0,23	0,24	0,21	0,24	0,24		0,24	1	0,21
	IV			0,15	0,18	0,18		0,18		0,17
	V			0,11	0,15	0,15	0,85	0,15		0,13
	VI	1	1	1	1	1		1		1
	VII	0,68	0,68	0,67	0,68	0,68		0,68		0,67
	X			0,29	0,31	0,31		0,31		0,31
	$\max_n$	**25,87**	**25,93**	**25,17**	**25,96**	**25,95**	**2,43**	**35,97**	**5,33**	**25,21**

Table 5b Matrix with average values of normalized coefficients of information security (right part).

		ATTACKS' GROUPS								
		XVIII	XIX	XX	XXI	XXIV	XXV	XXVII	XXXI	XXXIII
		=10=	=11=	=12=	=13=	=14=	=15=	=16=	=17=	=18=
METHODS' GROUPS	I	0,11	0,11	0,1	0,1	0,72	0,12	0,16	0,1	0,13
	II	0,17	0,16	0,15	0,16	1	0,18	0,24	0,16	0,18
	III	0,21	0,21	0,21	0,23		0,23	0,24	0,21	0,24
	IV	0,17	0,17	0,16	0,16		0,18	0,18	0,16	0,18
	V	0,13	0,13	0,12	0,13	0,82	0,14	0,21	0,12	0,15
	VI	1	1	1	1		1	1	1	1
	VII	0,67	0,67	0,67	0,67		0,68	0,68	0,67	0,68
	X	0,3	0,3	0,3	0,3		0,31	0,31	0,29	0,31
	$\max_n$	**25,25**	**25,17**	**25,06**	**25,17**	**4,64**	**25,73**	**25,96**	**25,06**	**25,99**

To use the multi-criteria evaluation methods a weighted co-efficient (λ_{ji}) for each attack has to be determined. It can be described as the possibility one of pre-chosen attacks' groups to get access to one objects' group from a pre-defined set of objects' groups. The weighted co-efficient of the attacks is shown in Tables 6a, 6b.

Table 6a
The weighted co-efficient of the attacks

ATTACKS' GROUPS	λ
I. Advertisements	0,06
V. Chat	3,2
VI. Criminal Investigations	0,2
VII. Cracking	7,4
VIII. Spying	6,2
X. Exploits	5,2
XIII. Scanners	3,4
XIV. Keyboard Modifiers	7,9
XVII. Computer Trojan Horses	12,15

Table 6b
The weighted co-efficient of the attacks

ATTACKS' GROUPS	λ
XVIII. Computer Backdoors	9,25
XIX. Computer Worms	8,73
XX. Computer Viruses	9,15
XXI. Accessible information	7,2
XXIV. Content	7,7
XXV. Data Encapsulation	0,07
XXVII. Spoofing	5,3
XXXI. Social Engineering	6,8
XXXIII. Zombie Computers	0,09

Method of linear combination of formal criteria

The matrix with normalized values $C_{(k,n)}$ is used. It uses the vector $\vec{\lambda} = \left(\lambda_1, \lambda_2, ..., \lambda_i, ..., \lambda_p\right)$ as an input parameter, whose components are real non-negative numbers and represents weight for decision-making. The following limitation $\sum_i \lambda_i = 1$ has to be observed.

The calculating is:

a) For each alternative (methods' group) is assigned the number S_k, where:

$$S_k = \sum_{i=1}^{p} \lambda_i c_{kn}$$

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

Method of maximum guaranteed result

The matrix with normalized values $C_{(k,n)}$ 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 $\sum_i \lambda_i = 1$ has to be observed for.

The calculating is:

a) For each alternative (methods' group) is assigned the number t_k where:

$$t_k = \min_n \left(\lambda_i c_{kn}\right) = \min\left(\lambda_1.c_{j1}, \lambda_2.c_{j2}, ..., \lambda_p.c_{kn}\right)$$

b) The alternatives are sorted in ascending order by the number t_k.

