TOISE: Trusted Computing for European Embedded devices

Iraklis Anagnostopoulos[1], Alexandros Bartzas[1], DimitriosSoudris[1], Bernard Candaele[2], François Tuot[3], Guido Bertoni[4], Laurent Sourgen[5], Alain Merle[6], Florentin Demetrescu[7], Louis Granboulan[8], Guillaume Duc[9], Phillippe Nguyen[10], Emmanuel Vaumorin[11], Paolo Amato[12], Massimo Toffeti[13], Luca Breveglieri[14], Segio Ruocco[15], Thierry Galere[16], Apostolos Leventis[17], Carles Ferrer[18], Bruno Cendron[19], Pablo Sanchez[20]

[1]Institute of Communication and Computer Systems Greece, [2]Thales France, [3]Gemalto France, [4]STMicroelectronics Italy, [5]STMicroelectronics France, [6]CEA Leti, [7]Cassidian, [8]EADS IW, [9]Institut Telecom Paris Tech, [10]Secure-IC, [11]Magillem Design Services, [12]Micron, [13]Azcom Technology Srl, [14]Politecnico di Milano, [15]Universita di Milano Biccoca, [16]Proton, [17]Hellenic Aerospace Industry, [18]Agencia Consejo Superior de Investigaciones CNM, [19]Technologias Servicios Telematicos Sistemas, [20]Universidad de Cantabria

Abstract

For the future European applications such as Smart Grids for electricity network, smart low energy controlled home appliance, environmental or infrastructure sensor networks, and more generally management of trusted components, more security over communication networks, wireless communications and access control, a number of technologies need to be developed and put in place to make the solutions smarter and more secure.

TOISE project proposes to address the secure tamper resistant solutions needed by the related embedded applications. Trusted Computing now in practice for the PC and workstation area provides a proven approach face to new attacks, by implementing a chain of authentication and integrity from the boot of the computing platform to the applications set up.

The TOISE project aims at the development of tamper resistant hardware and firmware mechanisms applicable for both lightweight embedded devices and as security anchors with embedded platforms required by the future European applications such as Smart power Grids, Smart networked and controlled home appliances, Environmental or Infrastructure sensor networks, and generally management of Trusted components, more Security over Communication networks and more Wireless Communications.

A recent study says that 60 percent of new virtualized servers will be less secure than the Physical servers they replace through 2012. Analysts warned that many virtualization deployment and new interconnected infrastructure projects are being undertaken without involving the information security team in the initial architecture and planning stages. TOISE is a European-wide proposal in the frame of ENIAC to study and develop the secure solutions required by future applications, namely energy grids, related smart and networked home appliances, sensor networks and wireless communications and management of trusted objects.

Electrical grid will require significant dependence on distributed intelligence and broadband communication capabilities. Power meters are demanded to control appliances at consumer homes to reduce energy. These demanded capabilities require the latest in proven security technology for large, wide area communications networks.

Sensor networks are used for applications such environmental monitoring, airports and critical sites safety, infrastructure monitoring, health care. Owing the property of the sensor devices in non-controlled environment, the network can easily be compromised by an attacker. Security and survivability are very important for applications onto wireless sensor networks

Wireless connected devices have to deal with two majors security issues, ie the protection of content and the protection of personal information. Robust stakeholders' segregation, security policy enforcement and mutual assets isolation is a challenge in increasingly open "computing" devices exposed and vulnerable to everyday new malware, software and hardware attacks. Some of the related security challenges address open trusted platforms and trusted execution environments, identification and authentication and secure storage

TOISE proposes to study and extend hardware and firmware tamper-resistance devices architectures and/or using lightweight TPM (Trusted Platform Module/TCG) concepts to smart grid and particularly smart-meters environments, which would address new "energy efficiency" in trusted applications. Also, investigating new anti-counterfeiting architectures and implementations so that they fit under Communications, Wireless networks and management of trusted devices.

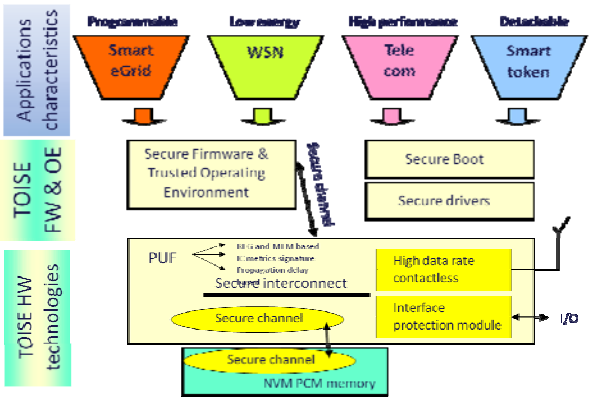

Figure 1: TOISE project overview

TOISE's objective are (i) to investigate and implement secure solutions for the design of smart-grid applications and their deployment in large-scale networked and systems and (ii) to investigate and implement secure wireless sensor networks, to address secure authentication devices, to study and implement new generation of trusted portable devices as well secure storage in memory and study hardware secure items to add to TPM for embedded system.

Partially supported by the ENIAC funded TOISE 282557-2Project – http://www.toise.eu