SECCRIT Newsletter 6 – November 2015

This is the sixth 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 second year with a positive and encouraging review and are now approaching the final months of the project. In year one the main focus of our activities 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.

The deliverables published during the second year of the project have been mainly RTD outputs, including a methodology for policy specification (see D3.2 Policy Specification Methodology), a cloud management framework to make the cloud domain resilient to unplanned challenges (see D4.2 Resilience Cloud Management) and a novel assurance evaluation method used to assure critical infrastructure providers that certain security levels are maintained despite a changing environment (see D5.2 Cloud assurance profile and evaluation method).

In the third year of the project, other RTD outputs have been published in the following deliverables, a tool for policy specification (see D3.3 Policy Specification Tool), a novel mechanism for anomaly detection particularly suitable for deployment in cloud environments because of their low computational complexity and high accuracy (see D4.3 Mechanisms and tools for anomaly detection), IND^{2}UCE policy enforcement framework (see D4.4 Policy decision and enforcement tool) and instantiations of tools for audit trails and root cause analysis with the aim to enable the generation of audit trails by continuously monitoring a given cloud deployment of critical infrastructure independently from the view of the cloud provider (see D5.3 Tools and evaluation of audit and root-cause tools). The main focus at this point of the project is to provide demonstrators results. These results will be published in deliverables D6.2 Demonstrators Validation and D6.3 Report on validation result, which are still work in progress. A number of corresponding scientific papers to the deliverable topics can be found on the SECCRIT webpage along with over 30 peer reviewed scientific articles.

In this newsletter we briefly present the update of the SECCRIT architectural framework for developing appropriate support (e.g., suitable monitoring and auditing tools) when critical infrastructure services are moved into a cloud environment.

2. Update of the SECCRIT Architectural Framework

During the last year we continuously updated the SECCRIT Architectural Framework which was introduced in Newsletter 3 (March 2014). In this current edition we briefly present the outcome of the update process. This updated Whitepaper can be downloaded from http://seccrit.eu/whitepaper. The whitepaper also contains a more detailed discussion of further legal aspects, a gap analysis, and also examples of how to map existing cloud virtualization platforms into the architectural framework.

First we added a new legal perspective of data protection law and civil law onto the SECCRIT Architectural Framework. Additionally, we mapped the SECCRIT output clusters onto the Architectural Framework, which are colorized in the figure 1: *Novel Risk Assessment Approaches*, *Cloud Security Policy Specification and Enforcement Framework*, *Forensic Analysis via Audit Trails for Root Cause Analysis*, *Resilience Framework including Anomaly Detection in the Cloud*, *Cloud Assurance Approaches*, *Process-oriented Security Guideline and Best Practice Approaches.* These output clusters are described in more detail in Deliverable 6.1 *Demonstrator Definition.*

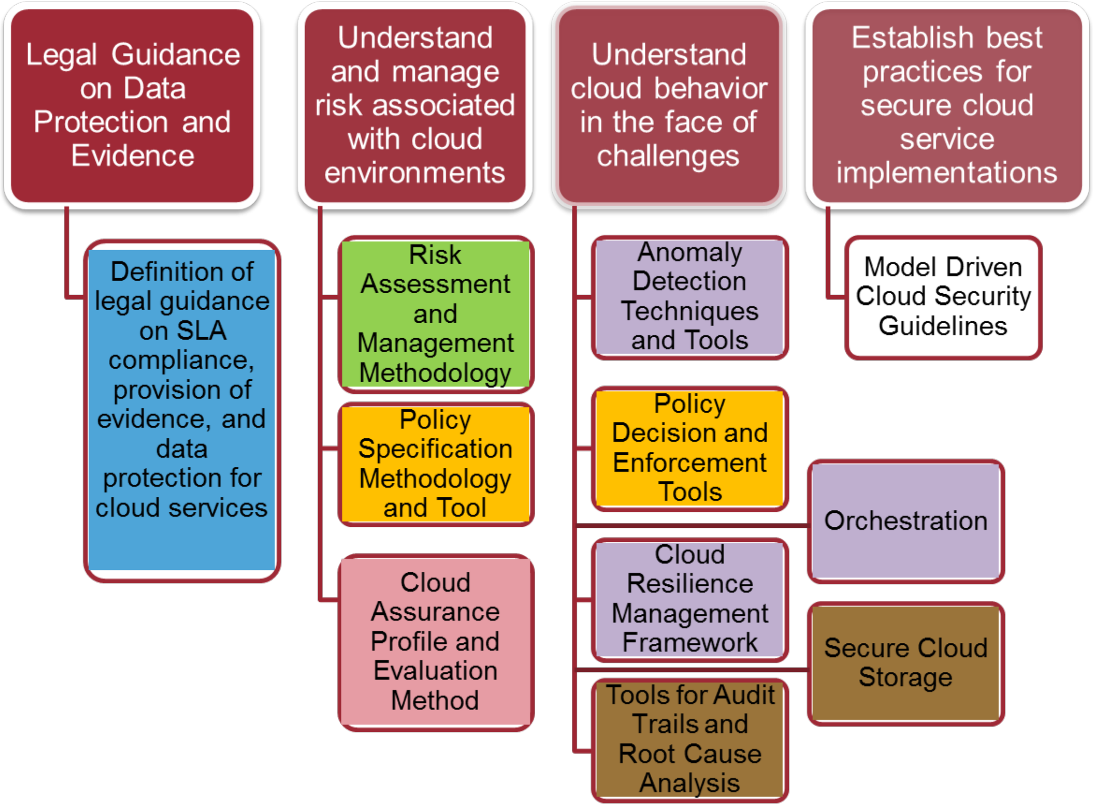
Legal Guidance on Data Protection and Evidence
Understand and manage risk associated with cloud environments
Understand cloud behavior in the face of challenges
Establish best practices for secure cloud service implementations
Definition of legal guidance on SLA compliance, provision of evidence, and data protection for cloud services
Risk Assessment and Management Methodology
Policy Specification Methodology and Tool
Cloud Assurance Profile and Evaluation Method
Anomaly Detection Techniques and Tools
Policy Decision and Enforcement Tools
Cloud Resilience Management Framework
Tools for Audit Trails and Root Cause Analysis
Model Driven Cloud Security Guidelines
Orchestration
Secure Cloud Storage

