EURO-MILS: Secure virtualisation for trustworthy applications in critical domains

EURO-MILS Use Cases and Transport Security

Based on embedded systems, cyber-physical transport networks are part of our society, and gain wider spread and importance. New generations of aircraft and cars include more and more embedded devices that are tightly interconnected with each other, with the internet and other infrastructures. The additional interface complexity, provides an overall increase in transport safety, but also, especially in software, opens new attack surfaces to malicious attackers.

The EURO-MILS project will develop two prototypes of certified secure embedded systems based on a common software architecture (MILS: Multiple Independent Levels of Security): a separation kernel, a special kind of embedded operating system, that effectively separates applications in different domains and allows to build system in an always-invoked, tamperproof, evaluatable and non-bypassable way.

The first EURO-MILS avionic use case studies a novel architecture for an avionics gateway that applies filtering mechanisms up to the application level on each data stream exchanged between two avionics domains with different security levels.

ARINC 664 Part 5 defines four avionics domains:

- Aircraft Control Domain
- Airline Information Service Domain
- Passenger Information and Entertainment Domain
- Passenger Owner Devices

with ACD being the one with the highest security requirements, the focus is put on the integrity attribute.

The gateway, developed by following the MILS principals of strict separation and controlled information flow, intends to protect the integrity of a high level security domain while allowing its bi-directional communication with other domains having lower security levels.
The target of this demonstrator is to apply the MILS principals to the development of real-time embedded systems but also to create new security evaluation strategies given by the separation properties between software components.

The second EURO-MILS use case is an automotive use case. It describes the system architecture of a vehicle head unit ECU that combines non-critical and non-trusted applications (e.g. music player), medium-critical applications (e.g. advanced driver assistance systems) and highly-critical applications (e.g. AUTOSAR realtime apps).

- It will support interactions such as remote updates of software by OEMs (e.g. car unlock by an authenticated car owner driver via an OEM service), stolen vehicle tracking (e.g. information on the position of the car is made available to the car owner), geo-fencing (e.g. warning message sent to the car owner if the car leaves a set perimeter), remote diagnostics (e.g. diagnostics information from the in-vehicle ECU made available to the car owner and/or to the OEM repair shops), remote charge control of electric vehicles.
- The target of security measures is the protection of instrument cluster and head unit display control, as well as the underlying virtualization platform. Under no circumstances, these units may be compromised or disturbed in their normal operation.

Moreover, while the focus of the prototypes is on an individual embedded system, the use cases encompass securing its connections to the systems (airplane or cars) and to the “system of systems” such as the Air Traffic Control or the Road Integrated Traffic Control System.

EURO-MILS at a glance

Project number:
318353

EURO-MILS mission:
The mission of the EURO-MILS project is to develop a solution for virtualisation of heterogeneous resources and provide strong guarantees for isolation of resources by means of Common Criteria certification with usage of formal methods.

Project start:
01.10.2012

Project end:
30.09.2015

Total costs:
EUR 8.447.558

EC contribution:
EUR 6.000.000

Consortium:
14 partners from 5 different countries.

Project Coordinator:
Dr. Klaus-Michael Koch
coordination@euromils.eu

Technical Leader:
Dr. Sergey Tverdyshev
sergey.tverdyshev@sysgo.com

Project website:
www.euromils.eu

Acknowledgements
The EURO-MILS project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-318353.

SEVENTH FRAMEWORK PROGRAMME