THE METHOD OF EVALUATION DEGREE OF CHANGES CONFIDENTIALITY ATTRIBUTE OF INFORMATION ASSET INSIDE ICT SYSTEM

METODA OCENY STOPNIA ZMIAN ATRYBUTU POUFNOŚCI ZASOBU INFORMACYJNEGO W SYSTEMIE TELEINFORMATYCZNYM

Artur Szleszyński

The General Tadeusz Kościuszko Military Academy of Land Forces
e-mail: a.szleszynski@wso.wroc.pl

Abstract: *The work presents the proposition of inference system that evaluates the possibility of information confidentiality attribute violation. Crisp and fuzzy variables have been defined. Values of output variables from fuzzy logic system have been presented. The way of counting the modified value of information confidentiality attribute has been described.*

Keywords: *information asset confidentiality attribute, fuzzy inference*

Streszczenie: *Praca przedstawia propozycję systemu wnioskującego wykorzystywanego do oceny możliwości naruszenia atrybutu poufności zasobu informacyjnego. W pracy zdefiniowano zmienne dokładne i rozmyte. Zostały zaprezentowane wyniki wnioskowania rozmytego. Pokazano metodę obliczania zmodyfikowanej wartości atrybutu poufności zasobu informacyjnego.*

Słowa kluczowe: *atrybut poufności zasobu informacyjnego, wnioskowanie rozmyte*

1. Introduction

Information belongs to the most important assets of organization. It enables the organization to fulfill its tasks. Each of information asset is described by three security attributes. These are: confidentiality, integrity and accessibility [2,10]. The confidentiality of information asset is one of the most important security attributes. It is first from the top on the list of attributes described in norms and scientific publications [4,10]. It is hard to estimate the degree of change in confidentiality attribute. The problem with its estimation derives from the specificity of confidentiality attribute [12]. Confidentiality attribute concerns the content of information asset. We cannot, therefore, be sure of violation of confidentiality attribute from the information asset until its content is revealed by unauthorized person [12,14].

The informative resource is a multiform entity. This work presents the method of evaluation of affectation degree of confidential attribute information asset within the data-communication system. Therefore, the term 'information asset' describes files that are exchanged among the users in computer network systems. The file is one of main parts of the system. It is used to: gathering, processing and exchanging data among users and operating system elements [1]. The other important functionality of a file is to cover the confidentiality attribute. The content of a file will affect the proper functioning of operating system and its software.

One of the methods used to secure the file content is encryption. It protects the content of information asset from potential intruders. However, as the study of literature reveals, badly designed crypto-system may be easily broken down and enables unauthorized person to acquaint the content of the resource [13]. Time required to reveal the encoded text of protected document is short. In Semjonov's works it has been proved that time required to reveal the three character long password protecting the file from encoding equals from 0,02 to 1s. The author did not provide the technical data of equipment used for encoding the crypto-system protecting the file, however, the time needed to violate the protection that is shorter than 1 second means that this protection does not exist.

This article focuses on estimation of possibility to change the information confidentiality attribute in a file created in an office computer. These assets are the major group because they are used in commanding and decision making processes within the corporation.

2. Problem identification

In the literature of the subject there are examples of attempts in security attributes change estimation, such as: integrity and accessibility. A. Szleszyński in his thesis shows how to estimate the degree of change introduced by i.e. malware software or an intruder in estimated file. The degree of change is estimated by comparison of bytes changed in the given message to total bytes in model message. On the basis of this measure the degree of change in the attribute of information asset integrity has been estimated.

The accessibility of information asset is estimated by the number of events while the asset is accessible and when it is not [14]. It is easy to make measurements of both types of attributes. The problem arises while estimating changes of confidentiality attribute from information assets. Similarly to Computer Forensics it is necessary to gather evidence that would confirm or deny the ability of partial or total violation of confidentiality attribute [1]. The term ‘ability’ is used on purpose, because the evidence will express the degree of subjective decision-maker’s opinion that such an event took place [9,12].

This inference is typical for fuzzy logic where, by determining the degree of belonging (the measure of subjective opinion) the degree of change in confidentiality attribute is expressed [9,11,12].

