Notice of Violation of IEEE Publication Principles

"Security Risk Analysis for Cloud Computing Systems,"
by Vadym Mukhin and Artem Volokyta
in the Proceedings of the 2011 IEEE 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), vol.2, September 2011, pp.737-742

After careful and considered review of the content and authorship of this paper by a duly constituted expert committee, this paper has been found to be in violation of IEEE's Publication Principles.

This paper is a duplication of the original text from the paper cited below. The original text was copied without attribution (including appropriate references to the original author(s) and/or paper title) and without permission.

Due to the nature of this violation, reasonable effort should be made to remove all past references to this paper, and future references should be made to the following article:

"Towards a Cloud-specific Risk Analysis Framework"
by Bernd Grobauer, Tobias Walloschek, Elmar Stocker
in Siemens IT Solutions and Services Monograph, Publication Date: 2010, pp. 1-24

The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
15-17 September 2011, Prague, Czech Republic

Security Risk Analysis for Cloud Computing Systems

Vadym Mukhin, Artem Volokyta
National Technical University of Ukraine "Kiev Polytechnic Institute",
Pr. Pobedy, 37, Kiev, 03056, Ukraine. E-mail: mukhin@comsys.ntu-kpi.kiev.ua

Abstract — **This paper devoted to the analysis of a cloud –specific vulnerabilities and risk analysis in the cloud systems. There are described the main characteristics of cloud systems and a reference architecture of cloud computing. Also, there is suggested the special estimations for the risk analysis, which are based on the preliminarily vulnerabilities analysis. The proposed approach allow to estimate the influence of the various factors on the effective risk level and to formulate the requirements to the security methods and mechanisms.**

Keywords — cloud systems; vulnerabilties analysis, security risk analysis

I. A Safety Issues for Cloud Computing

The data processed in the cloud systems must be protected from the unauthorized access. Due to the cloud systems specificity, the additional security tools and mechanisms should be implemented. First of all, let us describe in more detail the specifics of the cloud systems, that allows us to formulate the requirements for security of the cloud computing.

II. The Main Characteristics of Cloud Computing

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

A deeper understanding of cloud computing can be reached by examining essential characteristics of cloud computing, a cloud-computing reference architecture, and core technologies of cloud computing.

NIST [1] identifies the following essential cloud characteristics:

- **On-demand self-service.** Users can order and manage services without human interaction with the service provider, using, e.g., a web portal and management interface. Provisioning and de-provisioning of services and associated resources occur automatically at the provider.
- **Ubiquitous network access.** Cloud services are accessed via the network, usually the internet, using standard mechanisms and protocols.
- **Resource pooling.** Computing resources used to provide the cloud service are realized using a homogeneous infrastructure which is shared between all users of the service.
- **Rapid elasticity.** Resources can be scaled up and down rapidly and elastically.
- **Measured service.** Resource/service usage is constantly metered, supporting optimization of resource usage, usage reporting to the customer and pay-as-you-go business models.

III. A Reference Architecture of Cloud Computing

The stack of cloud service models Software as a Service (SAAS), Platform as a Service (PAAS) and Infrastructure as a Service (IAAS) is well established [2]. Fig. 1 shows a reference architecture with a special focus on making the most important security-relevant cloud components explicit and providing an abstract yet complete overview of cloud computing as the basis for the analysis of security issues.

The reference architecture inherits the layered approach in that layers may encompass one or more service components. Here, "service" must be understood in the broad sense of providing something that may be both material (e.g., shelter, power, hardware, etc.) as well as immaterial (e.g., a runtime environment). For two layers, namely "Cloud Software Environment" and "Cloud Software Infrastructure", the model makes the three main service components of these layers – computation, storage and communication – explicit. It is important to note that the services in the top layer can be implemented on the basis of layers further down the stack as well, in effect skipping intermediate layers. For example, a cloud web application can still be implemented and operated in the traditional way, namely running on top of a standard operating system without making use of dedicated cloud software infra-structure and environment components.

The layering and compositionality imply that the transition from providing some service / function in-house vs. sourcing the service / function can take place between any of the layers exhibited in the model.

In addition to the original model, supporting functions that have relevance for services in several layers have been identified and added to the model as vertical spans over several horizontal layers.

