ISSN 1330-3651 (Print), ISSN 1848-6339 (Online) https://doi.org/10.17559/TV-20150513123751
Original scientific paper

Evidential Reasoning Approach to Behavioural Analysis of ICT Users' Security Awareness

Tomislav GALBA, Kresimir SOLIC, Kresimir NENADIC

Abstract: The role of ICT system's user should be taken into consideration when developing different information security solutions because user, as its constitutive element, can significantly affect overall system security with his/her potentially risky behaviour depending on the level of user's security awareness. In this paper authors propose risk assessment approach of ICT users' behaviour based on the evidential reasoning technique. Performance testing was compared using combination of cluster analysis and discriminant analysis while empirical analysis was conducted on the total of 627 e-mail users grouped regarding gender, age, technical background knowledge and level of experience. Assessment methodology used in this paper has proven to be well suited for evaluation of users' awareness and identification of their potentially risky behaviour. Results of empirical analysis showed that all groups of users got overall utility grade higher than the simulated "minimally enough aware" user, but less than "average awareness" grade. As users of all groups are highly critical towards collocutor, it can mean that users are quite aware about the importance of information security foundation, but also about lack of knowledge regarding different security issues. Another possible reason may be the users' negligence toward security guidelines and protocols.

Keywords: behavioural analysis; cluster analysis; evidential reasoning approach; information security; users' awareness

1 INTRODUCTION

The role of users' behaviour should be taken into consideration when developing different information security solutions [1, 2], because users of the ICT system can significantly affect the system security [3-5] depending on the users' level of security awareness. The paper proposes novel assessment approach of users' behaviour caused by their level of security awareness based on evidential reasoning technique.

The Enhanced Evidential Reasoning Algorithm (EERA) is based on Dempster - Shafer theory and allows calculations with uncertainty, subjective judgment and partial information [6]. This algorithm has proven to be useful in many practical cases of analysis of different technical systems, both static and dynamic states, comparison between or with referent values [6-12]. In this work the user is considered to be a constitutive part of the ICT system which implies that the chosen algorithm for system state evaluation could be appropriate. The e-mail service has been chosen for security awareness analysis because it is widely accepted and frequently used among various ICT users. Also, e-mail service is one of the most corrupted communication channels by all sorts of malicious attacks like: spam, viruses, phishing or direct social attacks [13, 14].

Data about users' behaviour was collected by a specifically designed questionnaire [15]. Grades from poor to excellent were used in order to distinguish each answer. Moreover, a normalized grade interval was defined by simulating minimally aware or naïve, minimally enough secure and maximally aware or paranoid user's information security behaviour.

There were 627 users included in this survey and by using metadata from the first part of questionnaire they were grouped regarding: gender, age, technical background knowledge and number of e-mail addresses used. Statistical cluster analysis in combination with discriminant analysis was used for testing purposes of the proposed risk assessment approach. There were 306 cases in total used for testing purposes. The main goal of this paper is to present the usage of the evidential reasoning approach to behavioural analysis of ICT users' security awareness.

Analysis was conducted on the groups of ICT users obtained from cluster analysis in order to present many analytic possibilities of this approach: overall group evaluation, comparison between groups, evaluation of single user and comparison with referential values gained by simulation and/or expert's evaluation.

2 DESCRIPTION OF THE QUESTIONNAIRE

Our questionnaire was developed for data collection about security awareness. It consists of two main groups of questions: five demographic questions and 17 questions regarding e-mail user's behaviour covering five segments of user's security awareness such as habits of system usage, way of accessing the system, password quality, habits of e-mail address usage and attitude towards collocutor. Short explanations of questions regarding e-mail users' behaviour with associated answers and their grades according to EERA as poor, indifferent, average, good and excellent are presented in Tab. 1.

Items covered by each question were organized in hierarchical tree structure as this was required by EERA.

2.1 Enhanced Evidential Reasoning Algorithm

The EERA was chosen as assessment method for evaluation of e-mail users' behaviour caused by user's security awareness, described by grades of their answers given in questionnaire. Algorithm is well suited for dealing with a multiple-criteria decision analysis problem which takes the quantitative and qualitative measurements into consideration, and is assessed using subjective judgments with uncertainties.

