UDC 004

Fuzzy ontology structure for information leaks and ISC

Oleh Kozlenko[1]

[1]*National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Institute of Physics and Technology*

Abstract

The article proposes a variant of the fuzzy ontology for complex information security systems (CISS) analysis, which focuses on the most common variants scenarios for information leaks and on the peculiarities of information security culture. The analysis of CISS is based on many factors (attacks on the system, etc.), among which can be not only technical flaws . Common mistakes and misunderstandings in identifying security incidents and how to respond to them is also important. Therefore, for the basic protection of the system, it is necessary to identify many factors and the structure, which will identify these factors, scenarios, and the relationship between the security elements for future use will greatly simplify the understanding and construction of the CISS. This structure can be used scenarios for information leaks, taking into consideration information security culture and to further determination of the overall formal assessment of the organization's security.

Keywords: ontology, fuzzy ontology, information leaks, information security culture, information threats, level of information security culture.

Introduction

The process of building integrated information security systems (IISS) in connection with the need for a high level of detail of its structure, in particular, the allocation of main components, influential factors and the relations between them, requires analysis and research of this structure for clear formalized conceptual scheme. These particular features are present in ontological analysis, which is based on the concept of "ontology". Definition of ontology is given by T. Gruber [2] and means the specification of conceptualization, where as a conceptualization is description of a plurality of objects of the subject area and the connections between them. But such ontologies can not be used in areas where there is fuzzy information because of the inability to operate relationships without clear frameworks. One solution to this problem is to use a fuzzy ontology that contains elements of fuzzy logic in sets of concepts and relationships. The algorithm for constructing a fuzzy ontology was proposed by Lee [4] in the work associated with news. Later, [9] proposed $FOGA$ ($Fuzzy\ Ontology\ Generation\ Framework$)to create fuzzy ontologies based on fuzzy set theory andFCA ($Fuzzy\ Concept\ Analysis$). Verizon annually carries out research in the field of information security[12],[13],[14],[15] and divides incident data leakage into nine possible scenarios. These scenarios help identify necessary security measures to prevent information leaks, respectively, in each of them, but information security depends not only from hardware side.

1. Theoretical foundations for the construction of the subject domain ontology and fuzzy ontology

If we approach the definition of "ontology" according to [11], computer ontology of the subject domain is : O_F=<C,P_F,R_F,A_F>, where $C = \{ c_1, c_2 , \dots , c_i, \dots , c_n \}$, $i = \overline{1,n}$, $n = CardC$ – finite set of concepts (concepts) of a given subject domain. Each element of the set has properties that are fuzzy sets or values. $P_F = \{ p_1, p_2 , \dots , p_t \}$ – a finite set of properties of concepts of a domain. The property of the concept $p \in P$,$p = (c, v_F, q_F, f, U)$, where $c \in C$ – a concept of ontology, v_F – a reflection of the property c, q_F – linguistic meanings that can affect v_F, f limitations v, U – universe of discord. $R_F = \{ r_1, r_2 , \dots , r_k, \dots , r_m \}$, $k = \overline{1,m}$, $m = CardR_F$ – a finite set of semantically meaningful relations between the concepts of the subject area. Unlike formal ontology $r \in R_F$,$r = (c_1, c_2, t, s_F, U)$, where c_1, c_2 – concepts of ontology, t – relationship between concepts, s_F – depth of the relationship between the concepts and c_1 and c_2 , U – universe of discord. A_F – a set of fuzzy rules. Thus, for the construction of a fuzzy ontology for elements of information protection from leaks, it is necessary to analyze the subject area and identify the main fuzzy concepts, relationships, axioms, and properties.

2. Information leaks

Verizon annually conducts research in information security [12],[13],[14],[15] and demonstrate feasibility to divide incidents of information leaks into nine possible scenarios:

- Point of Sale invasion (POS-invasion)
- attacks on web applications
- crimeware
- cyber-espionage
- payment card scrimmers
- physical theft or loss
- mistakes
- insider attacks
- DOS

Verizon reports on data leaks for 2014 – 2017 identified the respective threats for each of the above scenarios.

Based on this information and factors that Verizon has highlighted in 2014 [12] it is possible to identify security measures for the above scenarios:

- "Inventory" of software
- Lack of unnecessary software, accounts, ports, etc.
- Updates and patches
- Integrity of system files
- Anti-virus software
- Updating security software
- DEP, $ASLR$, $EMET$
- Web application testing
- Enclosed documentation for the developed software
- Backup
- IS trainings
- Staff check
- Traffic filtering
- Separation of services
- Administrators control
- Flexible passwords
- Lack of passwords by default
- Black and white IPs
- Double Authentication
- $Netflow$
- Event Log
- Account Management
- Centralized authentication
- Input Monitoring
- Encryption
- Lack of confidential data in plain text
- DLP
- Incidents
- Roles in incidents
- Network segmentation
- Surveillance
- Terminals check
- User alerts
- Effective design

