The Eighth International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, Serbia

IMPACT ANALYSIS OF CYBER ATTACKS ON CLOUD SYSTEMS

IGOR OGNJANOVIĆ
MG-Soft Montenegro; University Donja Gorica, Montenegro; igor.ognjanovic@gmail.com

RAMO ŠENDELJ, IVANA OGNJANOVIĆ
University Donja Gorica, Montenegro; {ramo.sendelj, ivana.ognjanovic}@udg.edu.me

Abstract: *We are currently witnessing the maturing of Cloud Computing from a promising business concept to one of the fastest growing segments of the IT industry. Despite of all the hype surrounding the cloud, businesses are still reluctant to be deployed in the cloud, since security, data privacy and data protection continue to plague the market. As more and more information about both individuals as well as companies is placed within the cloud, unease keeps growing about just how safe an environment it is, making them potentially deliberate exploited by cyber attackers. This is a reason why exact analysis of causes and impacts of cyber attacks should be done over cloud systems in different domains of applications. In this paper, we show some models and features which could be used for assessing cyber attacks, their impacts, as well as some concepts of security intelligence that can defend these cyber threats.*

Keywords: *Cyber Attacks, Impact Analyses, Cloud Computing, Cloud Systems*

1. INTRODUCTION

We are currently witnessing the maturing of Cloud Computing from a promising business concept to one of the fastest growing segments of the IT industry. Cloud computing is replacing computing as a personal commodity by computing from public utility, where e.g., health data is collected by iWatch and stored in a health log book in the cloud. According to the most commonly used definition from NIST [8], cloud computing is a model for enabling ubiquitous, 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. The experts at global level expects the growth in cloud computing at a compound annual growth rate of 28.8%, with the market increasing from $46.0 billion in 2009 to $210.3 billion by 2015 [1].

Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of Cloud Computing and complications with data privacy and data protection continue to plague the market. As more and more information about both individuals as well as companies is placed within the cloud, unease keeps growing about just how safe an environment it is.

That is, as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. While worldwide IT spending is slightly down has slightly declined in recent years, spending on information security related products and services by small and large organizations alike large and small has been growing at a rate of increased by 17.6% per annum since 2004 [3]. According to the EMC Corporation and RSA Security, Cybercrime losses were around $5.9 billion in 2013 [2].

Security departments are facing new challenges in protecting valuable business data against an ever-increasing wave of cybercrime attacks. Recently, several models are proposed, such as: [4] proposes four-tier framework for web-based development); a Trusted Third Party is proposed in [5] with defined specific tasks aimed on assuring specific security characteristics within a cloud environment; [6] gives a quantitative model of security measurements that enables cloud service providers and cloud subscribers to quantify the risks; [7] proposes innovative approach for increasing cyber security over cloud services by using Semantic Web technology, hierarchical ontology and intelligent reasoning techniques. However, there is no unique model/approach which addresses cyber attacks and their impacts in cloud environment [5, 7].

In this paper we go one step further and analyze how attack-countermeasure tree (ACT) [14] a combinatorial modelling technique for analyzing cyber attacks and countermeasures can be used for analyzing impacts of cyber attacks in cloud environment. The paper is organised as follows: Section II introduces security models on cloud systems, Section III provides overview of attack countermeasure trees, while Section IV provides key considerations about using ACTs with cloud security models. Section V concludes the paper with key findings and conclusions moving towards development of innovative impact analysis models of cyber attacks in cloud environments.

2. SECURITY MODEL FOR CLOUD SYSTEMS

The basic idea behind cloud computing is replacing computing as a personal commodity by computing as a public utility (from storing data to community via e-mail to collaborating on documents or crunching numbers on large data sets) [9]. According to the most commonly used definition, *clouds*, as the first-class citizens of cloud

computing environments, are sets of hardware, networks, storage, services and interfaces that combine to deliver aspects of computing as a service. *Cloud computing* is a disruptive technology that has the potential to provide distinct benefits to businesses of all sizes to improve digital productivity and simplify electronic business, through gaining discernible benefits, such as increased flexibility, online operating service availability, maintainability, affordability, and scalability [7].

