

SECCRIT Newsletter – Nov. 2014, Special Edition on: International Symposium “Building Trust in Cloud”

Over 120 Cloud experts and stakeholders participated in the international symposium “Building Trust in Cloud” (<http://www.buildingtrustincloud.org/>) on the 23rd of September. The SECCRIT consortium organised its second user and advisory board workshop as part of this joint event. The event was organised together with EuroCloud Austria and with the Federal Computing Centre of Austria – Bundesrechenzentrum (BRZ), the latter kindly hosted the event. Cloud topics were presented in the following areas:

1. Commercial and industrial use of the Cloud
2. Cloud in the public administration and critical infrastructures
3. Security research activities regarding Cloud and critical infrastructures IT (SECCRIT)

The visitors discussed with a panel consisting of international experts and stakeholders from academia, industry and public administration the state of affairs regarding research and the future demand of innovative and secure Cloud solutions.

Cloud Computing is one of the important IT trends in the last few years. IT services are therefore potentially cheaper and more efficient; a maximum of automation and a high flexibility is possible via Cloud Technologies. This allows IT services to offer demand driven and flexible acquisitions for information and communication technology. Cloud Computing targets various aspects of currently established IT company infrastructures. However, information security in combination with legal conditions is often a barrier for adapting Cloud technologies. Organisations like Cloud Security Alliance, European Network and Information Security Agency (ENISA) or the Federal Association for Information Technology, Telecommunications and New Media (BITKOM) are starting to provide aids to address concerns of organisations, companies and service providers for “cloudifying” applications – mainly focusing on industrial usage. As not only industrial stakeholders but also public administration and critical infrastructure providers taking up this trend, activities have to be reviewed and consolidated in all these fields to steer and motivate research activities in Secure Cloud Computing. This was the goal of the, here reported on event.

Commercial and industrial use of the Cloud

EuroCloud was organising its quarterly held EuroCloud Brunch during this symposium. Representatives from the industry presented their opinions to the trends in the area of Cloud Computing, and introduced new solutions, Cloud applications and use cases, for example IBM Bluemix – a development environment for the Cloud. EuroCloud presented the Trust in Cloud initiative, which aim is to improve the acceptance of cloud computing in Austria. More than 20 local and global providers already joined and support this independent initiative. Also the latest developments regarding the EuroCloud Star Audit program (www.eurocloud-staraudit.eu) were presented, another cornerstone to ensure quality and transparency in cloud industry.

Use of Cloud computing in the public administration

The research project Cloud for Europe is funded by the European Commission and brings together 24 public sector and research partners from 12 countries, to identify obstacles, find

innovative solutions and build trust in European cloud computing. Cloud for Europe adjusts public sector requirements and establishes suitable contractual terms for future cloud procurements.

The BRZ as the market-leading e-government partner of the federal administration in Austria is exploring the possibilities of cloud computing in the public administration and exchanging know-how and best practices within Euritas, the European Association of Public IT Service Providers.

Dr. Jörn Oldag, from the public administration data centre “DVZ” (Germany), a Euritas member organisation, informed about latest cloud activities according to general regulations and conditions within Germany from the Euritas point of view.

A summarized cloud directive featuring the categorization and contracting options of cloud services for the public administration has been presented. Also the operational aspects of cloud services within the DOI (German core network for the public sector) and the regional networks of different state administrations were incorporated into the analysis. The achieved results were reviewed by the German public bodies ICT Planning Council (IT-Planungsrat), Federal Office for Information Security and a working group of the data protection officers (federal and state level).

Research activities regarding Cloud and critical infrastructures

The Austrian Institute of Technology (AIT) presented together with partner organisations the anticipated results from the SECCRIT project and held their second annual User and Advisory Board meeting as part of the event. SECCRIT’s mission is to analyse and evaluate Cloud technologies with respect to security risks in sensitive environments, and to develop methodologies, technologies, and best practices for creating a secure, trustworthy, and high assurance cloud computing environment for critical infrastructure IT. To do this and to evaluate research in real-world scenarios SECCRIT outputs were presented in the following structure:

Techno-legal guidance regarding Service Level Agreements (SLAs) and data protection for Cloud: These can be used by the various stakeholders to ensure that the deployment of high assurance ICT services in the Cloud is done in a legally sound manner.