As noted, not all threats directly depend on the technical features. "Human factor" is also a threat, which is not always associated with deficiencies or imperfections of security measures, but it is always associated with non-compliance with security policy requirements [6]. As noted in [5] users intentionally or due to lack of knowledge are the greatest threat to information security. In [7] Siponen notes that without adequate knowledge and collaboration with users of the security or management department, adequate security measures are becoming ineffective. Study of human factors in the field of information security is increasingly attracting attention, because they have a significant impact on information security in general and separately on its components. In the current literature, information security culture (ISC) is an important component in ensuring the security of information assets of organizations. In such works as [1] author defines ISC as behavior, values and assumptions that provide information security, researchers in [3] define ISC as a system in which motivation, direction, knowledge and mental models interact with each other. Van Nijkerk and Von Solms in their work [10] offer a conceptual model of information security culture. This model aims to determine the interaction between the various elements that constitute the culture of information security. The experiments carried out in [6],[9] help to disassociate the concept of "ISC" into components. Thus, "ISC" can be defined by the following components:

- «Personnel»
- «Staff Security»
- «ISC measures»
- «Management»
- «Management ISC Readiness»
- «Coordination»
- «Cooperation with IS staff»
- «Cooperation with Management»

This components will be used for further analysis and construction of the investigated structure.

3. Construction of fuzzy ontology

As noted in paragraph 1, for building an ontology, it is necessary to determine basic sets. Analysis in paragraphs 2 and 3 helped identify the main elements of interaction and characteristics between security measures against information leaks and measures to ensure an adequate level of information security culture. The main values obtained by using the preliminary analysis are given in 1. To construct a fuzzy ontology, we will use modified algorithm, which is proposed in [8], which is also based on the work [11]. Each of the security elements will be determined using 5 characteristics: G — main objectives of the attack $G = 1$, if only one property of the protected information is violated $G = 2$, if two properties of the protected information are violated $G = 3$, if all three properties of the protected information are violated SM — the elements of protection to prevent the implementation of information leaks for vulnerability $SM = k$, $k \in [1, n]$, n – number of security elements W — Possible ways to implement the threat (local, remote) $W = 1$, if the threat is realized by one of the methods (local or remote) $W = 2$, if the threat can be realized in both ways (locally and remotely) Criticality in number of incidents(R_i) — a parameter that determines the relative severity of vulnerability in a number of incidents of the realization of this threat. The criticality of the amount of information leaks(R_r) — parameter that determines the weight to the criticality of the impact on the amount of information leakage implementation for this threat. Definition of characteristics and determined using formulas

$$R_i = log_{10}(\sum incidents) \tag{1}$$

$$R_r = log_{10}(\sum leaks) \tag{2}$$

The statistics of the number of incidents and information leaks are from Verizon's research for 2014 – 2017 [12],[13],[14],[15]. Due to the lack of necessary information on the number of incidents and sources of information regarding to ISC, the relevant characteristics were taken as a mean of elements that are related to the ISC (such as "protection against insider attacks", etc.). Formula for determining the weighting factor is

$$F = G * R * \frac{R_r}{R_i} \tag{3}$$

The values, which characteristics are determined by the weight characteristic and the number of attributes of each characteristic. Thus, these values are represented by the formula

$$F_r = F * W_p * i(SM) \tag{4}$$

where $i(SM)$ — the number of possible common attributes between the two concepts. W_P— weight characteristic, which is defined as $W_P = (3, objective), (16, securitymeasures), (2, method)$ type of connection between the two concepts is determined by the following set: $T = weak, medium, good$ The relationship between the concepts, as noted in paragraph 1, is defined by the set $r = (c_1, c_2, T, s_F, U)$. c_1, c_2, s_F, U are already defiened . The power of ratio (s_F) is based on the definition of minimum and maximum values. Define these values as follows:

$$S_{F_{min}} = W_P * min(i) \tag{5}$$

$$S_{F_{max}} = W_P * max(i) \tag{6}$$

Defining the minimum and maximum values T,s_F will consist of the following values: S_F=[0 – 38,weak],[39 – 71,medium],[72 – 109,good] Thus, R will consist of (Security measures for web applications attacks , Security measeares for cyber-espionage,39,medium), (Security measures for web applications attacks, Security measures for crimeware,45,medium), (Security measures for DOS, Staff security,40,medium), (Security measures for DOS, ISC measures,40,medium), (Security measures for DOS, Management ISC Readiness,40,medium), (Security measures for insider attacks, Security measures for mistakes,37,medium), (Security measures for insider attacks, Management ISC Readiness,37,medium), (Security measures for cyber-espionage, Security measures for crimeware,71,medium), (Security measures for cyber-espionage, Staff Security,39,medium), (Security measures for cyber-espionage, ISC measurs,39,medium), (Security measures for crimeware, Security measures for POS-invasion,77,good),, (Security measures for POS-invasion, Staff Security,45, medium), (Staff Security, ISC measurs,77,good), (Staff Security, Management ISC Readiness,109,good), (ISC measurs, Management ISC Readiness,61, medium)

Conclusion

The work analyzed the information leaks scenarios that were derived from the information leakage reports for 2014-2017, and the peculiarities of the information security culture that relates to human-induced threats. As a result of the analysis, the necessary sets and relationships for fuzzy ontology have been identified. The resulting structure takes into account the possible elements of protection against information leakage scenarios identified by research data on incidents in the field of information security and taking into account the specificity of the ISC. As can be seen in the article, relation between the security elements can be one value from the set, which helps to conclude that the use of one element information security systems from the ones specified in the article may lead to the use of an element that is with it in weak or medium relation or vice versa. This structure can be used as the basis for the analysis of the CISS system.

