Objective

Develop a dynamic and scalable framework to support trustworthy services and applications in heterogeneous networks and devices, based on the enforcement of interoperable and changing security policies.

Addressing the needs of developers, integrators and operators.

Rationale

- Using dynamic security Service Level Agreements: the software services and components will interoperate communicating and sharing data in a secure trusted manner dictated by negotiated, common security policies.

- Using advanced vulnerability detection techniques: active and fuzz testing, to avoid security vulnerabilities introduced by the dynamic adaptation.

- Using privacy-preserving negotiation and delegation mechanisms, even in the presence of scarce resources. Integrating legal, social and economic constrains.

Innovation

- New architecture coping with dynamic secure interoperability by means of Aspect-Oriented Programming (AOP) techniques.

- New paradigms for modelling secure interoperability policies.

- Combined techniques: protection based on AOP, supervision based on monitoring and testing based on active and fuzz techniques.

- Tools to insure secure interoperability in all phases of software development.

Case Studies

Two completely different case studies with complex, high-demand critical services.

- Electronic voting, to assure the required high level of trustworthiness for people voting from anywhere using a multiplicity of devices.

- Vehicle-to-Vehicle and Vehicle-to-Infrastructure Communications, to address the security needs in today’s complex mobility scenarios for Citizens, Agencies, Mobility Services Providers and Car Manufacturers.

Project co-funded by the European Union under the Information and Communication Technologies theme of the 7th Framework Programme for R&D ICT-2011.1.4 Trustworthy ICT contract n. 317731
INTER-TRUST Framework

How it works

- Modelling languages to model security policies
- Negotiation/communication module defines a common security policy
- Aspects Generation module dynamically generates aspects
- Security Policy interpreter interprets the negotiated policy
- Monitoring and testing modules inject code for active and fuzz testing, generate traces (Notify) used by the Monitoring to generate warnings that will provoke the Reaction module
- Reaction module performs protection and mitigation strategies
- Aspect Weaver module weaves and un-weaves aspects

www.inter-trust.eu

Project Coordinator

Enrico Morten
Softeco Sismat
Via De Marini 1
16149 Genova, Italy
http://www.softeco.it/
tel. +39 010 6026 328
fax. +39 010 6026 350
e-mail: enrico.morten@softeco.it

Duration

From November 2012 to April 2015