The cloud reference architecture (Fig.1) exhibits three main parts:

- **Supporting (IT) infrastructure.** These are facilities / services that are common to any IT service, whether or not they are a cloud offering. We include them in the reference architecture, because we want to provide the complete picture: a complete treatment of IT security must also take non-cloud-specific components of a cloud service into account.
- **Cloud-specific infrastructure.** The indeed cloud-specific infrastructure components are: cloud-specific vulnerabilities and corresponding controls will be mapped mostly to these components.

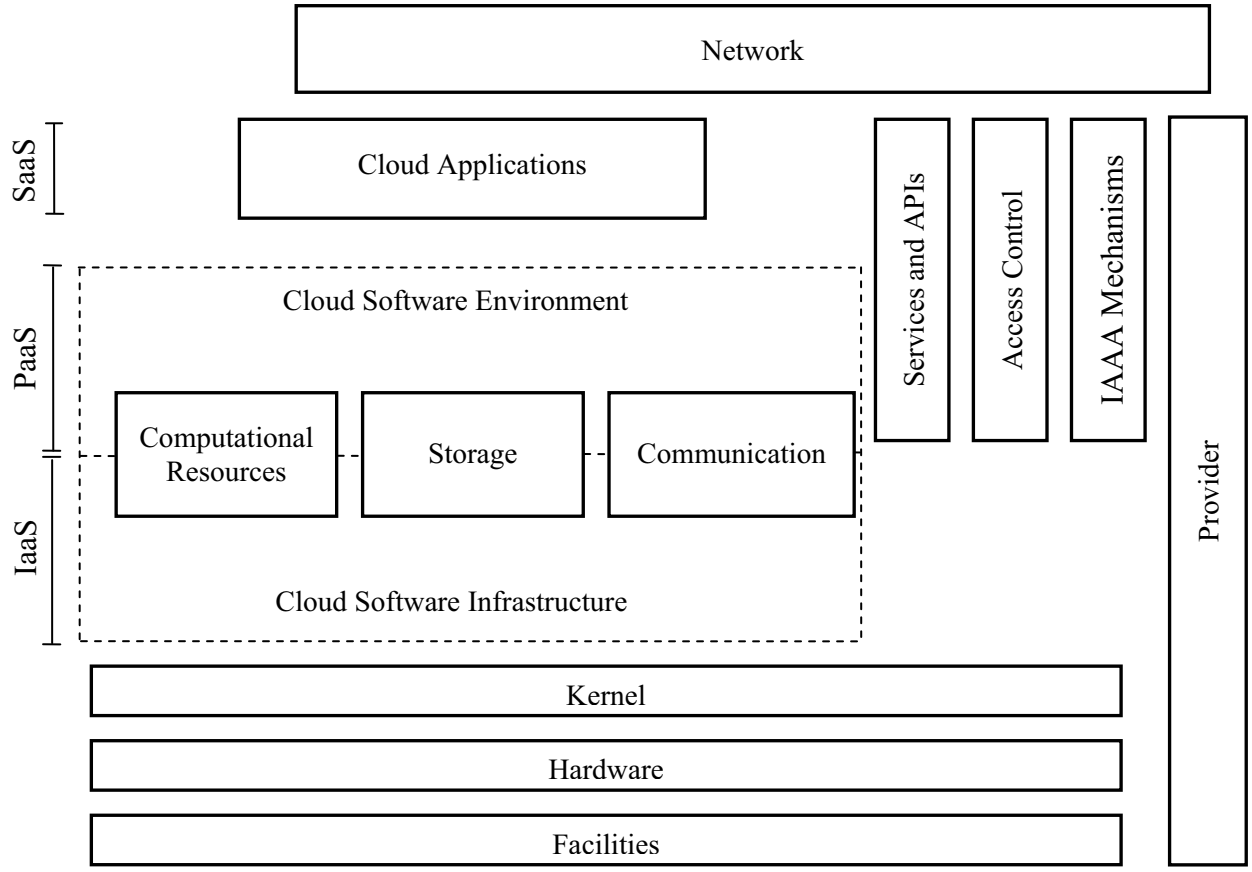

Figure 1. Cloud Reference Architecture

- **Cloud-service consumer.** In order to provide a complete picture, the cloud-service customer is included in the reference architecture, as it is of relevance for an all-encompassing security treatment.