References

[1] G. Dhillon, "Managing information system security", London: Macmillan, 1997.

[2] T.R. Gruber, "Toward principles for the design of ontologies used for knowledge sharing", *Hum.-Comput. Stud.,* vol. no. 43 (5-6), pp. 907-928. 1995.

[3] T. Helokunnas, "Information security culture in a value net", *In: Engineering Management Conference, IEMC'03 on Managing Technologically Driven Organizations: The Human Side of Innovation and Change,* New York: IEEE Press., pp. 190–194, 2003.

[4] C.S. Lee, "A fuzzy ontology and its application to news summarization", *IEEE Transactions on Systems, Man and Cybernetics (Part B).,* vol. 35 (5), pp. 859-880, 2005.

[5] K.D. Mitnick , W.L. Simon, *The art of deception: controlling the human element of security,* Wiley Publishing, p. 3, 2002.

[6] A.V. Potiy, D.Y. Pilipenko, I.N. Rebriy "The prerequisites of information security culture development and an approach to complex evaluation of its level", vol. no. 5 (57), pp.72–77, 2012.

[7] M.T. Siponen, *Five dimensions of information security awareness,* Computers and Society, pp.24-90, 2001.

[8] T. Tafazzoli, S.H. Sadjadi,"Malware fuzzy ontology for semantic web", *International Journal of Computer Science and Network Security,* vol. 8, pp. 157-159, 2008.

[9] Q.T. Tho, S.C. Hui, A.C.M. Fong, T.H. Cao, "Automatic fuzzy ontology generation for semantic web", *IEEE Transactions on Knowledge and Data Engineering,* vol. no.18 (6), pp. 842- 856, 2006.

[10] J.F. Van Niekerk, R. Von Solms, "Information security culture: A management perspective", *IEEE Transactions on Knowledge and Data Engineering,* pp. 478, 2006.

[11] J. Zhou, Y. Liang, "Fuzzy Ontology Model for Knowledge Management", *Atlantis-press.com,* pp. 2-3, 2006.

[12] *2014 Data Breach Investigation Report,* Verizon Enterprise Solutions, 2014.

[13] *2015 Data Breach Investigation Report,* Verizon Enterprise Solutions, 2015.

[14] *2016 Data Breach Investigation Report,* Verizon Enterprise Solutions, 2016.

[15] *2017 Data Breach Investigation Report,* Verizon Enterprise Solutions, 2017.

Table 1. Definitions of main elements

Element	CIA triad protection	Security measures	Use	R_i	R_r
Security measures for web applications attacks	CIA	Web application testing , Enclosed documentation for the developed software , Updates and patches, Double Authentication	remote,local	4	3
Security measures for DOS	CA	Incidents , Roles in incidents, DLP	remote	4	0
Security measures for insider attacks	C	Event Log, Account Management, Centralized authentication , Input Monitoring , Administrators control, DLP, Lack of confidential data in plain text	local	4	2
Security measures for mistakes	CIA	DLP, Lack of confidential data in plain text	remote, local	4	2
Security measures for cyber-espionage	C	IS trainings, Staff check, Network segmentation, "Inventory" of software, Black and white IPs, Updates and patches, Double Authentication	remote, local	3	3
Security measures for crimeware	CIA	"Inventory" of software, Anti-virus software , Updating security software , DEP, ASLR, EMET, Black and white IPs, Lack of unnecessary software, accounts, ports, etc., Updates and patches, Integrity of system files, Double Authentication	remote, local	4	2
Security measures for POS-invasion	CIA	Anti-virus software , Updating security software , DEP, ASLR, EMET, Traffic filtering, Event Log, NetFlow, Double Authentication, Administrators control, Separation of services , Flexible passwords, Lack of passwords by default	remote, local	3	3
Staff Security	CIA	Flexible passwords, Lack of passwords by default, Event Log, IS trainings, Staff check, Incidents , Roles in incidents	remote, local	4	2
ISC measurs	CIA	IS trainings, Staff check, Incidents , Roles in incidents	remote, local	4	2
Management ISC Readiness	CIA	Administrators control, Staff check, Incidents , Roles in incidents, Flexible passwords , Lack of passwords by default, Event Log	remote, local	4	2
Coordination	CA	Cooperation with IS staff, Cooperation with Management	remote, local	4	2