This approach was introduced in the 1990s [16, 17] and is based on the Dempster-Shafer theory [18, 19], the decision-making theory [20] and the evaluation analysis model [21]. This algorithm, which is chosen for risk modelling, includes a hierarchical model of human and organizational error taxonomy similar to Grabowski model [22]. It allows multiple questionnaire answers, thus enabling a particular user who did not answer one or more

questions to be graded as well. The missing data are considered as uncertainty. The impact of non-uniform user's risky behaviour can be expressed as weighting attributes of different system parts in the total calculation. Some examples of this algorithm applied onto technical systems are: the oil reserve forecast [7], motorcycle evaluation [6], car industry [8], expert system [9], knowledge reduction [10], risk analysis [11] and electric power grid state [12]. In order to perform the assessment with EERA, a minimum of two level hierarchy of attributes is needed as higher level attributes are assessed through associated lower level attributes in the hierarchical assessment. The uncertain judgments are allowed in case of indeterminism of a certain attribute.

Table 1 Short description of questions with possible answers and matching grades per each answer [15]

Basic attributes	Subject of question	Possible answers	Possible grades
Way of usage	Differentiation of an address on professional and private	NO YES	P E
Usage of free system	Usage of free e-mail systems and in what manner	NO YES a) for professional usage b) personal c) occasional	I A G E
Registration on Internet	Registration on all sort of Internet services and with what kind of e-mail address, mostly	NO YES a) professional b) personal c) occasional	P A G E
Leaving address on Internet	Leaving e-mail address readable/visible/accessible	YES a) professional b) personal c) occasional NO	 P I A E
Via Web browser	Usage of web browser for e-mail service and from what kind of PC	YES/occasionally a) public places (e.g. Internet cafe) b) only from home or office NO	P I A G E
Via e-mail client	Usage of e mail client, software tool	NO Mostly YES	I G E
Via protected PC	Taking care of PC's protection (antivirus, upgrades...)	NO YES	P E
Criticism	Critical attitude towards new collocutor	NO YES	P E
Opening attachments	Opening attachments sent by unknown collocutor	YES Sometimes NO	P I E
Usage of encryption	Usage of encryption in e-mail communication	NO/don't know* occasionally YES	I G E
Sending personal data	Sending personal data via e-mail (e.g. social security number)	YES/don't know* on an exceptional basis NO	P G E
Forwarding mass e-mails	Forwarding mass e-mails, known as "chain-letter"	YES/don't know* Occasionally NO	I G E
Logging out of system	Logging out of system	/NO/don't know* mostly YES	P A E

The following examples are showing cases where users give more answers or do not provide any answer. The evaluation grades for particular answer or combination of answers that represent basic or lower level attributes could be as follows [15]:

- The sum of grades would contain 50 % of grade for one answer and 50 % of grade for other answer, in case when the user chooses two of proposed answers.
- It would be 100 % of the related grade if the user gives only one particular answer.
- The sum of grades would contain the combination of two different grades, for example 50 % of one grade and 30 % of the other grade if the user's answer was something like "I do not know".
- The value 0 % for all grades would be if the user gave no answer.

The percentages in the above assessment examples are referred to as degrees of belief and may be used in decimal format as 0.3, 0.5 and 1.

The degree of belief, which is equal to 100 %, for one particular answer represents "absolutely sure" belief. The third assessment is incomplete as the total degree of belief is 0.8 while the first and second assessments are complete. The missing value of 0.2 in the third assessment represents the degree of ignorance or uncertainty. The forth assessment is a special case and represents the total ignorance or 100 % of uncertainty.

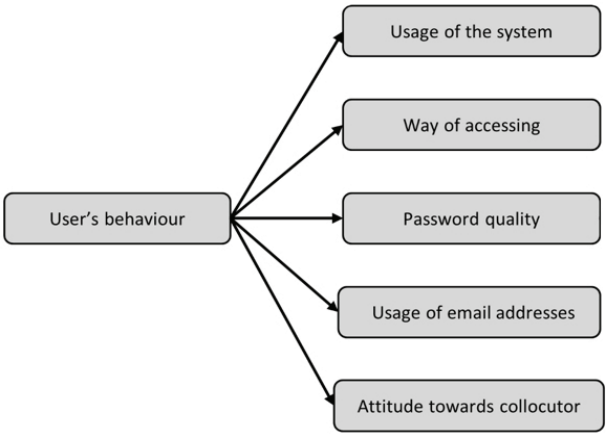

Figure 1 Part of the hierarchical tree construction of subjects covered by each corresponding question in Tab. 1

It is possible to define the proportion of grades as degrees of belief in order to perform assessment on the whole group of users [15]. For example, the basic group attribute of password, self-assessment would be distribution of proportions on how many users grade their password with particular evaluation grade. An example of distribution of grades under group of users is:

$$S(\text{password self-assessment}) = \{(\text{poor}, 0.19), (\text{average}, 0.43), (\text{excellent}, 0.32), (\text{uncertainty}, 0.06)\}. \quad (1)$$

In this example 32 % of users provided the answer of excellent, 43 % as average, 19 % as poor and 6 % did not know how to self-assess their password or did not answer that question at all.