The network that separates the cloud-service consumer from the cloud infrastructure is also made explicit: the fact that access to cloud resources is carried out via a (usually untrusted) network is one of the main characteristics of cloud computing [3],[4].

IV. Cloud-specific Vulnerabilities

Based on the abstract view of cloud computing presented in the previous section, we now can move towards a definition of what constitutes a cloud-specific vulnerability:

- A vulnerability is cloud specific, if at least one of the following indicators is true:
- it is intrinsic to or prevalent in a core technology of cloud computing
- it has its root cause in one of NIST's essential cloud characteristics
- it is caused by cloud innovations making tried and tested security controls hard or impossible to implement
- it is prevalent in established state-of-the-art cloud offerings

In the following, we examine each of these four indicators.

V. Vulnerabilities Intrinsic Core-technology of Cloud Computing

The core technologies of cloud computing – web applications / services, virtualization, and cryptography – have vulnerabilities that are either intrinsic to the technology or prevalent in state-of-the-art implementations of the technology [5].

To give a few examples of vulnerabilities:

- **Virtual-Machine Escape Vulnerability.** The possibility that an attacker may succeed in escaping

from a virtualized environment lies in the very nature of virtualization. Hence, this vulnerability must be considered as intrinsic to virtualization and is obviously highly relevant to cloud computing.

- **Session Riding & Session Hijacking.** Web application technologies have to over-come the problem that the HTTP protocol by design is a state-less protocol, whereas web applications require some notion of session state. There are many techniques to implement session handling and – as any security professional knowledgeable in web application security will testify – many implementations of session handling are vulnerable to session riding and session hijacking.
  One can argue whether session riding / hijacking vulnerabilities are intrinsic to web application technologies or "only" prevalent in many current implementations. In any case: these vulnerabilities are certainly relevant for cloud computing.
- **Insecure/Obsolete Cryptography.** For all crypto-graphic mechanisms and algorithms there is the danger that advances in cryptanalysis may render them insecure by finding novel methods of breaking the cryptography. It is even more common to find crucial flaws in the implementation of cryptographic algorithms that turn a very strong encryption into a very weak encryption (or sometimes no encryption at all). Because broad take-up of cloud computing is unthinkable without the use of cryptography to protect confidentiality and integrity of data in the cloud, vulnerabilities concerning insecure and / or obsolete cryptography are highly relevant for cloud computing.

VI. Vulnerabilities with Root Cause in an Essential Cloud Characteristic

As described above, the essential cloud characteristics according to NIST are [6]:

- on-demand self-service;
- ubiquitous network access;
- resource pooling;
- rapid elasticity;
- reasured service.

There are vulnerabilities that can be said to have their root cause in one or more of these characteristics. To give a few examples of vulnerabilities:

- **Unauthorized access to management interface.** The cloud characteristic "on-demand self-service" requires a management interface that is accessible to users of the cloud service. Unauthorized access to the management interface therefore is a vulnerability that must be considered especially relevant for cloud systems: the probability that unauthorized access could occur is much higher than for traditional systems where the management functionality is accessible only to a few administrators.
- **Intranet protocol vulnerabilities.** The cloud characteristic "ubiquitous network access" states that cloud services are accessed via network using standard protocols. In most cases, this network is the intranet and thus must be considered as an untrusted network. Intranet protocol vulnerabilities, e.g., vulnerabilities that allow man-in-the-middle attacks, are relevant for cloud computing.
- **Data recovery.** The cloud characteristics "pooling" and "elasticity" lead to a situation where resources that have been allocated to one user may be re-allocated to a different user at a later point of time. In the case of memory or storage resources, it may therefore be possible to recover data written by a previous user – hence a vulnerability that has its root cause in the said cloud characteristics.
- **Metering/Billing Evasion.** According to the cloud characteristic "measured ser-vice", any cloud service has a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, active user accounts, etc.);

Metering data is used for optimization of service delivery as well as billing. Vulnerabilities regarding the manipulation of metering / billing data or billing evasion therefore have their root cause in this particular characteristic of cloud computing.

