SECCRIT Newsletter 3 – March 2014

This is the third SECCRIT newsletter from a series that will keep you updated about our research activities and events. It is being sent out to members of the “User and Advisory Board” (UAB) directly and will also be available at www.seccrit.eu. This issue contains the current project status, a short overview of the SECCRIT architectural framework (a structured approach to support investigations in critical infrastructures and the Cloud), and an announcement regarding the next issue and upcoming events.

1 Project Status

We have successfully completed the first year with a positive and encouraging review. Main focus of our activities so far was the elicitation of requirements and constraints of industry and critical infrastructure providers regarding cloud usage. We have investigated those issues not only from a technical but also from a legal perspective. This was carried out to cater for our mission which is to analyse and evaluate cloud computing with respect to security risks in sensitive environments, i.e. critical infrastructures (focusing on SECCRIT use cases regarding Traffic Control & Public Safety (CCTV)), to develop: methodologies, technologies, best practices guidelines for secure and trustworthy high assurance, and legally compliant cloud computing environments for critical infrastructure IT. Our output is available at www.seccrit.eu and includes, for example, public reports and scientific papers on a vulnerability analysis and risk assessment, legal fundamentals, and work on an architectural framework.

2 The SECCRIT Architectural Framework

The Critical Infrastructure sector is characterized by strict regulatory constraints. Liability, for example, leads to the requirement of providing strong evidence for root causes in case of service failures. Similarly, data protection plays an important role in such infrastructures (e.g., consider storage of sensitive medical data within the cloud). Therefore, the need arises to support legal requirements by suitable technical means.

In this newsletter we briefly present the structure of an architectural framework for developing appropriate support (e.g., suitable monitoring and auditing tools) when critical infrastructure services are moved into a cloud environment, and we explain the motivation behind the framework. We analysed various existing architectural models from the viewpoint of a Critical Infrastructure service provider and found that most models assume a rather monolithic role of the Cloud Service Provider. Consideration of liability issues, however, suggests a clear separation of concerns and responsibilities between different stakeholders, and a clear separation of administrative duties. Existing architectural models show a lack of support for additional monitoring/metering capabilities and for interfaces supporting CI services. Moreover, they lack transparency across different abstraction levels and stakeholders.

While working towards technical means to support CI services in the cloud, we were facing several questions that an architectural framework will help us to address: Where are transparency-enhancing interfaces situated (e.g., root cause analysis, audit trails, or assuring specific properties of the used infrastructure)? What and where are sources for audit trails? What are possible locations of additional monitoring points (e.g., for anomaly detection) or policy enforcement points, respectively? Finally, we expected that an architectural framework would help clarify the relationships between the project’s technical outcomes.

The proposed SECCRIT Architectural Framework (cf. Figure 1) aims at a precise role distinction that allows for better security analysis, separation of responsibilities, identification of separate administrative interfaces, and for checking the influence and coverage of legal aspects. It is an architectural framework because it mainly serves descriptive and explanatory purposes rather than specification purposes as a reference architecture definition in a standards organisation. Therefore, we can map specific cloud architectures, deployments, and usage scenarios partially or fully to the SECCRIT Architectural Framework. A starting point is common terminology, followed by a clear distinction of different abstraction levels as well as a clear separation of responsibilities.

One important aspect within the SECCRIT project context is to consider that a single Cloud Infrastructure is typically simultaneously used by several *tenants* (i.e., customers of the Cloud Infrastructure Provider), whose virtual resources are usually isolated from each other to some degree within the Cloud Infrastructure.

The distinction between the virtual *Tenant Infrastructure* and the *physical Cloud Infrastructure* is important since a clear separation between responsibilities is necessary. If a CI service fails, a root cause analysis should reveal the responsible party—either the Cloud Infrastructure provider or the Tenant Infrastructure provider. To this end, additional monitoring or logging mechanisms for auditing can be located within the Cloud Infrastructure, as well as within the virtual infrastructure of the tenant. This will support identifying additional interfaces for increasing the trust level between tenants and cloud infrastructure providers by permitting some level of audits.

