Celtic-Plus
Smart Connected World

Project Information

SEED4C

Seed4C

Project ID: CPP2011/2-6

Start Date: 1 April 2012

Closure date: September 2014

Partners:

Alcatel-Lucent Bell Labs, France

Gemalto SA, France

ENSIB, France

INRIA, France

Wallix, France

Cygate, Finland

Mikkelin Puhelin Oy, Finland

Nokia Siemens Networks Oy, Finland

Finceptum Oy (Novell Suomi), Finland

VTT Technical Research Centre of Finland, Finland

SOLACIA, Korea

Innovalia Association, Spain

Nextel S.A, Spain

Software Quality Systems (SQS), Spain

Findación Vicomtech, Spain

IKUSI (Ángel Iglesias, S.A.), Spain

BISCAYTIK, Spain

Co-ordinator:

Bertrand Marquet

Alcatel-Lucent Bell Labs, France

E-mail: bertrand.marquet@alcatel-lucent.com

Project Website

www.celticplus.eu/project-seed4c

Security Embedded Element and Data privacy for Cloud

The cloud security challenge not only reflects on the secure running of software on one single machine, but rather on managing and guaranteeing security of a computer group or cluster seen as a single entity.

Seed4C focus is to evolve from cloud security with an isolated point or centralized points of enforcement for security to cloud security with cooperative points of enforcement for security.

Main focus

The current state of the art regarding security of cloud based services and infrastructure is based on isolated points of enforcement of security and policies.

The project approach is centred on security enhancement in the cloud from a cooperative enforcement standpoint. As a consequence, the concept of Network of Secure Elements (NoSEs) is introduced in Seed4C.

NoSEs are made of individual secure elements attached to computers, user or network appliances and possibly pre-provisioned with initial secret keys. They can establish security associations, communicate together to setup a trusted network of computers and propagate security conditions centrally defined to a group of machines.

The range of use cases addressed by this concept is very broad; NoSEs can be used to lock the execution of software to a group of specific machines, a particular application of this pertaining to tying virtual machines execution to specific servers. NoSEs can also be used to improve the security of distributed computing by certifying the integrity of the results returned by each one of them. Secure elements located in user appliances (such as a mobile handset) featuring a user interface can be part of a NoSE and help secure server side operations using two factors authentication.

The project will study the impact of NoSEs upon the different layers of the architecture, from hardware to service in order to define how the trust can be propagated from the lower layers to the upper ones.

Approach

The project's approach is divided into three levels:

Distribution of Secure Elements (SE) in the infrastructure and provide added value to platform and services. Study of the three layers of the Cloud (from hardware to service in order to define how the trust of the low levels can benefit to upper layers and development of consistent security policies at the different layers. For each layer, Management, Security Assurance and Monitoring functions are connected to offer an in depth security solution.

Secure load balancing and communication between SEs and from SEs embedding machines. This include transferring applications into another virtual machine on the same server with SEs, transferring applications into another machine with embedded SEs, and transferring applications into another machine without SEs. Communication between SEs in a NoSE will be studied at this point.

Policies execution, traceability and at the end assurance of services. The project will analyse the interaction between SEs and external software components executed on the network. These components encompass policy definition systems, identity and access control components, and management servers. The project will also be centred on tools and methods for the collection and tracing of different types of privacy-related information, as well as the validation of security, privacy and trust of the NoSEs.

Main results

The main results expected from the SEED4C project are enumerated in the following lines:

A new reference model for cloud security architecture where cooperative points of enforcement will play a pivotal role.

Protocols development for security elements communication, interaction and management. The management infrastructure will cover the full NoSE lifcycle. In addition, this middleware will address the policy execution and communication with local security elements.

SaaS and PaaS APIs will be implemented. This outer middleware will encompass the connection to the cloud stack layers as it is defined in the aforementioned architecture.

New privacy and identity policy mechanisms will lead to an increase of transparency between cloud service providers and users.

Novel architectural solutions for end-to-end trust management required for security assurance and monitoring solutions of secure element architecture will be deployed.

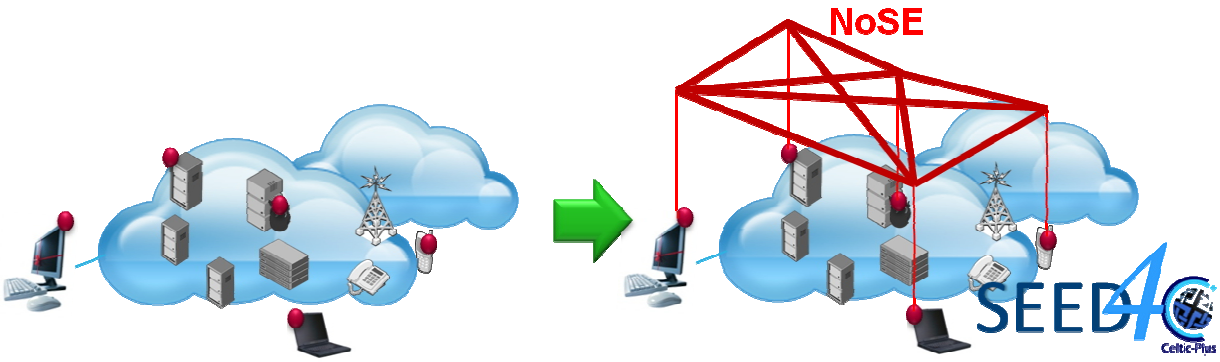
A demonstrator will be implemented over INRIA's Grid'5000 test bed, already used in cloud experiments extracted from the OpenNebula project.

Impact

The project ambition is to give answer within the European Cloud strategy and bring industrials means to compete against major us companies that currently drive the cloud market where security can be a major differentiator for telecom providers moving into cloud infrastructures.

The project will aim to develop more efficient and effective security solutions in cloud environments and will address the assurance of end-user security for real life in cases such as eGovernment or airport management services. Thus, SEED4C intends to contribute with significant advances in cloud services security, preserving users' privacy and enhancing trust between different stakeholders. Thanks to the plurality of the consortium and the different countries represented, the results will be disseminated and introduced in a myriad of scenarios.

In terms of industrial competition, the cloud market is currently led by large U.S. organizations. Europe needs a coordinated response and telco providers, which are becoming Cloud providers, to play a major role. Big European operators such as Telefonica, Orange, BT, DT could become involved and built together a first credible European cloud infrastructure before 2015. In this context, the SEED4C project can provide some important security bricks to this environment.



Isolated Security
by secure elements or not

Coordinated Security
by Network of Secure Elements (NoSE)

About Celtic-Plus

Celtic-Plus is an industry-driven European research initiative to define, perform and finance through public and private funding common research projects in the area of telecommunications, new media, future Internet, and applications & services focusing on a new „Smart Connected World" paradigm. Celtic-Plus is a EUREKA ICT cluster and belongs to the intergovernmental EUREKA network. Celtic-Plus is open to any type of company covering the Celtic-Plus research areas, large industry as well as small companies or universities and research organisations. Even companies outside the EUREKA countries may get some possibilities to joine a Celtic-Plus project under certain conditions.

Celtic Office

c/o Eurescom, Wieblinger Weg 19/4
69123 Heidelberg, Germany
Phone: +49 6221 989 210
E-mail: office@celticplus.eu
www.celticplus.eu

EUREKA