IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

An Approach for Modelling of Security Procedures for Information Resources Protection

Radi Romansky[1], Irina Noninska[2]

Department of Electronics, Computer Systems and Technologies, College of Energy and Electronics,

Technical University of Sofia, Sofia, Bulgaria [1]

Dept of Computer System, Faculty of Computer Systems and Control, Technical University of Sofia, Sofia, Bulgaria [2]

Abstract: This article discusses several core aspects of security system organization which are able to guarantee efficient protection of corporative resources. These resources could be stored in a common case as an internal sub-system. Recently many enterprises prefer to store them in data centres relying on cloud services. Nevertheless which one of these two approaches will be applied strong procedures for corporative information security and personal data protection must be defined. In order to investigate security procedures for accessing and using business information in a corporative system the article deals with formalization of the processes by using data flow diagram and modelling by Petri Nets (PN) apparatus (in the stochastic extension). An analytical evaluation of the results is carried out and calculated assessments for a case study are given.

Keywords: Information security, Modelling, Stochastic Petri Nets (SPN), Evaluation.

I. INTRODUCTION

Contemporary digital word proposes different opportunities for creating virtual environments, remote access to web objects, sharing information, social communication, etc. which make connectivity between people easy and fasts. At the same timethe variety of Web and mobile applications requires higher level of data privacy and information security [1, 2]. The cloud computing has different advantages including organizing business processes by using cloud services and importing corporative data in data centres. It is necessary to know that each activity in the digital word is connected with uploading personal data which could disturb the privacy [3] and the regulation in this area must be improved [4].

The companies collect, create and support different types of information accessed by global network. These resources could be public and private (corporative) and each business information system should be developed on the base of strong policy for information security and for personal data protection (PDP) [5]. In this reason it is very important to build precise system for secure access and protection of information (personal profiles of users and staff, business information resources, corporative archives, etc.) and implement contemporary means and tools for identification & verification, rights managing, biometric technologies, etc.

Before a new system development an investigation should be realized to obtain assessments for protection procedures efficiency. In this respect discrete formalization and investigation of secure access to corporative resources is presented in [6]. There are different apparatuses for systems and processes investigation classified based on the base of applied methods as simulation, functional and analytical modelling, statistical tools, etc. Among them as two main directions could be pointed out: discrete and stochastic approaches.

The main goal of this paper is to extend the investigation proposed in [6] with stochastic apparatus. The purpose is to obtain additional assessments for probabilities in the secure access organising, and in particularly to analyse the usage of main procedures in a corporative System for Information Security (SIS).

The paper is organized as follows: Section 2 discuses structural organization of business system with three types of resources – public, private internal and private external. Section 3 gives short information about theapproach for discrete analytical modelling by using Petri nets (PN) apparatus proposed in [6]. Section 4 presents description of the secure access process as a data flow diagram (DFD). Section 5deals with definition of stochastic model based on Markov's chain (MC) and their solution. Section 6 presents statistical assessment obtained by using Develve Statistical software [7] and finally conclusion is made in Section 7.

II. ORGANIZATION OF A BUSINESS SYSTEM

Each business information system should be developed with implementation of several important procedures as preliminary registration, identification, authentication, authorization, personal profiles protection, etc. Different information and system resources (files, databases, archives, etc.) must be defined to support the processes of secure access.

An architecture of the business environment is presented in Fig.1 as a collection of specialized sub-systems: Front-office(input portal for user's access and preliminary identification); Back-office (an administrative core for realisation of high level of resources protection by supporting administrative data structures); Information

DOI 10.17148/IARJSET.2016.3601

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

resources (collection of public and private information, including processing in the cloud); System for Information Security (SIS)which includes administrative data structures, technical and organizational measures for data protection.A short description of the main sub-systems displayed in Fig. 1 is presented below.

♦ Front office – this is an input point for remote user's access to the corporative system which is responsible forthe initial registration of a new user and preliminary identification of already registered users. The registration procedure creates a personal profile collecting a set of personal data. The identification procedure should guarantee legitimate access to the back office component. An audit file for registration of each access (time, IP address and relative attributes) and statistical data storing is included in this structure to enhance functionality of the front office.