Even though much effort is put on modelling and establishing innovative legal and technical procedures and standards for cyber security in all aspects of IT use and adoption, they cannot be directly applied in cloud computing environment as the. The cloud model is somewhat different: the cloud resource consumer and cloud resource provider are seldom rarely the same entity; the application software and databases are moved into the large data centres, where the management of the data and services are not trustworthy. Each participant has a different business strategy and thereby may stress some specific security aspects over others, and the implications of security breaches are confounded by the dynamics of communications and collaborations that occur throughout the network in the normal course of business. An increased understanding of Cloud Computing and the roles of various stakeholders in this realm is important. Furthermore, each participant operates autonomously and has legal and business control over its internal operations, data and other resources, and it is hardly to be expected that there exist homogeneity and compatibility between all parties. Traditional methods for collaboration between distributed systems include static and centralized approaches, trusted third party approaches and dynamic negotiation, which obviously expressed weaknesses associated with maintaining the security of the central security policy repository.

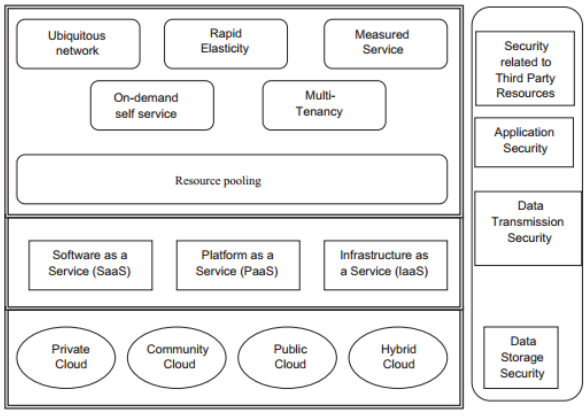

Figure 1. Complexity of security in cloud environment [26]

There are various security recommendations for Cloud Computing providers (e.g. international organizations like ENISA (European Union Agency for Network and Information Security) [10], etc.). It has also been shown, that security, privacy and usability is often contradictory what as been discussed in Al Abdulwahid et.al [11]. Consequently, security in cloud environments is currently one major area of interest with issues for both, scientific and ICT community, since threats and attacks are all modern and sophisticated, whereas cloud solutions are still vulnerable and thus, cloud providers and users are facing serious challenges of their protection [6][7]. The complexity of security risks in a complete cloud environment is illustrated in Figure 1.

Recently, we proposed innovative semantically enabled model (CSM) [7] which showed solid potentials for addressing all cyber security issues in one integral framework with defined metrics (quantitative and qualitative), as shown on Figure 2. The model is developed by following hierarchical ontological structure which integrates all semantic diversity in characteristics, relationships and dependencies between cloud computing models and all involved parties [7]. The CSM model also enables integration of intelligent reasoning techniques and mechanisms [12] based on service transformation of clouds, as commonly used in the literature [13].

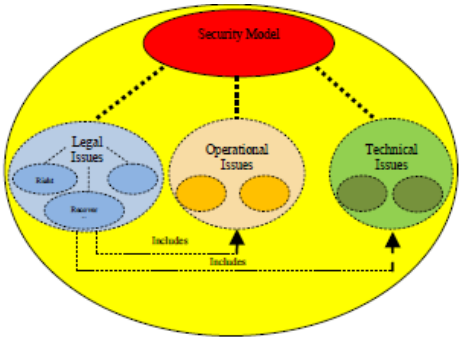

Figure 2. Cyber Security Model (CSM): Hierarchical structure [7]

3. IMPACT ANALYSIS OF CYBER ATTACKS: ATTACK COUNTERMEASURE TREES

The impact analysis is one of key issues in modelling system response to security threats, as focused on the interaction between the cyber and physical aspects of the system [18]. To this end, commonly used mathematical structure is a graph (defined as a collection of vertices and a collection of edges that connect node pairs), which is widely used for representation of pairwise relationships between a set of objects. Depending the use of a graph, its edges may or may not have direction leading to directed or undirected classes of graphs, respectively.

Recently developed attack-countermeasure tree (ACT) [14] is an example of graph based structure for modelling and analyzing cyber attacks and countermeasures. Structure of tree is much simpler for processing and reasoning since it is simplified graph. In ACT, there are three distinct nodes, so-called *classes of events*: attack events (e.g. install keystroke logger), detection events (e.g. detect keystroke loggers) and mitigation events (e.g. remove keystroke logger). ACT can be consists of [14]: (i) a single attack event (Figure 3a), (ii) an attack event and a detection event (Figure 3b), (iii) an attack event and multiple detection events (Figure 3c), (iv) an attack event, a detection event and a mitigation event (Figure 3d) or (v) an attack event, *n* detection events and corresponding *n* mitigation events (Figure 3e).

