SEcure Cloud computing for CRitical Infrastructure IT

Contract No 312758

Deliverable D7.2
Dissemination Report Year 2

AIT Austrian Institute of Technology • ETRA Investigación y Desarrollo • Fraunhofer Institute for Experimental Software Engineering IESE • Karlsruhe Institute of Technology • NEC Europe • Lancaster University • Mirasys • Hellenic Telecommunications Organization OTE • Ayuntamiento de Valencia • Amaris

Document control information		
Title	Dissemination report year 2	
Creator	ETRA	
Editor	Santiago Cáceres	
Description	This report summarises the dissemination activities carried out by SECCRIT consortium during the second period	
Classification	☐ **Red** – Highly sensible Information, limited access for: ☐ **Yellow** – restricted limited access for: ☐ **Green** – restricted to consortium members ☒ White – public	
Reviewers	☒ AIT ☐ ETRA ☐ IESE ☐ KIT ☒ NEC	☐ ULANC ☐ MIRASYS ☐ OTE ☐ VLC ☐ AMARIS
Review status	☐ Draft ☐ WP Manager accepted ☒ Co-ordinator accepted	
Action requested	☐ to be revised by Partners involved in the preparation of the Project Deliverable ☐ to be reviewed by applicable SECCRIT Partners ☐ for approval of the WP Manager ☐ for approval of the Project Co-ordinator	
Requested deadline	31/12/2014	

Versions			
Version	**Date**	**Change**	**Comment/Editor**
0	02/12/2014	Draft version and initial contents	Santiago Cáceres (ETRA)
1	09/12/2014	Update with information of SECCRIT partners	Santiago Cáceres (ETRA)
2	12/12/2014	Updated Standardisation Activities	Roland Bless (KIT), Simon Oechsner (NEC)
3	15/12/2014	Update Liaisons, UAB, Educational activities	Markus Tauber (AIT)
4	16/12/2014	Review	Petra Kölndorfer (AIT)
5	18/12/2014	Final version	Santiago Cáceres (ETRA)

Abstract

This document summarises the dissemination strategies for the SECCRIT project and the activities carried out during the second year of the project. The dissemination activities are divided into two main themes: scientific dissemination and general dissemination. General dissemination activities are maintaining the web site, producing brochures and newsletters. Scientific dissemination activities set out plans for publications/presentations in key conferences, workshops, magazines and journals.

Table of Contents

Table of Figures

1 Introduction

1.1 Purpose of the document

The SECCRIT dissemination plan is based on identifying and organising the activities to be performed in order to promote the project's results with the widest dissemination of knowledge from the project. Dissemination is a horizontal activity and concentrates on disseminating the results of the project itself to a wide range of existing or potential stakeholders. The SECCRIT consortium will promote project's results with:

- The dissemination of the project results in the scientific domain,
- The promotion of the project in the industrial world,
- The dissemination via centres and networks of excellence.

In addition, some advertising material has been developed and will be updated during the lifecycle of the project; in particular an interactive website and a Twitter profile will help to support both external dissemination and interaction between the project partners.

The aim is to form a critical mass of key industrialists and academics to promote the SECCRIT concept. Effective dissemination is important in order:

1. to make key individuals and groups aware of the work,
2. to enable them to understand the concepts and potential benefits, and
3. to obtain critical feedback from them to assess the perceived value of the approach.

1.2 Scope of the document

D7.2 is a key element to guide the consortium in the planning of all the dissemination and exploitation activities demanded by the project.

The templates used for the dissemination material were already produced and delivered at the Project Handbook and Website, D1.1 and D7.1. The Dissemination Report keeps a direct link with those documents, not only because of the templates used, but also because it settled the basis of the publication procedures and exchange of information.

Within the dissemination activities (WP7), there is a second but even more important link to Deliverable 8.2 – i.e., the website. It is one of the main tools for dissemination. Section 3.2 summarises graphically what can be found online, providing a description on the different information available in the Internet.

Last but not least, the table of publications and targeted conferences will be regularly updated at the Interim Management Reports (D1.x). In this way, it will be possible to keep track of the project progress with regards to the dissemination activities.

1.3 Structure of the document

The document is structured in six main sections. It starts with a short description on the general objectives of the dissemination and exploitation for the project and continues with the description of the general strategy and main means to promote the project results and SECCRIT approach.

The scientific dissemination has been considered as a special topic, due to the research nature of the project and the number of contributions that SECCRIT could make to the state of the art.

An important part of the dissemination strategy is the organisation of workshops and interaction with other groups working in the same research area.

The first sections cover the general strategy whereas chapter five lists the actual conducted activities.

2 Dissemination Objectives

The dissemination planned actions endeavour to create a large awareness of SECCRIT results in order to generate a worldwide market in which European players can expect to have an important role.

2.1 Target Audience

SECCRIT distinguishes between internal and external audiences.

2.1.1 Internal Audience

The internal audience of the SECCRIT project is directly involved in the project and comprises both academic and industrial SECCRIT partners and the European Commission:

- **Academic Partners**
  - Karlsruhe Institute of Technology
  - Lancaster University
- **Research Technology Organisations**
  - Austrian Institute of Technology
  - Fraunhofer IESE
- **Industrial Partners**
  - ETRA Investigación y Desarrollo
  - NEC Europe
  - Mirasys
  - Hellenic Telecommunications Organisation – OTE
  - AMARIS Technologies
- **End Users / Public Institutions**
  - Ayuntamiento de Valencia
- **European Commission**

2.1.2 External Audiences

The external target audience is not directly involved in the SECCRIT project and an indicative initial list comprises of:

- Research Communities
- Industry
- Other FP7 projects
- Standardisation Bodies and Alliances
- Students interested in the research areas identified above

- General Public
    - Potential customers that might buy services supported by SECCRIT developments
    - End users of applications that benefit result from SECCRIT result
- Citizens representations bodies

2.2 Dissemination Objectives

The dissemination plan's main objectives follow four levels of impact:

Level 1: Dissemination objectives within SECCRIT consortium (Internal communication)

The main objectives for the dissemination activities are to ensure and establish:

- Clear channels of responsibility between the coordinator, the different management bodies and the SECCRIT consortium.
- Install a functional and a secure knowledge management system through the implementation of a web collaborative platform to allow easy and efficient information transfer between SECCRIT partners.
- Identify and establish contacts with additional projects of interest to the research activities of SECCRIT.