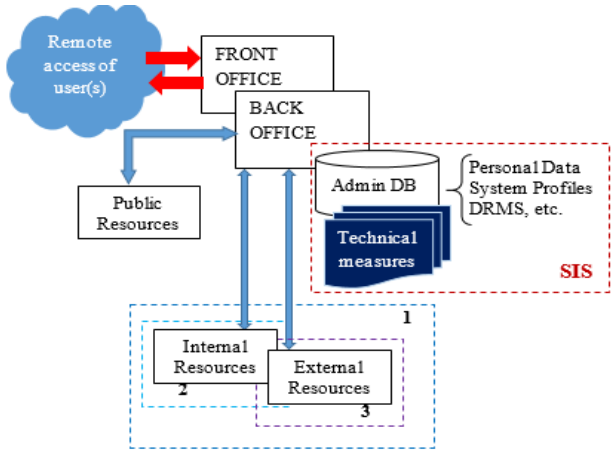


Fig. 1 General architecture of a corporative system for secure access to the resources

♦ Back office – it deals with the basic administrative procedures that support processes of secure access. The functionality of this sub-system is directly connected whit the administrative database (Admin DB) which consists of different components. They are as follows: profiles created during the user's registration collecting personal data; system profiles for the staff;personal rights for the users'access which are defined according to the security rules of the business information system (BIS); components of Digital Rights Management System (DRMS), etc.

♦ The System for Information Security (SIS) unites different technical and organizational measures for information protection of "Admin DB" components, including personal data protection (PDP) and rights management by DRMS.

♦ Information resources are determined as public, internal corporative resources and external corporative resources.In general, the information business resources could be defined as two types – public information (with free user's access without limitation) and private (corporative) information resources (with strong procedures for secure access). At the same time the corporative resources could be stored in an internal environment (internal resources) and/or in a data centre accessible by using cloud services (external resources).

♦ The functions of SIS are extended with several additional procedures for secure access to the information resources: (1) Corporative system for secure access to the internal resources (authentication); (2) Internal procedures for digital rights management (authorization); (3) System for security protection and rights checking in the cloud.

III.DISCRETE ANALYTICAL MODELLING

The approach proposed in [6] permits to investigate security procedures in a business information environment built on the base of the architecture shown in Fig.1 implementing a discrete formalization with directed graph structure and an analytical description of the processes by using the apparatus of Petri nets (PN) [8, 9]. The investigation has been made according the rules of policies for IT security and data protection in the contemporary digital word. The goal of this analytical approach was to analyse the secure access to business components, system and information resources and to calculate several numeric assessments based on evolution of the PN model realized as a tree of reach ability.

The analytical model PN = {T, P, I, O}; T∩P=∅proposed in [6] is based on two discrete sets:
✓ Set of transactions T (for describing main procedures): t_1 – remote user's access to the input point; t_2 – registration of a new user; t_3 – activating the identification procedure; t_4 – access to public resources; t_5 – authentication procedure for access to corporative resources (T - correct; F – incorrect); t_6 – finishing the work; t_7 – authorization procedure (rights checking) by using DRMS tools (T – correct; F – incorrect); t_8 – access to external corporative resources; t_9 – access to internal corporative resources.
✓Set of positions P (for describing conditions): p_1 – user's access is activated; p_2 –registered useraccess; p_3 – legitimated user's access; p_4 – successful authentication; p_5 – successful authorization.
The two functions I (input) and O (output) are defined on the base of processes for secure access in the business system and graph definition of the proposed PN-model is shown in Fig. 2.

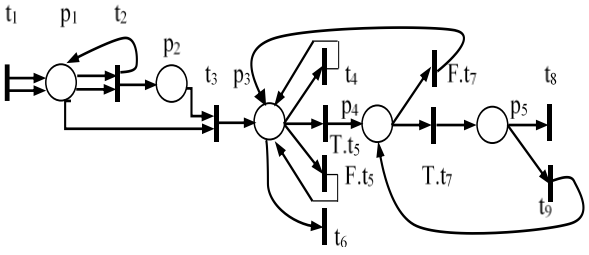


Fig. 2Graph of states for the designed analytical model

Fig. 3 presents the model execution by tree of reachability with initial marking μ_0=(0,0,0,0,0).

