Risk Management for Outsourcing to the Cloud

Security Risks and Safeguards as Selection Criteria for Extern Cloud Services

Johannes Viehmann
System Quality Center SQC
Fraunhofer Institute for Open Communication Systems FOKUS
Berlin, Germany
johannes.viehmann@fokus.fraunhofer.de

***Abstract*—This short paper describes our ongoing research about security risk management for IT projects which might eventually take benefit from outsourcing to external Cloud services. Choosing appropriate, secure enough Cloud services from multiple offers might be difficult. Hence, we develop the Cloud Security Guide CSG to assist. It contains a specialized methodology for Cloud risk assessment supporting particularly the extraction of security relevant information from user contracts or terms and conditions of public Cloud services. Discovering that many providers fail to communicate their safeguards, we also decided to develop a provider's guide for risk management and for the communication of risk treatments.**

Risk Management; Risk Assessment; Outsourcing; Cloud; Security

I. INTRODUCTION

IT security is crucial in various market sectors, including, eHealth, eCommerce and eGovernance. Perfect security is often unachievable. Before trusting, before taking residual risks, it is reasonable to carefully analyze the chances and the risks, i.e. the potential benefits and the potential losses.

Often those who offer security critical technical systems, applications or services do some kind of systematical risk assessment because it might help them to treat potential weaknesses in their products. Additionally, they can use the results to communicate the identified residual risks honestly, which might be very important to create trust.

For users of complex IT systems like Cloud services, it also makes perfectly sense to analyze the security risks that using these systems implies. If the used services are provided by external companies, then this might introduce some additional outsourcing specific risks.

This paper introduces two Cloud Security Guides: The *Cloud Security Guide CSG for users* is intended to support prospective users of external Cloud services in their security risk assessment so that they can choose the best services for their needs from multiple offers made by different providers without taking too high risks. We test and optimize the applicability of the CSG for users by analyzing existing offers for public Cloud services.

Additionally, we develop a *Cloud Security Guide CSG for developers and providers*, which is intended to help them to minimize risks and to communicate their safeguards with achieved security protection levels to potential customers.

Both Cloud Security Guides are currently implemented into the RACOMAT tool [14], a tool for risk analysis.

II. PROBLEMS

Security critical technical systems should be carefully analyzed. However, security risk assessment might be difficult and expensive.

With Outsourcing, (potential) users of external services and infrastructures who want to analyze the related security risks are facing additional challenges. Typically, the users do not have full access to the IT systems and to the internal processes of external providers. Thus, even if users were security experts, their possibilities to analyze the risks of external services would probably be quite limited. Being dependent on an external provider also introduces itself a number of serious non-technical risks that have to be taken into consideration.

III. SATE OF THE ART

ISO 31000 [1] is the standard for risk management, which contains risk assessment and risk treatment.

Risk assessment means to identify, analyze and evaluate risks which threaten assets [1] [2]. There are lots of different methods and technologies established for risk assessment, including fault tree analysis (FTA) [4], event tree analysis ETA [5], Failure Mode Effect (and Criticality) Analysis FMEA/FMECA [3] and the CORAS method [6]. Since Risk assessment might be difficult and expensive, using catalogues of common risk artifacts (e.g. [7] [8] [9]) makes sense. There are numerous publications (e.g. [12] [13]) about the security issues related especially to Cloud computing. NIST provides guidelines for secure public Cloud computing [11]. The German BSI (i.e. Federal Office for Information Security) is currently working on a module for Cloud usage [10]. Both [9] and [10] are used in the methodology introduced here.

Risk management also includes risk treatment, i.e. the reduction of risks with safeguards. For prospective users of external Cloud services, choosing compliant and secure enough services is the most important safeguard. While [9] and [10] contain some safeguards, they offer little support for deciding between multiple offers from different provider.

IV. CATALOGUES OF RISKS AND SECURITY MEASURES SPECIFIC TO USAGE OF EXTERNAL CLOUD SERVICES

Using Cloud services developed and provided by external companies creates a dependency upon these external players. If some service is no longer provided or technically changed, this might become a serious issue for users relying on the

availability of the unaltered service. Policy endorsements are also a potential threat if there is no way to quickly migrate to alternative providers ([9], module outsourcing). High dependency upon specific providers is called lock-in.

Security measures against the dependency on single providers and the lock-in include proper contract design and the development of migration or exit strategies.

The Cloud technology itself could also be vulnerable to attacks. A Cloud platform uses techniques for distributed virtualization. The platform is an additional layer besides the operating system layer and the application layer that could be attacked. Cloud platforms typically expose some interfaces and functionality. If attackers manage to maliciously utilize the exposed functionality of the Cloud platform or if they find weaknesses in the Cloud platform program, then they might eventually take advantage of it and do manipulations or read out secret information, for example.

Despite the mentioned risks that are introduced by the Cloud technology itself and by the outsourcing, all the risks that are typically relevant for IT systems and computer networks have to be taken into account, too.