In Jonsson, Anderson and Amusen thesis, authors present the method of system confidentiality estimation [6]. Confidentiality is treated by authors as the behavioral aspect of the system¹. To describe the confidentiality change in system object² (SO) the authors used Markov’s processes. The confidentiality has been treated as an element of system credibility [6]. To describe the confidentiality change the authors used four collections of data. The collection of system status, the collection of maintenance level, the collection of defect status, the collection of SO activity joined with the collection of maintenance levels. The collection of system status and the collection of maintenance levels are separate collections. The necessity of identification elements from four different collections, part of which is made due to combination of elements from two collections, make the method very complex. The attempt for applying it requests the ability to make transition matrixes for each moment in time.

The advantage of described method is the use of object analysis techniques that are used in reliability estimation. These techniques are well defined, examined and widely applied in engineering practice.

Therefore, if the method of security attribute confidentiality change estimation proposed in literature is difficult to be applied, which other technique can be used for the estimation of its degree of change?

3. The selection of sensible assets and factors influencing changes in confidentiality attribute.

Resources classified to the group of sensible assets will be studied in terms of a degree of change. Information asset is classified to the group of sensible assets when the violation of its security attributes results in disruptions in performance of the subject that uses it in its activity [2,8]. The security of selected group of information assets is enforced by law. This concerns personal data, medical record, etc. [2,8]. Inappropriate security of those assets may cause the penalties stipulated by the law [2,8].

¹ According to the authors of the thesis, security of electronic systems consists of two aspects: preventive and behavioral.

² The system object (SO) is the estimated electronic system [Jonsson].

An example of estimation method for incidents that influence the information assets belonging to a computer system were presented in thesis by I. Jóźwiak and A. Szleszyński [7]. The graph presented in the thesis, that is a substitute scheme of a system, pictures the data flow in it. The information assets in computer system may be described by two components such as confidentiality attribute and computer system element that consists of the asset that is the subject of the study. The description of information asset is presented by the following equation:

$$IA = \langle SA, E \rangle \quad (1)$$

where:

IA - information asset,

SA- security attributes of information asset,

E - element that consists of information asset that is the subject of study.

Security attributes consist of three elements: confidentiality attribute, integrity attribute and accessibility attribute. The above is presented by the following equation (2):

$$SA = \langle C, I, A \rangle \quad (2)$$

where:

C - confidentiality attribute,

I - integrity attribute,

A - accessibility attribute of an information asset being the subject of study.

The factors that influence the change of values in particular safety attributes are: malware software, intruder activities, computer system elements malfunctions, information assets protection software activity, etc.

The changes in values of integrity and accessibility attributes will indicate the possibility of confidentiality attribute violation. It is essential to use the inference mechanism to estimate the degree of change in confidentiality attribute. The inference outcome will perform a function of an indirect measure based on direct measures of other safety attributes, incidents occurring in estimated element and connections between them [12,14]. Because the value of confidentiality attribute change is unknown and there is no evidence confirming (or denying) this change, therefore the use of fuzzy logic inference is recommended [9,11]. This inference uses the belonging function that describes the degree of change in value of confidentiality attribute. The applied method allows the use of variables of estimated changes in information asset confidentiality attribute.

4. Fuzzy-logic system of estimation of change degree in information asset of confidentiality attribute

The construction of the system will be based on construction methods of fuzzy drivers described in the literature of the subject [3,16]. The estimation begins from determining the fuzzy values for particular elements.

The measures introduced to the estimation subsystem are:

- checksums of files qualified as sensible assets,
- the degree of change introduced to the estimated file,
- the significance of identified changes,
- appliance of cryptographic protection of a file contents,
- user imposing the changes, in case of unauthorized user - number of attempts to gain access to the asset,
- time of introducing the changes,
- information about the attempt to send the file via computer network or the attempt to copy it.

