Discrete Formalization and Investigation of Secure Access to Corporative Resources

Radi Romansky, Irina Noninska

***Abstract*— This article discusses organization of an extended sub-system for information security which is accomplished with analysis of cloud computing and data centers used by business to store corporative information resources. It is pointed out that the IT security policy should apply adequate technical and organizational measures for personal data protection and managing access rights to all resources in the business information environment. Basic principles of data protection as a part of information security policy in a corporation are presented and a general architecture of corporative security sub-system is proposed. A formalization by using discrete graph structure is made and main procedures for secure access to 3 types of resources (public, private internal and private external) are determined. The Petri nets (PN) apparatus for modeling of secure access processing is used. For the purposes of investigation an analytical definition of model is presented and evaluation of some characteristics is made.**

***Index Terms*— Formalization, Petri net modeling, secure access investigation, processes evaluation.**

I. Introduction

The digital world consists of different components accessed and used by individuals, public institution and business organizations. It permits virtual environments development, ensuring interactive communications (web-environments with a large collection of contents, distributed specialized information resources, tools for virtual reality, etc.). These components create challenges for information security [1] and privacy protection [2]. These opportunities should be extended by cloud computing and data centers [3, 4] which propose remote access to information and system resources based on services.

On the base of Information and Communication Technologies (ICT) different parts of the digital world have been created. They propose real environment for distribution and remote access to information resources and services, sharing personal and public information (content, video, audio, pictures, etc.). Many of these opportunities require creation of personal profiles and uploading personal information which imposes improving data protection rules [5]. At the same time Data Protection Policy (DPP) should be regarded as a part of the global IT Security Policy in the focus of the Cyber-physical security [6].

Now each company deals with different information resources (public and private) collecting many data including personal information about staff, clients and other counteragents. In this reason it is very important to realize adequate system for information security and personal data protection. Development of such system should be organized based on precise strategy using contemporary means and tools for identification & verification, tools for rights managing, biometric technologies, etc., but the efficiency should be previously evaluated and analyzed by using a reliable apparatus.

An approach for security procedures investigation in a business information environment could be based on a discrete formalization and description of the processes by using the apparatus of Petri nets in different forms [7, 8].

The purpose of the article is to carry out experiments based on a discrete formalization and modeling by using Petri nets (PN). The goal is to analyze the secure access to different business resources in the corporative system and to obtain numeric assessments. The investigation is made according the rules of IT security policy and principles of personal data protection (PDP).

The paper is organized as follows: next Section 2 presents some related works in the field; Section 3 discuses some problems of information security and data protection; Section 4 determines the object of the investigation and defines the formal description of the processes in a corporative system with remote access to resources; Section 5 contains the proposed Petri net solution for modeling and investigation; Section 6 is the conclusion.

II. Related Work

An important task of information security procedures is to protect system resources and to oppose eventual attacks – some of the most vulnerable cyber-attacks are presented in figure 1. The usual approach is to implement modern Internet security solutions as antivirus programs, firewalls, tools for browser protection, reputation-checking tools, etc. These tools must be regularly updated in order to guarantee sufficient protection. A risk analysis on web applications based on cloud computing is made in [9]. An important side of the protection is using effective policy for authentication and authorization. It is not a good practice to use one and the same password to access different network resources. All visiting network resources must be deliberated and the reputation and safety rating of websites before using must be analyzed. An adequate security policy is required when the access to the corporative resources is made by using mobile devises [10].

Manuscript received May 12, 2016.

Radi Romansky, Electronics, Computer Systems and Technologies Dept., Technical University of Sofia, Bulgaria

Irina Noninska, Computer Systems Dept., Technical University of Sofia, Bulgaria

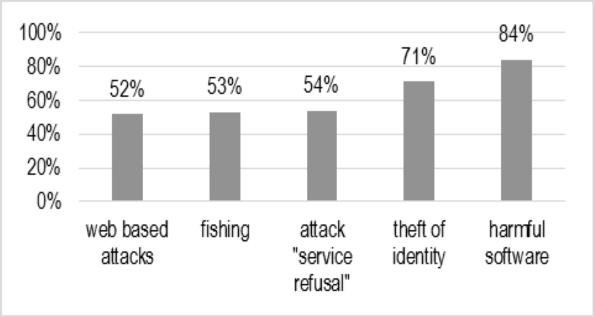

Fig. 1. Most vulnerable cyber-attacks

Grid technology increases the performance of tasks realization in case of very large data, but at the same time it increases the risk for attacks to the resources. In this reason Ref. [6] discuses cyber-physical security of Wide-Area Monitoring, Protection and Control from a coordinated cyber-attack perspective and introduces a game-theoretic approach to address the issue.