Level 2: Dissemination activities towards the scientific community (External communication)

The main objectives for the dissemination activities towards the scientific community are to:

- Identify suitable relevant scientific papers to inform scientist community of SECCRIT research results (cooperative systems).
- Identify suitable congresses or seminars to inform the objectives and scope of SECCRIT project.
- Plan and execute joint meetings and workshops with suitable projects to promote research exchange and share knowledge.
- Identify suitable collaboration projects relevant to SECCRIT.

Level 3: Dissemination activities towards society

The main objectives for the dissemination activities in Level 3 are to:

- Identify other stakeholders who would benefit of the knowledge acquired by the SECCRIT consortium.
- Establish a correct communication towards the identified stakeholders.

Level 4: Dissemination activities towards industry

The main objectives for the dissemination activities in Level 4 are to:

- Establish contacts with industrial associations on national and European level.
- Attendance to main international events relevant to SECCRIT.

The above objectives, and the means to achieve them, are tackled considering the different dissemination materials and actions available to promote the project. If the target audience identified in the previous section is considered, different strategies and goals can be pointed out:

Internal Target Audience

- Share knowledge within the consortium, focus consortium on research goals.
- Dissemination of knowledge within the consortium is crucial for the success of the project. A group collaboration tool (Redmine) is used as repository for all SECCRIT relevant documents and allows fast and easy access via the Internet. Furthermore, project meetings (Intra-WP, Inter-WP, and consortium meetings) will be held regularly to disseminate results within the consortium and to focus all partners on the research goals. Intra-WP meetings are only considered as dissemination meetings if two or more organisations are involved.
- Furthermore, the research addressed in SECCRIT can be useful for other departments and units within each of the involved organisations. Internal promotion does not only serve to grant an efficient collaboration among partners in the consortium, but also to extend the results of the project internally. In this way, synergies may arise with other research or business groups that could help the taking over of the project after its finalisation.

External Target Audience

- Make target audience aware of SECCRIT.

  This is a primary dissemination goal since it is a prerequisite to achieve further goals. A various number of means will be used for this purpose including the SECCRIT website, participation at conferences and workshops, presentation of SECCRIT at trade fairs and exhibitions, distribution of leaflets, fact sheets, posters etc.

- Share results with other research groups.

  The SECCRIT approach and results will be presented to other research groups (in particular other FP7 projects) working on alternative approaches to gain feedback and to ensure that the results will converge to a maximum extent. Hence, SECCRIT will participate in and/or organizes scientific conferences and workshops.

- Promoting deployment of SECCRIT results.

  The primary target audience for the deployment of SECCRIT results is the SECCRIT User and Advisory Group.

- Attracting students to participate in the SECCRIT project.

  All participating research organisations will incorporate research results in their courses thereby promoting and disseminating the idea and content of SECCRIT. These activities will attract students to participate in the SECCRIT project, e.g. by choosing their PhD, Bachelor's or Master's thesis from the SECCRIT field.

The dissemination objectives and means depend on the target audience. The following table summarizes the dissemination goals and means for the identified audiences.

Audience	Dissemination Goals	Dissemination Means
Academic and Industrial Partners	Share knowledge, focus on research goals.	Distribution of documents via group collaboration tool, project meetings and internal presentations to other units and departments.
Research Communities	Share knowledge, gain feedback.	Conferences and workshops; papers, posters and brochures.
Industry	Share knowledge, gain feedback, promoting deployment of SECCRIT results.	Workshops, conferences, exhibitions and trade fairs, posters and brochures.
Other FP7 and H2020 projects	Share knowledge, gain feedback, establish cooperation.	Joint workshops, conference tracks, research visits.
Students	Attract students to participate in SECCRIT project.	Lectures.
General Public	Inform general public about key ideas of SECCRIT.	Website, social networks, brochures, and public demonstrations.
Citizens representations bodies	Involve decision makers in the project in order to promote the saving of energy through the neighbourhood approach proposed by the project	Interest Group, Website, flash animations, brochures, video (YouTube) and public demonstrations

TABLE 1 - DISSEMINATION STRATEGY DEPENDING ON TARGET AUDIENCE

3 Strategy for General Dissemination

The strategy for general dissemination – not scientific specific – is first based on the promotion of a common corporative identity for the project in order to facilitate the identification of any SECCRIT material and result. This is done not only by creating a project logo and a visual identity, but also making use of a common set of templates to publish information internally and externally.

3.1 SECCRIT Identity

3.1.1 SECCRIT Logo and Acronym Usage

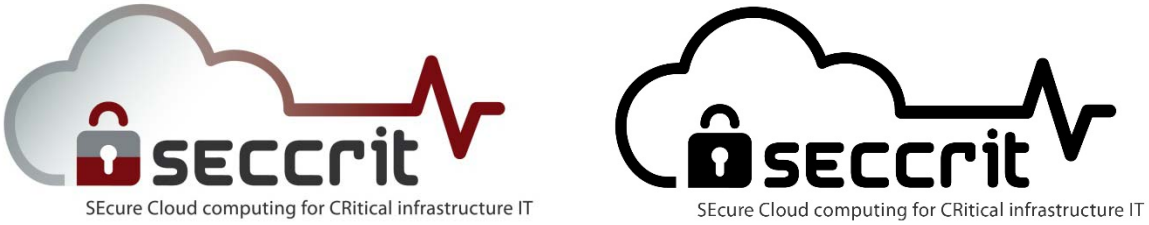


FIGURE 1: SECCRIT LOGOS

It is advised that the SECCRIT logo appears in all SECCRIT related documents. Any material co-funded with the project budget needs to make explicit reference to it and if possible make use of the SECCRIT logo. It has been developed in two different types in order to be able to use it in different formats and for different purposes.

In this way, the first logo is the official and corporative image of the project to be used by default. The acronym of the project – i.e., SECCRIT – is the main representative mark. When possible it has to be used with the above mentioned logo, respecting the fonts and colours. Otherwise, it should be written with capital letters.

3.1.2 Templates for Documentation and Presentation

As already explained, the templates for documentation and presentation were part of the contents included in the Project Handbook, and are available since Month 3 of the project.

3.2 SECCRIT Web Site

The SECCRIT website (http://www.seccrit.eu) is the main general dissemination tool, available to anyone with access to the Internet. It all serves as a distribution channel of the rest of dissemination material: brochures, presentations, posters, videos, etc.