In order to calculate an overall evaluation grade, presented as general or higher level attribute, by aggregating the above possible judgments in a rational way, the evidential reasoning approach can be used as it is a suitable method for dealing with aggregation problem through tree structure shown in Fig. 1 [23].

In order to use the evidential reasoning algorithm to aggregate attributes of a multilevel structure, certain enhancement was needed. There are four synthesis axioms used for enhancement purposes [16]:

- If no basic attribute is assessed to an evaluation grade at all, then the general attribute should not be assessed to the same grade either.
- If all basic attributes are precisely assessed to an individual grade, then the general attribute should also be precisely assessed to the same grade.
- If all basic attributes are completely assessed to a subset of grades, then the general attribute should be completely assessed to the same subset as well.
- If any basic assessment is incomplete, then a general assessment is obtained by aggregating the incomplete with the degree of incompleteness properly assigned.

The usage of the utility number and utility interval gives a single numerical value as the overall grade of users' awareness thus enabling a comparison between different users or groups of users. A detailed explanation on how to grade a whole group of users can be found in [15], while detailed explanation of the EERA can be found in [6]. Calculations were performed using open source System Assessor Software (SAS) [24]. Commercial software package called Intelligent Decision System (IDS) tool was also available [25]. Significant difference value between utility grades is defined as 5 % or 0.05. It is needed in order to compare the overall utility grades of awareness between e-mail users and groups of users.

3 PERFORMANCE TESTING

In order to test performance of users' behaviour evaluation with evidential reasoning approach, standard statistical methods were used in parallel manner on the same data. There were altogether 306 e-mail users included, representing cases in statistical analysis. Statistical cluster analysis, in combination with statistical discriminant analysis is commonly used in the field of economy, related to marketing for categorization of customers [26]. Input variables for both methods were evaluation grades of given answers from poor to excellent while output variables are statistical arithmetic means with standard deviation comparable to utility grades calculated by EERA.

3.1 Results of the Statistical Analysis

The cluster analysis is a statistical method that is used in order to identify homogeneous groups of cases or individuals in a population where optimal number of groups, properties of segments and group membership are unknown in advance. This means that a cluster analysis is used as an exploratory technique [26]. Cluster analysis procedure was chosen in order to categorize ICT system's users' regarding their security awareness. Drawing dendogram, also known as tree diagram, is a common way to visualize the cluster analysis's progress by displaying the distance level at which there was a combination of objects and clusters. It is possible to define the number of clusters by tracking differences between distance levels in previous and next step of the clustering algorithm [27].

Discriminant analysis was applied on groups analysing grouping variables in order to evaluate the quality of clustering and to identify grouping variables that have significant influence on group membership. Variables used in previously explained questionnaire for data gathering were divided onto external variables and dependent variables. External variables as: gender, age, professional qualification and number of e-mail addresses in use were not used for categorization. Dependent variables were collected from answers regarding ICT system users' awareness of security issues and were used for categorization. As each particular answer from those questions had a matching grade shown in Tab. 1, representing dependent variables in ordinal scale from one to five, named as: poor, indifferent, average, good and excellent there was a problem with questions that had only two or three possible answers. From the 17 questions, 11 were discarded from the cluster analysis because of the following reasons: questions with binary data are meaningless for cluster analysis, questions that correlate had to be reduced before performing the cluster analysis. Also, a relatively small size of dataset was an

additional reason for discarding these questions [27].

Altogether there were six questions selected. Detailed description of each question can be found in [28]. Hierarchical method was used as the most common approach to cluster analysis [27]. Also, Euclidean distance measure of (dis)similarity was chosen because data were measured in ordinal scale. Ward's method was chosen because there were no outliers and because this method produces similarly sized clusters [26]. Standardization of variables is needed when values are in different scales or variance differs significantly, which is not the case in this work [27].