A possibility to increase productivity and decrease the expenses in any corporation is to use cloud services, but the component failures in a large Infrastructure-as-a Service (IaaS) cloud could be a problem. A scalable, stochastic model-driven approach to quantify the availability of a large-scale IaaS cloud, where failures are typically dealt with through migration of physical machine are proposed in [4]. In general, the obligation of companies which use cloud computing should be managed by effective security system for resources protection [11].

The modeling as a tool for investigation is very useful approach for determination of structural discrepancy revealing special features of processes realization. Petri Nets (PN) is an apparatus for discrete analytical modeling and investigation which is discussed in [7, 8, 12]. For example, article [12] deals with cloud-based manufacturing (CBM) and introduces an approach for modeling and analyzing the concurrency and synchronization of the material flow of crowdsourcing processes in CBM systems, based on Stochastic Petri Nets (SPN). The purpose of the investigation is to verify the manufacturing performance.

Ref. [13] proposes a stochastic model for investigation cloud data center management as a key problem due to the numerous and heterogeneous strategies that can be applied. The author discuses performance evaluation of cloud computing infrastructure as an important part of cloud strategy which corresponds to quality of service (QoS) experienced by users. An analytical model based on stochastic reward nets (SRN) is presented in the paper and several performance metrics are defined and evaluated to analyze the behavior of a cloud data center (utilization, availability, waiting time, responsiveness).

III. Information Security and Data Protection

Information security deals with protection of information resources from all possible threats via the Internet communication. Some of main vulnerabilities, discussed in the scientific literature could be summarized as deliberate software attacks and acts of espionage or trespass (viruses, worms, macros, denial of service, unauthorized access, etc.); technical hardware & software failures and errors including acts of human error or failure; deliberate acts of sabotage or vandalism; illegal confiscation of equipment or information and compromises to intellectual property; information disclosure; etc.

An efficiently structured Information Security Management System (ISMS) should consist of tools and measures, applied to oppose all these threats. Main dimensions of this structure are: information security policy; organizational and technical components for data protection; rules for hardware, software and biometric identification; authorization by determining levels of digital rights for resources' using; rules for access restriction to information and systems' resources, rooms and servers for external (unauthorized) persons, etc. Most popular and efficient mechanisms for information security could be summarized as follows:

✓ Development a strong security policy in accordance with security requirements and implementation of a relevant ISMS;

✓ Installing and periodical renewing software for information and system resources;

✓ Improving applied authentication scheme by using reliable techniques for users' identification, biometric identification and smart card;

✓ Authorization on the base of a relevant Digital Rights Management System (DRMS) which is able to ensure access to all corporative resources from authorized users only. This mechanism could guarantee high level of information confidentiality including personal profiles.

Hence, technologies for authentication, authorization digital identity and protection of intellectual property occupy an important part of ISMS. It is very important to use cryptography in communications and data archiving, managing security training programs for professionals and staff.

Data protection is an obligation of each controller of personal data and DPP which must be regarded in the context of IT Security Policy as a part of Security Policy (figure 2). The first standard for Security Policy titled "Department of Defense Trusted Computer System Evaluation Criteria (TCSEC)" is accepted in 1985 in USA. TCSEC describes the security policy as a collection of security rules, standards, procedures, instruments and practical instructions for regulation of management, protection and dissemination of the information. This document gives rules for control of access to the information resources.

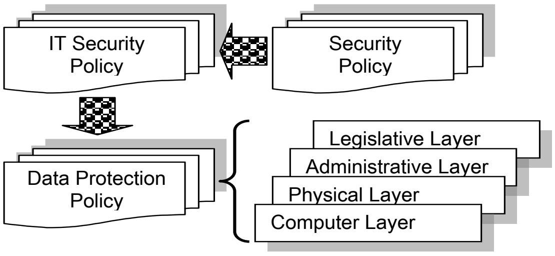

Fig. 2. Data protection policy in the frame of security policy

The computer layer (fig. 2) presents embedded instruments for protection of personal data structures (hardware, software, cryptographic, biometric). The physical layer consists of technical instruments, means and tools for unauthorized access blocking, separation of LAN segments, recognition of legitimate users, etc. The next two layers unite organizational rules, instructions and procedures for administrative control and legislative and normative documents.

Data Protection Policy should be harmonized with IT Security Policy by using security rules for all layers from internal computer layer to the external legislative layer. The general understanding for "personal data" is the information that permits identification of a person directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. In this reason any operation or set of operations with personal data (using automatic or not-automatic means) is called "processing of personal data".

