GTA / UFRJ
GRUPO DE TELEINFORMÁTICA E AUTOMAÇÃO

UFRJ COPPE

PALESTRA

Hans Brandl

Infineon Technologies AG, Platform Security group
Munich, Germany

Palestra: Dia 21/3/12 das 10:30 às 11:30 – Sala H - 301

Trusted computing Basics, Technology and Applications

Abstract – ***Trusted Computing (TC) is now an already established technology, which increases trust and security on computing platforms. The international standardisation organisation Trusted Computing Group (TCG) with about 20 specialized work groups created an open, free available standardisation framework containing architecture, implementation and applications. The hardware implementation of the standard, the Trusted Platform Module is meanwhile an integrated part in nearly every new PC and more new applications e.g. in the embedded computing area are coming up. This talk describes the basics of TC, the differences and synergies between TC and standard security technology, functionality, PC integration framework, upcoming new types and applications like mobile trusted module for mobile phones, embedded computing use cases in industrial control, traffic speeding cameras or gambling. Also an overview about related public research projects is given.***

Biography: Hans Brandl studied communication technology at the Technical University in Munich. Following the development and product management of cryptographic, security devices and systems for protected governmental communication applications at Siemens AG defence group, he changed 1997 to Infineon chipcard and security division. There he contributed to the development of the world´s first really secure smartcard processor and continued working on the field of integrated security. He is now responsible for technical marketing of trusted computing solutions like Trusted Platform modules and other advanced security devices. Related to these company activities he is widely engaged within the Trusted Computing Group [TCG] standardisation activities where he is chair of the embedded systems working groups which is currently defining new embedded TPM specifications for a broad spectrum of applications. He is also chair of the TCG certification program committee, chair of the next generation working group and member of the board of directors. Additionally he iniated and participated in several security and trust related public research programs of the European Union.