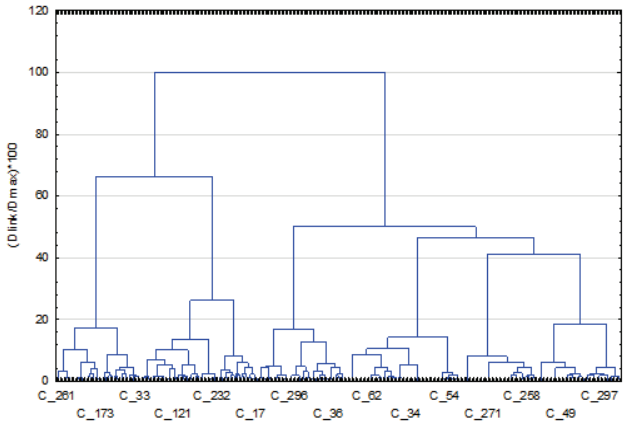

Figure 2 Three diagram results of the cluster analysis

Clustering and statistical calculations were performed with software tool Statistica 11.0 (StatSoft, Tulsa, OK, USA) with significance level defined as α=0,05. The number of clusters is defined while examining dendogram shown in Fig. 2, which graphically represents the result of the cluster analysis.

The steps in which Ward's algorithm can be stopped should be detected from the resulting dendogram depending on the number of clusters and distance between them. In this analysis the algorithm was stopped between 26 % and 41 % of the whole clustering procedure because it presents quite a big distance.

Growing distance in dendogram stands for the difference between groups and is graphically represented as a higher jump. This procedure resulted in six clusters representing six groups of users. The Classification of discriminant analysis showed that 98.7 % of originally grouped cases were correctly classified and canonical discriminant functions gave variables that significantly influenced group membership in Tab. 2. Overlapping between groups was only 1.3 %. None of the questions had significantly influenced the Group 3 and also question Q2 has equally influenced all six groups (p=0.578). Only Group 2 has value "excellent" for variable that has significant influence on clustering analysis and can be called "excellent password quality group". Groups 1, 4, 5 and 6 are "poor" or "indifferent" in related variable presenting grades of answers for question with significant influence. Only group 3 is "average" in a way regarding all six variables meaning grades on answers for all six questions.

Table 2 Results of statistical analysis: average answer grades per each cluster group of users

Selected questions with covered subjects	Grp 1/n=45	Grp 2/n=42	Grp 3/n=63	Grp 4/n=46	Grp 5/n=63	Grp 6/n=47	p**
Q2 (usage of free e-mail services)/mean ± SD	3.11±0.78	3.07±0.64	3.21±0.77	3.20±0.72	3.30±0.85	3.09±0.62	0.578
Q5 (way of access) / mean ± SD	1.09±0.29*	3.26±0.59	3.24±0.53	2.50±1.28	2.49±1.15	2.60±1.14	<0.001
Q10 (attachments from unknown senders)/ mean ± SD	5.00±0.00	4.95±0.22	4.98±0.13	5.00±0.00	1.86±0.35*	4.96±0.20	<0.001
Q12 (sending private/sensitive data)/ mean ± SD	4.27±0.45	4.33±0.48	4.48±0.50	4.50±0.51	3.27±1.58	1.02±0.15*	<0.001
Q14 (logging off the system)/ mean ± SD	5.00±0.00	5.00±0.00	5.00±0.00	2.43±0.78*	4.41±1.01	4.49±1.04	<0.001
Q15 (quality of password)/ mean ± SD	3.80±1.08	5.00±0.00*	2.65±0.77	3.30±1.46	3.35±1.32	3.40±1.46	<0.001

*significant influence of the particular question on the particular group; **One Way ANOVA test; p is significant at level <0.05

Table 3 Results of the evaluation with evidential reasoning approach: distribution of grades with associated utility grade per each cluster group of users

Distribution of grades	Grp 1/n=45	Grp 2/n=42	Grp 3/n=63	Grp 4/n=46	Grp 5/n=63	Grp 6/n=47
Poor	0.074	0.024	0.022	0.058	0.099	0.096
Indifferent	0.125	0.102	0.137	0.173	0.261	0.165
Average	0.076	0.098	0.132	0.136	0.117	0.120
Good	0.069	0.068	0.057	0.052	0.053	0.029
Excellent	0.655	0.707	0.652	0.581	0.468	0.590
Uncertainty	0.002	0.000	0.000	0.000	0.002	0.000
Utility with utility interval	0.799 (0.798-0.800)	0.855*	0.821*	0.760*	0.670 (0.669-0.671	0.739*

*utility interval is not defined, because uncertainty equals zero

Users that belong to the "excellent password quality group" have their password graded as excellent which is significantly different from the password grades for users of the other five groups. In the first group that can be called "less secure access group" users prefer less secure way of accessing their e-mail system, which significantly differs comparing them to other users. While the users of the "group of average awareness" are average regarding answers to the all six questions, users that belong to the forth group, "forgettable group" do not log off the system after finishing their work. Fifth group can be called "naive group" because these users are not critical to unknown collocutors and the sixth group can be called similarly, for example "security critical group" because users from that group are sending personal and sensitive data by e-mail carelessly and as plain text.