IV. Discrete Formalization of Secure Access

Formalization of an investigated process is a compulsory stage which should precede each model developing. The event-graph apparatus is the most popular tool for discrete formalization and it permits to describe process realization as a state transition network (STN). This approach is used because each process could be regarded as a sequence of connected discrete events. In this reason the formal model of the investigated object (or process) could be described by using an ordered graph structure with discrete set of states (presented events) with transition between them.

An architecture of e-service system with two sub-systems (Front Office and Back Office) is proposed in fig. 3. The information resources are integrated in the system (internal resources) or are stored in the cloud data center (external resources).

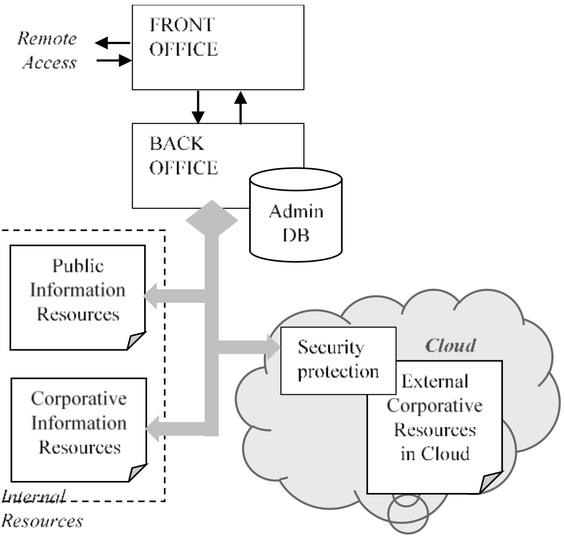
Remote Access
FRONT OFFICE
BACK OFFICE
Admin DB
Public Information Resources
Corporative Information Resources
Internal Resources
Security protection
Cloud
External Corporative Resources in Cloud

Fig. 3. General architecture of e-service system

Formal descriptions by using STN is proposed in fig. 4. The organization of the secure access to the internal and external resources is based on realization of the two main sub-systems.

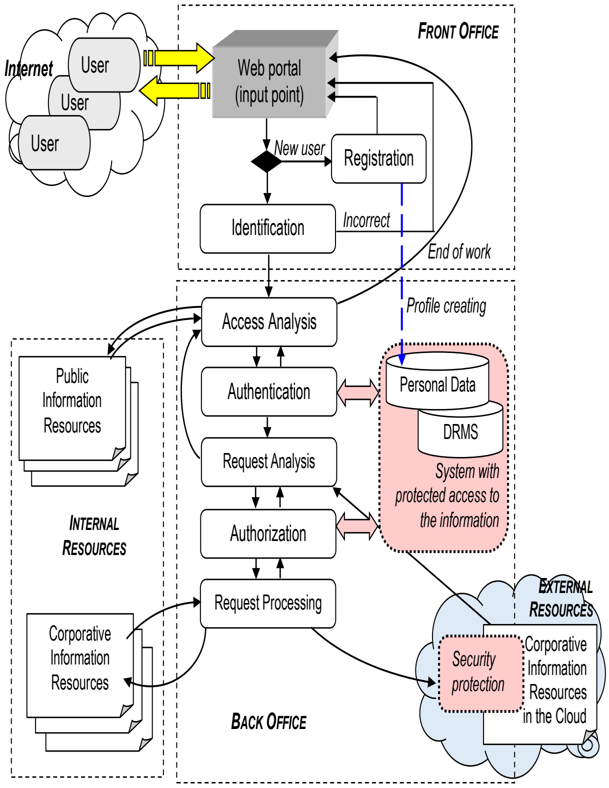

Fig. 4. Formal structural organization of system for secure access.

♦ Front office – it supports user's access by input point (web portal). The main functions of this system are user's identification, legitimate access checking and registration procedure for a new user. The registration procedure creates a personal profile (with personal data) and every user must be preliminary informed for his/her rights according the law. In addition an audit file for registration each access (time, IP address and relative attributes) and statistical data should be created.

♦ Back office – it deals with basic administrative procedures directing requests to a chosen component of the system for processing. The module "Access Analysis", which is designed as a gate of the back office, checks the type of legitimate access to system resources. Authentication is not compulsory if the information resources in the internal found are public, but the procedure should be made for all corporative (private) information resources – internal and external. The module "Request Analysis" determines 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 based on corporative policy. In this reason after finishing access to an external resource the process must return back to the module "Request Analysis" and new authorization.

V. Investigation by Using PN Model

The proposed description is based on the classical Petri Net (PN) apparatus where the main procedures are presented as a transitions, and the condition are presented as positions. The theoretical-set definition is presented below.

