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

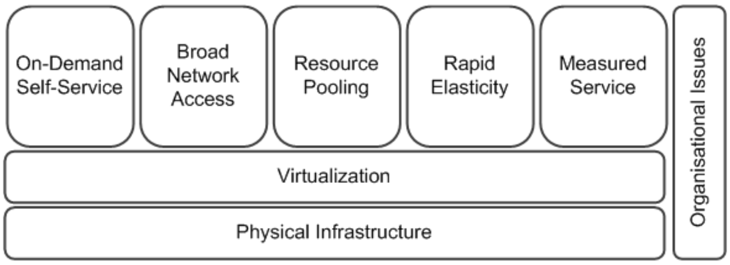
The SECCRIT consortium has successfully completed the first half of the project with specifying the project outputs and their evaluation in detail. This was achieved via various deliverables including a vulnerability catalogue (see publication section on www.seccrit.eu - D3.1 Methodology for risk assessment 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.



CATEGORIES IN THE SECCRIT THREAT AND VULNERABILITY CATALOGUE

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 Verinice (http://www.verinice.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.

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.