A SECURITY METRICS FRAMEWORK FOR THE CLOUD

Jesus Luna, Hamza Ghani, Daniel Germanus and Neeraj Suri
Department of Computer Science, Technische Universität Darmstadt, Hochschulstr. 10, 64289 Darmstadt, Germany
{*jluna, ghani, germanus, suri*}*@deeds.informatik.tu-darmstadt.de*

Keywords: Cloud dependability, Cloud security, security compliance, security measurements, security metrics.

Abstract: Cloud computing is redefining the on-demand usage of remotely-located, and highly available computing resources to the user. Unfortunately, while the many economic and technological advantages are apparent, the migration of key sector applications to the Cloud has been limited due to a major show-stopper: the paucity of *quantifiable* metrics to evaluate the tradeoffs (features, problems and the economics) of *security*. Despite the obvious value of metrics in different scenarios to evaluate such tradeoffs, a formal and standard-based approach for the addressing of security metrics in the Cloud is a much harder and very much an open issue. This paper presents our views on the importance and challenges for developing a security metrics framework for the Cloud, also taking into account our ongoing research with organizations like the Cloud Security Alliance and European projects like ABC4Trust, CoMiFin and INSPIRE. This paper also introduces the basic building blocks of a proposed security metrics framework for elements such as a Cloud provider's security assessment, taking into account the different service and deployment models of the Cloud.

1 INTRODUCTION

The Cloud just as defined in (Mell and Grance, 2009), has increasingly become a computing/communication paradigm that seems to have the potential to change the way we consider systems and services. Thanks to the rapid provisioning of computational resources taking place in the Cloud with minimal management effort or service provider interaction, now we are forced to rethink about the core Information Technology (IT) elements of data.

For Small and Medium Enterprises — SMEs — and sectors like eHealth and eGoverment the advantages of using the Cloud are clear, unfortunately as also highlighted by ENISA — the European Network and Information Security Agency (ENISA, 2011) — in their report (Catteddu and Hogben, 2009) *the Cloud also conveys serious security and privacy issues* that nowadays represent major "show-stoppers" for its adoption.

The importance of creating secure and trusted Cloud services has resulted in a central question: *how to objectively and quantitatively measure the security of a Cloud service provider?*

In other IT ecosystems, (e.g. critical infrastructures) well designed security metrics have proven useful not only in helping formally understand the security guarantees provided by a system, but also raising awareness about its vulnerabilities and even assessing the effectiveness of the different security mechanisms being implemented. Unfortunately due to the Cloud's special characteristics, at the state of the art, there are just a few efforts aimed at using a *framework* or common set of objectives and, quantitative security metrics for the Cloud.

The main contributions of this paper are *(i)* a scenario-driven approach to obtain a set of common requirements for designing Cloud security metrics (Section 2), *(ii)* an analysis of the state of the art related with the use of security metrics in the Cloud (Section 3) and, *(iii)* a presentation of our initial research results aimed to create a security metrics framework as an essential milestone required to build trust in Cloud environments (Section 4). Finally in Section 5 this paper presents our conclusions and future work.

2 WHY CLOUD SECURITY METRICS?

In this section we motivate the creation of a framework for Cloud security metrics, by presenting some scenarios where such basic building blocks are required in order to deploy the full potential of Cloud computing whilst *guaranteeing its security*.

2.1 Cloud Security Metrics Scenarios

The four scenarios presented next have been inspired from our ongoing collaboration with the Cloud Security Alliance — CSA (CSA, 2011).

1. *Security Compliance and Dependability*: The term compliance is closely related to the notion of measurements and metrics. For Cloud providers security compliance can become difficult to demonstrate. From our perspective, a well designed security metric should allow Cloud providers to quantify and objectively demonstrate their security compliance with some specific set of requirements (Travis and Annie, 2008) for example a Digital Forensic's readiness policy (Tan, 2001).
2. *Cloud Federations*: The current proliferation and diversity of Cloud providers has resulted in the idea of creating "Cloud Federations" (Rochwerger et al., 2010)), where users might be able to compose complex workflows by combining the capabilities of different providers while avoiding dependency on one particular vendor (lock-in risk as defined by ENISA (Catteddu and Hogben, 2009)). Just as in computational Grid environments, the creation of Cloud federations depends on the correct use of objective security metrics ((IGTF, 2011) and (Casola et al., 2010)).
3. *Dark Clouds*: The *infinite* availability of computational resources provided by the Cloud has caught the attention of a wide range of cybercriminals willing to use it for their purposes (Antonopoulos, 2011) and (Samson, 2011)) Our belief is that quantitative, run-time security metrics can be used by Cloud providers in order to build architectures able to monitor and detect potential abuses or, cyberattacks targeting or even originating inside their systems.