The checksum of a file being the subject of study consists of information about changes introduced to the file. The checksum allows fast identification of files that have been changed. This identification method is used in operating systems and antivirus software. The next step is estimation of a degree of change on the basis of number of bytes changed (dbm). The degree of introduced bytes (dbm) is determined by comparison of the changed file contents to the reference file, accordingly to the following equation (3) [12,14].

$$dbm = \frac{ncb}{nbcf} \quad (3)$$

where:

- dbm - factor of bytes changed in file,
- ncb - number of bytes changed in the file,
- nbcf - number of bytes in reference file.

The reference file consists of non-modified version of the asset. This file should be located in a secured place and the access to source files should be supervised. After the degree of change is determined by dbm factor [14] it should be determined if the file was secured cryptographically. If yes, were standard tools of content security used? Were another encryption system used? The research made by Sejmonov reveals that the use of RC4 cryptosystem with 40-bit encrypting key for file content security with password shorter than 7 characters does not ensure adequate file content security [13]. The results of that research are confirmed in thesis by Szleszyński and Wojaczek. Time required to find the passwords made of 3 and 4 characters was shorter than 3 minutes [15]. Mechanism used to secure the file content was ineffective with short password. The software used in research did not use parallel data processing, which would slow down the process of finding the password. The software did not use the abilities of modern computer processors [15].

Another action is to estimate the importance of change made in the file content. This is an example of subjective or expert judgment. The estimation process is based on linguistic variable with the belonging function described by a triangle [3,16]. The next step in estimation process is the answer to question of who and when made the identified changes. This information is obtained from verification subsystem within the operational system of the device storing the asset. To obtain information about changes done to the file, file metrics may be useful. This metrics consists of information on the person (or persons) that introduce modifications, date and time of introduced changes. The review of metrics allows to identify the persons that are potential source of an incident.

The given information is the quantified data that is to be used for the initial selection of modified files. In the fuzzy inference process there are fuzzy variables, such as: importance of introduced changes and information activity about the place of file being sent. Both variables belong to linguistic variables described by triangular belonging functions [3,16,17]. The use of triangular belonging functions is described in the literature of the subject, which allows detailed distribution of belongings to chosen collections. This action allows to make detailed expert judgment expressed by linguistic variable [3,9,16]. Some variables may be related to each other, which is the result of connections between parameters introduced to the inference system. The connections between elements of estimation system shall confirm the correctness of estimated judgment. Those connections shall arise between the number of changed bytes in the file and significance of stated changes in file content. The confirmation of stated thesis is the research that describe the number of bytes changed in encrypted file. The dbm factor for encoded files is between 0,4 and 1 [15]. The described event alerts that there was a violation in information accessibility attribute if the encryption was done not by the authorized user of a file. Therefore, the encrypted file will not be available for the user if the password or method to obtain the open text is unknown.

In case, when values of dbm factor are between 0 and 0,3 and the significance of introduced changes is little, it can be assumed that errors that occurred were made in result of file transmission between computers or as an effect of transmission errors.

The possibility of confidentiality attribute violation in a file may be discovered by: attempts of access to the file by unauthorized persons ³ and time of access to the file. In case of unauthorized user, access to the asset should be controlled. The other option is much more difficult. The user that has the permissions to access the files is eligible to acknowledge its content. What may suggest the attempt to violate confidentiality attribute of an asset is attempt to access the files in non-typical working hours. The attempt (attempts) of transferring the file by authorized user

³ The term 'unauthorized persons' is understood as software ran by operating system during user's work and attempts to access the assets by remote users.

outside the organization IT environment⁴. To determine if the attempt to transfer the file outside the organization IT environment had place it is necessary to use a dedicated tool such as a network scanner or Intrusion Prevention System (IPS) tools. To use a network scanner it is necessary to analyze the record of a scanner software. If it is necessary to analyze scanner files larger than 10 MB, this task will be time-consuming. The longer time needed for the analysis the later comes the outcome of possible information asset confidentiality attribute violation. Similar situation takes place with the IPS software. Such software may generate files containing MB or even GB of data, dependent on desired filters. IPS tools are equipped with procedures supporting the data analyses and presentations of the outcomes. However, it is the personnel responsible for security of information assets in the organization who has the obligation to select the assets that are endangered and choose the ways to protect them.