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

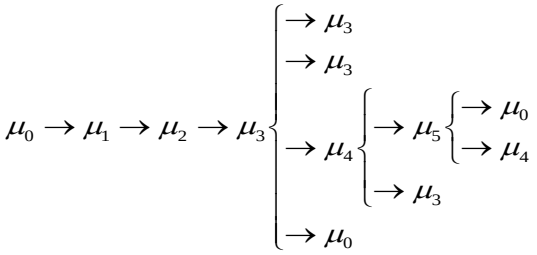


Fig. 3Evolution of the model (tree of reachability)

The other markings are as follows:

μ_1=(2,0,0,0,0); μ_2=(1,1,0,0,0); μ_3=(0,0,1,0,0);
μ_4=(0,0,0,1,0); μ_5=(0,0,0,0,1).

IV. FORMALIZATION BY USING DATA FLOW DIAGRAM

A formal description of the processes supported protection of the system and information resources by using data Flow Diagram (DFD) is proposed in the Fig. 4.

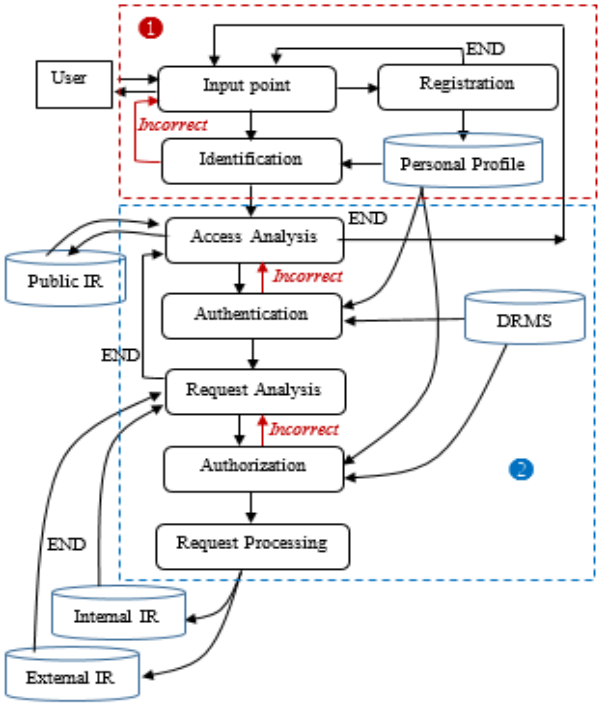


Fig. 4 Formal description of the security processes by using DFD

The two sub-systems are realized as separate units: ❶ Front office; ❷- Back office. The formal model consists of 1 external entity (User) which has two roles – source of data flow and acceptor of results; 8 functional blocks for main procedures realized in the system; 5 storages (system information resources and databases). If the result from a procedure is incorrect ("Incorrect") the access is rejected and the process returns to the previously step. All transitions marked by "END" describe finishing the work of this component and branching to other procedure.

The additional procedures that support the process of secure access are described below:

✓Module "Access Analysis" is the input gate of the back office and this procedure checks the type of legitimate access to system resources. This type determines the level of access – unlimited (for all public resources) or strong limited after authentication (for all corporative resources).

✓ Module "Request Analysis" is a procedure determining the type of accessed resources and initializes the authorization based on DRMS and personal profiles. The main principle is that each access must be authorized according to the corporative policy.

✓ Module "Request Processing" is responsible for permitted access and usage of corporative resources, which is limited to one access only. Each next request for access to corporative resources must be analysed by procedure "Request Analysis" and new authorization must be provided.