3.2 Evaluation with EERA and Comparison with Results of Statistical Cluster Analysis

Each one of six groups of users defined by statistical clustering method was evaluated by EERA shown in Tab. 3. Results are presented as distribution of grades fulfilled with uncertainty and additionally with utility grade. Utility grade fulfilled with utility interval that is defined by uncertainty is used as one overall grade suitable for

comparison among different groups of users.

Matching of evaluation results is evident for all six groups when comparing the results gained by statistical cluster and discriminant analysis (arithmetic mean with standard deviation) and results gained by evidential reasoning approach (utility with utility interval).

The highest utility grade (U = 0.855) got "excellent password quality group" while utility grades of all four "poor or indifferent" groups are lower than utility grade of the "group of average awareness" (U = 0.821). Performance testing confirms the accuracy of ICT users' evaluation with evidential reasoning approach, because the results are comparable similarly among and between all six groups.

4 EMPIRICAL RESULTS OF BEHAVIOURAL ANALYSIS

The 627 analysed e-mail users were grouped according to external variables gained from introductory questions in questionnaire about gender, age, technical background knowledge and number of e-mail addresses used. Results of the users' security awareness show that users with university degree have greatest awareness about security issues when using e-mail system. Unlike them, users that have only one address, meaning that are less experienced, have the lowest awareness regarding e-mail system's security issues. Although all groups got an overall utility grade higher than the simulated minimally enough aware user, the first four groups did not get significantly higher grade as difference is less than 5 %.

Those e-mail users have only one address, younger user, users without technical background knowledge and users without university degree shown in Tab. 4 where P, I, A, G, E and U stands for poor, indifferent, average, good, excellent and uncertainty.

All other groups of e-mail users got significantly higher overall utility grade of their security awareness, but none of the groups got a grade close to "excellent". However, grades of five groups were close to the grade of group of "average awareness", as their grades differ in less than 5 % than referent value (U=0.821). The overall utility grades of all groups are less than 10 % higher comparing to the referent value of the "minimally enough aware user" and more than 20 % below "excellent", except grade of users that use more than two e-mail addresses.

By analysing groups of questions, it is possible to identify security critical group of questions for particular group of e-mail users shown in Tab. 5.

Table 4 Comparing assessment results between simulated e-mail users and graded groups of e-mail users

Different groups of e-mail users/n	Distribution of grades						Utility number	
	P	*I*	*A*	*G*	*E*	*U*	*Grade*	*Interval*
Simulated naive user*	0.810	0.190	0.000	0.000	0.000	-	0.066	-
Simulated minimally enough aware user*	0.000	0.156	0.366	0.176	0.303	-	0.708	-
Users that use only one e-mail address /197	0.071	0.211	0.101	0.049	0.564	0.005	0.738	0.735-0.740
Young users (≤21 age) /318	0.075	0.171	0.128	0.047	0.578	0.002	0.749	0.748-0.750
Users without technical background knowledge /182	0.073	0.182	0.108	0.052	0.582	0.005	0.752	0.749-0.754
Users without university degree /426	0.072	0.173	0.122	0.048	0.583	0.003	0.753	0.751-0.754
Female users /302	0.059	0.175	0.117	0.055	0.591	0.005	0.766	0.763-0.768
Users that use two e-mail addresses /280	0.067	0.153	0.124	0.053	0.601	0.002	0.769	0.768-0.770
Male users /325	0.073	0.148	0.114	0.053	0.610	0.002	0.771	0.770-0.771
Users with technical background knowledge /146	0.063	0.140	0.118	0.059	0.617	0.004	0.783	0.781-0.785
Older users (>21 age) /309	0.059	0.151	0.103	0.060	0.624	0.004	0.787	0.785-0.789
Users with university degree /201	0.056	0.139	0.102	0.066	0.636	0.001	0.797	0.797-0.798
Users that use more than two e-mail addresses /147	0.058	0.124	0.111	0.063	0.644	0.001	0.803	0.802-0.803
Averagely aware user (from clustering)	0.022	0.137	0.132	0.057	0.652	-	0.821	-
Simulated paranoid user*	0.000	0.000	0.000	0.000	1.000	-	1.000	-

*utility interval is not defined, because uncertainty equals zero

Table 5 Comparing assessment results between subclasses for each group of users.