PN = {*T*, *P*, *I*, *O*}, *T*∩*P*=∅

Set of transactions T = {t_i / *i*=1÷9}:

t₁ – remote user's access to the input point;
t₂ – registration of a new user;
t₃ – activate the identification procedure;
t₄ – access to public resources;
t₅ – authentication procedure for access to corporative (private) resources (T - correct; F – incorrect);
t₆ – finishing the work;
t₇ – authorization procedure (rights checking) by using DRMS tools (T – correct; F – incorrect);
t₈ – access to external corporative resources;
t₉ – access to internal corporative resources.

Set of positions P = {p_j / *j*=1÷5}:

p₁ – user's access is activated;
p₂ – access of a registered user;
p₃ – legitimated user's access;
p₄ – successful authentication;
p₅ – successful authorization.

Input functions:

$I(t_1) = \varnothing$
$I(t_2) = \{p_1, p_1\}$
$I(t_3) = \{p_1, p_2\}$
$I(t_4) = I(t_5) = I(t_6) = \{p_3\}$
$I(t_7) = \{p_4\}$
$I(t_8) = I(t_9) = \{p_5\}$

Output functions:

$O(t_1) = \{p_1, p_1\}$
$O(t_2) = \{p_1, p_2\}$
$O(t_3) = O(t_4) = O(F.t_5) = O(F.t_7) = \{p_3\}$
$O(T.t_5) = \{p_4\}$
$O(t_6) = O(t_8) = \varnothing$
$O(T.t_7) = \{p_5\}$
$O(t_9) = \{p_4\}$

The graph scheme of the model based on the presented theoretical-set definition is shown in the figure 5.

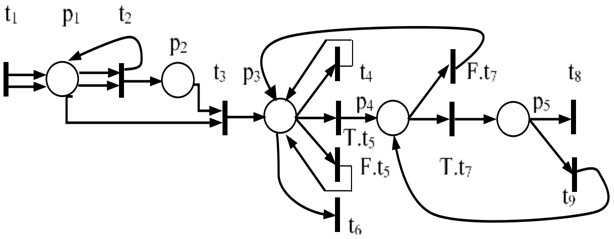

Fig. 5. Graph presentation of the PN model

The evolution of the PN-model is presented by the tree given in the fig. 6 and the marks in the positions during the evolutions (model execution) are shown in table 1.

The investigation of the defined PN description is made based on the analysis of the evolution tree shown in fig. 6. The main PN-model characteristics are determined below.

✓ *Reachability* – the model permits cyclic recurrence with reiteration of some phases based on activation of the selected transition.

✓ *Liveness* – this characteristic deals with initial marking μ₀, bearing in mind that minimum one permitted transaction for each step of the evolution exists.

$$\mu_0 = (0,0,0,0,0) \xrightarrow{t1} \mu_1 = (2,0,0,0,0)$$
$$\mu_1 \xrightarrow{t2} \mu_2 = (1,1,0,0,0) \xrightarrow{t3} \mu_3 = (0,0,1,0,0)$$
$$\mu_3 \xrightarrow{t4} \mu_3$$
$$\mu_3 \xrightarrow{t5F} \mu_3$$
$$\mu_3 \xrightarrow{t6} \mu_0$$
$$\mu_3 \xrightarrow{t5T} \mu_4 = (0,0,0,1,0) \xrightarrow{t7F} \mu_3$$
$$\mu_4 \xrightarrow{t7T} \mu_5 = (0,0,0,0,1) \xrightarrow{t9} \mu_4$$
$$\mu_5 \xrightarrow{t8} \mu_0$$

$$\mu_0 \to \mu_1 \to \mu_2 \to \mu_3 \begin{cases} \to \mu_3 \\ \to \mu_3 \\ \to \mu_4 \begin{cases} \to \mu_5 \begin{cases} \to \mu_0 \\ \to \mu_4 \end{cases} \\ \to \mu_3 \end{cases} \\ \to \mu_0 \end{cases}$$

Fig. 6. Evaluation tree of the PN model

Table 1.

t	*μ*	*Marks in the each position pᵢ*				
		1	**2**	**3**	**4**	**5**
	μ₀	0	0	0	0	0
t₁	*μ₁*	2	0	0	0	0
t₂	*μ₂*	1	1	0	0	0
t₃	*μ₃*	0	0	1	0	0
t₄	*μ₃*					
T*.t₅*	*μ₄*	0	0	0	1	0
F*.t₅*	*μ₃*					
t₆	*μ₀*					
T*.t₇*	*μ₅*	0	0	0	0	1
F*.t₇*	*μ₃*					
t₈	*μ₀*					
t₉	*μ₄*					

✓ *Blocking* – the PN-model has not any blocked marking and the model is active, so there are not conflict situations.

