



SECURED

SECURity at the network EDge



Motivation

People use different networked devices in their everyday activities, including tablets, computers, and smartphones, but also interact with smart-objects and Internet-of-Things elements.

However, **all these devices – and hence their users – do not experience coherent and robust protection** from network threats as they have different capabilities, architectures and available applications.

Objectives

SECURED will offer consistent protection by **offloading security applications** from the end-point devices to a trusted and secure node at the edge of the network.

Additionally it will establish the conditions for a **marketplace of security applications**, to stimulate innovation and competition.

Expected results

SECURED will design an integrated architecture for providing consistent protection to end users, independently from the terminal they use and their network technology and location.

This will be enabled by novel protocols and personal security mechanisms, in a general framework of network functions virtualization.

Open-source proof-of-concept prototypes will be developed and used for evaluation in near real-life pilots.

Technical approach

The SECURED work plan focuses on three main components: a novel class of network devices, user-oriented security policies, and policy-driven applications.

A trusted and secure **Network Edge Device (NED)** is charged with execution of the security software selected by the end users for their protection. The NED exploits various trust technologies to provide users with strong guarantees about the software executed at this node. Security and privacy are guaranteed also by technologies that offer no possibility for intercepting or modifying the user's traffic before it's processed by the NED.

Security policies will offer also to non-experienced users the ability to configure the desired level of protection through human-friendly paradigms (e.g. web interfaces, high-level languages). User policies are then automatically mapped to the appropriate security configuration.

User-selected **policy-driven security applications** will be executed on the NED to enforce the desired level of protection according to the user policy. APIs for the independent development of security applications will be provided, along with an open web-based marketplace for such applications.

Validation is foreseen with users selected among the partners' customers. However validation of the SECURED architecture with different use cases or technologies is welcome: interested parties are invited to contact the Coordinator.

Fact sheet

Duration: October 2013 – September 2016
Funding scheme: STREP
Total cost: 4.1 M €
EC contribution: 2.7 M €
Contract number: 611458
Project website: www.secured-fp7.eu

Project Coordinator
Prof. Antonio Lioy
Politecnico di Torino, Italy
Tel: +39 011-090-7021
Fax: +39 011-090-7099
Email: coordinator@secured-fp7.eu

Partners

The consortium includes 7 partners from 5 different countries, with a good mix of leading research universities, major ICT companies, and user representatives.

1



Politecnico di Torino
(Torino, Italy)

2



Hewlett-Packard Limited
(Bristol, United Kingdom)



3

Primetel
(Limassol, Cyprus)

5



**United Nations Interregional
Crime and Justice Research
Institute** (Torino, Italy)

4



**Telefónica Investigación y
Desarrollo** (Madrid, Spain)

6



**Universitat Politècnica de
Catalunya** (Barcelona, Spain)

7



**VTT Technical Research Centre
of Finland** (Oulu, Finland)