Different groups of e-mail users /n	Utility grade (Utility interval)				
	Usage of e-mail address	Way of access	Attitude towards collocutor	Usage of e-mail system	Password quality
Users that use only one e-mail address /197	0.606* (0.601-0.612)	0.625 (0.622-0.628)	0.856 (0.852-0.860)	0.727 (0.726-0.729)	0.743 (0.742-0.744)
Young users (≤21 age) /318	0.657 (0.656-0.659)	0.558* (0.557-0.559)	0.832 (0.830-0.835)	0.767 (0.767-0.768)	0.793 (0.791-0.794)
Users without technical background knowledge /182	0.656 (0.651-0.660)	0.616* (0.610-0.622)	0.842 (0.840-0.845)	0.745 (0.743-0.747)	0.758 (0.755-0.760)
Users without university degree /426	0.656 (0.655-0.658)	0.585* (0.583-0.587)	0.840 (0.837-0.843)	0.760 (0.760-0.761)	0.783 (0.782-0.784)
Female users /302	0.656 (0.652-0.661)	0.626* (0.622-0.629)	0.888 (0.884-0.893)	0.750 (0.749-0.752)	0.767 (0.765-0.769)
Users that use two e-mail addresses /280	0.673 (0.670-0.675)	0.598* (0.597-0.600)	0.868 (0.867-0.870)	0.763 (0.762-0.764)	0.799 (0.798-0.799)
Male users /325	0.659 (0.658-0.661)	0.618* (0.617-0.619)	0.834 (0.833-0.835)	0.772 (0.771-0.773)	0.816 (0.815-0.816)
Users with technical background knowledge /146	0.655 (0.653-0.658)	0.649*	0.873	0.763 (0.756-0.771)	0.827 (0.825-0.828)
Older users (>21 age) /309	0.660* (0.655-0.665)	0.684 (0.681-0.687)	0.889 (0.886-0.891)	0.755 (0.753-0.757)	0.794 (0.793-0.795)
Users with university degree /201	0.662* (0.661-0.663)	0.701 (0.697-0.705)	0.901 (0.899-0.903)	0.765 (0.764-0.767)	0.813 (0.812-0.814)
Users that use more than two e-mail addresses /147	0.692 (0.690-0.693)	0.662*	0.879	0.780 (0.779-0.781)	0.842 (0.840-0.844)

Young users got the lowest utility grade for group of questions regarding the way of accessing the e-mail system. Also, most of the groups of e-mail users got the lowest utility grade regarding the same subject.

All groups got the highest utility grade for group of questions on subject regarding attitude towards collocutor.

Detailed analysis of answers regarding each question for all interviewed users gave the following results:

- E-mail users rarely differentiate private from professional e-mail communication.
- Most users are using free e-mail services (like Gmail and Yahoo) for professional communication.
- Users rarely use third "temporal" e-mail address for registration on security questionable Internet services.
- Users too often use public PCs with questionable software protection for accessing e-mail system.
- Users rarely take into account the software protection of their private PCs.
- All groups of e-mail users are very critical when communicating with unknown collocutors (utility grade for subject regarding attitude towards collocutor is "very good" for all groups of users).

It is possible to calculate utility grades of basic attributes as well, especially for the questions belonging to groups of questions that got lower utility grade.

5 DISCUSSION AND CONCLUSION

In this paper the usage of the evidential reasoning approach to behavioural analysis of ICT system users' security awareness is presented. The analysis was conducted on groups of users in order to present many analytic possibilities of the enhanced evidential reasoning algorithm: overall group evaluation, comparison between groups, evaluation of single user and comparison with referent values gained by simulation and/or expert's valuation. Also, a specific questionnaire was developed for data gathering.

Assessment methodology used in this paper has proven its applicability on the evaluation of user's and users' behaviour. It is possible to rank potentially risky behaviour by using utility grades and normalized interval between minimally aware "naïve" and maximally aware "paranoid" user's behaviour. When discussing results of the users' behaviour evaluation grouped by demographic questions, certain general conclusions could be made. Obtained results were expected regarding less experienced users. This group got the lowest utility grade of their information security awareness. Also, users without technical background knowledge and without university degree got an expected low overall utility grade. However, low overall utility grade was not expected for young users because they are mostly well familiar and are frequently using all kinds of electronic communication systems. Maybe those users are too credulous. All groups of users are highly critical towards collocutor. This may mean that all kinds of ICT users are quite aware of the importance regarding security issues, but do not know enough about different security issues and/or are showing negligence towards information security guidelines and protocols.

