Security Standards Taxonomy for Cloud Applications in Critical Infrastructure IT

Sarita Paudel
Vienna University of Technology
Vienna, Austria
Email: e1029083@student.tuwien.ac.at

Markus Tauber
Austrian Institute of Technology
Vienna, Austria
Email: Markus.Tauber@ait.ac.at

Ivona Brandic
Vienna University of Technology
Vienna, Auatria
Email: ivona@infosys.tuwien.ac.at

***Abstract*—The trend of using the Cloud will soon reach Critical Infrastructure (CI) IT. Due to the lack of relevant taxonomies and criteria catalogs, it is often difficult for software development teams who work in the CI and cloud domain to adopt the right standard or tool for the context at hand. This work motivates the investigation of the applicability of software security standards and tools for CI IT, outlines the relevant security issues and investigates gaps in existing work on this topic.**

***Keywords*—Cloud, Critical Infrastructure, Secure Software.**

I. Introduction

Critical Infrastructures (CI) provide the utilities and basic needs including electricity, water supply, and in so called smart-cities even traffic control and CCTV systems[1]. The increasing flexibility and unpredictable usage of such utilities often means that many challenges such as load balancing can occur in the utility networks we use. The usage of modern IT systems to control and manage CI helps in dealing with such issues. However, this exposes CI to cyber risks and results in demand for protection against cyber-attacks, even more than traditional IT systems as failing CI may have a cascading effect on each other and hence fatal effects. Devices for management and control IT for CI are normally equipped with limited computation resources. Also data from an individual device does not make sense when being looked at in isolation and hence data from multiple devices needs to be accumulated. Thus, adoption of cloud technologies allows CI to benefit from dynamic resources allocation for managing unpredictable load peaks. Given the public awareness of CI and its importance, the public wants to be assured that these systems are built to function in a secure manner. Hence, appropriate security means have to be selected when developing such systems and documented accordingly.

Most existing methodologies and techniques for developing secure applications only explore security issues and security requirements in either CI or Cloud. Individual methodologies and techniques or standards may even only support a subset of specific CI requirements.

Requirements based security issues can be quite different for CI applications and for (common IT) cloud applications but need to be considered in combination for the given context. For instance, a special challenge in developing (common IT) cloud application is that cloud systems are particularly vulnerable to security breaches. This is because typically such applications are characterized by their distributed nature. Meaning an increased number of data transfer/storage issues over the Internet, from the client to the cloud application - allowing compromising the transferred data over WAN. Another issue is represented by shared infrastructure amount cloud tenants. On the other hand, for CI, for instance, we have to consider that they are historical isolated setups, and often consist of limited resources of its (Supervisory Control and Data Acquisition, i.e. SCADA) components only allowing limited encryption and security measures to be installed. These are significant differences of CI to common IT systems. Thus, integration of CI to the Cloud has several open security issues which need to be considered in combination. Choosing the appropriate software security standards and tools to develop secure cloud applications for CI will help to overcome these security issues.

Therefore, the overall research issues addressed by our work, beyond this paper, are: *(i) Evaluation of available software security standards and tools to support CI and the Cloud, (ii) Development of a multidimensional taxonomy based on open security issues for CI in the Cloud to point out multiple standards and tools, and (iii) Mapping of security requirements to the available standards and tools based on evaluation.* Corresponding results will eventually also be useful for service assurance when documenting the used software development security standards, guidelines or tools.

Related Work [1], [2], [3], [4], [5], [6] mostly addresses issues related to either CI or Cloud and provides no support of a taxonomy that would help selecting appropriate secure software development standards for a given CI-Cloud context.

The purpose of this paper is to investigate the need and to motivate our overall research by outlining the relevant security issues and providing an overview of gaps in existing work. We give an indication on which kind of metrics and criteria catalogs are required, and outline how we will investigate identified security issues in future work - which will include the evaluation of our findings in a showcase development.

Output of our overall work will help Cloud and CI providers, as well as other stakeholders to select the right software security standards and tools to build secure software.

II. Security issues in CI, and software security standards and tools

Various software security standards, guidelines and other "means" to build secure software are available, some with focus on specific security issues. Applying these contribute to data confidentiality, integrity, availability (CIA) and other

[1]SEcure Cloud computing for CRitical infrastructure IT (SECCRIT) (see www.seccrit.eu) is an EU FP7 research project looking at CCTV and traffic control (Contract Nbr. 312758) which motivates and supports this work.

security related issues. Based on these issues, we investigate if software security standards are applicable to CI in the Cloud and extend it to establish a taxonomy that will help to identify the most appropriate one for a given CI-Cloud context.

A. Our Taxonomy will be based on the open security issues in CI and Cloud (identified in [7], [8], [9], [10])

- *Data Storage Security:* Correctness and availability of data in the Cloud must be guaranteed. This is of fundamental importance when considering a case where the Cloud is used in a CI context e.g. for storing metering data of a utility network.
- *Data Transmission Security:* Historically CI components were used in isolated setups and using the Cloud requires additional caution regarding secure transmission as unsecured transmissions allow eavesdropping or alteration of data.
- *Application Security:* CI applications are often not built for being exposed to public internet and its users, and were only accessible by trained personal.
- *Cloud Integrity Security:* Regular basis of data backup and storing outside Cloud is done to be safe from data-loss incident. The CI metadata is important for billing and provision of basic needs but it also allows to identify the behavioral patterns. This critical information could be misused, so it needs to be secured.
- *Security Related to Third- Party:* Third Party establishes connection between two parties and provides end-to-end security services. All critical transactions between the two parties are reviewed by the Third Party. Thus, Third party requires security on confidentiality, client and server authentication, certificate-based authorization and creation of security domain.