V. EXTENDED MODELLING OF SECURITY PROCESS

The proposed in [6] model is a discrete one because the PN apparatus is a discrete structure. At the same time each process which takes part in information service for a corporative structure has a probability nature. This obstacle requires implementation of probability apparatus for modelling and investigation. An approach is based on the apparatus Timed PN (TPN) that is an extension of PN and is defined by TPN:=(P,T,I,O,Θ). The standard PN-definition is extended by the set $\Theta = \{\theta_1, \theta_2, \ldots, \theta_n\}$ that presents transactions' realization delays. They could be presented as determined values but more precise manner is to use stochastic values that extend the PN to the Stochastic PN (SPN). The formal SPN definition is by the ordered structure SPN:=(P,T,I,O,L), where$L=\{\lambda_1,\ldots,\lambda_n\}$ is a set of intensities of activation $\lambda_i=1/\theta_i$ for each transaction in the defined model. In this way each transaction t_i is associated with an intensity of activation λ_i. As a result of the analysis of TPN/SPN is reduced to an investigation of the condition for stationarity of a Markovian process. In this case the SPN could be described as a Markovian model whit discrete set of states $S=\{s_1,\ldots,s_n\}$ and intensities as a transactions between them. Each state corresponds to a reachable marking at the PN-evaluation ($s_i \equiv \mu_i$).

Let the transactions $\{t_1,t_2,t_3,t_4,t_5,t_6,t_7,t_8,t_9\}$ are presented by the delays Θ={1,a,a, 1,a,1,a,1,1} and this permits to define the vector of intensities L={1,1/a,1/a,1,1/a,1,1/a,1,1}. Based on this assumption a stochastic model as Markov's chain (MC) with discrete states for each marking $\mu_j$of the evolution could be defined. This model is presented as a graph of states in Fig. 5.

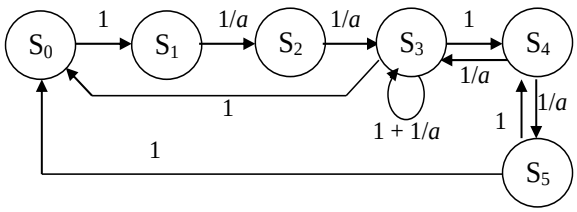


Fig. 5Graph of states of the proposed MC-model

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

Analytical definition of the proposed model is presented below.

$$(0): p_0 = p_3 + p_5$$

$$(1): \frac{1}{a} p_1 = p_0 \Rightarrow p_1 = a.p_0$$

$$(2): \frac{1}{a} p_2 = \frac{1}{a} p_1 \Rightarrow p_2 = p_1 = a.p_0$$

$$(3): 2(1+\frac{1}{a}) p_3 = \frac{1}{a} p_2 + (1+\frac{1}{a}) p_3 + p_4$$

$$(4): (1+\frac{1}{a}) p_4 = \frac{1}{a} p_3 + p_5 \Rightarrow (a+1).p_4 = p_3 + a.p_5$$

$$(5): 2p_5 = \frac{1}{a} p_4$$

$$(6): \sum_{i=1}^{5} p_i = 1$$

Solution of the analytical model:

$$Eq(1) \& Eq(2): p_1 = p_2 = a.p_0$$

$$Eq(5): p_5 = \frac{1}{2a}.p_4$$

$$Eq(4): p_3 = (a+1).p_4 - a.p_5 = (a+1).p_4 - \frac{a}{2a} p_4$$

$$\Rightarrow p_3 = (a+1-1/2).p_4 \Rightarrow p_3 = \frac{2a+1}{2} p_4$$

$$Eq(3): 2.\left(\frac{a+1}{a}\right) p_3 = \frac{1}{a} p_2 + \left(\frac{a+1}{a}\right) p_3 + p_4$$

$$\Rightarrow \frac{1}{a} p_2 = \frac{a+1}{a} p_3 - p_4 = \frac{a+1}{a}\left[\frac{2a+1}{2} p_4\right] - p_4$$

$$\Rightarrow p_2 = a\left[\frac{a+1}{a}.\frac{2a+1}{2} p_4 - p_4\right]$$

$$\Rightarrow p_2 = a.p_4\left[\frac{(a+1)(2a+1)}{2a} - 1\right]$$

$$\Rightarrow p_2 = p_4 \frac{2a^2+2a+a+1-2a}{2} = \frac{2a^2+a+1}{2} p_4$$

$$Eq(0): p_0 = p_3 + p_5 = \left[\frac{2a+1}{2} p_4\right] + \left[\frac{1}{2a} p_4\right] =$$