Results of empirical analysis had shown that all groups of users got an overall utility grade higher than the simulated "minimally enough aware" user, but lower than the grade of "average awareness". This implies that e-mail users of all groups need additional education, frequent alerts and remainders regarding their risky behaviour caused by security awareness while using not only e-mail communication system, but also while using different ICT systems in everyday life. The correction of users' risky behaviour should be done by raising the users' information security awareness applying education and training [29-31].

Some limitations of this work arise from a rather small number of questions defined in questionnaire used in this work, because there is little focus placed on this area from the technicians' perspective. Also most of the intervened users belong simultaneously to several groups. For example a user can simultaneously belong to male group, group with technical background knowledge and also group of older users.

However, the comparison between opposite groups is well defined, for example the comparison of overall utility grades between male and female users can produce constructive conclusions.

Another drawback is the subjective assessment of answers that can be questionable from the perspective of a security expert. This is partly solved by using evidential reasoning approach that is well suited for calculations with subjective judgments and their main aim was to present the usage of the novel assessment approach and not to identify security critical users among population of ICT users.

Future work should involve all major security aspects that describe ICT user's awareness and its possible risky behaviour in evaluation. This should be achieved by developing and verifying more general questionnaire. Also, by following the presented modelling procedure, it should be possible to develop a model for assessment on the overall ICT system regarding its security, maintenance and/or cost effectiveness.

6 REFERENCES

[1] Johnson, M. E. & Pfleger, S. L. (2011). The Human Side of Risk Management. *IEEE Security & Privacy, 9*(1), 51.

[2] Crosser, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

[3] Lukasik, S. J. (2011). Protecting Users of the Cyber Commons. *Communications of the ACM, 54*(9), 54-61. https://doi.org/10.1145/1995376.1995393

[4] Thompson, H. (2013). The Human Element of Information Security. *IEEE Security & Privacy, 11*(1), 32-35. https://doi.org/10.1109/MSP.2012.161

[5] Solic, K., Nenadic, K., & Galic, D. (2012). Empirical Study on the Correlation between User Awareness and Information Security - Case study. *International Journal of Electrical and Computer Engineering Systems, 3*(2), 2-5.

[6] Yang, J. B. & Xu, D. L. (2002). On the Evidential Reasoning Algorithm for Multiple Attribute Decision Analysis under Uncertainty. *IEEE Transactions on Systems, Man and Cybernetics, 32*(3), 289-304. https://doi.org/10.1109/TSMCA.2002.802746

[7] Zhang, X. D., Zao, H., & Wei, S. Z. (2005). Research on Subjective and objective evidence fusion method in oil reserve forecast. *Journal of System Simulation, 17*, 2537-2540.

[8] Liu, X. B., Zhou, M., Yang, J. B., & Yang, S. L. (2008). Assessment of strategic R&D projects for car

