TECOM
(ITEA 2 06038)

Antonio Kung, Trialog
France

Enabling Trust for Safety and Security in Embedded Systems

The ITEA 2 TECOM project has developed mechanisms in terms of 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 and ensuring bug-free software upgrades in domestic appliances to safe operation of the multiple control systems now found in cars and, potentially, partitioned systems for safety-critical applications in aircraft.

Industry and society are increasingly dependent on embedded systems that are getting ever more complex, dynamic and open, while interacting with progressively more demanding and heterogeneous environments. Consequently, reliability and security have become major concerns, yet current approaches provide little or no support to determine the level of dependability and trustworthiness in a system.

The growing number of external security attacks as well as design weaknesses in operating systems, especially in personal computers (PCs), has resulted in major economic damage. As a result, it has been difficult to attain user acceptance and gain favourable recognition in the market for such systems.

Consequently, stakeholders in embedded systems are increasingly demanding execution platforms which address both their integrity and security concerns. The worries include:

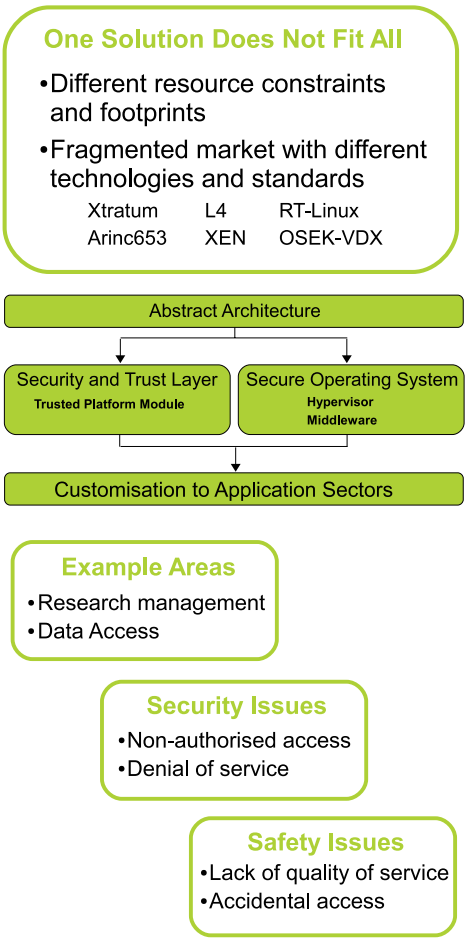
- Denial-of-service security issues provoked by shortage of resources such as memory and processing power, while ensuring availability of resource budget; and
- Malicious access to data created by another application and, from an integrity viewpoint, unexpected memory access caused by programming errors.

ESTABLISHING TRUST BETWEEN STAKEHOLDERS

The ITEA 2 project therefore set out to investigate solutions and architectures for embedded systems platforms which have to meet both security and integrity requirements. The basis of the TECOM approach was to apply the concept of trusted platforms to real-time embedded systems.

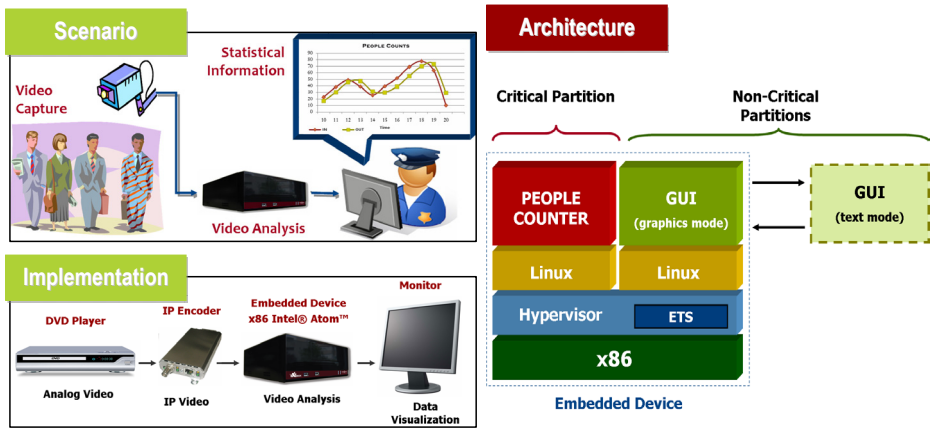
Trusted computing involves the accepted dependence between two stakeholders, one of which is responsible for a trusted computing artefact such as an electronic device. Such trust is achieved by involving means for security and dependability, and providing some form of evidence for trust that can be examined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

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.