We have started to create an extensive catalogue of all the threats that might typically be relevant for users of external Cloud services by merging existing threat and attack databases, removing irrelevant entries, and creating fitting descriptions especially for Cloud users. While [10] only contains Cloud specific threats and thus requires taking other modules of [9] into account, our catalogue is going to be independently applicable.

Similarly, we have also started to create a catalogue of common safeguards and security measures which are applicable to reduce the risk of identified threats. We create relations between the threat scenarios and the security measures. In contrast to the safeguards defined in [9] and [10], we define multiple complete packages of safeguards offering different protection levels.

V. The Cloud Security Guide CSG

A. Cloud Security Guide CSG for Users

The CSG for users contains a service independent risk assessment methodology and a service selection method (see Figure 1). Risk Assessment starts with an asset analysis. To support this first step, the CSG contains several predefined stakeholders and assets which are typically relevant for using external Cloud services. Next, threats are identified with the help of our Cloud threat catalogue. For each threat it is evaluated how it could affect the assets. Then the required safeguards with the minimal protection levels are identified with the help of our Cloud safeguard catalogue.

So far, the entire analysis process has been independent from specific Cloud services. The next step is to look for functionally suitable offers for Cloud services. Then for each of the candidates the security risks have to be analyzed. For users, the one and only reliable source for such an analysis are the legally binding regulations, policies and contract clauses that would be applicable.

Of course, the legal texts typically do not provide information about the threats and risks. Hence, the best method for users to analyze the risks is to look for the security measures that the provider promises and guarantees to offer. In the best case, the provider does have certificates from independent institutions stating that the promised safeguards are implemented correctly. However, even if there are no certificates, a legally binding promise to provide certain security measures is still somehow trustworthy.

Enabling prospective users who are neither security experts nor lawyers to extract the guaranteed safeguards from certificates, contracts, general terms and conditions is actually the major task of our research. Therefore, we started collecting terms and conditions for various Cloud services of different providers. For each safeguard and protection level, we try to identify the related clauses if any are present. We build a

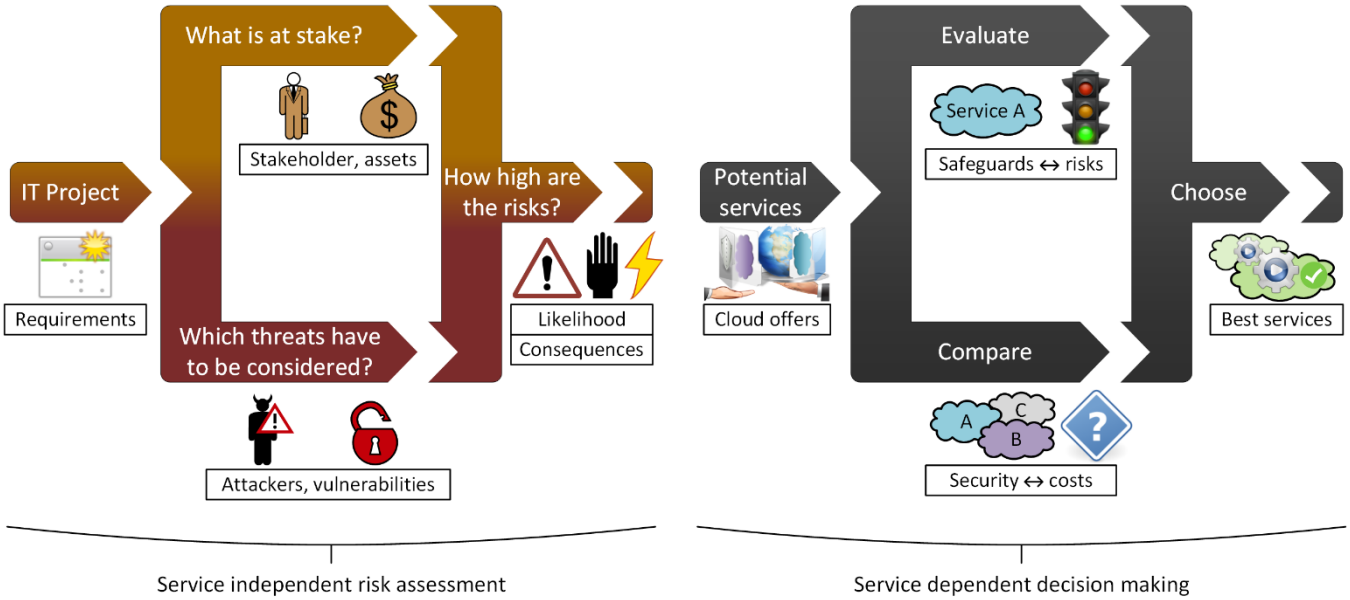

Figure 1. Cloud Security Guide CSG for users methodology

database with the different wordings and phrases. Finally, we add examples of common verbalizations to the documentation of the different safeguards and protection levels in our Cloud catalogues. Hence, the users will be able to look for these hints in order to assess the security measures.

B. CSG for Service Developers and Providers

Containing examples that support users to extract data about safeguards and protection levels from the user contracts, license terms or general terms and conditions, the CSG for users should be applicable for any external Cloud service. However, we figured out that many providers of Cloud services do not communicate their safeguards accurately.