✓ *Boundless* – the model is 2-limited because the number of marcs at each position during the evaluation <μ₀→μ₁→μ₂→ … →μ₀> is no more than 2, i.e. $\Sigma\mu(p_i) \leq 2$.

VI. Conclusion

This paper presents an investigation approach, intended to analyze the processes applied to protect corporative resources in an organization by using contemporary security means and tools, where special place have procedures for users identification. Personal profiles creating and protection of the corporative (private) information resources based on procedures for authentication and authorization have been taken into account, as well. It should pointed clearly that the most important obligation of each data controller is to protect personal data (profiles) created during the preliminary registration. In this reason an important part of information security in any corporative structure is to apply adequate technical and organizational measures for personal data protection – the data of registered users and the data of its own staff. This obligation has a high significance in the sense of the last regulation of the European Commission in the field of data protection in the cyber world [5].

The proposed approach for investigation is based on a discrete formalization of the main processes connected to the remote access to different types of corporative resources – public and private (internal and external – stored in the cloud and/or data centers). This formalization is made based on a graph description of the actions that must be realized in a corporative system that proposes e-servicing and access to information files and system resources.

The investigation has been carried out based on discrete modeling by using Petri nets apparatus. We think that this investigation could be extended by using a stochastic approach based on the theory of stochastic Petri nets (SPN) and this will give better results and assessments for the discussed processes and service parameters. It is possible to extend the investigation of the proposed structure of secure access in other directions, for example by using Markovian chains (with discrete states and discrete time for transactions), statistical analysis (empirical modeling), simulation, etc. These opportunities could be regarded as a possibility for future work of the authors.

REFERENCES

[1] L. Garber. The challenges of securing the virtualized environment. *Computer. January* 2012, pp.17-23.

[2] R. Romansky. Digital privacy in the network world. *Proceedings of the International Conference on Information Technologies (InfoTech-2014)*, 18-19 September 2014, Bulgaria, pp.273-284.

[3] D. Chen and H. Zhao. Data security and privacy protection issues in cloud computing, *International Conference on Computer Science and Electronics Engineering (ICCSEE)*. 23-25 March 2012, Vol. 1, pp.647-651.

[4] R. Ghosh, F. Longo, F. Fratini, S. Russo and K.S. Trivedi, Scalable analytics for IaaS cloud availability. *IEEE Transactions on Cloud Computing, 2 (1)*, January-March 2014, pp.57-70.

[5] 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.

[6] A. Ashok, A. Hahn and M. Govindarasu. Cyber-physical security of wide-area monitoring, protection and control in a smart grid environment. *Journal of Advances Research, 5 (4)*, July 2014, pp.481-489.

[7] P. Rygieski and S. Kounev. Data center network throughput analysis using queueing Petri nets. *34th IEEE Int'l Conf. on Distributed Computing Systems Workshops*, 30 June – 03 July 2014, Madrid, Spain, pp.100-105.

[8] A. Rogge-Solt, W. van der Aalst and M. Weske. Discovering stochastic Petri nets with arbitrary delay distributions from events logs. *Lecture Notes in Business Information Processing*, vol. 171, 2014, pp.15-27.

[9] S. Rana and Pr. Kumar Joshi. Risk analysis in web applications by using cloud computing, *International Journal of Multidisciplinary Research, 2 (1)*, 2012, pp. 386-394.

[10] Hasan, B. et al. User acceptance identification of restrictions caused by mobile security countermeasures. *5th International Conference on Mobile Services, Resources, and Users*. 21-26 June 2015, Belgium, pp.31-37.

[11] Viti, P. A. F. et al. Current issues in cloud computing security and management. *8th Int'l Conf. on Emerging Security Information, Systems and Technologies*. 6-20 November 2014, Lisbon, Portugal, pp.36-42.

[12] D. Wu, D. Rosen and D. Schaefer. Modeling and analyzing the material flow of crowdsourcing processes in cloud-based manufacturing systems using stochastic Petri nets. *ASME 2014 Int'l Manufacturing Science and Engineering Conference (MSEC2014)*, vol. 1, 9-13 June 2014, Detroit, Michigan, USA, 9 p.

[13] D. Bruneo, (March 2013). "A Stochastic Model to Investigate Data Center Performance and QoS in IaaS Cloud Computing Systems. *IEEE Transactions on Parallel and Distributed Systems*, "*25 (3)*, pp.560-569.

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.