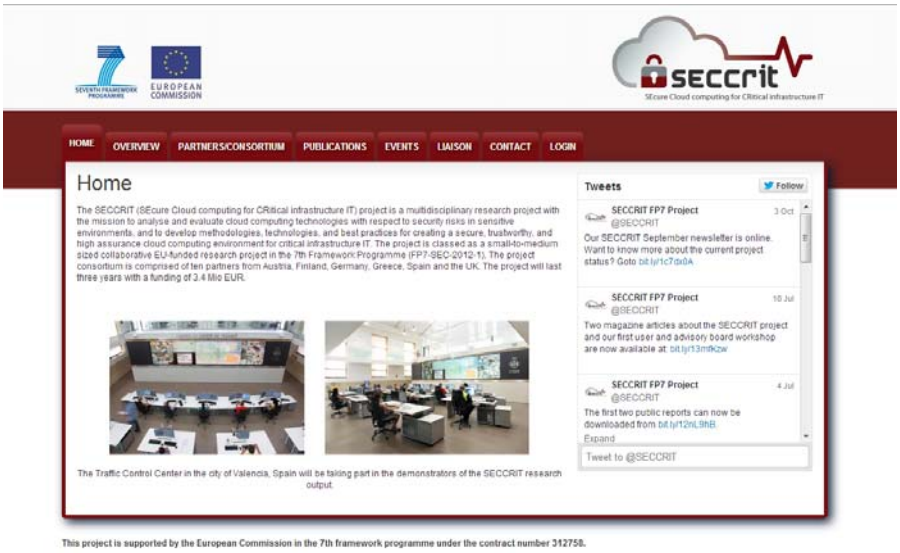


FIGURE 2: SECCRIT WEB SITE

The website will be periodically updated with news and summaries on the progress of the project.

All the website transactions are logged, in order to track any kind off attack, wrong usage or similar situations.

The public space of the project website includes a description of the project; the available sections are the following ones:

- **HOME**: This section is the homepage and contains a general brief description of the project, as well as a feed to the SECCRIT Twitter account where news about the project is publicly published.
- **OVERVIEW**: more details of the project are given in this section, including main outcomes and description of the work carried out in each work package.
- **PARTNERS CONSORTIUM**: Description of the project consortium members.
- **PUBLICATIONS**: An updated list of publications including:
    - Newsletters
    - Public Deliverables
    - Presentations at different events
    - Peer Reviewed Scientific Papers
- **EVENTS**: This section contains all the events internal and external to the project that keep a tight relation with SECCRIT, including the project workshops, industrial seminars, summer schools and academic seminars.
- **LIASION**: This section introduces the SECCRIT User and Advisory Board as well as the liaisons established with other projects and initiatives.
- **CONTACT**: This section contains the contact details of the project.
- **LOGIN**: Access to private area for administrators.

3.2.1 Private area and repository

The website has a private area accessible to the members of the consortium that enables the publication of events, and to upload publications and deliverables.

Last but not least, in addition to the private area, each partner in the consortium has access to a project repository where documents, deliverables, templates, etc. are stored and exchanged. This part of the website is not directly accessible from the homepage in order to maximise security. Each project participant has a username and a password, providing unrestricted access to all the folders and files.

3.3 Social Networks

In order to maximise the awareness and impact of the project, the project consortium has set up a profile account for the SECCRIT project in Twitter (https://twitter.com/SECCRIT), and it is connected with the SECCRIT webpage by providing news to the HOME section.

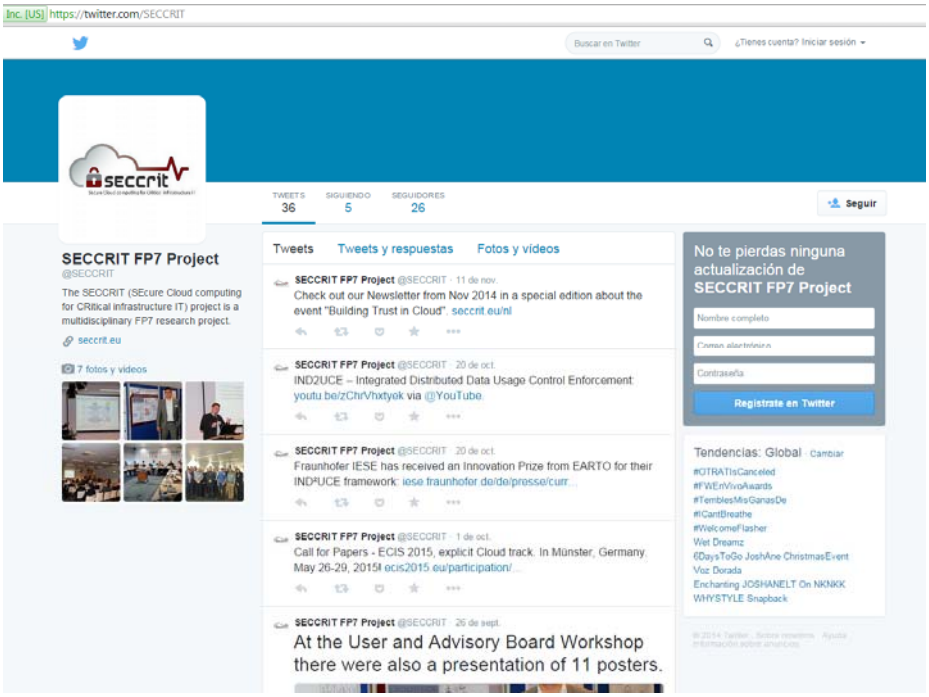


FIGURE 3: SECCRIT @ TWITTER

FIGURE 4: TWITTER FEED IN SECCRIT WEB PAGE

3.4 SECCRIT Newsletters

There are periodic newsletters containing summaries of the project's achievements. The newsletter are distributed by any of the consortium members participating at European or national events dealing with related subjects by e-mail to the User and Advisory Board members and relevant bodies.

3.5 SECCRIT Lectures

The SECCRIT project is being presented in several courses at different universities. The goal is to attract students to contribute to SECCRIT, e.g., by choosing their PhD, Master's or Bachelor's thesis from the field of SECCRIT.

The preliminary list of universities where lectures could be given includes, obviously, the academic institutions participating in the project.

4 Strategy for Scientific Dissemination

The considerations made above for general dissemination should be considered also for the specific scientific strategy.

4.1 Journals and Magazines

The journal publications are planned for the later phase of the project when the results and findings of the project research will be available. The SECCRIT project consortium will target scientific journals and magazines to disseminate its research results and findings.