$$= \frac{a(2a+1)+1}{2a} p_4 \Rightarrow p_0 = \frac{2a^2+a+1}{2a} p_4$$

After substitution in the last equation Eq(6):

$$p_4\left[\frac{2a^2+a+1}{2a} + 2.\frac{2a^2+a+1}{2} + \frac{2a+1}{2} + 1 + \frac{1}{2a}\right] = 1$$

$$p_4[2a^2+a+1+2a(2a^2+a+1)+(2a+1)a+2a+1] = 2a$$

$$p_4(2a^2+a+1+4a^3+2a^2+2a+2a^2+a+2a+1) = 2a$$

$$\Rightarrow p_4 = \frac{a}{2a^3+3a^2+3a+1}$$

Let $(2a^3+3a^2+3a+1) = \beta$ and the calculated values of the final probabilities are as follows:

$$p_0 = (2a^2+a+1)/(2\beta)$$
$$p_1 = p_2 = [a(2a^2+a+1)]/[2\beta]$$
$$p_3 = [a(2a+1)]/[2\beta]$$
$$p_4 = a/\beta$$
$$p_5 = (2\beta)^{-1}$$

VI. INVESTIGATION AND STATISTICAL ANALYSIS

An ordered one-factor experimental plan to carry out the investigation of the process realization is accepted. In this connection a step of **Δ=0,1** is determined for the parameter **a**, and calculated values obtained for the final probabilities in stationer regime are presented in Tabl.1. A generalization of this calculation by average values of the final probabilities is presented in Fig. 6. The assessments show that major value is determined for p_0 which corresponds to the initial marking μ_0. On the other hand, for the average values **a=0,5**all probabilities from p1 to p5 have equal value **p_j= 0,14286**.

Table 1. Values for the final probabilities

a	p_0	p_1	p_2	p_3	p_4	p_5	Total
Average	**0,293**	**0,145**	**0,145**	**0,131**	**0,124**	**0,162**	1,000
0,10	0,42	0,04	0,04	0,05	0,08	0,38	1,00
0,20	0,37	0,07	0,07	0,08	0,12	0,29	1,00
0,30	0,33	0,10	0,10	0,11	0,13	0,22	1,00
0,40	0,31	0,12	0,12	0,13	0,14	0,18	1,00
0,50	0,29	0,14	0,14	0,14	0,14	0,14	1,00
0,60	0,27	0,16	0,16	0,15	0,14	0,12	1,00
0,70	0,25	0,18	0,18	0,16	0,13	0,10	1,00
0,80	0,24	0,19	0,19	0,16	0,13	0,08	1,00
0,90	0,23	0,21	0,21	0,17	0,12	0,07	1,00
1,00	0,22	0,22	0,22	0,17	0,11	0,06	1,00

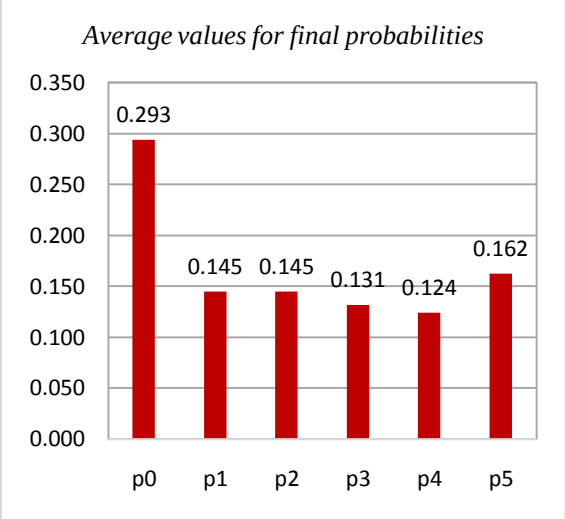


Fig. 6Average final probabilities for the states (procedures) calculated on the base of various values of parameter a

An additional statistical analysis is carried out by using Statistical software Develve [7] giving results which are presented and discussed below.

