

Project Profile

Trusted Embedded Computing Solutions and architectures for integrity and security requirements

.....

The strategic objective of the TECOM project is to investigate solutions and architectures for embedded-systems platforms which need to meet both security and integrity requirements. The TECOM approach will apply the concept of trusted platforms to real-time embedded systems.

Industrialised societies are increasingly dependent on embedded systems that are constantly becoming more complex, dynamic and open, while interacting with a progressively more demanding and heterogeneous environment.

Current systems provide little or no support to determine their level of dependability and trustworthiness. An increasing number of external security attacks and design weaknesses in operating systems, especially in the personal computer (PC) world, have resulted in large economic damages, leading to lower user and market acceptance.

Therefore, stakeholders in embedded systems for execution platforms need solutions which addresses both integrity and security concerns, in particular to:

- Avoid denial of service (DOS) issues provoked by resource shortage such as memory or central processing unit (CPU), while from an integrity viewpoint it is important to ensure availability of resources such as memory or CPU budget
- Prevent malicious access to data created by another application, and from an integrity viewpoint it is important to avoid unexpected memory access due to programming errors.

DEVELOPING A GENERAL PLATFORM ARCHITECTURE

Real-time embedded systems cover a large number of application sectors with specific needs. TECOM will develop a general abstract execution-platform architecture for real-time embedded systems that can

be specialised/instantiated to a specific application sector, and customised to adapt to specific standards and needs such as AUTOSAR in the automotive sector, OSGi (Java middleware framework) in gateways, or the Windows CE operating system for embedded systems.

The key components of the general abstract execution platform are:

- A security layer which sits between applications and the underlying operating systems. The security layer is responsible for consistency between the execution flow control, data flow within the execution system and security policies. This applies as well to systems resources including security services, e.g. updating credentials. This layer also provides a framework to allow the secure integration of device drivers
- A secure operating system, which relies on the underlying hardware platform to interface with the security layer. TECOM will investigate two approaches:
 - 1 Partitioning or virtualisation through hypervisor capabilities, where the processor is made virtual through a software layer which emulates multiple virtual processors. Consequently, several operating systems can be executed in parallel
 - 2 A microkernel approach using a classical operating system with an onion-based structure. The inner part of the onion is the microkernel, which supplies basic operating-system functions; additional layers provide other richer operating services.

APPLYING CUSTOMISATION

From the general abstract architecture, customisation can be applied to take into account hardware and operating –system specific aspects.

- Trango hypervisors – virtualisation technology adapted to mobile

TECOM (ITEA 2 ~ 06038)

.....

■ Partners

Aonix
EADS DS
Fagor Electrodomecos
Ikerlan
Technikon
Thomson
Trango
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, France

Email :
antonio.kung@trialog.com

Project website :
www.tecom-itea.org

Project Profile

applications, usable in other application sectors

- Xtratum hypervisor for real-time embedded systems – open-source virtualisation technology from Universidad Polit cnica de Valencia
- Arinc653 (Avionics Application Standard Software Interface) – partitioning standard in the avionics sector
- XEN – industry standard open source virtualisation technology
- L4Linux – Linux with a microkernel implementation based on a secure architecture
- Real-time Linux (RTLinux)
- OSEK – operating system for the automotive sector

The abstract architecture will be customised for application sectors with different requirements:

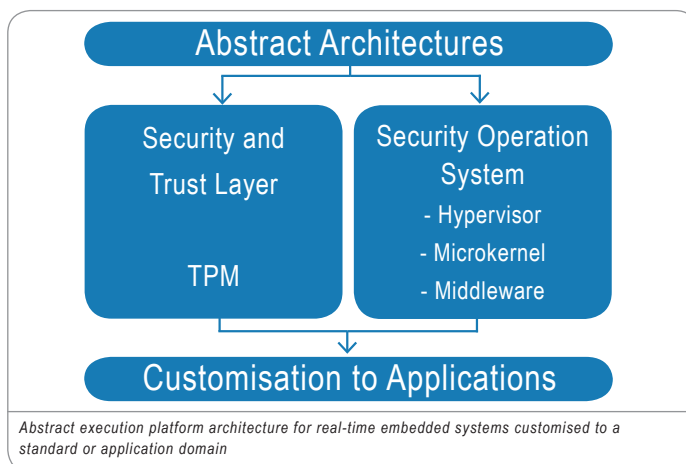
- **Mobile applications** offer support for multiple independent applications. From a security viewpoint, secure dynamic deployment of applications must be achieved, so that it is not possible to download a malicious application. From an integrity viewpoint, system resource sharing between applications must be achieved, so that it is not possible to prevent an application from running because many resources are occupied by other applications.
- **Home control systems** manage devices as diverse as kitchen appliances, entertainment equipment, PCs and mobile phones for communication, and health monitoring systems. Home control will rely upon a gateway TPM device which can deliver high integrity and confidentiality.

This gateway will manage all in-home information while offering trusted communication when external access is needed.

- **Video surveillance systems** deliver high integrity and confidentiality both in real-time video streaming and in recorded video sequences. The use of public communication networks (e.g. Internet) calls for an increase in the mechanisms to protect multimedia contents (video and data) in security applications.
- **Automotive applications** handle software updates as well as components provided by different suppliers. There are integrity requirements (i.e. the obtained system must have been suitably validated), and specific component isolation requirements when an error is detected in order to help identify the component that might be faulty.
- **Avionics applications** offer a high level of assurance at the process level and the use of platforms that enforce strict, static resource usage with partitioning capabilities. They need to run independent applications in parallel with different levels of assurance.

Expected results from the TECOM project include:

- Security solutions based on different approaches, such as hypervisors, microkernels and middleware
- Demonstrators using the security solutions in different domains: mobile applications, home control and video surveillance
- A study in two sector domains: automotive and avionics.



ITEA 2 Office

High Tech Campus 69 - 3
5656 AG Eindhoven
The Netherlands

Tel : +31 88 003 6136
Fax : +31 88 003 6130
Email : itea2@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.