Some relevant Security Journals include (but are not limited to):

- International Journal of Secure Software Engineering (IJSSE)
- Computers and Security (Elsevier)
- IEEE Security and Privacy
- International Journal of Information Security (Springer)

Some relevant Service- and Cloud Computing Journals include (but are not limited to):

- IEEE Transactions on Services Computing
- Journal of Services and Cloud Computing
- International Journal of Cloud Computing

4.2 Conferences and Workshops

The list of conferences and workshops relevant to the project is kept updated on the website and SECCRIT repository. Each partner detecting a new opportunity is expected to circulate the information to the consortium, update the List of Conferences Table and, if possible, upload to the repository the relevant Call for Papers.

The objective is to be present – through the submission of papers and posters – in the most relevant conferences.

Some relevant Security Events include (but are not limited to):

- IEEE Symposium on Security and Privacy
- ACM Conference on Computer and Communications Security
- Usenix Security Symposium
- ISOC Network and Distributed System Security Symposium
- IEEE Computer Security Foundations Symposium
- The International Conference on Dependable Systems and Networks
- Annual Computer Security Applications Conference
- International Conference on Information and Communications Security
- ACM Symposium on Access Control Models and Technologies

- Some relevant Cloud Events include (but are not limited to):
- IEEE International Conference on Cloud Computing
- USENIX HotCloud (http://www.usenix.org/events/hotcloud/)
- The ACM Cloud Computing Security Workshop

4.3 Technical Reports

The public technical deliverable produced as a result of the project should also be considered and used as scientific dissemination output.

The editors of technical reports should keep in mind, when preparing the document, the dissemination level of the deliverable (Public, Restricted or Private). In the two first cases, the report should be as self-contained as possible, in order to facilitate the reading and understanding of the proposed scientific advances.

Public Technical Reports will be available at the website as well as whitepapers produced during the course of the project.

4.4 Publication procedure

Publication procedure must follow the rules already defined in D1.1 Project Handbook and Website.

5 List of Dissemination Activities Year 2

This section reports the activities carried out in the second year of the SECCRIT Project. To avoid redundant information we only provide a summary of Year 1: 11 Papers and 6 presentations.

5.1 Dissemination activities overview

5.1.1 Peer Reviewed Scientific Papers

1. Frederik Armknecht, Jens-Matthias Bohli, Ghassan O. Karame, Zongren Liu, Christian A. Reuter. Outsourced Proofs of Retrievability. In: *ACM Conference on Computer and Communications Security*. Nov. 2014.
2. Dan Dobre, Paolo Viotti, Marko Vukolic. Hybris: Efficient and Robust Hybrid Cloud Storage. In: *ACM Symposium on Cloud Computing.* Nov. 2014.
3. Manuel Rudolph, Christian Jung, Reinhard Schwarz. Security Policy Specification Templates for Critical Infrastructure Services in the Cloud. In: *the 5th International Workshop on Cloud Applications and Security (CAS'14).* December 2014 .
4. Sarita Paudel, Christian Wagner, Markus Tauber, Aleksandar Hudic, Wee-Keong. Categorization of Standards, Guidelines and Tools for Secure System Design for Critical Infrastructure IT in the Cloud. In: *CloudCom 2014*
5. Frank Pallas. An Agency Perspective to Cloud Computing. In: *GECON 2014*. Oct 2014
6. Paul Smith, Thomas Hecht, Marcus Schöller. Critical Services in the Cloud, understanding security and resilience risks. In: *RNDM 2014*.
7. P. Smith, A. Schaeffer-Fihlo, D. Hutchison, A. Mauthe. Management Patterns: SDN-Enabled Network Resilience Management. In: *IEEE/IFIP NOMS 2014.* May, 2014.
8. Noor-ul-hassan Shirazi, Steven Simpson, Angelos K. Marnerides, Michael Watson, Andreas Mauthe and David Hutchison. Assessing the Impact of Intra-Cloud Live Migration on Anomaly Detection. In: *CloudNet 2014*.
9. Aleksandar Hudic, Maria Krotsiani, Markus Tauber, George Spanoudakis and Andreas Mauthe. A Multi-Layer and Multi-Tenant Cloud Assurance Evaluation Methodology. In: *CloudCom 2014*. URL: http://2014.cloudcom.org/
10. Aleksandar Hudic, Thomas Hecht, Markus Tauber, Andreas Mauthe and Santiago Cáceres Elvira. Towards Continuous Cloud Service Assurance for Critical Infrastructure IT. In: *FiCloud 2014*. URL: http://scim.brad.ac.uk/~iawan/FiCloud-2014/
11. Roland Bless, Matthias Flittner. Towards Corporate Confidentiality Preserving Auditing Mechanisms for Clouds. In: *CloudNet 2014.*
12. Christian Jung, Andreas Eitel, Reinhard Schwarz. Enhancing Cloud Security with Context-aware Usage Control Policies. In: *CloudCycle 2014 Workshop on Provisioning and Management of Portable and Secure Cloud-Services*
13. Kirila Adamova, Dominik Schatzmann, Paul Smith, Bernhard Plattner. Anomaly Detection in the Cloud: The Challenges of Virtual Service Migration. In: *ICC 2014.* June 2014.

5.1.2 Under Submission

- Michael R. Watson, Noor-ul-hassan Shirazi, Angelos K. Marnerides, Andreas Mauthe and David Hutchison. Malware Detection in Cloud Computing Infrastructures. Submitted to: *IEEE Transaction on dependable and secure computing*
- Roland Bless, Matthias Flittner. Corporate Confidentiality Preserving Auditing Mechanisms for Clouds, Submitted to: Special Issue on “Cloud Networking” IEEE Transactions on Cloud Computing

5.1.3 Presentations

Title	Authors	Conference/ Workshop	Date
Secure Cloud Computing for Critical Infrastructure IT	Markus Tauber, Sergio Emanuele, Francesco Oliviero	CPExpo 2014 & SRC Security Research Conference 2014 (The global expo-conference on Community Protection), participating in the EC stand	09/12/2014
Secure Cloud Computing for Critical Infrastructure IT	Christian Wagner and Alex Hudic	ITSecX Conference	07/11/2014
SECCRIT Poster Presentation	Christian Wagner	IKT-Sicherheitskonferenz	04/11/2014
SECCRIT (SEcure Cloud computing for CRitical infrastructure IT)	Christian Wagner, Markus Tauber,	Building Trust in Cloud, 2014	6/2014
SECCRIT (SEcure Cloud computing for CRitical infrastructure IT)	Aleksandar Hudic, Christian Wagner	FS InfoSec Dialogue	12/2014
SECCRIT (SEcure Cloud computing for CRitical infrastructure IT)	Markus Tauber	CMG-AE Tagung, IT Sicherheit in kritischen Infrastrukturen und vernetzten Systemen	7/10/2014
Impact-of-VM-migration-on-AD	Noorulhassan Shirazi	Coseners 2014 (Next Neneration Networking, Multi-Service Networks workshop -UK Academic Meeting on Systems and Networks)	2014/07/10
Assurance in Multi-Layer Cloud Infrastructures	Aleksandar Hudic and Markus Tauber	Coseners 2014 (Next Neneration Networking, Multi-Service Networks workshop -UK Academic Meeting on Systems and Networks)	2014/07/10
Security Engineering and Software Development for Critical Infrastructure IT in the Cloud	Sarita Paudel, Markus Tauber, Ivona Brandic	AIT Poster Award 2014	2014/06/11

