EURO-MILS: Secure European Virtualisation for Trustworthy Applications in Critical Domains

Newsletter

NOVEMBER 2014 ISSUE 3

In this Issue

Message from the Coordinator

The second year of the EURO-MILS project has passed and the partners can look back at a quite successful project period. The progress achieved by all work packages within the second project year is in line with the initial plan. During the second year, five deliverables have been submitted and two major milestones have been pursued and achieved.

Call for Papers: EURO-MILS Workshop at HiPEAC

You are welcome to make a submission at "**International Workshop on MILS: Architecture and Assurance for Secure Systems Amsterdam"**, 20.01.2015, co-located with the HiPEAC Conference 2015.

QUICK LINKS

- MILS Workshop: http://mils-workshop.euromils.eu/
- Call for Papers: http://mils-workshop.euromils.eu/downloads/EUROMILS-HIPEAC-MILS-Workshop-2015-CfP.pdf
- Submission: https://easychair.org/conferences/?conf=mils15

IMPORTANT DATES

- Paper submission	20 November 2014
- Notification of Acceptance	19 December 2014
- Camera-Ready Paper	11 January 2015
- MILS Workshop	20 January 2015

The workshop topics include, but are not limited to:

- MILS architectural approach for security and safety
- MILS components and ecosystem
- MILS use-cases, e.g. from avionics, automotive, communications, industrial automation, medical, railway, consumer and similar domains
- Real-time separation kernels
- MILS certification
- MILS testing and vulnerability analysis of MILS systems
- Cross-European/world-wide high-assurance security
- Formal methods for MILS systems as a basis for high assurance

Submissions do not need to be full papers: this is a workshop and we are looking for interesting experience, work, and ideas (possibly preliminary and exploratory) that will stimulate discussion and thought.

Submissions should be in PDF format between 3-12 pages. We recommend the guidelines for ACM SIG Proceedings.

Workshop committee:

Romain Bergé (ITSEF Thales, France);
Igor Furgel (ITSEF T-Systems, Germany);
Kevin Müller (Airbus Group Innovations, Germany);
Michael Paulitsch (Thales, Austria);
Joseph Bergmann (The Open Group),
Rance Delong (The Open Group, UK);
Harald Rueß (Fortiss, Germany);
Andreas Lindinger (Continental Corporation, Germany);
Sergey Tverdyshev (SYSGO, Germany);
Bertrand Leconte (Airbus Operations SAS, France);
Cristina Simache (Altran Sud Ouest, France)

Main Project Information

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

The project aims 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.

Key Data:

Start date:	1st October 2012
End date:	30th September 2015
Duration:	36 months
Project reference:	318353
Project cost:	€ 8.447.558
Project funding:	€ 6.000.000

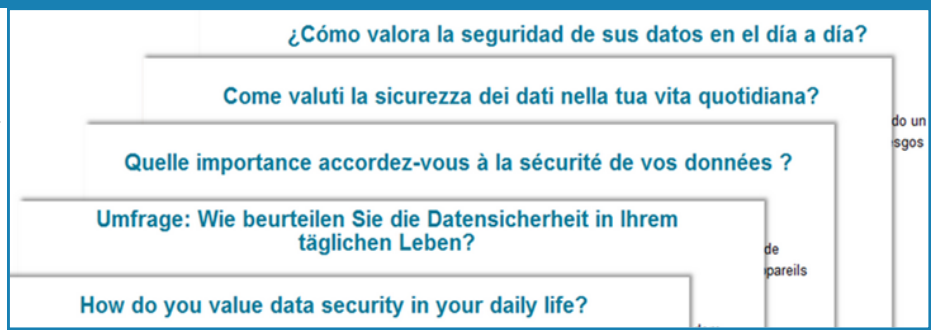
One of the EURO-MILS goals is to discover the business, legal and social acceptance of trustworthy technology in several key markets (e.g. healthcare, finances, transports, etc.). **Do you wish to participate and share your opinion as a key representative of your industry? Send a message to: interview@euromils.eu and we will contact you to participate in the EURO-MILS Industry Panel.**

EURO-MILS: Secure European Virtualisation for Trustworthy Applications in Critical Domains

Newsletter

NOVEMBER 2014 ISSUE 3

IT Magazine Reader Security Survey



One work package of the project (WP13: Business, Legal and Social Acceptance) is to analyse the business impact of such a trustworthy technology in markets adjacent to the core automotive and avionics targets. It studies the potential of the EURO-MILS platform in markets such as healthcare, finance, smart home, mobile communication, etc. During the first year, we have interviewed several professionals working in various industries on the following themes: security and safety, virtualisation and partitioning, certification and user assurance. The general results were that, despite some differences in interpretation, security and safety become key requirements in many industries and many embedded systems are crossing the line toward criticality. Many markets are making security a high priority. But industries professionals are wondering how to create secure products without slowing down business. Virtualization is becoming the norm to operate independent software stacks with different criticalities on the same platform, but complexity can be a barrier, especially for high volume markets that need to keep costs under control. Finally, as security evaluation is a time consuming and complex process, the business value derived from the certification has to be well evaluated.

In the second year of the project, to pursue the analysis at the consumer level, we created a questionnaire for a European audience on how consumers valued data security in their daily life. We ran this survey for two months (June and July 2014) and received 547 filled in questionnaires from 6 geographies (Benelux, France, Germany, Italy, Spain, UK). Confirming the EURO-MILS approach, preliminary analysis results show that security evaluation is the most important criterium followed by a declaration of conformity or a security label (see Figure "Criteria of Choice"). Early results analysis showed that there is a strong correlation between the consumer security attitude and the age of the consumer as well as his country of origin. An interesting point is that consumers are more aware of privacy (how to protect personal data against becoming known to third parties) than information security (how to ensure the integrity of and limit access to information stored on and communicated via a personal device). And if our panel members are worried about the protection of personal data and its use, it is not stopping them from sharing data on social networks.