VII. Vulnerabilities Caused by Defects of Known Security Controls in a Cloud Setting

As discussed above, the vulnerability exists when a threat agent's attack capabilities exceed the strength of the system to resist the attack. Hence, the weakness or absence of security control, i.e., a counter measure against certain attacks, constitutes the vulnerability. Vulnerabilities concerning problems with standard security controls must be considered cloud-specific, if cloud innovations directly cause difficulties in implementing these controls. We refer to such vulnerabilities as "control challenges".

Here are some examples of control challenges:

- **Insufficient network-based controls in virtualized networks.** By the very nature of cloud services, the administrative access to IaaS network infrastructure and the possibility of tailoring network infrastructure are usually limited: hence, standard controls such as IP-based network zoning usually cannot be applied. Standard techniques such as network-based vulnerability scanning are usually forbidden by IaaS providers, e.g. because "friendly" scans cannot be distinguished from attacker activity. Finally, technologies such as virtualization lead to a situation where network traffic occurs not only on physical networks but also within virtualized networks (e.g., for communication between two virtual machine environments hosted on the same server). All in all, this constitutes a control challenge, because tried and tested security controls at network level may not work in a given cloud environment.
- **Poor key-management procedures.** As pointed out in

a recent study by ENISA [7], cloud computing infrastructures require the management and storage of many different kinds of keys. Because virtual machines do not have a fixed hardware infrastructure and cloud-based content tends to be geographically distributed, it is more difficult to apply standard controls, such as hardware security module (HSM) storage, to keys on cloud infrastructures.

- **Security metrics not adapted to cloud infrastructures.** Currently, no standardized cloud-specific security metrics exist that could be used by cloud customers to monitor the security status of their cloud resources. Until such standard security metrics are developed and implemented, controls with respect to security assessment and the audit and accountability are more difficult / costly or may even be impossible to employ.

VIII. Vulnerabilities Prevalent in State-of-the-art Cloud Offerings

Although cloud computing is a relatively young topic, there already are myriads of cloud offerings on the market. Hence, the three indicators of cloud-specific vulnerabilities presented above can be complemented with a fourth, empirical indicator: if the vulnerability is prevalent in state-of-the-art cloud offerings, it must be regarded as cloud-specific. Obviously, most such vulnerabilities should also fit one of the other three indicators. Indeed, the following examples are also typical for the core technology web applications and services:

- **Insufficient/faulty authorization checks.** If the implementation of an application carries out insufficient or faulty authorization checks, then service / application users may be able to view information or carry out actions for which they are not authorized. For example, missing authorization checks are the root cause of URL-guessing attacks in which users modify URLs so that they point to information regarding a different user account – missing authorization checks then allow the user to view content of a different user. Security assessments of current cloud-computing offerings show that faulty /missing authorization checks occur frequently in state-of-the-art cloud SaaS offerings.
- **Injection vulnerabilities.** Injection vulnerabilities are exploited by manipulating input to a service / application so that parts of the input are interpreted and executed as code against the intentions of the programmer. Examples of injection vulnerabilities are:
  - *SQL injection:* the input contains SQL code that is erroneously executed in the database backend;
  - *command injection:* the input contains OS commands that are erroneously executed via the operating system;
  - *cross-site scripting:* the input contains Java-script code that is erroneously executed by a victim's browser.

  Security assessments of web components of current cloud offerings show the prevalence of injection vulnerabilities in state-of-the-art offerings.
- **Weak authentication schemes.** Many widely used authentication mechanisms are weak. For example, the use of usernames and passwords for authentication is weak because of (1) insecure user behavior (users tend to use weak passwords, re-use passwords, etc.) and (2) inherent limitations of one-factor authentication mechanisms. The implementation of authentication mechanisms may also have weaknesses allowing, for example, the interception and replay of credentials [8]. The majority of current web applications used in state-of-the-art cloud services employ usernames and passwords as authentication mechanism.

IX. Security Risk Analysis in the Cloud Systems

There are many risk assessment methodologies, but in all of these methodologies, similar steps are carried out. Fig. 2 shows the steps of NIST's risk assessment methodology as described in "NIST SP 800-30: Risk Management Guide for Information Technology Systems" [6].