Hence, to help developers and providers to design their offers and to communicate their security measures, but also to help them to understand their own Cloud related risks and to improve their safeguards, we have started to create a second Cloud Security Guide CSG for developers and providers.

The initial risk assessment of the CSG for providers is similar to the risk assessment for the users. However, it is a risk analysis specific to the Cloud service that should be offered. The results of the risk analysis are then used to identify the required safeguards. Those required security measures are compared with the already implemented safeguards to identify where some improvement by implementing additional safeguards might be required.

Finally, the CSG for developers and providers provides help for expressing the safeguards in legal binding ways. Our catalogue of Cloud safeguards mentioned earlier contains exemplary verbalizations for safeguards and protection levels in the terms and conditions of Cloud services. These examples might be used as templates by providers designing their terms and conditions for their own Cloud service offers. With their CSG, providers could even add element IDs referring to the implemented safeguards of the same standard catalogues that the CSG for users of Cloud services contains. Using the CSG is also going to be a good starting point for certification according to [9] since our catalogues are based upon [9].

C. Implementing the CSG into the RACOMAT Tool

Both CSGs could be applied without any specialized tool support. For instance, simple tables could be used to identify the required safeguards. But for a better usability, we have decided to implement the CSG into RACOMAT [14], a risk analysis tool currently being developed that is already taking advantage of risk artifact databases. The tool for example automatically suggests typical threats for common assets. Users just decide about the severity of mentioned potential consequences. For the entire system with all threats, the tool lists up appropriate safeguards with the required protection levels and it suggests hints how the presence of the safeguard could be expressed within the terms of a Cloud service.

We will evaluate the CSGs and the RACOMAT tool within the research projects Trusted Cloud (http://trusted-Cloud.de/) and RASEN (http://rasenproject.eu/) by analyzing the Cloud services of industrial partners with the CSG for users. If it is not applicable, we will try to improve the terms and conditions with the help of the CSG for developers and providers. Afterwards, we will retry using the CSG for users.

VI. Conclusion and Future Work

Security is difficult. Enabling users of external Cloud services who are most likely not security experts to do a sound security risk management is a serious challenge. The CSG for users is intended to give support with simple risk assessment and decision making processes using predefined risk analysis artifacts and safeguards with protection levels. Nevertheless, as long as many terms and conditions for Cloud services fail to communicate the safeguards, CSG based risk assessment is still infeasible for (potential) users. The CSG for developers and providers might help to increase awareness for this problem and it could be utilized to improve the situation.

In general there seems to be urgent demand for security management techniques that are applicable for end users who are no security experts and who typically do not even want to read the entire terms and conditions. Communicating element IDs from standardized catalogues of safeguards in a legal binding way would eventually allow prospective clients to do some automated security requirements checking and legal compliance management with appropriate tools. Further research could try to extend the security guides for other not Cloud related systems like social networks or web services.

Acknowledgment

This paper was developed as part of the Trusted Cloud Joint Research, funded by the German Federal Ministry for Economic Affairs and Energy.

References

[1] International Organization for Standardization: ISO 31000 Risk management – Principles and guidelines (2009)

[2] International Organization for Standardization: ISO Guide 73 Risk management – Vocabulary (2009)

[3] Bouti, A., Kadi, D.A.: A state-of-the-art review of FMEA/FMECA. International Journal of Reliability, Quality and Safety Engineering 1, pp. 515–543 (1994)

[4] International Electrotechnical Commission: IEC 61025 Fault Tree Analysis (FTA) (1990)

[5] International Electrotechnical Commission: IEC 60300-3-9 Dependability management – Part 3: Application guide – Sec. 9: Risk analysis of technological systems – Event Tree Analysis (ETA) (1995)

[6] Lund, M. S., Solhaug, B., Stølen, K.: Model-Driven Risk Analysis – The CORAS Approach. Springer (2011)

[7] Mitre: CWE – Common Weakness Enumeration, Mitre 2006-2014

[8] Mitre: CAPEC – Common Attack Pattern Enumeration and Classification, Mitre 2007-2014

[9] BSI: IT-Grundschutz Catalogues, Federal Office for Information Security, Bonn Germany 2013

[10] BSI: Preliminary Version of Module Cloud Usage, IT-Grundschutz Catalogues, Federal Office for Information Security, Bonn Germany, to be published 2014

[11] Jansen, Wayne; Grace, Timothy: Guidelines on Security and Privacy in Public Cloud Computing - SP800-144, NIST 2011

[12] Pearson, S.: Privacy, Security and Trust Issues Arising from Cloud Computing, Second International Conference on Cloud Computing Technology and Science (CloudCom) pp. 693-702, IEEE 2010

[13] Ren, K.; Wang, C.; Wang, Q.: Security Challenges for the Public Cloud, Internet Computing Vol. 16 Issue 1, pp 69-73, IEEE 2012

[14] Viehmann, J: Risikoanalyse mit automatischen Sicherheitstests, RACOMAT Methode und Tool, GI-TAV 36, Leipzig 2014