Security und Datenschutz in Cloud Computing	Christian Wagner	Austrian Trade Union Federation	24/06/2014
Vortrag Sicherheit im Netz (Cloud-Security)	Christian Jung	presentation at local industry event	2014/05/15
Towards Cloud Resilience: The Challenges of Virtual Machine Migration	Noor ul Hassan Shirazi, Steven Simpson and David Hutchison	"EINS Workshop on Understanding the inter-play between sustainability, resilience, and robustness in networks (USRR)	2014/06/01
Datennutzungskontrolle für Software-as-a-Service	Manuel Rudolph, Michael Eisenbarth	Jahrestagung der Software Technologie Initiative Kaiserslautern	2014/06/24

5.1.4 Completed Student Theses

Finishing Date	Title	Student	University	Supervisor	Start Date
August 2014	Infrastructure Auditing as Trust-building Measure for Cloud Computing: Development of an Independent Transparency-as-a-Service Component	Robert Bauer	KIT, Karlsruhe	Prof. Martina Zitterbart, PD Dr. Roland Bless, Matthias Flittner M. Sc.	15.2.2014
15.07.2014	Security Engineering and Software Development for Critical Infraatructure IT in the Cloud	Sarita Paudel	Vienna University of Technology	Priv.-Doz. Dr. Ivona Brandic, Dr. Markus Tauber	15.07.2013

5.1.5 Other Educational Dissemination Activities

In addition to the completed MSc Theses above, SECCRIT supports six Doctoral Theses in the Domain of Cloud Computing.

Silvia Balaban (KIT), Andreas Mauthe (ULANC), Christian Jung (IESE) and Markus Tauber (AIT) presented the SECCRIT project and their respective research topics as part of the lecture series “bits that byte” (www.bitsthatbyte) at the University of Applied Sciences in Eisenstadt (Austria) on the 26th of Sept. 2014.

5.2 User and Advisory Board

A User and Advisory Board has been established in order to get feedback from potential stakeholders. The board is pro-actively informed about research outputs via a mailing list through which they receive newsletters, status update emails and invitations to annual workshops.

The second SECCRIT User and Advisory Board workshop took place the 23rd of September 2014. Over 120 Cloud experts and stakeholders participated in the international symposium "Building Trust in Cloud" (http://www.buildingtrustincloud.org/) as part of which the second SECCRIT UAB workshop was organised. The event was organised together with EuroCloud Austria, Cloud4Europe 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.

Following the reviewers advice we have not aimed at increasing the UAB board as such, but had invited all visitors of the workshop to participate in a questionnaire. The focus of this questionnaire was to identify differences in the security requirements between industry and public administration and to support our work in Task 3.3 on the process oriented best practice guideline. More details of the workshop have been reported in the November issue of the SECCRIT regular newsletter.

We would like to highlight the huge number of attendants present in the meeting, a total of 119 participants coming from 85 different institutions.

5.3 Dagstuhl Seminar

The consortium submitted a proposal for a three day Dagstuhl seminar (http://www.dagstuhl.de/15151) entitled "Assuring Resilience, Security and Privacy for Flexible Networked Systems and Organisations". The seminar will be held from 2015-04-07 to 2015-04-10 at Dagstuhl, Germany. 28 international participants already confirmed their participation, some of the original invitees are still pending and additional 20 have been invited.

Goal of the seminar is to create a research agenda regarding above topics which is based on activities carried out in SECCRIT but is content wise going far beyond SECCRIT's current research agenda. IT systems' composability will in future encompass not only traditional office and industrial applications, but also new critical infrastructure applications. Using flexible service composition, computational work is increasingly done in a shared manner among different physical infrastructures and devices, virtualised resources and providers. This will soon be achieved with technologies based on the principles of what we refer to as "cloud computing" today. Furthermore, the omnipresence of composable and flexible services will result in the utilisation of devices currently not explicitly recognised as IT systems, including wearable devices, physical enhancement via IT or control devices in (critical) infrastructures, such as smart grids. In such applications, it is absolutely crucial to be able to assure security, privacy and perhaps above

all property of resilience, which is the ability to continue to provide the required – and indeed the legally contracted – quality of service to the system's users.

These multi-disciplinary challenges are highly interrelated and therefore have to be addressed by researchers and industry experts from different disciplines concurrently. Only individual aspects of the issues above have been investigated so far. Hence the goal of this seminar is to bring together researchers and engineers who can contribute to the overall goals of helping to create a research agenda in assuring resilience, security and privacy for networked systems and organisations.

5.4 Liaison and Standardisation activities

There are a number of projects with which SECCRIT has already established **liaison activities:**

- **Archistar** is a research project focusing on virtual cloud storage systems. It was agreed to pro-actively inform each other about research outputs.
- **PRECYSE** is an FP7 research project focused on cyber-security in CI. A total of three SECCRIT partners are participating on it (AIT, ETRA and Valencia), it has been already identified some areas where synergies will be explored, especially the risk assessment methodologies and the demonstrations in the traffic management centre in Valencia.
- **Cumulus** is a FP7 research project which focuses on assurance, it was decided after last year's UAB workshop that a researcher from the CUMULUS project will spend some time at AIT to support the assurance activities in order to avoid redundancies in the anticipated outputs. A result of this was a researcher exchange of Maria Krotsiani who worked with and at AIT on the following publication:
    - Aleksandar Hudic, Maria Krotsiani, Markus Tauber, George Spanoudakis and Andreas Mauthe. A Multi-Layer and Multi-Tenant Cloud Assurance Evaluation Methodology. In: IEEE CloudCom 2014. URL: http://2014.cloudcom.org/
- **EuroCloud** is an organisation offering audits and certificates for cloud infrastructure providers. It was decided to inform each other about relevant outputs and to give SECCRIT the possibility to address the members of EuroCloud with surveys. We have successfully organised a joint event with the EuroCloud Brunch in September 2014 together with our User and Advisory Board workshop (see Section 5.2).
- **CLOSER**, the 4th International Conference on Cloud Computing and Services Science, lists SECCRIT as academic partner, further interaction is planned.
- Another strategic liaison partner is the project **Cloud4Europe** (www.cloudforeurope.eu), in which public administration which is considered a critical infrastructure is focus.