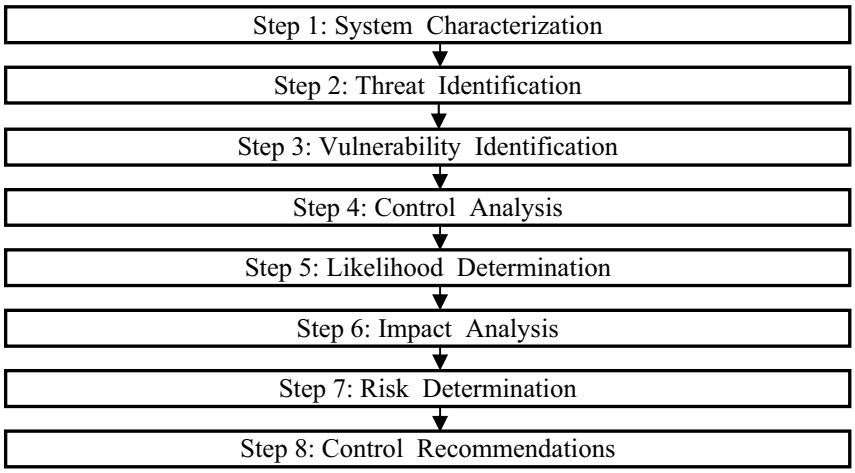

Figure 2. Assessment Activities according to NIST SP800-30

ISO 27005 [9] defines risk as *"the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization"* and adds that it is measured in terms of a combination of the likelihood of an event and its consequences. A useful overview of factors contributing to risk [10],[11] is presented in Fig. 3.