Having structure of a tree, it is easily to automate the generation of attack scenarios [14] by using its minimal cut sets. Furthermore, each node is assigned with p-probabilistic of attack success at the goal; and starightforward mathematical equations are defined for each gate type and combination of attacks and detection events [14].

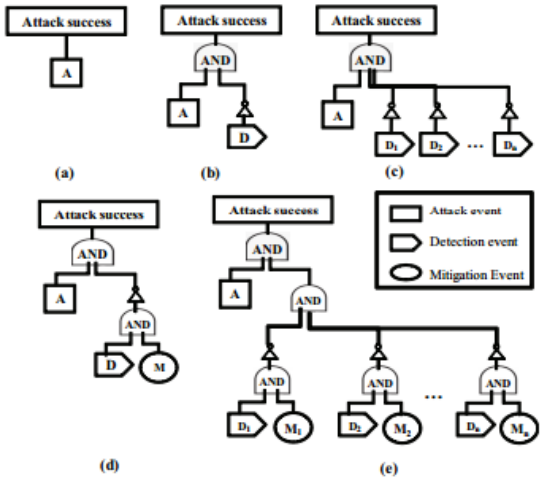

Figure 3. Attack Countermeasure Trees [14]

ACT is thus a structure which enables to perform probabilistic analysis (e.g. probability of attack at the goal node, attack and security investment cost, impact of an attack, system risk, return on attack (ROA) and return on investment (ROI)) in an integrated manner [14, 19].

4. ATTACK COUNTERMEASURE TREES FOR CLOUD BASED SYSTEMS

Having in mind that cloud computing can be defined as computing paradigm based on delivery of applications to users as services over the Internet [7, 15], each having specific requirements and available for participants; we will use service-oriented transformation of cloud based solutions [13, 7]. Furthermore, recent research shows [16, 12, 17] that semantically enhanced presentation of service-oriented architectures provides bases for intelligent reasoning over the model [16], automatic configuration and management [17], etc. That is a reason, why we decided to analyse how to use the advantages of using service orientation and ontological security model over clouds.

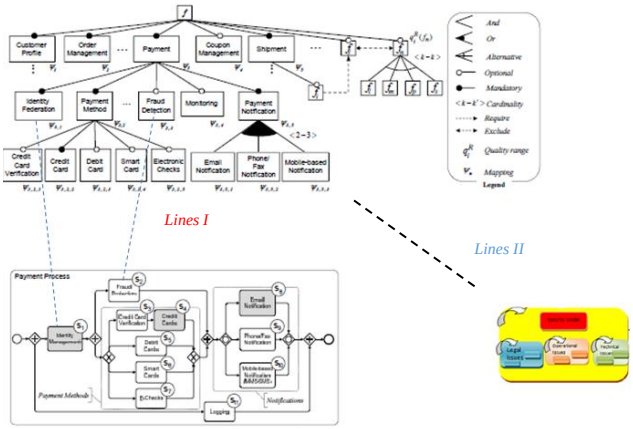

Figure 4. Service-oriented transformation of cloud models and corresponding security model

Both proposed models have structures of tree, ACT (see Figure 3) and service-oriented transformation of cloud based systems (e.g. service-oriented architectures, which is commonly presented by means of two models: business model templates and feature models). Due to limited space for the paper, we provide illustrative example (see Figure 4) which shows high-level representation of e-shop service oriented architecture. Key findings is one-to-one mapping between the two models (Figure 4-lines I), and its mapping to CSM model (Figure 4- lines II).

However, in order to develop comprehensive model for measuring impacts of cyber attacks on cloud systems, we propose integration of ACT with semantically enhanced CSM model, by following step-wised approach:

(i) create ACT for each activity in service transformed cloud model;
(ii) establish links to leafs in CSM model (having in mind all, legal, operational and technical issues);
(iii) propagate values from leafs to the root by respecting relations at all models (and mappings – at Figure 4).

Even proposed solution presents methodological approach which needs more approval and theoretical analyses, they have strong roots in the following similar approach developed for the same models:

- Propagation of non-functional values over service-oriented model with mappings (Figure 4-line I) is formalised with simple mathematical functions: aggregation, multiplication, max, min. Figure 5 presents an excerpt from the fill version (available in [20]) and it is related to one non-functional property-cost;
- Aggregation of probabilities of attack success (as introduced in [14]- see Figure 6).

