D07.1 Third Periodic Report (M25-M39)

Part 2 – Publishable Summary

Project number:	216888
Project acronym:	TECOM
Project title:	Trusted Embedded Computing
Start date of the project:	January 1, 2008
Duration:	39 months
Funding Scheme:	FP7 ICT IP

Date of the reference Annex I:	November 24, 2010
Deliverable	Third Periodic Report
Period covered:	01.01.2010 – 31.03.2011 (M25-M39)
WP contributing to the deliverable:	All
Due date:	M39
Actual submission date:	11.05.2011

Responsible organisation:	Project Coordinator: TECHNIKON Forschungs- und Planungsgesellschaft mbH (TEC)
Tel: **Fax:**	+43 4242 23355 +43 4242 23355 77
Email: **Project website:**	coordination@tecom-project.eu www.tecom-project.eu

Table of Contents

List of figures

1 Publishable summary

1.1 General overview

The collaborative FP7 ICT IP project TECOM (Trusted Embedded Computing) aims to support, continue and intensify the work on Trusted Computing for embedded platforms and related applications. In the last years the security for embedded systems became very crucial for the IT industry as the importance of these heterogeneous platforms is still rising due to their large numbers (much more than PCs) and the growing security relevance.

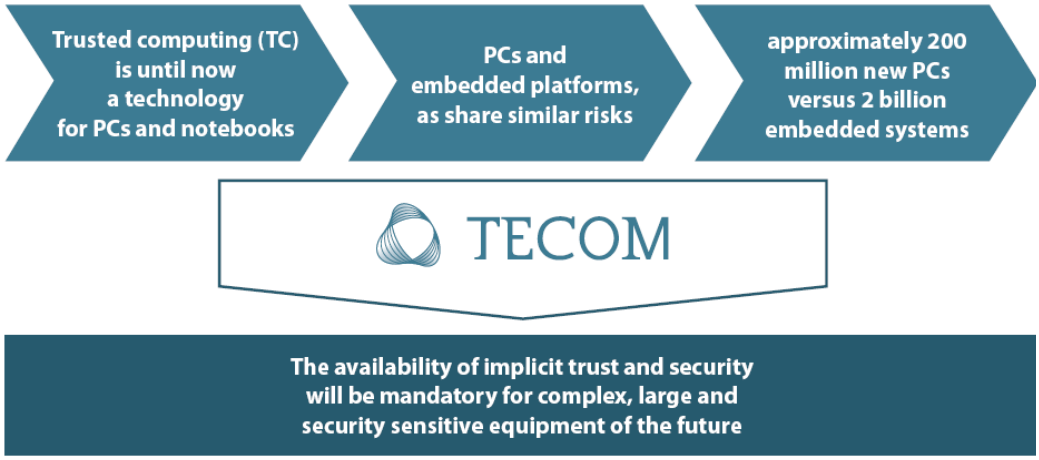

Figure 1: Motivation of the TECOM project

In today's networked environment the well-known lack of the platform security has given rise to waves of successful attacks on IT structures and networks, resulting in severe damages to enterprises and potential failure of critical infrastructures. From the point of European industrial policy, the integration of trust and security into European products can be a major differentiating issue against competition, especially from low price productions in other parts of the world, and also to contribute to a trusted and secure infrastructure and product quality in Europe which could further improve a trust and reliability image for European products. Industrialized societies are increasingly dependant on embedded systems that are getting more and more complex, dynamic and open, while interacting with ever more demanding and heterogeneous environment. However, current systems provide little or no support to determine their level of dependability, security and trustworthiness.

Therefore, the partners within the TECOM project started working on the development of Trusted Computing systems (HW and SW modules together) with the necessary Trusted OS technology and application kernels for the trust and security enhancement of embedded computing platforms.

As TECOM supports all aspects of Embedded Trusted Computing Systems, it focused on the following 3 major working areas:

1. Next generation hardware implementation of the TPM as the central Trusted Computing security element for embedded computing environments.
2. Developing trusted operating systems for embedded platforms concentrating on Virtualization/Hypervisor technology.
3. Integrating these components into a system approach, developing test cases and giving feedback to the OS-, SW- and HW development.