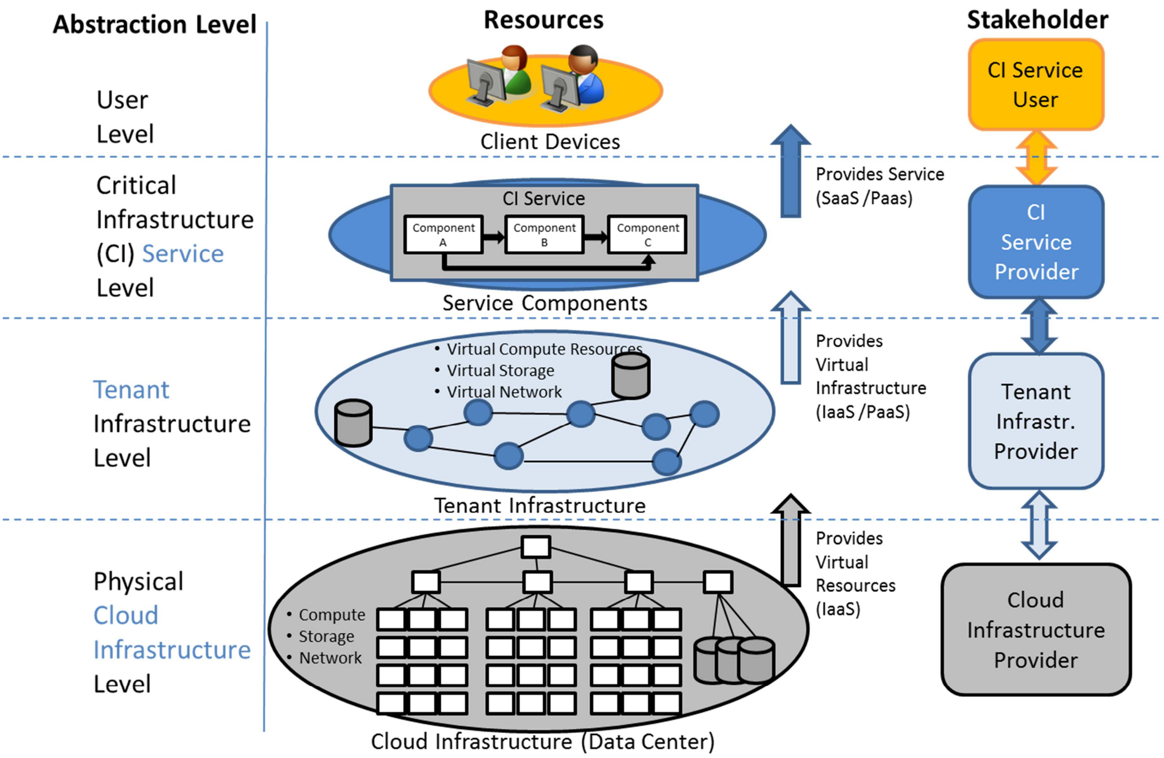
Abstraction Level
Resources
Stakeholder
User Level
Client Devices
CI Service User
Provides Service (SaaS /Paas)
Critical Infrastructure (CI) Service Level
CI Service
Component A
Component B
Component C
Service Components
CI Service Provider
Tenant Infrastructure Level
• Virtual Compute Resources
• Virtual Storage
• Virtual Network
Provides Virtual Infrastructure (IaaS /PaaS)
Tenant Infrastructure
Tenant Infrastr. Provider
Physical Cloud Infrastructure Level
• Compute
• Storage
• Network
Provides Virtual Resources (IaaS)
Cloud Infrastructure Provider
Cloud Infrastructure (Data Center)

Figure 1 The SECCRIT Architectural Framework – Abstraction Level View

Furthermore, the architecture must clearly distinguish the *Service Provider* from the virtual *Tenant Infrastructure* provider. This allows separating two important aspects of any CI service: functional and behavioural features. On the *service layer*, the functional features of the service are dealt with as well as which components are required to compose the service and how these components need to be interconnected. On the *tenant infrastructure level,* the behavioural features of the service are dealt with. This includes elasticity features, component redundancy, and overload control. Failures on the physical infrastructure level can be made opaque to the service by self-healing mechanisms on the tenant infrastructure level, such as automatic fail-over to redundant components. In addition, geo-diversity can be realized on the tenant infrastructure level by requesting resources from multiple independent cloud infrastructure providers for increased dependability but also for higher privacy and security.