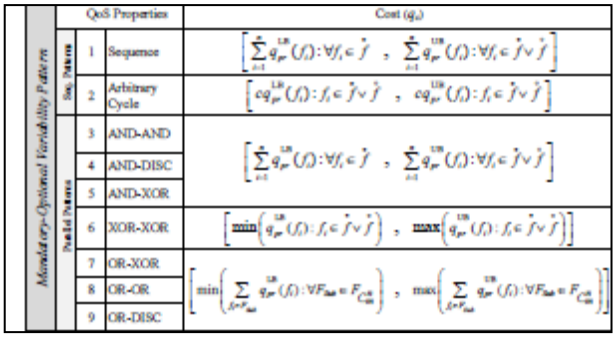

Figure 5. Aggregation rules for non-functional property: Cost [20]

Gate type	Prob. of attack success	attack cost	impact
AND	$\prod_{i=1}^{n} p(i)$	$\sum_{i=1}^{n} C_i$	$\sum_{i=1}^{n} I_i$
OR	$1-\prod_{i=1}^{n}(1-p(i))$	$\forall i \min C_i$	$\forall i \max I_i$
k-out-of-n*	$\sum_{i=k}^{n} \binom{n}{i} p^j (1-p)^{n-j}$	$\sum_{i=1}^{k} C_i$	$\sum_{i=1}^{k} I_i$

Figure 6. Formulae for probability of attack success [14]

Having in mind dynamical nature of cyber space and cyber attacks, dynamical cyber system can be presented as a mathematical formalisation to describe time-

evolution of a state x (which can represent a vector of physical quantities) [18], and the following mappings:

- mapping f between models for presentation of service transformed cloud computing model (Fig. 4- lines I);
- mapping g between service oriented model and CSM model (Fig.4- lines II);
- mapping h between CSM and ACT model.

In continuous time, the imapcts of cyber attacks can be presented as the deterministic evolution of the current states of the system, as follows:

$$\bar{x} = F(x, f, g, h, u) \quad (1)$$

where $\bar{x}$ is the time-derivative of x and u an input vector [14].

4. DISCUSSION

Development of security models is well known issue for both, researchers and developers [7, 14, 13, 19]. In addition to existing technical challenges to overcome, the legal situation is continuously changing.

The EU General Data Protection Regulation ("GDPR") has been adopted at the EU level on14. April 2016 and is one big step towards a privacy-friendly Cloud. Most notable requirements are data breach notification, data security and risk assessment. The personal data breaches notification requires public electronic communications providers such as telcos and ISPs to report such breaches to the relevant national regulator, and this has led to a range of national guidance on when and how such reporting should be made. ENISA has also produced extensive guidelines on this matter [21].

There are many best practices, white papers, etc., which gives advice how to operate Cloud infrastructure in a secure and privacy protecting way [22]. To prove that all security controls are set have to be audited by third party and certified by e.g. STAR . Cloud audits are challenging by its dynamic infrastructure changes. Changing Cloud infrastructures are continuously audited using software agent technology [23], Ruebsamen et.al [24] discusses privacy issues during audits, and Ruebsamen et.al [25] uses the Cloud Trust Protocol to do auditing of Cloud provider chains.

5. CONCLUSION

In this paper we have introduced an approach to cyber attack impact analysis for cloud based solutions. The advantage of the propsoed solution can be modelled within one framework allowing a single, but potentially powerful analysis approach which intergates different aspects, legal, economical and technical. Thus, effect relations for cyber-attacks are better managed for comprehensive impact modelling and analysis, also allowing intelligetn reasoning and predicting. Future work will include completed solution of mathematical formalisms, formal verification of the model and simulation testing and analyses.

Acknowledgment. Research presented in this paper is conducted within the TEMPUS project '*Enhancement of Cyber Educational System in Montenegro (ECESM)*', project no. 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

REFERENCES

[1] Australian Information Industry Association, 'Modeling the Economic Impact of Cloud Computing', 2012

[2] EMC, 'The current state of cybercrime 2014', USA

[3] C. Derrick Huang et al. 'Economics of Information Security Investment in the Case of Simultaneous Attacks', WEIS 2006

[4] W. Tsai, Z. Jin, and X. Bai, "Internetware computing: issues and perspectives", 1st Asia-pacific symposium on Internetware, China, 2009, pp.1-10

[5] Z. Dimitrios, and L. Dimitrios, „Addressing cloud computing security issues", Future Generation Computer Systems, 2012,Vol.28, pp.583-592