The SECCRIT project's **standardization activities** are focusing on three SDOs: IETF, ONF, and ETSI. The details are depicted in the following subsections. In addition, ENISA is one of our User and Advisory Board members and they are an important dissemination target for SECCRIT outputs for example in the areas of cloud security, risk assessment and resilience.

5.4.1 IETF

The Internet Engineering Task Force (IETF) is an open standardisation body for Internet protocols, whose mission is to produce high quality, relevant technical and engineering

documents that influence the way people design, use, and manage the Internet in such a way as to make the Internet work better. The IETF work is organized in roughly 120 different working groups (WGs), of which some are doing standardisation work that is related to the secure cloud computing context of SECCRIT. Since the IETF mainly standardises protocols, but not architectures, the work may contain pieces that can be used as basis for SECCRIT solutions. NEC, ULANC, and KIT are active in the IETF contributing in various ways to its activities; we are below giving updates on the activities in the working groups identified in D7.1 as most relevant for SECCRIT.

The NVO3 (Network Virtualization Overlays) WG is working on practical networking problems within data centres that form the basis for physical cloud infrastructures. A number of drafts have been updated in this working group recently, including the general architecture description as well as a security draft that defines a catalogue of requirements for a secure networking infrastructure in a data centre. KIT and NEC are monitoring these activities and analyse the impact on SECCRIT.

Further working groups of interest in the SECCRIT context are MILE (Managed Incident Lightweight Exchange) that specified a standardised incident report format (useful to notify security incidents), as well as NEA (Network Endpoint Assessment), and SACM (Security Automation and Continuous Monitoring). The NEA WG defined protocols that support the assessment of the security "posture" of endpoint devices, whereby posture refers to the hardware or software configuration of an endpoint as it pertains to an organization's security policy. The work from the meanwhile concluded NEA WG could be useful for auditing and is taken as basis for SACM that works on assessment of endpoint posture for a whole environment (e.g., an enterprise). Though NEA and SACM are considering different environments, their work may be leveraged for performing audits within the SECCRIT context. KIT is monitoring these activities and analysing the impact on SECCRIT – the corresponding findings will be described in D5.3. Moreover, typical network monitoring and management WGs like IPFIX (IP flow information export – network monitoring) or NETCONF (Network Configuration – XML and RPC based configuration of network elements) standardised open protocols that could be used within the cloud infrastructure as well as within the (virtual) tenant infrastructure. The earlier work of the SYSLOG (Security Issues in Network Event Logging) WG is also applicable within SECCRIT's work on auditing and root cause analysis, e.g., SYSLOG defined mechanisms for signed log messages. Thus, it is for example planned to use this standard for the communication between the independent transparency enhancement framework (KIT) and the reliable storage (NEC) PoC.

The Service Function Chaining (SFC) working group was chartered at the end of 2013 and started its work in 2014. Several drafts, mainly related to the problem statement, definitions and use-cases, have been created in this WG. While there is no specific vision of service function chains being moved to the cloud, the goal of minimizing overhead in managing service chains corresponds to the advantages of virtualization and cloud computing. Thus, the SFC use cases form an additional use-case for SECCRIT.

In addition to existing working groups, SECCRIT members continue to monitor IETF BOFs – discussion groups which might lead to a working group in the near future. One recent activity in this respect was the I2NSF (Interface to Network Security Functions) BOF that discusses interfaces for clients (e.g., enterprises) to request, negotiate, operate, and/or verify network security functions from a provider. Such functions could be firewalling, DDOS/Anti-DOS measures, access control/authorization/authentication, identity and secure key management, or Intrusion Detection/Prevention Systems (IDS/IPS). Such functionality is useful in a SECCRIT context, but assurance that the requested functions are actually working and available is something that could be checked by the independent transparency framework.

5.4.2 ONF

Open Networking Foundation (ONF) is a standardization body dedicated to the promotion and adoption of Software-Defined Networking (SDN). SDN is a new approach to networking in which network control is decoupled from the data forwarding functionality using a protocol such as OpenFlow. The expected result is an extremely dynamic, manageable, cost-effective, and adaptable architecture that gives administrators unprecedented programmability, automation, and control. A dominant use-case of OpenFlow is data-centre operation and management as well as cloud infrastructure management. The OpenStack Quantum plugin implements the OpenFlow specification to provide network connectivity to VMs. NEC is a leading contributor to ONF.

As identified in D7.1, the OpenFlow Security discussion group is continuing to be of particular interest in the context of the SECCRIT project. Recently, it has been mainly producing threat analysis and security requirements for securing the control protocols and interfaces, and establishing best practices for securing SDN implementations. Here, it is of interest that similar issues as in SECCRIT have been identified, namely, the problem of breaking up administrative domain boundaries by allowing clients access to the infrastructure (in this case the network), and the continued and increased necessity for multi-tenant isolation. Moreover, the security group has recognized as well the importance of auditability and logs. This, on the one hand, confirms the value of the according clusters in SECCRIT, and on the other hand is complementing this work in the key area of networking and network virtualization in the cloud.

5.4.3 ETSI ISG NFV

The European Telecommunications Standards Institute (ETSI) has established an Industry Specification Group (ISG) for Network Function Virtualisation (NFV) in late 2012. NFV aims to leverage standard IT virtualisation technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in Datacentres, Network Nodes and in the end user premises – in other words network functions are moved from purpose-built hardware to the cloud. This activity encompasses any data plane packet processing and control plane function in fixed and mobile network infrastructures. Within the ISG a working group on ‘Reliability and Availability’ was created to analyse gaps in technology, which hinder the transition from purpose-built hardware to the cloud and to define requirements for dependability and fault management. Dr. Marcus Schöller (NEC) was vice-chair to this group providing a strong link between this international activity and the SECCRIT project.

The final deliverables of the first phase of the ISG are to be published in January 2015. NEC and ULANC have been active in the ISG, and have provided direct input to the standardization process by contributing to the draft document on resiliency requirements (Draft ETSI GS NFV-REL 001[1]). In particular, contributions to resiliency requirements and fault management were made, and the Fault and Challenge Catalogue, one of the main results from WP3, was included in the draft. The draft document containing these contributions has been accepted for publication and will thus become officially published as well by January 2015.