Because MILS is about virtualization, we also took a closer look at the groups who answered “yes” to the question statement that they "use virtualization as additional measure of protection" for their personal data (about 15%), versus those who said "no" (about 85%). The strongest correlation (probability $p < 0.0005$ established by a Chi square test) is in the country category, where we can conclude that virtualization is more used for protection of personal data in Germany than in Spain. Other significant ($p < 0.05$) results were that IT architects use virtualization more than "database / storage managers". In the sector category, computer and IT persons use virtualization more than manufacturing/industrial persons. Additionally, the banking sector uses virtualization less than government. These results suggest that, when marketing MILS, IT architects and security managers could be one potential target, as they already have more hands-on experience with virtualization.

Greetings from Munich

The EURO-MILS partners regularly communicate electronically to discuss progress and issues at hand. The entire EURO-MILS consortium also met for a technical meeting in Munich from 23rd to 25th September 2014. The meeting was hosted by Airbus Group Innovations.

EURO-MILS: Secure European Virtualisation for Trustworthy Applications in Critical Domains

Newsletter

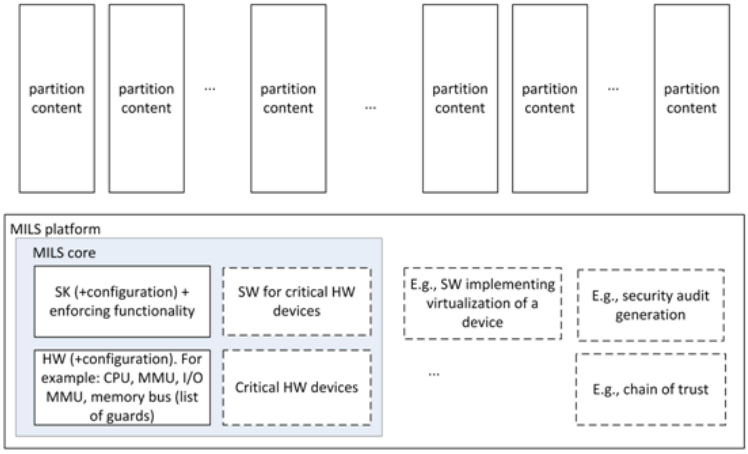
NOVEMBER 2014 ISSUE 3

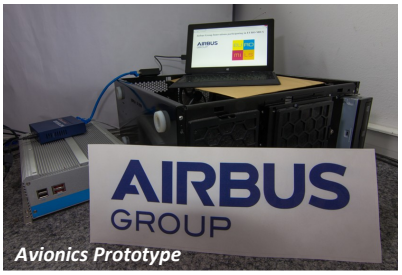
Instantiating the MILS Architecture Template

As announced in the last newsletter, this year we have worked out a generic template for the MILS architecture, while at the same time formulating the requirements of the prototypes, the avionics gateway and the automotive telematics ECU.

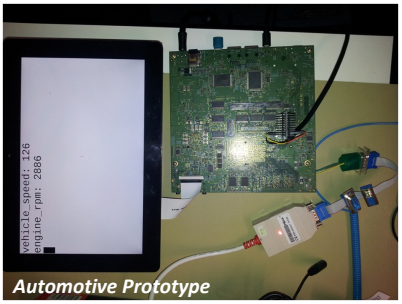
We used the template to decompose the prototypes into several components. In the avionics gateway, most of the components realise the gateway function; however, several components are also needed in the MILS core and MILS platform levels. Similarly, in the automotive telematics unit, again the MILS core and MILS platform are realized by a plurality of components. Common components identified between the two prototypes' architecture were the separation kernel, a processing unit, a memory management unit, IOMMU, timers, and an audit component. Implementation work included, for the avionics platform, the FreeScale P4080, secure support for persistent storage in the form of a SATA driver, DPAA and PAMU. For the automotive prototype, which is based on the Texas Instruments OMAP5 ARM-based (Jacinto6 HS) platform, we have focused on support for hardware virtualization and for its Level 3 (L3) interconnect firewalls.

MILS System





Avionics Prototype


Automotive Prototype

Formal Model for Real-World Separation Kernels

We agreed that the most interesting security property to model was non-interference. An approach was developed that allows to express local security properties of applications and to show that they remain valid within a system with a separation kernel. The model consists of a model of an abstract multicore separation kernel with state MultiCISK (Controlled Interruptible Separation Kernel for Multicore) and its implementation by the PikeOS separation kernel. A snapshot of an early (single-core) version is available for download and use at the Isabelle/HOL Archive for Formal Proof (http://afp.sourceforge.net/entries/CISC-Kernel.shtml).

Open Group

EURO-MILS actively follows and participates in the meetings of the Open Group Real-time & Embedded Systems Forum and especially its MILS working group (http://www.opengroup.org/getinvolved/forums/systems). EURO-MILS has presented at the last meeting in London and also plans to present at the Feb 2015 Open Group Forum in San Diego. Upcoming events in general can be found at http://www.euromils.eu/index.php/news. The next upcoming event is escar – embedded security in Cars Conference, Hamburg in Nov 2014.

Contacts:
EURO-MILS Project Coordination Team
Dr. Klaus-Michael Koch
Technikon Forschungsgesellschaft mbH
Burgplatz 3a, A-9500 Villach
Tel.: +43 4242 23355—71
Fax: +43 4242 23355—77
E-Mail: coordination@euromils.eu
Web: www.euromils.eu

FOLLOW US ON twitter
www.twitter.com/euromils