2.2 Summary of Requirements

From the analysis of different scenarios presented in Subsection 2.1, the research introduced in this paper proposes to classify their requirements in three different classes:

1. Taxonomies: There is a need for a taxonomy or hierarchical classification, of the different elements that model the security behavior of the Cloud service. Taxonomies are the first step in designing flexible and interoperable security metrics (Seddigh et al., 2004).
2. Metrics: This is the set of security metrics developed from the proposed taxonomy. The presented scenarios require comprehensive (from the Cloud service-level to underlying algorithms), quantitative and objective metrics.
3. Reference architectures: The basic building blocks required to implement and deploy the proposed set of security metrics. Monitoring the fulfillment of an expected security level can be integrated as a functionality of the proposed architectures.

This common set of requirements is being used to propose the Cloud security metrics framework introduced in Section 4.

3 STATE OF THE ART

Next, we survey and analyze the state of the art related with Cloud security metrics, mapped to the three groups of requirements proposed in Section 2.

3.1 Taxonomies

One of the first taxonomies tackling Cloud security can be found on ENISA's report (Trimintzios, 2011), where a risk-driven approach is proposed by the authors. This taxonomy focuses on risks-based considerations and associates qualitative scores to them, moreover it also introduces a set of vulnerabilities and affected assets that can be used to develop specific metrics for the Cloud. The work of (Grobauer and Walloschek, 2010) is complementary to ENISA's report, where the authors further elaborate about the need for measuring a Cloud provider's security level trough a vulnerability-based approach. Their major contribution is an overview of Cloud-specific vulnerabilities, that can be further organized into a taxonomy for Infrastructure as a Service models (IaaS).

Based on his previous research on security metrics taxonomies, Savola (Savola et al., 2010) uses a threat-based approach to propose a high level taxonomy and associated metrics for measuring the Cloud's security, privacy and trustworthiness. The proposed taxonomy contributes to the state of the art with the inclusion of a new taxonomy class focused on the Cloud's privacy features. The Cloud Security Alliance's (CSA) Common Assurance Maturity Model (CAMM) and Cloud Controls Matrix Work Group, are the leading initiatives of industrial Cloud security metrics research. CAMM (CAMM, 2010) is an ongoing industrial project that aims to create a framework to attest the information assurance maturity of a Cloud provider. In order to fulfill its goal CAMM proposes a set of controls based on ENISA's taxonomy (Catteddu et al., 2009), the Cloud Control Matrix

from the CSA (CCM, 2011), and existing standards such as ISO 27001 (ISO27001, 2005). CAMM is an ongoing initiative that has not proposed any new high-level taxonomy or metrics so far. The CSA also promotes the Cloud Controls Matrix (CSA CCM (CCM, 2011)), which is based on (Brunette et al., 2009) and proposes a set of questions providing fundamental security requirements to guide Cloud vendors, and Cloud customers in assessing the overall security risk of a Cloud provider. The CSA CCM seeks to create both, a Cloud security metrics taxonomy and a set of associated security measures. The CCM taxonomy is derived from (Brunette et al., 2009), and despite its usefulness it turns out to be challenging with regard to the derivation of quantitative and objective metrics from it.

Despite not being focused on the Cloud, there are two security taxonomies worth to mention due to their broad community use: the National Institute of Security and Standards' (NIST) taxonomy (Chew et al., 2008), and the one contributed by the Center for Internet Security (CIS) in (Center for Internet Security, 2010)). Both are quite similar about defined categories and proposed set of metric definitions. Due to their flexibility, our belief is that the metrics proposed in both documents can be also applied to the Cloud via taxonomies like e.g. the one from ENISA (Trimintzios, 2011).