In addition, the expert group on ‘Security’ was monitored. This group focuses on differences with respect to security of the aforementioned transition, i.e., protection of previously private interfaces that become exposed by running on the cloud.

The original charter of the ISG was planned to expire in January 2015. However, a continuation of the work (Phase 2) is planned, but the details on the specifics of this group are still discussed.

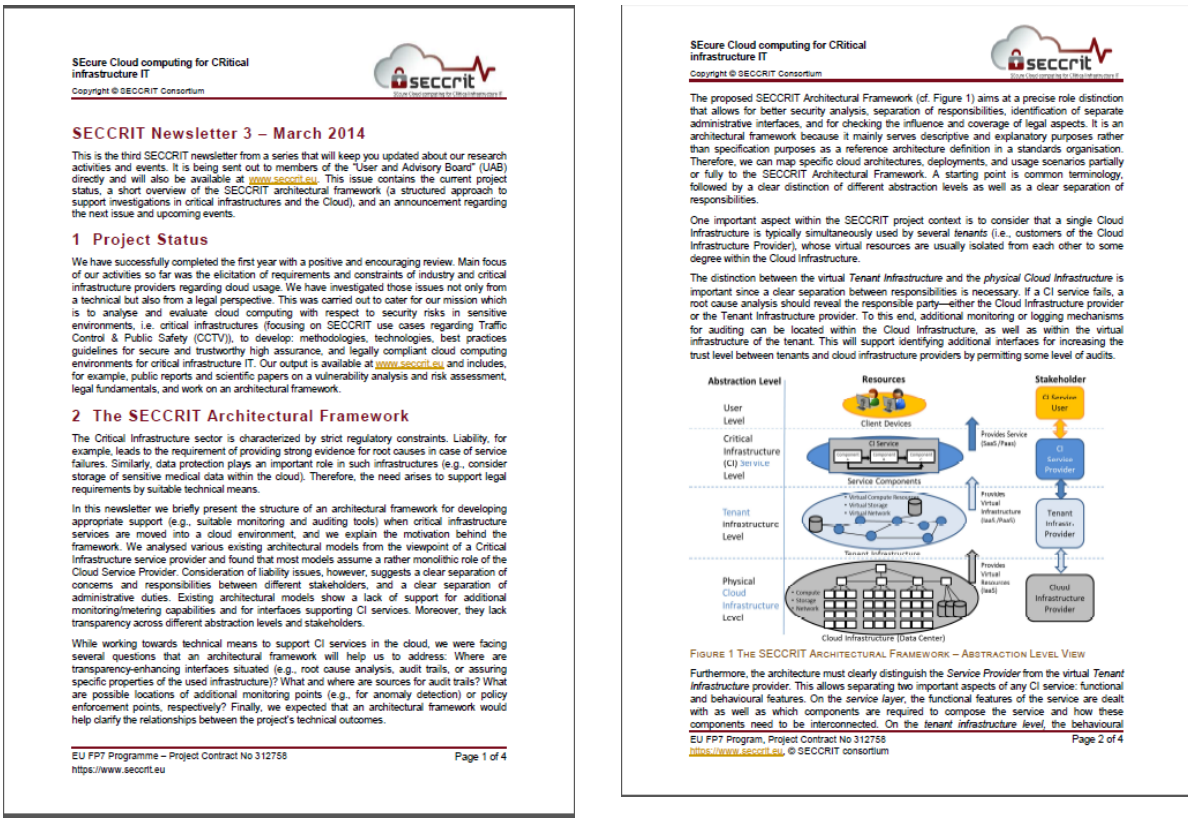
[1] http://docbox.etsi.org/ISG/NFV/Open/Latest_Drafts/nfv-rel001v100%20resiliency%20requirements.pdf

Due to the success of the interaction between the project and Phase 1, delegates will continue to evaluate the possibilities for SECCRIT project result promotion in Phase 2.

5.5 Newsletters

Three newsletter issues were produced during the second year of the project. They were distributed among the User and Advisory Board mailing list and are available on the project website.

The third newsletter was released on March 2014 and contains a short overview of the SECCRIT architectural framework.



SEcure Cloud computing for CRitical infrastructure IT

Copyright © SECCRIT Consortium

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.

EU FP7 Programme – Project Contract No 312758 Page 1 of 4
https://www.seccrit.eu

SEcure Cloud computing for CRitical infrastructure IT

Copyright © SECCRIT Consortium

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.

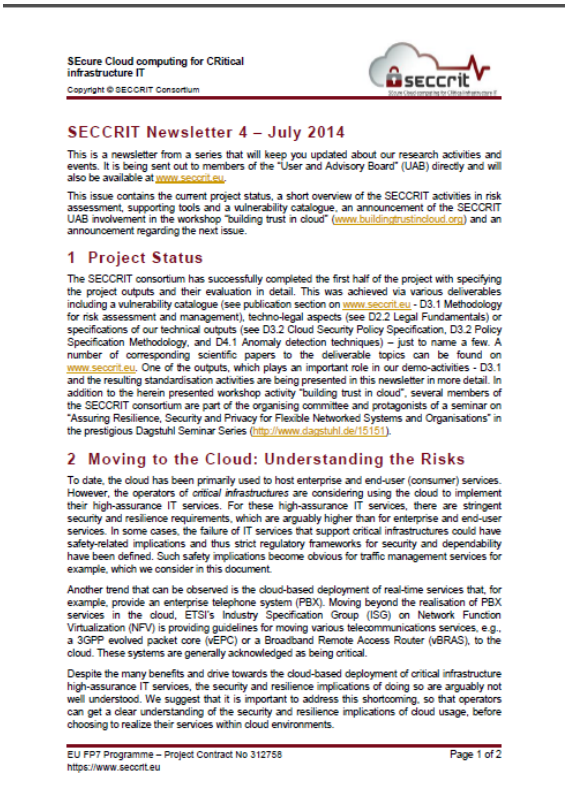
FIGURE 1 THE SECCRIT ARCHITECTURAL FRAMEWORK – ABSTRACTION LEVEL VIEW

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

EU FP7 Program, Project Contract No 312758 Page 2 of 4
https://www.seccrit.eu, © SECCRIT consortium

FIGURE 5: SECCRIT NEWSLETTER #3

The forth newsletter was released on July 2014 and contained a short overview of the SECCRIT activities in risk assessment, supporting tools and a vulnerability catalogue, an announcement of the SECCRIT UAB involvement in the workshop “Building Trust in Cloud”.