DOI 10.17148/IARJSET.2016.3601

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 6, June 2016

Develve (http://develve.en.softonic.com/) is a professional statistical software application which delivers all the necessary tools for a fast interpretation of experimental and statistical data in various fields. Develve is able to compare data sets, indicating whether the difference in average and variation is significant. It also detects if the sample size is large enough in order to prevent false assumptions. The main features of this software tool are basic statistics calculation, design of experiments, Weibull analyses, sample size calculations, etc. The initial screen for statistical analysis of this application is shown in Fig. 7.

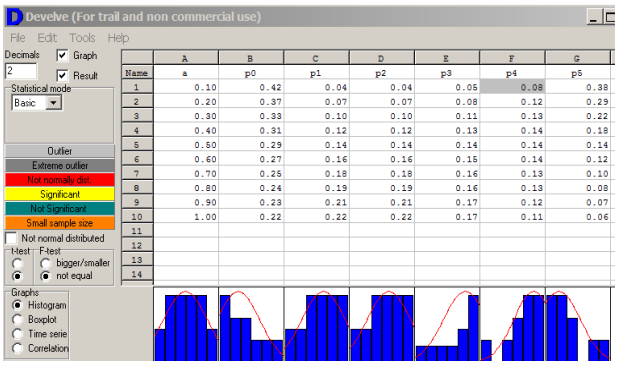
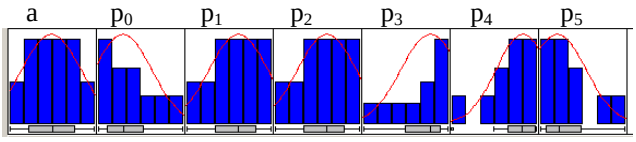


Fig. 7Initial screen for statistical analysis

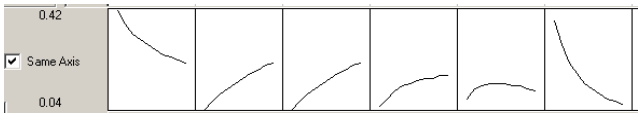
Several experimental results calculated by Develvesoftware are presented in Fig. 8, as follows: (a) statistical assessments; (b) histograms; (c) time series; (d) boxplots.

	a	p_0	p_1	p_2	p_3	p_4	p_5
Min Tol.							
Mean	0.55	0.29	0.14	0.14	0.13	0.12	0.16
n	10	10	10	10	10	10	10
Median	0.55	0.28	0.15	0.15	0.15	0.13	0.13
STDEV	0.30	0.07	0.06	0.06	0.04	0.02	0.11
Skewness	0.000	0.712	-0.353	-0.353	-0.957	-1.417	0.946
Kurtois	-1.224	-0.582	-1.055	-1.055	-0.325	1.315	-0.254
Max	1.00	0.42	0.22	0.22	0.17	0.14	0.38
Min	0.10	0.22	0.04	0.04	0.05	0.08	0.06
Normality A²	0.141	0.301	0.184	0.184	0.540	0.706	0.465
Normality p	0.94	0.52	0.87	0.87	0.13	0.05	0.20

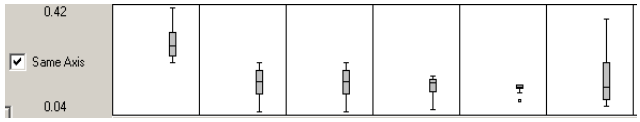
(a) statistical assessments



(b) histograms



(c) time series [0,04 – 0,42]



(d) boxplots [0,04 – 0,42]

Fig. 8Statistical results obtained by using software DEVELVE

VII. CONCLUSION AND FUTURE WORK

This paper presents an extension of investigation which has been carried out by using the Petri nets (PN) apparatus. Since PN modelling permits discrete describing of systems and processes, the goal of this article is to propose an approach for stochastic extension of the PN-investigation based on Stochastic PN (SPN).

For this purposean evaluation scheme (tree of reachability) is presented as a Markov chain in which each marking is described by discrete state with intensities for the transitions between them. We think that this combined investigation will be able to give better results and assessments for the discussed processes and service parameters in a corporative system with heterogeneous information resources.