Novel Risk Assessment Approaches: A Cloud-specific threat and vulnerability catalogue, including an approach to assess risks when “cloudifying” critical infrastructure ICT services, has been created and implemented as plugin for - “Verinice”, a tool for managing information security.

Cloud Security Policy Specification and Enforcement Framework: The elicitation of Cloud-specific security policies, techniques for their refinement into machine-readable format and enforcement approaches are being investigated and implemented as add-on to cloud infrastructures.

Resilience Management Framework (incl. Anomaly Detection): A novel Cloud anomaly detection method is being investigated, thus enabling cyber-attacks to be detected and counteracted via network and cloud management remediation actions, which is evaluated as infrastructure add-on.

Forensic Analysis via Audit Trails: To support cyber forensic analysis, a Trust Enhancement Framework was developed to provide information to Cloud tenants about their virtual resources.

Cloud Security Assurance Approach: A method and supporting tools are being developed to offer a uniformed methodology for delivering security guarantees across distinct levels of the Cloud.

Cloud Security Best Practice Guideline: Cloud migration security guidelines, which focus on the SECCRIT outputs, will be provided along with pointers to existing standards.

The desired outcomes and its usage were presented by the project coordinator Dr. Markus Tauber (AIT). Silvia Balaban (KIT) was talking about the legal aspects and Dr. Paul Smith (AIT) presented the finished results in the area of risk assessment. Christian Jung (Fraunhofer) showed his approaches to “Usage Control for the Cloud”, Dr. Steven Simpson (Lancaster University) presented work in the area of “Resilience Management for the Cloud”, Dr. Roland Bless (KIT) showed “Tools for Audit Trails and Root Cause Analysis” and Aleksandar Hudic (AIT) presented his work of “Cloud Assurance Framework”. Christian Wagner (AIT) presented a questionnaire for a survey he conducted at the event as initial activity for the “Best Practice Guideline”.

Cloud research involvement

For the achievement of the goals of SECCRIT ongoing exchange between experts is a must. Because of that fact a “User and Advisory Board” was established. The board consist of potential users of the research results, political stakeholders as well as experts from research and industry. In annual workshops they provide feedback on SECCRIT results and are actively involved in the research. They gain access earlier than others to the relevant project outcomes. Visitors of this year’s workshop were invited to fill out a questionnaire for giving input to the research work.

At the end of the workshop the visitors were able to discuss with the panel about the presented topics and the future focus. The panel was moderated by Dr. Andreas Mauthe (Lancaster University). Participants were representatives of jurisprudence, network science, industry and public administration:

- Prof. Reinhard Posch, TU Graz and CIO Austrian Federal Chancellery, www.digitales.oesterreich.gv.at/site/5631/default.aspx
- Prof. Burkhard Schafer, Techno-legal Expert, University of Edinburgh, www.law.ed.ac.uk/people/burkhardschafer
- Prof. James Sterbenz, Cloud & Networking Expert, University of Kansas, www.ittc.ku.edu/~jpgs/
- Dr. David Watrin, Security & Intelligence Expert, Swisscom, www.swisscom.com

Prof. Burkhard Schafer concluded: *“The most exciting and rewarding form of interdisciplinary research takes place when all participating disciplines can add to the knowledge both in their own field and to that of the collaborators. All too often, law is seen as a mere “service” in ICT projects, but not an equal partner in the exploration of new ideas. The project should be highly recommended for the excellent integration of legal research into a technology-led programme, which resulted in truly new insights for both law and technology.”*

Afterwards there was a discussion on research directions, in particular in the SECCRIT project: The focus should be more laid on the one hand on the representation of the use case scenarios and on the other hand on the combination of legal aspects with technical approaches. Especially the legal evidence of the developed technical solutions out of SECCRIT should be supported.

Further Information

You can find additional information of the SECCRIT project at www.seccrit.eu and about the event at www.buildingtrustincloud.org

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

Authors: Markus Tauber, Petra Köndorfer, Manoela Bodiroza, Tobias Höllwarth