3.2 Metrics

One of the few works focused on quantitatively evaluating the security of a "pure" IaaS Cloud has been presented in (Arshad et al., 2010), where the authors introduce the idea of integrating security metrics into an IaaS scheduler. Unfortunately, no further details are given about the architecture or policies used by the proposed security evaluation system. The Common Assurance Maturity Model (CAMM) (CAMM, 2010) explores metrics and measurements by proposing to quantify the level of assessment required to achieve greater confidence. CAMM considers two basic principles: *(i)* objective metrics can be used to obtain scores, and *(ii)* scores from different components that can be composed to model the security level of a Cloud provider (Hogben, 2011). At the time of writing this paper, CAMM has not released further information about the proposed metrics. The CSA Metrics Work Group complements the CSA CCM (CCM, 2011), by developing the security metrics needed to evaluate CCM's requirements. The CSA Metrics WG has created a template that characterizes each metric with attributes, and also has proposed their first 10 metrics covering approximately 25 of CCM's control areas. From our perspective this is a useful work in progress, but that still needs to be complemented with the formal models in order to achieve required features like the composability of two or more metrics. Our research group is collaborating with CSA Metrics Work Group in order to achieve these goals.

In (Catteddu et al., 2011) ENISA analyzes the risks associated with the use of Cloud computing for eGoverment. This report proposes a set of security and resilience parameters that can be evaluated in order to compare different Cloud service providers. The proposed parameters are divided into high-level categories (preparedness, service delivery, response and recovery and, legal and regulatory compliance), but unfortunately some of these are qualitative (e.g. tolerance to malicious attacks). It is also worth to mention the security metrics contributions made by (Wang, 2005), NIST (Chew et al., 2008) and CIS (Center for Internet Security, 2010) in particular with the definition of a flexible metric "template" that allows for creating more specific metrics that are objective and quantitative. A missing point with these metrics (apart from not having a focus on Clouds), is the lack of a set of rules or "algebra" that allows to model complex Cloud services (e.g. Federations).

3.3 Reference Architectures

Reference architectures and technologies enabling the use of security metrics in the Cloud are still on a very early stage, however the most representative effort is the CloudAudit API (CloudAudit, 2011), that aims to give more "transparency" to Cloud providers by creating a common interface and namespace that allows them to automate the audit, assertion, assessment, and assurance of their environments. The CloudAudit API can be used to automatically retrieve and transport attributes from the provider, therefore enabling customers to perform on-the-fly security measurements. CloudAudit will be an essential piece of the framework proposed by our research, because it has been designed in such a way that it can be used with new taxonomies and metrics.

For the ongoing research presented in this paper, it is also worth to mention three EU-funded projects that are developing reference architectures that use security metrics in order to improve the security, privacy and resilience of IT infrastructures. The first project is INSPIRE ((D'Antonio et al., 2008), (INSPIRE, 2011)) an EC funded research project whose name stands for "INcreasing Security and Protection through Infrastructure REsilience", with a focus on Supervisory Control and Data Acquisition (SCADA) systems. Within the INSPIRE project, an overlay ap-

proach was taken to propose an architecture to monitor and react to perturbations in the communication layer of the SCADA network. Secondly, the CoMiFin — Communication Middleware for Monitoring Financial Critical Infrastructure (CoMiFin, 2011) — project takes an approach similar to INSPIRE and provides an overlay architecture for financial institutions for sharing security relevant information such as alerts about cyberattacks and other threats. The CoMiFin middleware is capable of collaborative cyberattack detection stemming from patterns that a single financial institution is unable to monitor. A *metrics monitoring framework* has been developed within this project (Ghani et al., 2010) in order to calculate the security metrics and monitor compliance with security requirements. Finally, it is worth to mention the recently started project ABC4Trust (ABC4Trust, 2011), which aims (among other goals) to establish a comparison framework and associated architecture for the so-called *anonymous credentials* (Chaum, 1985). We hope that the security metrics architecture to be developed in ABC4Trust, can also be applied to Cloud services because of the approach being taken (service-level metrics, technology-neutral).