manufacturers based on the evidential reasoning approach. *International Journal of Computational Intelligence Systems, 1*(1), 24-49.
[9] Beynon, M., Cosker, D., & Marshall, D. (2001). An expert system for multi-criteria decision making using Dempster-Shafer theory. *Expert Systems with Applications, 20*(4), 357-367. https://doi.org/10.1016/S0957-4174(01)00020-3
[10] Wu, W. Z., Zhang, M., Li, H. Z., & Mi, J. S. (2005). Knowledge reduction in random information systems via Dempster-Shafer theory of evidence. *Information Sciences, 74*, 143-164. https://doi.org/10.1016/j.ins.2004.09.002
[11] Srivastava, R. P. & Liu, L. (2003). Applications of belief functions in business decisions: a review. *Inf Syst Frontiers, 5*, 359-378. https://doi.org/10.1023/B:ISFI.0000005651.93751.4b
[12] Jovic, F., Filipovic, M., Blazevic, D., & Slavek, N. (2004). Condition Based Maintenance in Distributed Production Environment. *Machine engineering, 4*, 180-192.
[13] State of Spam & Phishing (Symantec) available at: www.symantec.com/content/eu/us/other_resources/b-state_of_spam_and_phishing_report_12-2010.en-us.pdf (14.12.2011).
[14] IT Security Guidelines. Federal Office for Information Security, available at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines_pdf.pdf (14.12.2011).
[15] Solic, K., Jovic, F., & Blazevic, D. (2013). An Approach to the Assessment of Potentially Risky behavior of ICT System's Users. *Technical Gazette, 20*(2), 335-342.
[16] Yang, J. B. & Singh, M. G. (1994). An evidential reasoning approach for multiple attribute decision making with uncertainty. *IEEE Trans Syst Man Cybern, 24*(1), 1-18. https://doi.org/10.1109/21.259681
[17] Yang, J. B. & Sen, P. A. (1994). General multi-level evaluation process for hybrid MADM with uncertainty. *IEEE Trans Syst Man Cybern, 24*(10), 1458-1473. https://doi.org/10.1109/21.310529
[18] Dempster, A. P. (1967). Upper and lower probabilities induced by a multivalued mapping. *The Annals of Mathematical Statistics, 32*(2), 325-339. https://doi.org/10.1214/aoms/1177698950
[19] Shafer, G. A. (1976). *Mathematical theory of evidence*. Princeton University Press, New Jersey.
[20] Zhou, M., Liu, X. B., & Yang, J. B. (2010). Evidential Reasoning-Based Nonlinear Programming Model for MCDA Under Fuzzy Weights and Utilities. *International Journal of Inteligent Systems, 25*, 31-58. https://doi.org/10.1002/int.20387
[21] Zhang, Z. J., Yang, J. B., & Xu, D. L. A. (1990). *Hierarchical analysis model for multiobjective decision making, Analysis, Design and Evaluation of Man–Machine Systems*. Pergamon, Oxford, U. K., 13-18.
[22] Grabowski, M., Merrick, J. R. W., Harrald, J. R., Mazzuchi, T. A., & Dorp, R. V. (2000). Risk Modeling in Distributed, Large-Scale Systems. *IEEE Trans. on Systems, Man, and Cybernetics - Part A: Systems and Humans, 30*, 651-660. https://doi.org/10.1109/3468.895888
[23] Yager, R. P. (1995). On the Dempster-Shafer framework and new combination rules. *Inf. Sci, 41*, 317-323.
[24] Jagnjic, Z., Slavek, N., & Blazevic, D. (2004). Condition Based Maintenance of Power Distribution System. Proc EUROSIM, Attiya, G.; Hamam, Y, 13-14.
[25] Xu, D. L. & Yang, J. B. (2003). Intelligent decision system for self-assessment. *J Multi-Crit Decis Anal, 12*, 43-60. https://doi.org/10.1002/mcda.343
[26] Mooi, E. & Sarstedt, M. (2011). A Concise Guide to Market Research, Cluster Analysis, Springer, 237-284.
[27] Jobson, J. D. (1992). *Applied Multivariate Data Analysis*, Springer, 518-616.
[28] Solic, K., Tovjanin, B., & Ilakovac, V. (2012). Assessment Methodology for the Categorization of ICT System Users Security Awareness. *Proc. IEEE 35th MIPRO*, 1560-1564.
[29] Paulsen, C., McDuffie, E., Newhouse, W., & Toth, P. (2012). NICE: Creating a Cybersecurity Workforce and Aware Public. *IEEE Security & Privacy, 10*, 76-79. https://doi.org/10.1109/MSP.2012.73
[30] Iacovos, K. & Sasse, M. A. (2012). Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security & Privacy, 10*, 24-32. https://doi.org/10.1109/MSP.2011.179
[31] Furman, S., Theofanos, M. F., Choong, Y. Y., & Stanton, B. (2012). Basing Cybersecurity Training on User Perceptions. *IEEE Security & Privacy, 10*, 40-50. https://doi.org/10.1109/MSP.2011.180

Contact information:

Tomislav GALBA, mag. ing.
Faculty of Electrical Engineering, Computer Science and Information Technology Osijek
J. J. Strossmayer University of Osijek
Kneza Trpimira 2b
31000 Osijek, Croatia
tomislav.galba@ferit.hr

Kresimir SOLIC, PhD in Computer Processing
Faculty of Medicine
J. J. Strossmayer University of Osijek
Cara Hadrijana 10/E
31000 Osijek, Croatia

Kresimir NENADIC, PhD in Computer Processing
Faculty of Electrical Engineering, Computer Science and Information Technology Osijek
J. J. Strossmayer University of Osijek
Kneza Trpimira 2b
31000 Osijek, Croatia