FIGURE 1 –SECCRIT OUTPUT CLUSTERS

The following table describes to what extend SECCRIT output clusters affecting the Architectural Framework levels. In the revised Whitepaper each output cluster and its relation to the SECCRIT Architectural Framework is described in more detail.

Logo	Cluster	Cloud Infrastructure	Tenant Infrastructure	Service	User
	Novel Risk Assessment Approaches	SECCRIT vulnerability and threat catalogue, where specific threats and vulnerabilities have been mapped to the infrastructure level.	SECCRIT vulnerability and threat catalogue, where specific threats and vulnerabilities have been mapped to the tenant level.	SECCRIT vulnerability and threat catalogue, where specific threats and vulnerabilities have been mapped to the service level. The cloud adoption risk assessment process, used to model cloud specific scenarios and related risks.	SECCRIT vulnerability and threat catalogue, where specific threats and vulnerabilities have been mapped to the user level. The results of cloud adoption risk assessment process, are typically recorded in a document that can be automatically generated by the Verinice tool, a tool that allows the user to define risk acceptance levels appropriate for their organization
	Cloud Security Policy Specification and Enforcement Framework	IND^{2}UCE for VMware, namely a PEP to intercept VMware specific events, a PXP to execute VMware specific actions and two PIPs for providing additional information have been developed to interact with the physical cloud infrastructure management system. The PAP is the interface to the cloud infrastructure operator for specifying security policies	IND^{2}UCE for VMware interacts also with tenant infrastructure management system. The PAP is the interface to the tenant infrastructure operator for specifying security policies.	IND^{2}UCE for HBase & Hadoop: a PEP and PXP integrated into the HBase to interact with a cloud storage environment on the service layer. The PAP is the interface to the CI service operator for specifying security policies.	The PAP is the interface to the CI service user for specifying security policies.
	Forensic Analysis via Audit Trails for Root Cause Analysis	Installation of TCM, TEM and LAM within the Physical Cloud Infrastructure. LAM with external Hybris storage. Management-Access for the Cloud Provider	Tenant specific TCM access for real-time auditing and specifying audit trail collection	No relevance	No relevance

	Resilience Framework including Anomaly Detection in the Cloud	CRMF Resilience Manager. Anomaly detectors AD3 and SOFM	Deployment Function (DF) to deploy resilience patterns according to tenant requirements	No relevance	No relevance
	Cloud Assurance Approaches	Infrastructure specific data set is extracted via security property collectors that have been designed to acquire security based information. These information sets are then being used to aggregate and calculate assurance across the independent components in each level and derive final overall assurance level for the assessed service	Tenant specific data set is extracted via security property collectors, deployed with VMs, that have been designed to acquire security based information. These information sets are then being used to aggregate and calculate assurance across the independent components in each level and derive final overall assurance level for the assessed service	Service specific data set is extracted via security property collectors that have been designed to acquire security based information. These information sets are then being used to aggregate and calculate assurance across the independent components in each level and derive final overall assurance level for the assessed service	User is offered to define custom based evaluation and aggregation policy that based on the personal preferences of an individual user can derive a different level of assurance
	Process-oriented Security Guideline and Best Practice Approaches	No relevance with respect to the Guideline, there are however links to the infrastructure layer as the guideline mentions other SECCRIT outputs part of the cloudificaiton process which link to the infrastructure layer	No relevance with respect to the Guideline, there are however links to the tenant layer as the guideline mentions other SECCRIT outputs part of the cloudificaiton process which link to the infrastructure layer	As part of our process-oriented security guideline we have developed an approach for a cloudification security development life cycle (CloudSDL) together with a mapping of security relevant issues to current best practice guidelines and standards. The developed methodology can be used for the migration of legacy IT services to the cloud.	No relevance

3. Dissemination activities

This year was characterised by a lot of collaborative scientific work which manifests itself in the publication track-record of the project, including organisation of scientific events.