While creating fuzzy-logic change of confidentiality attribute estimation system, the variables that will participate in the process of making decisions should be defined and classified. Crisp variables - binary - are shown in table 1. Two types of variables will be used: quantified and binary variables (the latter may be treated as variables of singleton type). They are supporting the process of analysis and reduce the calculation complexity of the system [3,5,16]. Their task is to guide the process of inference in the system.

Table 1. Crisp variables used in the process of estimation of changes in confidentiality attributes and accessibility of information assets (source: own study)

VARIABLE	MIN VALUE	MAX VALUE	VARIABLE TYPE
Changed_checksum (ChCKS)	0 (not changed)	1 (changed)	binary
Person_making_the_change (Pmch)	0 (attacker)	1 (authorized user)	binary
Time_of_change (Toch)	0 (typical working hours)	1 (not typical working hours)	binary
Attempt_to_transfer_the_file (Atf)	0 (not stated)	1 (attempt stated)	binary
Attempt_to_access_the_file_by_unauthorized_user (Afu)	0 (not stated)	1 (there was at least one attempt)	binary

The other collection consists of fuzzy variables (shown in table 2) they are used to estimate possible changes in safety attributes and accessibility of information assets. Those variables will affect the result of changes in value of confidentiality attribute and accessibility.

⁴ Assuming that this kind of transmission is not required.

Table 2. Fuzzy variables used in the process of estimation of changes in confidentiality attributes and accessibility of information assets (source: own study)

VARIABLE	MIN VALUE	TYPICAL VALUE	MAX VALUE
Large_dbm_fuzzy (dbmL)	0,5	0,75	1
Medium_dbm_fuzzy (dbmM)	0,2	0,35	0,52
Small_dbm_fuzzy (dbmS)	0	0,125	0,25
Fuzzy_Significance_Small (SS)	0	0,125	0,25
Fuzzy_Significance_Medium (SM)	0,2	0,35	0,52
Fuzzy_Significance_Large (SL)	0,5	0,75	1

The reference to the accessibility attribute derives from the fact that when the file content is encrypted by the attacker, the file will not be available for the authorized user. In the described situation the accessibility attribute is lost.

The last type of variables that needs to be defined is output variable that defines the degree of change in information asset confidentiality attribute. The value of this variable is shown in Table 3.

Table 3. The value of output variable - estimation of change degree in information asset confidentiality attribute (source: own study)

VARIABLE	MIN VALUE	MAX VALUE	QUANTIFIED VALUE
Change_in_large_big (Cvb)	0,9	1	5
Change_big (Cb)	0,6	0,89	4
Change_middle (Cm)	0,4	0,61	3
Change_small (Cs)	0,2	0,41	2
Change_very_small (Cvs)	0,1	0,21	1

Crisp value of output variable is subtracted from the initial value of confidentiality attribute of the asset. The value of confidentiality attribute may be described by vector {5,4,3,2,1}. Where 5 is unchanged value of confidentiality attribute and 1 is the lack of confidentiality attribute of the asset being the subject of study. Similarly the value of accessibility attribute will be determined when the value of blurred factor dbm is between 0,4 and 1. To determine the new value of safety attributes for information asset the equation 4 should be used.

$$SA_i(t_j) = 5 - VoE \quad (4)$$

where:

- $SA_i(t_i)$ - the value of safety attribute of i-th information asset in time t_i ,
- 5 - initial value of confidentiality attribute of i-th information asset,
- VoE - value of estimated possible change in confidentiality attribute.

The value of VoE derives from the system decision, that is processed on the basis of table 4. This table describes relations between blurred variables used in the analysis process and the answer of the structure. The answer is calculated on the basis of rules that describe the possible value of the change.

Table 4. Dependency between blurred variables and system decision (source: own study)

Fdbm \ SC	SL	SM	SS
dbmL	Cvs	Cvs	Cvs
dbmM	Cvb	Cb	Cb
dbmS	Cvb	Cm	Cs

If the value of confidentiality attribute changes from the 2 to 0, there is a need to undertake urgent actions that will lead to security level rise in information asset. Values shown, indicate that given information asset does not fulfill the confidentiality attribute.