By analogy a variant of these both methods for multi-criteria evaluation can be examined when the values of weighted coefficients are equal. For more detailed analysis can be assumed that the weighted co-efficient λ_i can not always be known. In that case can be made the assumption that all values of λ_i are equal (which is assigned as λ_i^L). Then:

$$S_k^L = \sum \lambda_i^L c_{kn}$$

$$t_k^L = \min_n \left(\lambda_i^L c_{kn}\right)$$

These methods for multi-criteria evaluation are applied for each matrix (i.e. for each objects' group). Thus, for each objects' group we can choose an alternative (methods' group) we give preference to, with respect to the co-efficient of information security to all attacks' groups. The obtained average values are shown in Table 7.

Table 7 Average values when methods for multi-criteria evaluation are applied

S_k	t_k	S_k^L	t_k^L
Dictionary lossy methods	Dictionary lossy methods	Dictionary lossy methods	Dictionary lossy methods
Image lossy methods	Image lossy methods	Image lossy methods	Image lossy methods
Dictionary lossless methods	Audio lossy methods	Dictionary lossless methods	Audio lossy methods
Image lossless methods	Statistical lossless methods	Image lossless methods	Statistical lossless methods
Audio lossy methods	Dictionary lossless methods	Audio lossy methods	Dictionary lossless methods
Other lossless methods	Image lossless methods	Other lossless methods	Image lossless methods
Statistical lossless methods	Audio lossless methods	Statistical lossless methods	Audio lossless methods
Audio lossless methods	Other lossless methods	Audio lossless methods	Other lossless methods

4) To choose an alternative.

On the base of the obtained results in Table 7 a conclusion for the best alternative (methods' group) for decision making with respect to these methods for multi-criteria evaluation can be made. From chosen methods of compression we can make the conclusion, that with respect to the information security attacking objects' groups with different attacks, the lowest risk is when method of compression from the group of Dictionary lossy methods are applied.

5) To determine the methods with lowest risk with respect to the co-efficient of information security.

Matrices and methods for multi-criteria evaluation, which are described higher up, are applied for each objects' group. On the base on the obtained results is made a conclusion, which indicates the methods' groups with

lowest risk with respect to the co-efficient of information security for each objects' group in relation to all attacks' groups. The results are shown in Table 8.

Table 8. Methods' groups with lowest risk with respect to the co-efficient of information security for each group of objects in relation to all attacks' groups

OBJECTS' GROUPS	METHODS' GROUP
II. Scientific	Statistical lossless methods
III. Data	Dictionary lossless methods
IV. Graphics	Dictionary lossy methods, image lossy methods
V. Sound	Audio lossy methods
VII. Internet	Dictionary lossless methods
VIII. Binaries	Statistical lossless methods
X. Miscellaneous	Dictionary lossless methods

Conclusions

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.

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.

Recommendations

Investigations have to be made for the influence of the number of methods for multi-criteria evaluation on the order of the alternatives and respectively on the decision for decision-maker.

Future investigations have to be made with respect to the password, which can be applied, and its influence on the co-efficient of information security and the respective decision for the decision-maker.

Bibliography

[1] Milenko Drinić, Darko Kirovski, Hoi Vo, Code Optimization for Code Compression, Proceedings of the International Symposium on Code Generation and Optimization (CGO'03), 2003 IEEE.

[2] Dimitrina Polimirova, Eugene Nickolov, Cecko Nikolov, Research Of The Influence Of Methods Of Compression On The Co-Efficient Of Information Security Of Objects Under Attacks, Proceedings of International Conference Information Theories and Applications: Cyber Security, 28-29 June 2006, Varna, to be published.

[3] Иван Попчев, Боян Метев, Лорета Маркова, Класиране на системни програмни пакети чрез многокритериална оценка, сп. Техническа мисъл, №1р 1987.

[4] Dimitrina Polimirova, Eugene Nickolov, Cecko Nikolov, Investigating The Relations Of Attacks, Methods And Objects In Regard To Information Security In Network TCP/IP Environment, Proceedings of International Conference Information Theories and Applications: Cyber Security, 28-29 June 2006, Varna, to be published.

Authors' Information

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

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

Cecko Nikolov – PhD Student, Research Associate, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Phone: +359-2-9733398, e-mail: nikolov@nlcv.bas.bg