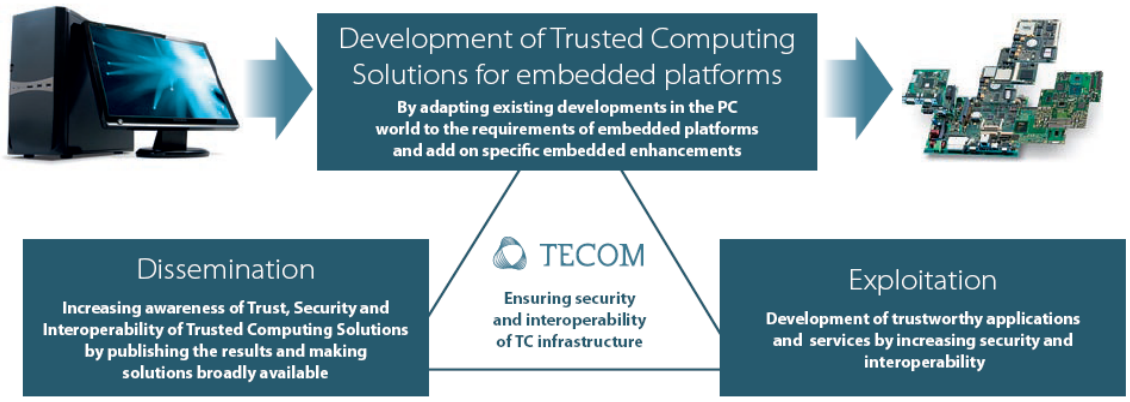

Figure 2: The TECOM activities

1.2 Work performed and the final results

As planned at the beginning of the project, there is now a collection of building blocks and tools made available, which can be further enhanced and brought into the market for making progress in the platform security and for economical and scientific exploitation.

Trusted platform module (TPM) chips with a modified standard for embedded systems

Within the project a TPM as a synthesizable VHDL–library element was developed and can now be integrated together with other embedded host processor systems. It is useful for trusted secure embedded platforms as embedded platforms are limited in size and chip numbers and therefore, a separate chip would not be accepted by the market.

A further difference is the structure of typical embedded OS and application structure. While conventional embedded processor systems are mostly based on standard processor architectures with a homogenous code and data space, it was known from general security research that the logical and physical separation of system and user space was needed to prevent especially integrity attacks from the application program world. Therefore, the already existent TrustZone technology was analysed (which has mechanisms for fulfilling exactly these needs) for interoperability with TC systems. The different features of TC standard and implementation examples with the TrustZone approach were compared and brought together. It was analyzed how they could fit together and benefit from each others functionality.

For fulfilling the needs of embedded system developers, the embedded TPM firmware and the required SW drivers had to be adapted to the needs of potential TECOM users. An example C application package for using the TPMs with ARM processors was developed and is now available as open source to the public for a much easier development of systems, even by newcomers.

Trusted operating systems for embedded computing platforms

Within the project the necessary trusted SW support was developed to make complete trusted solutions (SW and HW) available to the market, as the major package for system development and also as a main issue of exploitation.

Based on the TrustZone supported virtualisation, it was shown that full virtualisation on embedded platforms gives a clear advantage for hosting other state of the art operating systems or middleware, and allows also the integration of existing solution packages together with the guest OS, which can then run on TC platforms with no critical modifications to their kernel. The resulting development effort is then reduced, making

the TrustZone solution the first choice for devices, for which performance and battery life are important.

As these developments were done either by companies which are interested in marketing the results and by universities which make their results public, all the results from WP2 were made public and could be broadly exploited from the beginning of the project. Furthermore, as TECOM was supporting new software technologies, like Android OS (with a broad embedded use scenario not only for smart phones) the usefulness of the findings for the market was shown and the economical exploitation was done together with the newest market trends and technologies.

Support-, middleware and management SW for the control and handling of trusted embedded platforms

The embedded security layers were necessary to develop within the project to enable the delivery of secure and trusted infrastructure, which would drive the trusted embedded OS from WP2 and enable security assurances and applications. These supported functionalities are a main requirement for trusted embedded solutions and therefore, a precondition for acceptance of TECOM results in the market and in public understanding.

The prototype of “Embedded Security Management Framework” was made available and can be further used outside of the project. Also a widely useful application interface, which is based on hardware security functions like TPM or TrustZone equipped processors, was built.

Further, the trusted device drivers and an embedded TSS as basis for setting up all hardware related services were provided. For a better programmability and to ease the use and exploitation of TECOM results for building real embedded systems, further infrastructure services were added, which gives advantages to the expected developers.

Trusted Protocols

For a trusted and secure communication between trusted Platforms as well as untrusted platforms, trustworthy protocols were required to guarantee a reliable, trusted and secure operation of large trusted systems and networks. Such basic technology was a further precondition for making TECOM based results practical useful and deployable into real world applications.