The analytical defining of Markov model is made by using one independent and controlled factor aand model solution permits to calculate all final probabilities using the following analytical formulas:$p_j=f(a)$, $\forall j=0\div5$.

An additional investigation of obtained statistical assessments is carried out by using specialized software. General values' space for all probabilities is [0.04, 0.42] and at the same time individual sets are determined by each p_j. Bearing in mind that the selected factor (parameter a) is connected with the procedures of identification, authentication and authorization these experimental results permit to analyse means, medians, standard deviation and other assessments that allow to make conclusion about efficiency level of secure access to the corporative resources.

This investigation could be enhanced by additional stochastic modelling or by simulation which will be the future work of the authors.

REFERENCES

[1] R. Romansky, "Digital Privacy in the Network World". Proceedings of the International Conference on Information Technologies (InfoTech-2014), 18-19 Sept. 2014, St. St. Constantine and Elena, Bulgaria, pp.273-284.
[2] L. Garber, "The Challenges of Securing the Virtualized Environment, Computer, January 2012, pp.17-23."
[3] R. Romansky&I. Noninska, "Globalization and Digital Privacy", Electrotechnika& Electronica (E+E), ISSN: 0861-4717, Bulgaria, No 11/12, vol.50, 2015, pp. 36-41. (http://ceec.fnts.bg/journal.html)
[4] A. E. Fischer, "Improving User Protection and Security in Cyberspace", Report of Committee on Culture, Science, Education and Media, Council of Europe, 12.03.2014. Available: http://www.statewatch.org/news/2014/mar/coe-parl-ass-cyberspace-security.pdf.
[5] R. Romansky, "Privacy and Security Considerations" (Chapter 7), pp.9-16. in "PSTNization of the Internet", ed. R. Romansky&B. Khasnatish, Intarea Working Group, USA, 13 Nov.2014 (19 p.), http://datatracker.ietf.org/doc/draft-rdsx1-intarea-pstnize-internet/
[6] R. Romansky&I.Noninska, "Discrete Formalization and Investigation of Secure Access to Corporative Resources", International Journal of Engineering Research and Management (ISSN: 2349-2058), No 5, vol. 3, 2016, pp.97-101, Available:http://www.ijera.com/
[7] DevelveStatistical software for Quality Improvement, Design of Experiments (DOE), Available: http://develve.net/

[8] W.M.P. vanderAalst, "The Application of Petri Netsto Work flow Management", Department ofMathematicsandComputing Science, EindhovenUniversityof Technology,TheNetherlands, Available: http://wwwis.win.tue.nl/~wvdaalst/publications/p53.pdf

[9] K. Jensen&G.Rozenberg, "High-Level Petri Nets: Theory and Application", Springer Science & Business Media, Dec 6, 2012 (724p.)

BIOGRAPHIES

Radi Romansky – Full professor in Technical University of Sofia, Bulgaria; Doctor of Science in Informatics and Computer Science, Vice Rector. Hi has over 190 scientific publications and 18 published monographies, books and manuals. Participant in 33 scientific research projects in the field of computer systems and technologies, e-learning, etc. Full member of the European Network of Excellence on High Performance and Embedded Architectures and Compilation – HiPEAC. Member of the International Editorial Board of scientific journals (Bulgaria, India, Slovakia, USA, etc.), chairman of the Organizing and Program committee of International Conference on Information Technologies. Scientific areas: Computer systems and architectures, Computer modeling, Information technologies, Personal data protection, etc.

Irina Noninska, PhD, Associate professor in Cryptography. She has obtained her PhD degree in Databases and Local Area Networks from Technical University of Sofia. Now she is a lecturer at Computer Systems Department, Technical University of Sofia, delivering courses "Cryptography" and "E-business technologies". Her scientific and research interests are in the area of Information and Network Security, Data Protection, Cryptographic Algorithms and Protocols, Internet of Things, M2M Standards and Applications. She is author and co-author of more than 90 scientific papers, articles and 8 books. She is a member of: Union of Scientists, Bulgaria; Union of Automatics and Informatics; International Editorial Board of International Journal on IT and Security; Organizing and Program Committee of Information Technologies.

DOI 10.17148/IARJSET.2016.3601