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

Newsletter

APRIL 2016 ISSUE 4

In this Issue

Message from the Consortium

There have been numerous events and achievements since the last issue of the EURO-MILS newsletter. The project partners participated in various workshops, meetings and conferences dedicated to the dissemination of EURO-MILS, as well as to support progress of the project (http://euromils.eu/publications/).

Among the main events were the technical meeting in Villach, Austria beginning of March 2015, and the technical & General Assembly meeting in Toulouse, France in September 2015. Partners were immersed in vivid discussions about the technical progress and further planning of EURO-MILS beyond the project lifetime. Moreover, the project was extended by six months, in order to fully reach the objectives of EURO-MILS and to successfully develop targeted prototypes.

Furthermore, a MILS Community has been established (http://mils-community.euromils.eu/) which brings together individuals and organizations involved in or just interested by MILS architecture and technologies. Two international workshops on MILS architecture and the assurance for secure systems were organized in Amsterdam (2015) and Prague (2016), both co-located with the HiPEAC conference. Partners are now preparing the final review meeting, which will take place on European Commission premises in May 2016.

Finally, it is with great pleasure to announce that the objectives targeted in EURO-MILS were reached and the project successfully ended in March 2016. Knowledge and technology gained within the project will help to maintain and further increase competitiveness of the European MILS security market, as well as of the project industry partners.

MILS Workshops / MILS Community

The MILS Community is a global international, open membership, not-for-profit technology consortium with potential to become the leading competence network on MILS architecture and technologies. This MILS Community is an interest group for architecture-based security, which aims to exchange ideas about meaningful work that could be done (in an industrial or research context).

The first International Workshop on **"MILS: Architecture and Assurance for Secure Systems"**, in January 2015 in Amsterdam, was co-located with the HiPEAC Conference and focused mainly on the MILS architectural approach for security and safety, MILS components and eco-system as well as the certification or the possible MILS use-cases. Furthermore, real-time separation kernels and cross-European and world-wide high-assurance security were among the discussed topics.

The second workshop on MILS took place on 20th January 2016 in Prague as well as the MILS Community meeting for which, additionally, it was offered the possibility to join the sessions via teleconference. Hot topics were Common Criteria certification, hardware (testing versus compliance), how to agree on common definitions in the form of a glossary, a possible catalogue of known (published) MILS systems, and how to complement other standardisation efforts. Both workshops have been organised by the technical leader, *Sergey Tverdyshev (SYSGO AG, Germany).*

For more information about the **MILS Community,** please follow http://mils-community.euromils.eu/ and we kindly invite you to subscribe to the **MILS Community mailing list** via the web form http://lists.euromils.eu/mailman/listinfo/mils.

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

Technical Leader: Sergey Tverdyshev

SYSGO AG, Office Mainz, **E-Mail:** sergey.tverdyshev@sysgo.com

LinkedIn

FOLLOW US ON twitter

www.twitter.com/euromils

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

Newsletter

APRIL 2016 ISSUE 4

The 3rd EURO-MILS project period — Summary of RTD WPs

During the third project period, all objectives and work plans were successfully finalized. **WP12 "Certification Requirements"** investigated and produced domain specific functional security requirements for avionics and automotive use cases. Those requirements were formulated in a way to meet demands of the CC composite evaluation approach in WP21 with a separation kernel complying with the ST and the PP. All objectives of **WP13 "Business, Legal and Social Acceptance"** for the third period have been achieved: gather additional data by running a social survey using a Big data analysis, work on the legal aspect, finalize and consolidate and document the work done during the project, and to publish the final D13.2.

In **WP21 "MILS Architecture"** partners established the non-interference of the model used in EURO-MILS which is comparable to the GWV non-interference used in some other MILS separation kernel models. Furthermore, partners produced a formal installation of the firewall based on the CISK separation kernel. Within **WP22 "MILS components"**, the Core Component for Secure IO (IOMMU) including support for dynamically assigning an IO device from one partition to another was finalized and successfully implemented for the automotive platform, which followed the avionics platform that was developed earlier. **WP23 "Prototype Integration"** developed three testbeds: *MILS platform based on PikeOS testbed, avionic & automotive testbed.* In the avionics domain, the prototype software modules have been developed and successfully integrated on top of PikeOS running on the P4080 based hardware. For the automotive prototype, PikeOS has been extended to support the hardware virtualization and the firewall features of the Texas Instrument Jacinto 6. The integration of the automotive prototype architecture on top of PikeOS running on TI Jacinto6 has also been successfully achieved. The validation report shows that the MILS architecture formed a solid basis for the implementation of the avionic and automotive use cases and the majority of executed tests show that the security features have been correctly implemented.

WP31 "Assurance by Formal Methods" focused on providing assurance by application of formal methods. We studied whether it is possible to formulate the entire generic model as a series of monadic transformations. Furthermore, the research was on the role of formal model in a certification context, such as EAL5+ certification.

Within **WP32 "Common Criteria Security Evaluation"** partners worked on the evaluation of the separation kernel according to the CC evaluation methodology, with insights not limited to the project's separation kernel, but also including knowledge generation on the general evaluation of separation kernels.

WP33 "Cross-European Certification" dealt with assurance for high EAL and with composition. A suggestion for a methodology allowing high assurance evaluation in composition with software platform was provided in D33.1 "Addendum to CEM". Furthermore, a draft version of "composition for software platform" has been released in order to address the question of composition on top of software platform.

Overview of EURO-MILS most recent publications and deliverables

The following EURO-MILS scientific publications and public deliverables have been recently published:

- *White paper:* **"Non-Interfering Composed Evaluation":** The white paper describes how to establish the properties of the TOEs a-priori as opposed to the traditional a posteriori approach of Common Criteria compositional certification.
- *Deliverables:* D12.3 "Common Criteria Protection Profile – Multiple Independent Levels of Security: Operating System", D13.2 "MILS: business, legal and social acceptance", D21.3 "Trustworthy MILS: CC Composite Evaluation Approach", D31.2 "Used formal methods", D31.4 "Test generation methods", D33.1 "Addendum to CEM"

Public deliverables and publications can be accessed via the **project website** (http://www.euromils.eu/publications) and also via the online repository **"Zenodo"** (https://zenodo.org/collection/user-mils/).

Summary of the final prototypes & main project results

The EURO-MILS project yielded the targeted outcomes. The Trustworthy ICT for high critical automotive and avionics domains was developed using the MILS approach. Both automotive and avionics prototypes were successfully developed and implemented, meeting the majority of initially targeted requirements. The MILS platform based on virtualization techniques was designed, developed and is being used to provide trustworthiness. Further, it contains a framework to develop secure and safe products and integrate domain specific functionality and components. Another outcome achieved is high assurance in the trustworthiness of the MILS platform, using formal models and the Common Criteria for IT Security Evaluations standard.

The project results offer market participants the opportunity to use a trustworthy virtualization made in Europe, which proves to have strong strategic impact. Furthermore, the EURO-MILS project has described a generic process that is being generally applicable for national certification authorities in Europe (D33.1). The project results are empowering the European software sector, specifically virtualisation and integration businesses and its competitiveness not only by supporting a highly innovative technology, but also by bringing together the essential European players, including research, industries or SMEs.