B. Software security standards and tools

To give an indication on which kind of "means" we are investigating, we provide the following list of standards and guidelines: *i) Secure Development Lifecycle (SDL), ii) Correct by construction (CbC), iii) Common Criteria (CC) - ISO/IEC 15408, iv) ISO/IEC 27001:2005, v) ISO/IEC 27002:2005, vi) Computer Emergency Response Team (CERT) best practices, vii) European Network and Information Security Agency (ENSIA) guidelines, viii) Cloud Security Alliances (CSA) best practices, ix) Intern. Society of Automation (ISA) - ISA99 standards, x) North American Electric Reliability Corporation (NERC) Critical infrastructure protection (CIP): 002-009 standards.*

We are currently investigating the applicability of the individual standards, guidelines and tools to the CI domain under consideration of a CI show case we are developing. The list of security issues above will serve as taxonomy for identifying the scope of the individual standard or guideline. The considered multiple dimensions based on the usability in e.g. software specifications or documentations we distinguish between *i) standards ii) guidelines* and motivated by Futcher et.al [2], we will sub-categories these two dimensions in *a) security standards or guidelines and tools b) software development standards or guidelines and tools*. A Schematic illustration of the resulting mapping options is shown in Figure: 1.

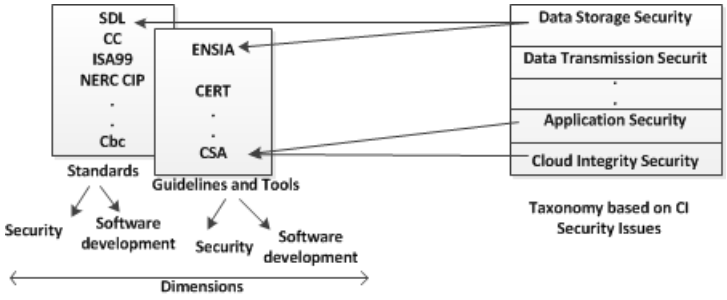

Figure 1. Schematic illustration of usage of our results. Arrows show the mapping of standards & tools to identified security issues. For example to address the Data Storage security issue ENSIA and SDL are selected.

III. Conclusion

We set out to motivate investigations on the applicability of secure software development standards and tools for the Cloud and CI domain in combination. We have presented different security issues (e.g. data storage security, data transmission security, application security) in CI in the Cloud. Software security standards and guidelines need to be integrated in the development process to deal with such security issues. We show the need for a taxonomy to support these activities and illustrate how it can be used. We also provide an example list of candidate standards and guidelines which we currently investigate (e.g. SDL, CbC methodology, CC, NERC CIP).

To investigate the specific requirements of cloud applications for the CI domain in more detail we are working on a showcase in which CI data is being stored in an elastic database. This and the identified security issues will serve the investigation of applicability of standards/guidelines and the categorization based on the developed multidimensional taxonomy. Once completing these steps we plan to revisit the showcase development process for applying our findings.

Our output will help CI and Cloud providers or stakeholders to select the right means to build a secure software for the given context.

References

[1] D. M. Dekker, "Critical cloud computing:ciip perspective on cloud computing," 2013, [Online; accessed 19-July-2013].

[2] L. Futcher and R. von Solms, "Guidelines for secure software development," ser. SAICSIT '08. New York, NY, USA: ACM, 2008.

[3] R. Dukaric and M. B. Juric, "Towards a unified taxonomy and architecture of cloud frameworks," *Future Generation Comp. Systems*, 2013.

[4] R. M. Savola, "Towards a taxonomy for information security metrics," in *Proc. of the 2007 ACM workshop on Quality of protection*, 2007.

[5] P. Karger, S. McIntosh, E. Palmer, D. Toll, and S. Weber, "Lessons learned: Building the caernarvon high-assurance operating system," *Security Privacy, IEEE*, vol. 9, no. 1, pp. 22–30, 2011.

[6] N. Santos, R. Rodrigues, K. P. Gummadi, and S. Saroiu, "Policy-sealed data: A new abstraction for building trusted cloud services," in *In USENIX Security*, 2012.

[7] H. Tianfield, "Security issues in cloud computing," in *Systems, Man, and Cybernetics (SMC), 2012 IEEE International Conference on*, 2012.

[8] M. Z. Meetei and A. Goel, "Security issues in cloud computing," in *Biomedical Engineering and Informatics (BMEI), 2012 5th International Conference on*, 2012, pp. 1321–1325.

[9] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in *MIPRO, 2010 Proceedings of the 33rd International Convention*, 2010, pp. 344–349.

[10] M. M. Younis A.Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: A survey," Liverpool John Moores University, United Kingdom, Tech. Rep., 2013.