Thus, an implementation of the TNC security network protocol for trusted secure interaction of platforms was done. Further, as the isolated TNC was not sufficient to cover all the requirements needed to address network security, a TNC/VPN solution was implemented, enabling to proper combine the trusted features of TNC with data confidentiality, data integrity, data origin authentication and anti-replay offered by VPN technology, for protecting communication and assuring at the same time the attestation of platforms.

Components of the TECOM platform combined with widespread technologies were also made available. Following the TNC specifications of the fully integrated endpoint solution, the three main entities composing the TNC architecture were developed in the same physical device.

1.2.1 The impact and use of the results

Strategic and economical impact

The TECOM project brought together several parties, which are interested in the development and economical exploitation of TC technology in the field of embedded computer platforms. By combining their capabilities and knowhow they further extended their capabilities in the area of trust and security and became more fitted to the competing requirements of the international market and research environment.

As the results of TECOM were already used and exploited during the project lifetime, TECOM gave indirectly also to other players in the market a boost to innovative products and solutions in the embedded area. Additionally, TECOM resulted in building up new networks and cooperation within the industry and research. TECOM consortium was able to convince them of the advantages of this new technology and several business implementation projects were set for practical use of the findings.

The participation of TECOM members in international standardisation organisations (especially in the Trusted Computing Group) brought the interest of the trusted computing community to new fields of developments. TECOM brought different standards and protocols together, dealing with trust and security (TNC, TCG, TPM, several operating systems, virtualisation etc.), and showed the advantage of combining these for future applications. New technologies and chances for products rose from this work.

Especially European technologies, such as industrial control, intelligent equipment with embedded computing, advanced machinery and automotive got advantage from the use of TECOM ideas and results.

Within the project, progress was gained on how to solve the upcoming problem of software and complexity as well as related testing capability limitations, which occur due to the over proportional rising testing effort. Software packages are becoming larger and larger, time to market will shrink every day and also testing is under time limitations. It becomes more and more difficult to prevent critical software not influencing the other system parts. A typical example is the “blue-screen on the highway”, communicating wrong information to cars due to error propagation from uncritical parts. These effects are producing safety problems due to undetected code errors, which will then generate troubles during execution time. Using Trusted Computing in general, but especially the results from TECOM about the application of virtualised and compartmented operating systems to protect the different processes from each other, promises practical solutions for the next generation of complex industrial systems, such as automotive or protection of critical infrastructures. This will allow the European industry to walk ahead on the way to more intelligent solutions and gain benefit in the international markets.

Substantially improved and implicit trust and security functions in networks and infrastructures, as well as control equipment arising from TECOM, will assist system developers and the industry in general with the development of next generation to more safe and secure equipment and products.

Socio-economic and society Impacts

The broad application of trusted embedded computing in the field of widely used products and services and in technical infrastructures will enable and further increase advanced solutions and products. In parallel, it will also protect citizens, consumers and providers from safety and security deficits as well as from malfunctions of complex equipment and the associated negative effects in daily life. The protection of personal rights through the use of such safe systems is a public task in the interest of the EU and national governments.

TECOM was the first worldwide research and development initiative on embedded trusted computing which brought all relevant stakeholders together. It will give in the future further impulses for research and advances in the use of this technology.

Already today, most of the development and production of trusted computing based security products (especially TPM) is located in Europe, where about 2/3 of the world market is produced. Most of the members of the new TCG workgroup originate from Europe. They all see the large chance for expediting further development and producing such technology worldwide. Europe could have advantage in becoming a leader in producing hardware solutions for trust.

TECOM has given impetus for enabling new technologies and new business models with a high economic impact. Many economical chances for new products and services with a worldwide market capability will now be enabled. The creation and safety of economical progress, and most important creation of new jobs and stabilizing existent jobs will support the further economical and societal development in Europe.

1.3 The TECOM consortium

The composition of the consortium guaranteed an optimal processing of the project targets, as it included every important representative for the different requirements of the TC spectrum. The TECOM consortium included all important groups needed for all aspects of testing and verification of trust and security protocols. In order to cover the topic extensively and to deliver meaningful research results, cooperation was indispensable.

Figure 3: The TECOM consortium

1.4 TECOM Disclaimer

All public information will be marked with the following TECOM project disclaimer:

The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

If you need further public information, please visit our website www.tecom-project.eu or contact the coordinator:

TECOM Project Coordinator
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a, Villach, 9500, Austria
Tel.: +43 4242 233 55, Fax: +43 4242 233 55 77
Email: coordination@tecom-project.eu