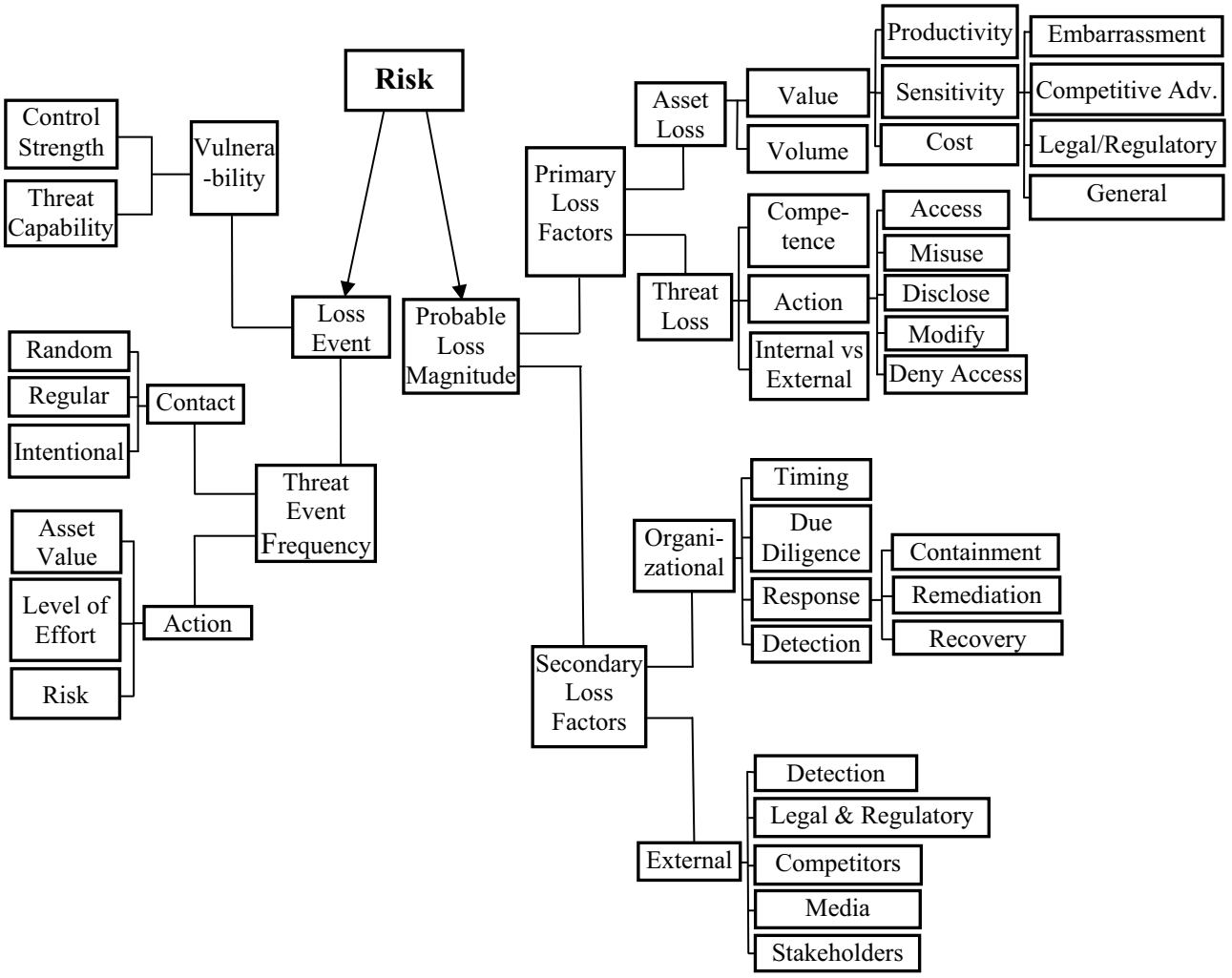

Figure 3. Factors contributing to security risk

There are identified around 40 cloud-specific vulnerabilities (nine of which are control challenges) and each vulnerability has been positioned in relevant layer(s) and supporting function(s) of the cloud reference architecture. Thus, a cloud-specific risk assessment following, e.g., the steps outlined in Figure 2 is supported as follows:

- **System Characterization.** By positioning relevant system components in the cloud reference architecture, a standardized abstract view on a system under evaluation can be achieved.
- **Vulnerability Identification.** Because all identified cloud-specific vulnerabilities have also been positioned in the cloud reference architecture, it is immediately clear, which vulnerabilities are relevant for the system under consideration (and which system components may be affected). Thus, the usually time-consuming process of vulnerability identification can be carried out very efficiently.
- **Control Analysis & Control Recommendations.** The mapping of vulnerabilities into controls provides a sound basis for control analysis and control recommendations.

There are 6 main factors, which make influence on the vulnerability: the point of vulnerability appearance, the level of security, the value of the processed information, the influence of cloud-specifics, the adequateness of security tools applying, the qualification of safety administrator.

Let's enter the concept of the vulnerability of types I and II. The type I are such vulnerability which are potentially prevented by the security tools implemented in cloud systems, and the type II are those, which are not prevented even potentially. We generate an integral estimation C, determined the potential damage due to the to attack on the vulnerability:

$$C = \sum_{i=1}^{N} \frac{UI_i}{U} + \sum_{j=1}^{M} K_j * \frac{UII_j}{U} \quad (1)$$

where *UI* – the number of the users, who are compromated as a result of attack to the vulnerability of the type I; *N* – the number of vulnerabilities of type I; UII– the number of the users, who are compromated as a result of attack to the vulnerability of the type II; *M* - the number of vulnerabilities of type II; *U* – the total number of users in system; K_j - the coefficient, characterizing the vulnerability of type II.

To obtain this estimation it is necessary for the each revealed vulnerability:

1. To define the vulnerability type: I or II;

2. If there is the vulnerability type II with the experts estimations to define the possible consequences of this vulnerability realization and to calculate coefficient K_i;

3. To estimate the number of users, who may suffer the attacks, realized with vulnerabilities types I and II using, in relation to the total number of users in cloud systems.

The security risk analysis is based on the probability estimation of the unauthorized actions realization which is performed using the vulnerabilities in safety mechanisms.

We suggest to use the function *TR,* reflecting the possibility of threat realization, for the estimation of the risk of the threats realization by intruders:

$$TR = \frac{1}{m} * \sum_{i=1}^{m} \sum_{j=1}^{n} K_{ij} PE_j = \frac{1}{m} * \sum_{i=1}^{m} \sum_{j=1}^{n} K_{ij} PB_j TL_j, m \le n \quad (2)$$

where K_{ij} =0, if the *i*-th position in the threats list is not related to the *j*-th intruder (non-dangerous factor), K_{ij} =1, if the *i*-th position in the threats list is related to the *j*-th intruder (dangerous factor), *m* – the number of potentially dangerous subjects, *n* – the total number of the subjects, PE_j – the effective probability of threat realization, PB_j – the basic probability of threat realization, i.e. the well-known or standard probability of certain threat.

