Security

2A502: Trusted secure computing (TSC)

Ensuring electronic platforms are secure by design

Computer platforms in business, administrations, industry and consumer electronics tend to be vulnerable simply because security methods are too often external to core processing. TSC developed a family of hardware and software components to overcome this problem. It demonstrated secure-processing capabilities that can be embedded in or close to the core hardware, making them usable by European companies or institutions for critical applications. These concepts and products are already helping Europe develop its own trusted-computing facilities and are interoperable with international standards.

Security and privacy in the average computer tend to be very low grade, relying on add-ons rather than being incorporated into or close to the core processing system. Security-conscious users will typically deploy external security software or specially-protected hardware modules if their applications require additional protection.

Even when trusted-processor modules (TPMs) are standard, their abilities are often not used at full scale because of complicated wake-up routines and a lack of privacy perceived in the interface proposed.

The fundamental problem is that malicious users can circumvent application-security features relatively easily. The MEDEA+ 2A502 TSC project set out to build secure-processing abilities into the hardware itself right from the design stage, completed by removable external secure personal tokens to empower the user and manage privacy.

Designed-in security

Fundamental conditions were seen as:

- **Control of critical technology** – no European organisation or group of users should employ a system in which critical elements are available only from US or Asian companies;
- **Full-system approach** – development of trusted components has to take security of the complete system into account as overall security is no higher than the weakest element; this involved the best trade-off between system integrity management, user identification/authentication and privacy management; and
- **Evaluation and certification by independent third parties** – the security and trust level of critical components must be proven and certified by independent bodies with the expertise to assess the robustness of critical components.

TSC developed a family of secure hardware and components – TPMs, personal secure tokens, software boot loaders and virtualisation kernels – to enable the right system-protection mechanisms to be put in place to ensure the integrity and protection of a complete platform. It covers most components in the critical chain including basic processor hardware, basic input/output system (BIOS), operating system and user-interaction and personal-data protection. Advanced concepts included enabling remote secure management of removable security elements.

Security in the hardware

The consortium demonstrated enforcement of secure and trusted computing for applications in the computer, consumer, telecommunications and wireless areas. The new modules can also be applied to a wide range of devices such as personal digital assistants, mobile phones, TV set-top boxes (STBs), professional mobile radio (PMR) and personal video recorders (PVRs).

Achievements involved:

1. A new scalable 32-bit architecture for TPM circuits with up to a 10x increase in performance and a flexible interface;
2. A new generation of personal secure USB tokens for secure remote administration of fixed and mobile terminals and user-privacy management; and
3. High-performance cryptographic engines for servers with 10x faster processing speeds than before.

Additional software bricks enabled easy introduction of these components in real platforms. Combinations of all these pieces were shown in numerous demonstrators. These included integration of TPMs and personal secure tokens into standard, trusted and even multi-level security computer-operating systems; integration of a TPM in an STB to manage complex transactions over a TV network; and integration of secure tokens into PMR terminals with direct voice-encryption capabilities.

Other demonstrators showed direct transcoding of digital-rights information from Blue-ray to Omarlin DVD recorders, file-transfer control in entertainment networks and anonymity management in 3G mobile phone networks.

Rapid market take-up

TSC results were translatable into commercial products and services almost immediately. STMicroelectronics has sold TPM solutions to personal computer (PC) manufacturers in Asia and the USA. Currently about 90% of PCs are equipped with a TPM, and TSC has helped STMicroelectronics maintain leadership in a market where Europe holds over a 70% market share and to widen its global customer base.

Gemalto is exploiting personal secure tokens and related infrastructure worldwide. Key markets include Internet access and mobile identity management. Several global corporations have adopted this technology – including Orange and Telia.

Bull SAS is working with French secure-credentials agency ANTS on using the TSC cryptographic engine in the next generation of biometric passports. These modules will be incorporated by all countries worldwide that launch such passports.

The mobile anonymous access-control services (MACCS) system developed by Orange and Gemalto will be used in Orange's global service infrastructure. This privacy-enhancing solution enables mobile-phone users to access ticketing services without revealing unnecessary personal information.

And Philips has shown that interchangeability for digital-rights management systems can be achieved at minimum cost to the consumer. With rising demand for Internet access that can handle Blue-ray and digital video broadcasting bandwidths, the availability of a platform that can manage copyright content over the open Internet is a boost to applications developers the world over.

Critical technology in Europe

The secure-processing modules developed within TSC will ensure Europe retains its ability to design and develop trusted computing facilities without having to rely on external suppliers. European industry and market sectors that will benefit include almost any activity that requires processing facilities hardened against external attack.

Security

2A502: Trusted secure computing (TSC)

PARTNERS:

Bertin Technologies
Bull
CEA-LETI
Celestica Valencia
EADS
Ecole Nationale Supérieure des Mines de Saint-Etienne
FT R&D/Orange
Fundacion European Software Institute
Gemalto (Axalto SA and Gemplus SA)
Philips AT
STMicroelectronics
TB-Security
TB-Solutions Technologies Software
Technikon
Uni Paris VI (LIP 6)

PROJECT LEADER:

Jean-Pierre Tual
Gemalto

KEY PROJECT DATES:

Start:	September 2006
End:	December 2009

COUNTRIES INVOLVED:

Austria
France
The Netherlands
Spain

MEDEA+ Office
140bis, Rue de Rennes
F-75006 Paris
France
Tel.: +33 1 40 64 45 60
Fax: +33 1 40 64 45 89
Email: medeaplus@medeaplus.org
http://www.medeaplus.org

EUREKA Σ!

MEDEA+ Σ!2365 is the industry-driven pan-European programme for advanced co-operative R&D in microelectronics to ensure Europe's technological and industrial competitiveness in this sector on a worldwide basis.

MEDEA+ focuses on enabling technologies for the Information Society and aims to make Europe a leader in system innovation on silicon.