3.4 Summary of Research Challenges

The state of the art presented in this section contains a common set of research challenges, to be taken into account for developing the proposed security metrics framework:

1. Taxonomies: It is necessary to "adapt" well-known taxonomies like the one from CIS (Center for Internet Security, 2010) to model the Cloud's unique features. The taxonomy should be flexible enough (represent the Cloud's security, privacy or risk) and able to cope with the Cloud's service oriented nature.

2. Metrics: There is the need for researching formal models and algebras for using quantitative metrics. Also both, the creation of pragmatical measurement methodologies and the use of prediction capabilities based on historical data, should be further explored.

3. Reference architectures: Research should focus on proposing non-intrusive, scalable, interoperable and comprehensive security metric architectures (from services to algorithms). These should support the automatic monitoring of static and dynamic measurements, while considering the Cloud provider's "opacity".

4 INTRODUCING A SECURITY METRICS FRAMEWORK FOR THE CLOUD

Taking into account the security requirements and challenges from Sections 2 and 3, this section introduces our ongoing research towards creating a security metrics framework for the Cloud. The proposed framework is composed of the three building blocks introduced in Section 2, and shown in Figure 1, and takes as a starting point the Cloud's service oriented perspective also known as the SPI model[1], in order to have a multi-layer, comprehensive metric that considers interfaces, network infrastructures, and algorithms at the further end. Depending on the scenario requirements it might be possible to adopt a taxonomy focused on either security, privacy or risks associated with the Cloud service. A security-oriented taxonomy might be useful for compliance scenarios (where a baseline security level exists), whereas a risk-oriented one could be more suitable for the dark-cloud scenario presented in Section 2.

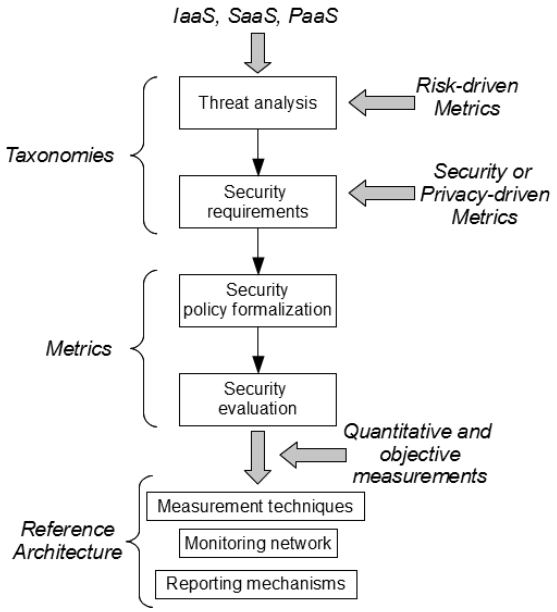

Figure 1: Basic building blocks of the proposed security metrics framework for the Cloud.

The metrics used by the proposed framework should be *objective and quantitative* to promote automatization and composition to model more complex services. Chosen metrics should be able to give an answer to security provisions like "What is the

[1]SPI stands for Software as a Service — SaaS —, Platform as a Service — PaaS — and Infrastructure as a Service — IaaS —

security level of the authentication mechanism used by the IaaS' management interface?". For security-oriented taxonomies our current research is taking an approach like the one used by the Reference Evaluation Methodology (REM, (Casola et al., 2007) and (Casola et al., 2005)), so it might be possible to formally compose the security levels of different Cloud services. In previous works we have used this approach for quantitatively measuring the security of complex Grid infrastructures i.e. in (Luna et al., 2008) and (Luna et al., 2010), nevertheless we are also considering other formal methodologies like the one proposed in (Schryen et al., 2011). The final building block of the proposed taxonomy is the reference architecture comprehending measurement techniques, monitoring network and reporting mechanisms. At this early stage of our research, the reference architecture is being planned as an non-intrusive overlay network just as the one we proposed in (Ghani et al., 2010). Despite its final shape, the reference architecture should be able to integrate a set of monitors able to alert if the Security Level Agreement is violated. In the architecture, the process of reporting to external entities (like Third Party Auditors) may be realized via mechanisms like CloudAudit (Section 3), which are flexible enough to represent risks, security or privacy measurements depending on the taxonomy that was chosen.

