ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Project Results

Delivering trust in embedded systems

Offering secure and dependable solutions for a wide range of applications

The TECOM (Trusted Embedded Computing) project has developed architectures and solutions combining embedded trust services and trusted operating system technologies to ensure security and dependability in a wide range of complex and dynamic embedded systems. The project focused on enabling multiple applications to be run safely on the same systems and processors while acting totally independently of each other. Applications range from protecting film rights in video-on-demand applications to ensuring bug-free software upgrades in domestic appliances.

Industry and society are increasingly dependent on embedded systems that are becoming ever more complex, dynamic and open, while interacting with progressively more demanding and heterogeneous environments. As a consequence, systems reliability and security have become major concerns.

Current approaches provide little or no support to determine the level of dependability and trustworthiness in a system. An increasing number of external security attacks as well as design weaknesses in operating systems, especially in the PC world, have resulted in major economic damage. As a consequence, it has been difficult to obtain user acceptance and market acceptance.

Trust involves the accepted dependence between two stakeholders, one of which is responsible for a trusted artefact. In trusted computing, this involves a trusted computing artefact such as an electronic device. Such trust is achieved by involving means for security and dependability and providing some form of evidence for trust that can be examined by the stakeholders involved. The trustworthiness of a computing system is important as it allows the reliance placed on the service it delivers to be justified.

ABSTRACT ARCHITECTURES

TECOM focused on the growing demand for execution platforms in embedded systems that address both integrity and security concerns. It developed abstract architectures based on generic modules involving on one side an embedded trust services layer offering hardware security, and on the other trusted operating system technology involving system and middleware space. The result can be customised to a specific application.

The state-of-the art approach to trust at systems level, close to the processor, is some form of hypervisor or virtualisation application for securely partitioning the applications. While this has already been developed for use on PCs where it was possible to run two windows independently at the same time, it has not been available for embedded systems.

RESULTING SOLUTION

TECOM resulted in an open-source and evolvable solution with the XtratuM hypervisor for safety critical embedded system which can meet stringent certification needs in the avionics industry.

On the middleware side, TECOM worked on extending the PERC Ultra Java virtual machine technology from Atego to support multiple applications. PERC was integrated with the TECOM middleware security layer and TECOM trusted operating systems. The outcome was a proof of concept that it is possible to add partitioning applications in such a virtual machine.

APPLICATIONS DEMONSTRATED

TECOM demonstrated its approach in five applications:

1. Isolation of the film stream from other action in video-on-demand applications to protect rights;
2. Separated counting of numbers of accesses for events in video-surveillance applications for legal or financial purposes;

TECOM
(ITEA 2 - 06038)

Partners
Atego
EADS DS
Fagor
Ikerlan
Technicolor
Technikon
Trialog
Universidad Politécnica de Madrid
Universidad Politécnica de Valencia
Visual Tools

Countries involved
Austria
France
Spain

Project start
September 2007

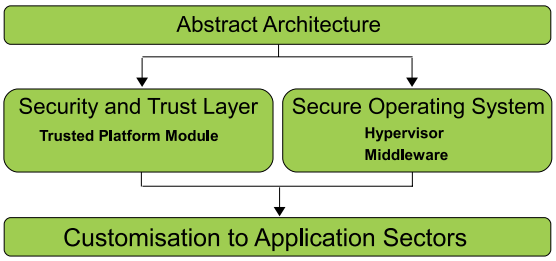
Project end
August 2010

Contact
Project leader :
Antonio Kung, Trialog
Email :
antonio.kung@trialog.com

Project website :
www.tecom-itea.org

Project Results

3. Quarantine of software updates in domestic appliances until an update has proved bug free;
4. Independent operation of multiple separate functions, including dependable control and infotainment, on processors in automotive applications to reduce the number of processors required; and
5. Combination of a series of independently operating safety-critical applications on single processors in avionics for weight and cost reasons.



COMMERCIAL APPLICATIONS

The resulting convergence of security and dependability developed in this ITEA 2 project is already leading to commercial applications of both the operating systems and virtual machines. The XTratuM secure operating system is now on the market with support from FentiSS, a spin-off from the University of Valencia. And the Atego PERC virtual machine is ready for integration once the required functions are identified. The concepts developed in the other demonstrators are also serving as a basis for future products.

Major project outcomes

DISSEMINATION

- 27 papers were published.
- 19 dissemination actions were carried out.

EXPLOITATION

- XTratuM will be further disseminated by UPV.
- Trialog jointly with FentiSS will support XTratuM in France.
- UPV and Trialog are involved in the Oversee FP7 project which is building a platform for the automotive industry, based on XTratuM and the TECOM abstract architecture.
- Aonix-Perc will integrate the isolation capability into a new release to be offered by Atego, based on market requirements.

STANDARDISATION

- Through the IMA for Space project, UPV is involved in the standisation for TSP (Temporal and Spatial Partitioning) based on ARINC-653, with XtratuM as the hypervisor technology used as the input for the standard elaboration.
- XtratuM is compliant with the SKPP and it is the process to be certified for the aerospace community.
- XtratuM can be adapted to be AUTOSAR compliant with low effort.
- UPV will follow up all activities related to standarisation in system isolation.
- Atego is involved in JSR-282, which is defining a revision of RTSJ (Real-Time Specification for Java).
- Atego is involved in JSR-302 for the definition of safety-critical Java
- Atego will follow up all the activities related to standarisation in middleware isolation that have an impact on Aonix-Perc.

SPIN-OFFS

- Taking into account the growing interest of the aerospace sector in the development of partitioned systems and the need of industrialisation of XtratuM to be used in final applications, UPV decided to setup the spin-off FentiSS.

ITEA 2 Office
High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands
Tel : +31 88 003 6136
Fax : +31 88 003 6130
Email : info@itea2.org
Web : www.itea2.org

ITEA 2 – Information Technology for European Advancement – is Europe's premier co-operative R&D programme driving pre-competitive research on embedded and distributed software-intensive systems and services.
As a EUREKA strategic Cluster, we support co-ordinated national funding submissions and provide the link between those who provide finance, technology and software engineering.
Our aim is to mobilise a total of 20,000 person-years over the full eight-year period of our programme from 2006 to 2013.

ITEA 2-labelled projects are industry-driven initiatives building vital middleware and preparing standards to lay the foundations for the next generation of products, systems, appliances and services.
Our programme results in real product innovation that boosts European competitiveness in a wide range of industries. Specifically, we play a key role in crucial application domains where software dominates, such as aerospace, automotive, consumer electronics, healthcare/medical systems and telecommunications.

ITEA 2 projects involve complementary R&D from at least two companies in two countries. We issue annual Calls for Projects, evaluate projects and help bring research partners together. Our projects are open to partners from large industrial companies and small and medium-sized enterprises (SMEs) as well as public research institutes and universities.

EUREKA

TECOM
(ITEA 2 - 06038)

October 2010