5. Conclusions and further work

The method described above allows to estimate possible changes in safety attributes in information asset. The application of blurred logic to describe the situation of possible information asset confidentiality attribute violation derives from the lack of evidence that would confirm the fact of attribute violation. The possibility of confidentiality attribute change is estimated on the basis of premises of estimation. The simplification of inference method derives from the necessity to check files in number larger than one. In case of large number of files, the estimation method that requires long time is inadequate. Assuming that the time required to determine the possibility of change for 1 file equals 1s, than in case of 60 files this time arises 60 times. If the number of locations in the computer system is enlarged to i.e. 10 measurement points (computers, IT devices, etc.) than this estimation time arises 10 times. Long time of determining the possible changes causes that the inertia of this solution arises.

The aim of further works will be verification of this solution effectiveness and improvement of calculation efficiency.

6. Bibliography

1. Altheid C., Harlan C.: *Digital Forensics with Open Source Tools*, Elsevier 2011.
2. Białas A., Bezpieczeństwo informacji i usług we współczesnej firmie i organizacji, WNT, Warszawa 2006. (in polish)
3. Bryan L.A., Bryan E.A.: *Programmable Controllers. Theory and Implementation*, An Industrial Text Company Publication, Atlanta 1997.
4. ISO/IEC 15408 – 1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. International Standardization Organization Geneva 2009.

5. Jantzen J.: Design of Fuzzy Control, Technical Report, Technical University of Denmark, 1998.
6. Jonnson E.: Anderson A., Amussen S., An Attempt to Qualitative Modeling of Behaviour Security, [on-line] http://publications.lib.chalmers.se/records/fulltext/174253/local_174253.pdf
7. Józwiak I., Szleszyński A.: Ocena poziomu bezpieczeństwa zasobów informacyjnych z wykorzystaniem techniki analizy architektury systemu informatycznego, Zeszyty Naukowe Politechniki Śląskiej, Organizacja i Zarządzanie, z. 68, Gliwice 2014, pp.321-334. (in polish)
8. Liderman K.: Analiza ryzyka i bezpieczeństwo informacji, PWN, Warszawa 2008. (in polish)
9. McNeill F., M., Thro E.: Fuzzy Logic. A Practical Approach, Accademic Press, Chestnut Hill MA 1994.
10. Polish Standard PN ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa - Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, Warszawa 2007. (in polish)
11. Rutkowski L.: Metody i techniki sztucznej inteligencji, PWN, Warszawa 2012. (in polish)
12. Rybicki W., Szleszyński A.: Zarządzanie poziomem bezpieczeństwa informacyjnego w systemach teleinformatycznych. Etap I. Metody pomiaru bezpieczeństwa zasobów informacyjnych w systemach teleinformatycznych, Scientific work, WSOWL, Wrocław 2014. (in polish)
13. Semjonov P.: Password Recovery/Cracking FAQ, [on-line, last access on 03.02.2014] <http://www.password-crackers.com/en/articles/12/#3.2> .
14. Szleszyński A.: Pomiar bezpieczeństwa informacji w zarządzaniu bezpieczeństwem w systemie teleinformatycznym, Zeszyty Naukowe Politechniki Śląskiej, s. Organizacja i zarządzanie, z. 74, pp. 83-92, Gliwice 2014. (in polish)
15. Szleszyński A., Wojaczek A.: Bezpieczeństwo zasobów informacyjnych chronionych przy pomocy haseł, Zeszyty Naukowe WSOWL, Wrocław [in progress].
16. Vernon J.: Fuzzy Logic Systems, [on-line] www.control-systems-principles.co.
17. Yager R., R., Filev D.: Essentials of Fuzzy Modeling and Control , Wiley & Sons, 1994.

***Artur Szleszyński Msc** – is a lecturer at Command Institute of the General Tadeusz Kościuszko Land Forces Military Academy. His works are focus on computer simulation and ICT systems security (a specially information security). He uses artificial intelligence method to evaluate information security attributes violation.*