5 CONCLUSIONS AND FUTURE WORK

In this position paper we have presented several scenarios to introduce our views on the importance of creating a security metrics framework for the Cloud. To contribute towards the development of such a framework, we analyzed the features and challenges of relevant related work in this area. This paper also introduced the initial research results of our proposed security metrics framework for the Cloud, which aims to improve tasks like compliance evaluation or dependability assessment. Our goal is to create an open, flexible and technology-agnostic framework able to be extended through the integration of new security metrics that might be developed for specific scenarios.

We have identified a set of research challenges related with the formal aspects of Cloud security metrics that will be part of our future work, in particular the composition of different security parameters which allows for the computation of an overall security level (like e.g. in (Casola et al., 2007)). Furthermore, the reference architecture proposed in this position paper will explore some of our experiences with projects like INSPIRE, CoMiFin and ABC4Trust (reviewed in Section 3) in order to develop an architecture able to enforce security level agreements in the Cloud.

In order to obtain community feedback about the proposed framework, we have begun to collaborate with groups like the CSA's Security Metrics WG. The resulting framework should be able to model existing use cases, like the governmental Clouds analyzed in (Catteddu et al., 2011).

Finally, as a proof of concept study we are planning to develop an architecture that integrates the proposed framework into a Cloud Federation's data storage broker, in order to perform data allocation based on the evaluation of a predefined Security Level Agreement. We hope that this work will aid to show the tradeoffs between security and performance, therefore supporting the decision making process by providing a metrology basis for the quantitative assessment of different security attributes.

ACKNOWLEDGEMENTS

Research supported in part by EC FP7 IP ABC4TRUST and Loewe TUD CASED.

REFERENCES

ABC4Trust (2011). ABC4Trust FP7. *Online: http://www.abc4trust.eu/*.

Antonopoulos, A. (2011). Dark cloud computing. *Online: http://www.networkworld.com/columnists/2009/051209-antonopoulos.html*.

Arshad, J., Townend, P., and Xu, J. (2010). Quantification of Security for Compute Intensive Workloads in Clouds. In *Parallel and Distributed Systems (ICPADS), 2009 15th International Conference on*, pages 479–486. IEEE.

Brunette, G., Mogull, R., et al. (2009). Security Guidance for Critical Areas of Focus in Cloud Computing V2. 1. *CSA (Cloud Security Alliance), USA. Online: http://www. cloudsecurityalliance. org/guidance/csaguide. v2*, 1.

CAMM (2010). Common Assurance Maturity Model. *Online: http://common-assurance.com/*.

Casola, V., Luna, J., Manso, O., Mazzocca, N., Medina, M., and Rak, M. (2007). Interoperable grid pkis among untrusted domains: An architectural proposal. In Cérin, C. and Li, K., editors, *GPC*, volume 4459 of *Lecture Notes in Computer Science*, pages 39–51. Springer.

Casola, V., Preziosi, R., Rak, M., and Troiano, L. (2005). A Reference Model for Security Level Evaluation: Policy and Fuzzy Techniques. *J. UCS*, 11(1):150–174.

Casola, V., Rak, M., and Villano, U. (2010). Identity Federation in Cloud Computing. In *Sixth International Conference on Information Assurance and Security (IAS)*, pages 253–259. IEEE.

Catteddu, D. et al. (2011). Security & Resilience in Governmental Clouds. *European Network and Information Security Agency (ENISA)*.

Catteddu, D. and Hogben, G. (2009). Cloud Computing Risk Assessment. *European Network and Information Security Agency (ENISA)*.

Catteddu, D., Hogben, G., et al. (2009). Cloud Computing Information Assurance Framework. *European Network and Information Security Agency (ENISA)*.

CCM (2011). Cloud Control Matrix. *Online: http://www.cloudsecurityalliance.org/cm.html*.

Center for Internet Security (2010). The CIS security metrics. Technical Report 28, Center for Internet Security.

Chaum, D. (1985). Security without identification, card computers to make big brother obsolete. *Original Version appeared in: Communications of the ACM*, 28(10):1030–1044.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., and Robinson, W. (2008). Performance measurement guide for information security. Technical Report July, National Institute of Standards and Technology.