Dagstuhl Seminar 15151

Dagstuhl Seminar 15151 entitled "Assuring Resilience, Security and Privacy for Flexible Networked Systems and Organizations" took place on 07-10 of April 2015. It brought together researchers from different disciplines in order to establish a research agenda for making future services in our increasingly connected world more resilient and secure, as well as addressing privacy. The main use cases discussed during Daghstuhl Seminar covered the Internet of Thing (IoT) and Cloud-based applications.
The research questions produced during the seminar, discussed:

- How to enable Resilience, by design, of composable flexible systems?
- What is the role of law in supporting resilience, privacy and security?
- Traceability of (personal and non-personal) data in service provision?
- How can we improve the perception of assurance, privacy, security and resilience?
- What constitutes a security problem?
- How to deal with unforeseen new context of usage?

A summary of the findings for each research question / topic can be found at Dagstuhl Research Online Publication Server, http://drops.dagstuhl.de/opus/volltexte/2015/5272/pdf/dagrep_v005_i004_p001_s15151.pdf

UAB Workshop @The Future of Cloud

The Future of Cloud (www.thefutureofcloud.org) event took place on the 17th of June 2015. The event was hosted by AIT and organized together with EuroCloud Austria, presenting research from SECCRIT and its liaison projects PRISMACLOUD, CREDENTIALS, and CI2C.

The event was centred on two panel discussions, engaged in debate to answer the following targeted questions:

- Getting a clearer picture of how the cloud will develop over the next few years
- Taking a look at the future from different perspectives to be able to form one's own opinion and make one's own decisions.
- Presenting complex research topics in an innovative and exciting manner in an overall context

The SECCRIT consortium organised the third UAB workshop as part of this joint event. Additionally, poster sessions were held to explain the research topics in detail. A final engagement with members of the user and advisory board and with industrial stakeholders is planned at the InfoCom Event in Athens on the 24th of November.

4. Liaisons, survey and continuation of our work

As our work in SECCRIT is about to be completed we would like to introduce two liaison projects to you in which some of the work from SECCRIT will be carried on.
The EU Project PRISMACLOUD (Horizon 2020 programme; duration 2/2015-7/2018) addresses challenges in trustworthy cloud computing and yields a portfolio of novel agile cryptographic technologies to build security and privacy preserving services in the cloud. Its goal is to protect data throughout the whole lifecycle in the cloud and from end-to-end, i.e. it allows of trustworthy services on semi-trusted infrastructure. The work from SECCRIT plays an important role for PRISMACLOUD and riks assessment results as well as the released guildelines and reference architecture will help to strengthen the project outcome.
During "The Future of Cloud" event a questionnaire for liaison project PismaCloud has been presented to members of the SECCRIT User and Advisory Board, who were invited to participate in the survey directly at the event. The survey can be also found online at: https://de.surveymonkey.com/r/?sm=pKUTcoKGhQeaHzMAtiFZgA%3d%3d.
The survey analysis is expected to provide a clear view, how the importance of security related aspects, such as integrity, confidentiality, availability, differentiates between academia and industry partners when it comes to cryptographic solutions.
The EU Project CREDENTIAL (Horizon 2020 programme; duration 10/2015-9/2018) engages in developing, testing, and showcasing innovative cloud-based services for storing, managing, and sharing digital identity information and other highly critical personal data with a demonstrably higher level of security and privacy than other current solutions. This is achieved by advancing novel cryptographic technologies and improving strong authentication mechanisms. The SECCRIT work on assurance is going to be extended and applied in the specific application domain of federated identity and access management in the cloud.
If you want to learn more on the above projects, please visit their homepages at https://www.prismacloud.eu and https://www.credential.eu.

5. Next Issue

The next issue of this newsletter is planned for March 2016, and it will focus on results regarding the demonstrators, where two different environments have been defined to test and validate the technologies: one related to VMWare technology, and another one based on OpenStack. 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. 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.

Further Information

You can find additional information of the SECCRIT project at www.seccrit.eu

Additional information can be also requested via info@seccrit.eu

Authors: Dr. Markus Tauber, Silia Maksuti