SEcure Cloud computing for CRitical infrastructure IT

Copyright © SECCRIT Consortium

SECCRIT Newsletter 4 – July 2014

This is a 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 activities in risk assessment, supporting tools and a vulnerability catalogue, an announcement of the SECCRIT UAB involvement in the workshop "building trust in cloud" (www.buildingtrustincloud.org) and an announcement regarding the next issue.

1 Project Status

The SECCRIT consortium has successfully completed the first half of the project with specifying the project outputs and their evaluation in detail. This was achieved via various deliverables including a vulnerability catalogue (see publication section on www.seccrit.eu - D3.1 Methodology for risk assessment and management), techno-legal aspects (see D2.2 Legal Fundamentals) or specifications of our technical outputs (see D3.2 Cloud Security Policy Specification, D3.2 Policy Specification Methodology, and D4.1 Anomaly detection techniques) – just to name a few. A number of corresponding scientific papers to the deliverable topics can be found on www.seccrit.eu. One of the outputs, which plays an important role in our demo-activities - D3.1 and the resulting standardisation activities are being presented in this newsletter in more detail. In addition to the herein presented workshop activity "building trust in cloud", several members of the SECCRIT consortium are part of the organising committee and protagonists of a seminar on "Assuring Resilience, Security and Privacy for Flexible Networked Systems and Organisations" in the prestigious Dagstuhl Seminar Series (http://www.dagstuhl.de/15151).

2 Moving to the Cloud: Understanding the Risks

To date, the cloud has been primarily used to host enterprise and end-user (consumer) services. However, the operators of *critical infrastructures* are considering using the cloud to implement their high-assurance IT services. For these high-assurance IT services, there are stringent security and resilience requirements, which are arguably higher than for enterprise and end-user services. In some cases, the failure of IT services that support critical infrastructures could have safety-related implications and thus strict regulatory frameworks for security and dependability have been defined. Such safety implications become obvious for traffic management services for example, which we consider in this document.

Another trend that can be observed is the cloud-based deployment of real-time services that, for example, provide an enterprise telephone system (PBX). Moving beyond the realisation of PBX services in the cloud, ETSI's Industry Specification Group (ISG) on Network Function Virtualization (NFV) is providing guidelines for moving various telecommunications services, e.g., a 3GPP evolved packet core (vEPC) or a Broadband Remote Access Router (vBRAS), to the cloud. These systems are generally acknowledged as being critical.

Despite the many benefits and drive towards the cloud-based deployment of critical infrastructure high-assurance IT services, the security and resilience implications of doing so are arguably not well understood. We suggest that it is important to address this shortcoming, so that operators can get a clear understanding of the security and resilience implications of cloud usage, before choosing to realize their services within cloud environments.

EU FP7 Programme – Project Contract No 312758 Page 1 of 2
https://www.seccrit.eu

SEcure Cloud computing for CRitical infrastructure IT

Copyright © SECCRIT Consortium

In the SECCRIT project, we have developed an extensive cloud-specific threat and vulnerability catalogue that can be used to shed light on this issue. Entries in the catalogue are organised into categories that relate to different aspects of cloud usage; the core of this categorisation are NIST's essential cloud characteristics. The entries in the catalogue were derived via the systematic analysis of related work, such as that produced by the Cloud Security Alliance (CSA), and the SECCRIT architectural framework, which is targeted to support high-assurance services, such as those from the telecommunications sector. The catalogue can be used as input to a risk assessment method for determining the security and resilience of cloud usage. To support this, we have developed an extension to a risk assessment method that operators can use to understand the risks that are specifically associated with cloud usage. The SECCRIT threat and vulnerability catalogue can be downloaded from the project's homepage in a format that can be imported into the open-source information security management tool Vernice (http://www.vernice.org). Additionally, a description of the entries in the catalogue and the different entry types can be found in the project deliverable D3.1 on a "Methodology for Risk Assessment." Furthermore, in the deliverable, we describe the extended risk assessment process and how it can be realised using the Verinice tool. In order to address a need for understanding the threats and vulnerabilities associated with Network Functions Virtualization, we have applied the SECCRIT catalogue to the architectural model that is being developed by the ETSI ISG on NFV. This process involved assigning vulnerabilities to the components in the architecture and threats to the interfaces they expose.

CATEGORIES IN THE SECCRIT THREAT AND VULNERABILITY CATALOGUE

3 UAB workshop @ Building Trust in Cloud

The Second UAB workshop will take place on the 23rd of September 2014, during a joint event with other major organisations and projects in the cloud community. Organising parties are:

- the SECCRIT consortium, which focuses on cloud for critical infrastructures
- EuroCloud who represents a striving community for cloud provider certification – the event will be in conjunction with EuroCloud's quarterly EuroCloud brunch
- EURITAS together with BRZ who represent the governmental cloud infrastructure provider also partners on the FP7 project CloudforEurope, which identifies obstacles, finds innovative solutions and builds trust in European cloud computing.

Additionally, work from other projects will be presented within poster sessions. An overall goal is it to get feedback for the individual initiatives and projects from potential beneficiaries and experts on the outputs and to discuss issues relevant for shaping the future of cloud computing. More information and a registration opportunity can be found at http://www.buildingtrustincloud.org.

4 Next Issue

The next issue of this newsletter is planned for Q4 2014, and will focus on details of further SECCRIT outputs and on more cloud community and standardisation activities. In the meantime, we will keep you updated via the SECCRIT webpage and twitter (@SECCRIT). UAB Members are invited to send us feedback directly or via our emailing list at any time.

EU FP7 Program, Project Contract No 312758 Page 2 of 2
https://www.seccrit.eu, © SECCRIT consortium

FIGURE 6: SECCRIT NEWSLETTER #4

The fifth newsletter was released on November 2014 and contained a special edition about the SECCRIT UAB involvement in the workshop “Building Trust in Cloud”.

SEcure Cloud computing for CRitical infrastructure IT

Copyright © SECCRIT Consortium

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

EU FP7 Programme – Contract No. 312758
https://www.seccrit.eu

Page 1 of 3

SEcure Cloud computing for CRitical infrastructure IT

Copyright © SECCRIT Consortium

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.

EU FP7 Programme – Contract No. 312758
https://www.seccrit.eu

Page 2 of 3

FIGURE 7: SECCRIT NEWSLETTER #5