CloudAudit (2011). CloudAudit. *Online: http://cloudaudit.googlecode.com/svn/trunk/docs/draft-hoff-cloudaudit.txt*.

CoMiFin (2011). Communication Middleware for Monitoring Financial Critical Infrastructure. *Online: http://www.comifin.eu/*.

CSA (2011). Cloud Security Alliance. *Online: http://www.cloudsecurityalliance.org*.

D'Antonio, S., Romano, L., Khelil, A., and Suri, N. (2008). INcreasing Security and Protection through Infrastructure REsilience: the INSPIRE Project. In *Proceedings of The 3rd International Workshop on Critical Information Infrastructures Security (CRITIS'08)*.

ENISA (2011). European Network and Information Security Agency. *Online: http://www.enisa.europa.eu*.

Ghani, H., Khelil, A., Suri, N., Csertn, G., Gnczy, L., Urbanics, G., and Clarke, J. (2010). Assessing the Security of Internet Connected Critical Infrastructures (The CoMiFin Project Approach). In *Proceedings of the Workshop on Security of the Internet of Things (SecIoT 2010)*.

Grobauer, B. and Walloschek, T. (2010). Understanding cloud-computing vulnerabilities. *IEEE Security and Privacy*, pages 1–14.

Hogben, G. (2011). ENISA Cloud Computing Strategy. *Online: http://www.terena.org/activities/tf-csirt/meeting30*.

IGTF (2011). The International Grid Trust Federation. *Online: http://www.igtf.net/*.

INSPIRE (2011). INcreasing Security and Protection through Infrastructure REsilience. *Online: http://www.inspire-strep.eu/*.

ISO27001 (2005). Information Security Management System (ISMS) standard. *Online: http://www.27000.org/iso-27001.htm*.

Luna, J., Dikaiakos, M. D., Marazakis, M., and Kyprianou, T. (2010). Data-centric privacy protocol for intensive care grids. *IEEE Transactions on Information Technology in Biomedicine*, 14(6):1327–1337.

Luna, J., Flouris, M., Marazakis, M., and Bilas, A. (2008). Providing security to the Desktop Data Grid. pages 1–8.

Mell, P. and Grance, T. (2009). The NIST Definition of Cloud Computing. *National Institute of Standards and Technology (NIST)*.

Rochwerger, B., Breitgand, D., Levy, E., Galis, A., Nagin, K., Llorente, I., Montero, R., Wolfsthal, Y., Elmroth, E., and Caceres, J. (2010). The Reservoir Model and Architecture for Open Federated Cloud Computing. *IBM Journal of Research and Development*, 53(4):4.

Samson, T. (2011). Amazon EC2 Enables Brute-force Attacks on the Cheap. *Online: http://infoworld.com/t/data-security/amazon-ec2-enables-brute-force-attacks-the-cheap-447*.

Savola, R., Juhola, A., and Uusitalo, I. (2010). Towards Wider Cloud Service Applicability by Security, Privacy and Trust Measurements. In *4th International Conference on Application of Information and Communication Technologies (AICT)*, pages 1–6. IEEE.

Schryen, G., Volkamer, M., Ries, S., and Habib, S. (2011). A formal approach towards measuring trust in distributed systems. In *ACM Symp. on Applied Computing*, pages 1739–1745.

Seddigh, N., Pieda, P., Matrawy, A., Nandy, B., Lambadaris, J., and Hatfield, A. (2004). Current trends and advances in information assurance metrics. In *Proceeding of the Second Annual Conference on Privacy, Security and Trust*, pages 197–205.

Tan, J. (2001). Forensic Readiness. Technical report, @Stake Organization.

Travis, D. and Annie, I. (2008). Analyzing Regulatory Rules for Privacy and Security Requirements. *IEEE Trans. Software Eng.*, 34(1):5–20.

Trimintzios, P. (2011). Survey on Resilience Metrics. *European Network and Information Security Agency (ENISA)*.

Wang, J. (2005). Information Security Models and Metrics. In Guimarães, M., editor, *ACM Southeast Regional Conference*, volume 2, pages 178–184. ACM.