Consequently, Figure 1 shows different levels of abstraction that we want to distinguish. The different abstraction levels correspond to different stakeholders and their view on the managed resources. Most existing architectures concentrate on the provisioning of resources at the Cloud Infrastructure level, i.e., on providing and managing cloud resources within a data centre. However, a more overarching view covering different levels and stakeholders is needed:

- At the *User Level*, we have the Critical Infrastructure *Service User* who remotely accesses the Critical Infrastructure Service.
- The next lower level is controlled by the CI Service Provider who manages the resources at the *Service Level*. The CI Service is composed of several components that interact with each other in order to provide the actual service. The *CI Service Provider* monitors the service operation and performance at this level. The service components either provide the application or the platform that is required at the user level. The service components are instantiated on the virtual infrastructure that is provided by the Tenant Infrastructure level.
- The *Tenant Infrastructure Level* provides a virtual infrastructure that consists of virtual compute resources, virtual storage, and virtual network resources. This set of resources is sometimes referred to as a Virtual Data Centre (vDC), and it is managed by the *Tenant Infrastructure Provider*. We distinguish this stakeholder from the service provider since they may be separate organisations. Several such tenants are typically hosted within one Cloud Infrastructure, which is the next lower level. The Tenant Infrastructure Provider may provide either the pure virtual infrastructure (IaaS) or some basic services as a platform (PaaS) to the CI Service Provider. The Tenant Infrastructure Provider is not aware of what services and applications are running inside the virtual Tenant Infrastructure.
- The *Physical Cloud Infrastructure Level* provides real physical (sometimes called “bare metal” or “substrate”) compute, storage, and network resources, which are hosted in a data centre administered by the *Cloud Infrastructure Provider*. This level usually provides virtual resources (IaaS) to its upper level, i.e., the tenant. The virtualization solution usually provides (a certain degree of) isolation between the different tenants that are multiplexed onto the same physical infrastructure and thus permits the sharing of resources. For increasing resource efficiency, the Cloud Infrastructure Provider can usually transparently move virtual resources across its physical infrastructure, unnoticed by the tenant. However, for a tenant it would be helpful to obtain evidence about such migrations in case that they entail a service failure or a violation of a non-functional constraint (e.g., a legal obligation to keep data processing inside a given jurisdiction).

It should be noted that multiple stakeholder roles may sometimes be realised by the same organisation. Moreover, in order to address the various questions mentioned in the beginning, we need several different views within the framework suitable to focus on specific aspects that need to be investigated. Those additional views are explained in a recently published whitepaper that can be downloaded from http://seccrit.eu/whitepaper. The whitepaper also contains a more detailed discussion of legal aspects, a gap analysis, and also examples of how to map existing cloud virtualization platforms into the architectural framework. It will be updated as the SECCRIT project progresses.

3 Survey on Cloud Security for Critical Infrastructure IT

To provide potential beneficiaries of our research output the chance to steer our research direction, we approached them with a survey. Our survey elicited cloud security needs with respect to methodologies and tools for improving the security in cloud infrastructures. It was presented to members of the SECCRIT User and Advisory Board who were invited to participate in the survey directly at the event.

Judging from the survey results, there is a general strong trend towards cloud computing. Thus, many future services are planned as cloud services, mainly in private clouds. Our poll revealed a number of expectations and concerns when deploying infrastructure services into the cloud. Especially for *critical* infrastructure services, strong objections prevail over non-private cloud deployment.

Participants stated cost reduction, scalability, elasticity and especially availability, reliability, and resilience as the main advantages of cloud infrastructures for their organisations. The majority of the respondents claimed security and privacy as well as loss of control over key IT systems and the infrastructure itself as their main concerns regarding service deployment in cloud infrastructures.

The survey confirmed the need for data usage control in cloud infrastructures. Especially context-aware security policies gained strong acceptance among the respondents. Moreover, many respondents expressed a need for end users to specify security policies, but doubts arose whether the average user is capable of providing correct policy specifications that do not jeopardise security. The survey was carried out by Fraunhofer IESE in Kaiserslautern, Germany. The detailed results can be found here: https://seccrit.eu/upload/CloudCritITSurvey.pdf. We plan to substantiate the results from this survey by approaching the UAB again for eliciting concrete security policies that UAB members would demand for running critical infrastructure IT in clouds in a secure way.

4 Next Issue

The next issue of this newsletter is planned for July 2014, and it will focus on details regarding the demonstrator outputs. In this issue, we will specify how specific technical outputs are being evaluated in our demonstrators, based on feedback from internal workshops with the consortium and various stakeholders. This will be the basis for our next UAB workshop in September 2014 in Vienna. In the meantime, we will keep you updated via the SECCRIT webpage and twitter (@SECCRIT). User and Advisory Board Members are invited to send us their feedback directly or via our emailing list at any time.