Smart **O**n **S**mart

An innovative secured system architecture concept

Michel Agoyan, Bruno Robisson

CEA LETI /DSIS/LCS/SAS CMP GC, 880 route de Mimet 13541 Gardanne, FRANCE

michel.agoyan@cea.fr, bruno.robisson@cea.fr

Pirouz Bazargan-Sabet

UPMC - LIP6, Boîte courrier 167, 4 place Jussieu 75252 PARIS cedex 05, FRANCE

Pirouz.Bazargan-Sabet@lip6.fr

Guillaume Phan

TRUSTED-Logic, 5 rue du Bailliage 78000 Versailles, FRANCE

guillaume.phan@trusted-logic.fr

Sébastien Le Henaff

VIACCESS, Les Collines de l'Arche,Opéra C, 92057 Paris La Defense Cedex, FRANCE

sebastien.lehenaff@viaccess.com

Abstract

'Smart On Smart' (SOS) is a project launched in 2008 and funded by the 'Agence Nationale pour la Recherche'. This project aims at helping the partnership formed by Trusted Logic, Viaccess, LIP6, and the CEA-LETI to study an innovative secure system architecture. This architecture is based on two parts. The first one called the host system is in charge of the main application and processes the sensitive data. Connected to the host system the second part called the audit system is strictly dedicated to the security strategy response of the whole system.
The underlying idea is that such an architecture will help to build a better secure system. For instance it becomes possible to improve the intelligence of the security policy to be able to differentiate a normal error behaviour from a suspect one. Since the whole system's security reliability is adjustable it becomes also possible to maximise the performance when nonsensitive data are processed. Non repeatable behaviour and response of the system under attack could be also programmed in order to counter the attacker.
One of the main tasks is to define a hardware architecture corresponding to this concept for which a safe boundary has to be established between the two systems. The software part and in particular the way the security policy is implemented on the audit system is also a non obvious task especially because the overhead due to this additional audit system has to be the lowest possible in order to be cost-effective.
We are building a proof of concept around a pay TV application. Additional hardware features are used to emulate fault injection attacks for the demo. We are

building the hardware model on an FPGA board proving also that such an architecture fits an FPGA based system.