The volume of the possible damage due to the threat realization is defined as:

$$PL_i = c_i \sum_{k=1}^{3} K_{ki} A_k \quad (3)$$

where A_k – the apriory-formed requirements on support of 3 main features of the secured information: confidentiality, integrity and availability. These requirements can be expressed on the relative scale, thus K_{ki} = 0, if the certain threat has no influence on *k*-feature of the information, K_{ki} = 1, if the certain threat has influence on *k*-features of the information, c_i – the normalizing coefficient.

Thus, the risk of the safety threats realization *R* in DCS is next:

$$R = \left(\frac{1}{m} * \sum_{i=1}^{m} \sum_{j=1}^{n} K_{ij} PB_j TL_j \right) x \left(c_i \sum_{k=1}^{3} K_{ki} A_k \right) \quad (4)$$

This approach allows to estimate the influence of the various factors on the effective risk level and to formulate the requirements to the security methods and mechanisms.

X. Conclusion

Cloud computing is in constant development. We are certain that additional cloud-specific vulnerabilities will be identified; other vulnerabilities will become less of an issue as the field of cloud computing matures. Using a precise definition of what constitutes a vulnerability and the four indicators of cloud-specific vulnerabilities identified in this report will provide a level of precision and clarity that the current discourse about cloud-computing security often lacks.

The kind of vulnerability termed “control challenge” is of special interest for further research into cloud-computing security: control challenges point to situations where security controls that have been successfully used for many years cannot be effectively used in a cloud setting.

Finally, an analysis of cloud-specific vulnerabilities to security controls can provide information about which security controls are especially relevant for cloud-computing infrastructures, which is a first stepping stone towards cloud-specific certification and audit schemes.

References

[1] *NIST SP800-53 rev 3: Recommended Security Controls for Federal Information Systems and Organizations*, NIST Publication, August 2009, http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final-errata.pdf.

[2] L. Youseff, M. Butrico, and D. Da Silva, Towards a Unified Ontology of Cloud Computing, *Proc. of Grid Computing Environments Workshop (GCE)*, 2008.

[3] P. Mell and T. Grance, *Effectively and Securely Using the Cloud Computing Paradigm (v0.25)*, NIST Publication, 2009, http://csrc.nist.gov/groups/SNS/ cloud-computing/index.html.

[4] *Security Guidance for Critical Areas of Focus in Cloud Computing, V2.1* Cloud Security Alliance Publication, 2009, http://www.cloudsecurityalliance.org/csaguide.pdf.

[5] R.C. Cardoso, M.M. Friere, *Security vulnerabilities and exposures in internet systems and services. Encyclopedia of multimedia technology and networking.* IDEA Group Reference. Hershey, Pennsylvania, 2005. – pp. 910 – 916.

[6] G. Stonebruner, A. Goguen, and A. Feringa, *NIST SP 800-30: Risk Management Guide for Information Technology Systems*, NIST Publication, July 2002. http://csrc.nist.gov/publications/nistpubs/ 800-30/sp800-30.pdf

[7] *Cloud Computing: Benefits, risks and recommendations for information security.* European Network and Information Security Agency (ENISA), November 2009.

[8] R. Tassabehji, *Information security threats. Encyclopedia of multimedia technology and networking*. IDEA Group Reference. Hershey, Pennsylvania, 2005. – pp. 404 – 410.

[9] *Information technology – Security techniques – Information securely risk management*, ISO/IEC27005:2007,Geneva, Switzerland,2007

[10] *Risk Taxonomy,* Open Group Publication, January 2009. http://www.opengroup.org/onlinepubs/9699919899/toc.pdf.

[11] M. Hentea, “Enhancing information security risk management with a fuzzy model”, *Proc. of 19th International Conference on Computer Application in Industry and Engineering. Las Vegas, USA,* 2006. – pp. 132 – 139.