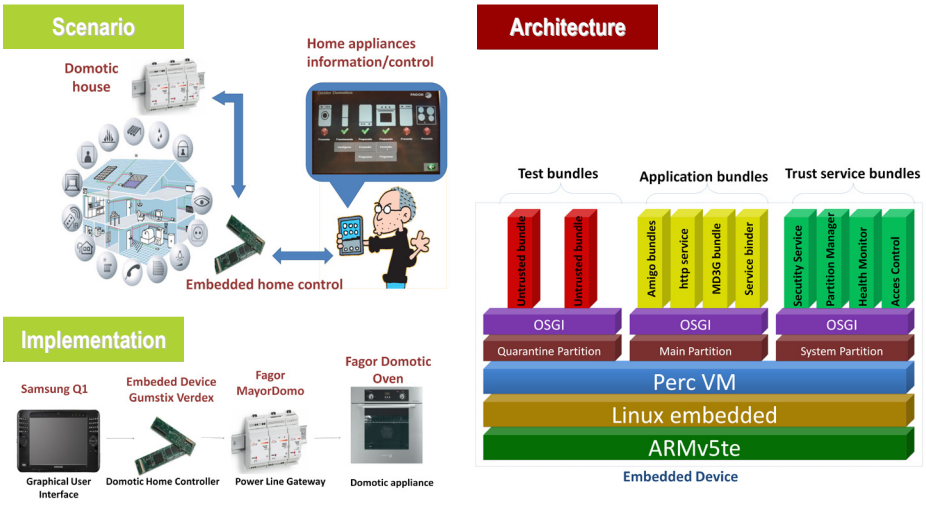


The state-of-the art approach to trust at systems level, close to the processor, has been some form of hypervisor or virtualisation application for securely partitioning the applications. While this had already been developed for use on main-frame computers and on PCs where it was possible to run two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

VIDEO SURVEILLANCE DEMONSTRATOR: TRUSTED PEOPLE COUNTER



HOME CONTROLLER DEMONSTRATOR: TRUSTED HOME CONTROL



OPEN-SOURCE SOLUTION

Partner Universidad Politécnica de Valencia had already started development of a hypervisor system for the European Space Agency. This was intended to enable several partitioned applications to be run safely at the same time on the same processor to reduce space requirements. The hypervisor provides a framework to run several operating systems in a robust partitioned environment.

This work was taken further in the ITEA 2 project, resulting in an open-source and evolvable virtual machine solution now available as the XtratuM hypervisor. This can be used to build an architecture with Multiple Independent Levels of Security (MILS) for safety-critical embedded systems which can meet stringent certification needs in the avionics industry.

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

FIVE APPLICATIONS DEMONSTRATED

TECOM demonstrated its approach in five applications:

1. Isolation of the film stream from other activities in a PC for video-on-demand applications to prevent copying and thus protect copyrights. This was led by Technicolor;
2. Separated counting of numbers of accesses for exhibitions or sports events in video-surveillance applications for legal or accounting purposes. This was led by Visual Tools;
3. Quarantining of software updates in domestic appliances until an update has proved bug free. This was led by Fagor;
4. Independent operation of multiple separate functions, such as engine control and telematics, in automotive applications to reduce the number of processors required. Such partitioning is intended to enable full control in separate partitions for greater safety and dependable services. This was led by Trialog;
5. Combination of a series of independently operating safety-critical applications on single processors in avionics for weight and cost reasons. This was seen as a more long-term possibility and the work in TECOM was principally a proof of concept for such applications. This was lead by EADS DS.

DEVELOPING COMMERCIAL USE

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. These include:

- The XTratuM secure operating system, which is now available as an open-source product (www.xtratum.org). Support in the use of the product is available from FentiSS, a spin-off set up by the Universidad Politécnica de Valencia that specialises in the development of safety secure and critical embedded solutions using virtualisation technologies. Universidad Politécnica de Valencia, FentiSS, and Trialog are also co-operating on further work based on XTratuM; and
- The Atego PERC virtual machine, which is ready for integration once the required isolation functions are identified by potential customers.

Concepts developed in the other demonstrators are also serving as a basis for future products with Visual Tools, Fagor, and Technicolor ready to integrate isolation and Embedded Trust Services (ETS) features into future applications.

TAKING WORK FURTHER

Work developed in the ITEA 2 TECOM project is also being taken further in an EU Seventh Framework Programme (FP7) project which involves several TECOM partners. The OVERSEE project is an initiative for the automotive sector intended to provide a secure, standardised and generic communication and application platform for vehicles.

MORE INFORMATION:

www.tecom-itea.org