[6] L. B. A. Rabai, M. Jouini, A. B. Aissa, and A. Mili, „A cyber security model in cloud computing environments", J. of King Saud University- Computer and Information Sciences, 2013, vol. 25, pp.63-75

[7] R.Šendelj, I.Ognjanović , "Semantically enhanced cyber security over *clouds: Methodological approach"*, International Journal of Advances in Computer Networks and Its Security, 2014, Vol 4, No.3, ISSN: 2250-3757

[8] P. M. Mell and T. Grance, 'SP 800-145. The NIST Definition of Cloud Computing', Jan. 2011

[9] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing", Communications of ACM, 53 (4), 2010, pp.50-58

[10] ENISA paper: Cloud Computing: Benefits, risks and recommendations for information security; https://www.enisa.europa.eu/events/speak/cloud.jpg/view

[11] Al Abdulwahid A, Clarke NL, Furnell SM, Stengel I, Reich C; Security, Privacy and Usability - A Survey of Users' Perceptions and Attitudes; 12th Int. Conf. on Trust, Privacy and Security in Digital Business (TrustBus 2015), Valencia, Spain, pp153-168

[12] M. Bošković, E. Bagheri, G.grossmann, D. Gašević, and M. Stumptner, „Towards Integration of Semantically Enabled Service Families in the Cloud", CSWS 2011, Vol. 774, pp.58-69

[13] T. Takahashi, Y. Kadobayashi, and H. Fujiwara, „Ontological Approach toward Cybersecurity in Cloud Computing", SIN 2010, pp.7-11

[14] A. Roy, D. Seong, K. S. Trivedi, „Cyber Security Analysis using Attack Countermeasure Trees", CSIIRW 2010, Oak Ridge, Tennessee, USA

[15] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing." Communications of the ACM, 2010, 53(4), pp. 50-58

[16] M. Asadi, B. Mohabbati, D. Gasevic, E. Bagheri, and M.Hatala, “Developing Semantically-Enabled Families of Method-Oriented Architectures”, IJISMD, 2012, 3(4), pp. 1-26

[17] I.Ognjanović , B.Mohabbati, D.Gašević, E.Bagheri, M.Bošković, "A Metaheuristic Approach for the Configuration of Business Process Families", IEEE International Conference on service Computing (SCC2012) , Hawaii, USA, 2012

[18] D. Kundur, et. al., “Towards modelling the impact of cyber attacks on a smart grid”, Int. J. Security and Networks, Vol. 6 (1), 2011, pp.2-13

[19] B. B. Madan, K. S. Trivedi, „Security Modeling and Quantification of Intrusion Tolerant Systems Using Attack-response Graph“, J. of High Speed Networks, 13(4):297–308, 2004

[20] B. Mohabbati, D. Gasevic, M. Hatala, M. Asadi, E. Bagheri, and M. Boskovic, “A Quality Aggregation Model for Service-Oriented Software Product Lines Based on Variability and Composition Patterns”, ICSOC 2011, pp. 436-451

[21] Andreas Rockelmann, Joshua Budd, Michael Vorisek, ‘Data Breach Notification in the EU’ (ENISA, 13 January 2011); Marnix Dekker and ChristofferKarsberg ‘Technical guidance on the incident reporting in Article 13a’ (ENISA, November 2013); Marnix Dekker, ChristofferKarsberg ‘Technical guidance on the security measures in Article 13a’ (ENISA, November 2013)

[22] NIST, “Security and Privacy Controls for Federal Information Systems and Organizations.”SP 800-53. National Institute of Standards and Technology (NIST), April 2013

[23] F. Doelitzscher, C. Fischer, D. Moskal, C. Reich, M. Knahl and N. Clarke, "Validating Cloud Infrastructure Changes by Cloud Audits," *2012 IEEE Eighth World Congress on Services*, Honolulu, HI, 2012, pp. 377-384. doi: 10.1109/SERVICES.2012.12

[24] T. Rübsamen, C. Reich; Cloud Audits and Privacy Risks; On the Move to Meaningful Internet Systems: OTM 2013 Conferences, Lecture Notes in Computer Science Volume 8185, p: 403-413; 2013

[25] T. Rübsamen, D. Hölscher, Ch. Reich; Towards Auditing of Cloud Provider Chains Using Cloud Trust Protocol; CLOSER 2016: Rom, Italy, 2016