Using Trusted Computing for enhancing Embedded Computing Platforms

Overview:

The Trusted Computing (TC) technology is today already widely applied on Personal Computer (PC) oriented platforms. Typical use scenarios are measuring system integrity for Trusted Operating Systems, secure storage for key material and certificates, identification of platforms and together with other technology like smartcards and biometrics also the authentication and identification of computer users.

Parallel to the PC world there is an additional computing universe, the world of embedded computing.

An embedded computing system is a special-purpose system in which the computer is completely encapsulated by the device it controls. Physically, embedded systems range from portable devices such as MP3 players, to large stationary installations like traffic lights or factory controllers.

Embedded systems are designed to do some specific task, rather than be a general-purpose computer for multiple tasks. Some also have real-time performance constraints that must be met, for reason such as safety and usability; others may have low or no performance requirements, allowing the system hardware to be simplified to reduce costs.

Due to the upcoming broad use and importance of these application in daily life, similar trust and security requirements are coming up, where the application of TC or at least the integration of a Trusted Platform Module (TPM) could increase system security and performance.

Especially Trusted Operating Systems based on virtualization and compartment technology can not only increase trust and security but also the reliability and safety by protecting computing processes as well as application kernels against negative influence or erroneous states from other parts of the total system or from external networks. This broad use of TC will allow protecting the upcoming generation of embedded systems against the whole variation of security incidents well known from the PC world.

Based on the public available standards of the Trusted Computing Group it will be shown how software modules and operating systems for all areas of trusted and secure computing in the embedded regime like mobile phones, trusted networking, and secure content management for Digital Rights Management (DRM), industrial control, automotive and a lot of similar applications will benefit from the integration of protective security and trust requirements.

Contents

1 Overview:

The Trusted Computing (TC) technology is today already widely applied on Personal Computer (PC) oriented platforms. Typical use scenarios are measuring system integrity for Trusted Operating Systems, secure storage for key material and certificates, identification of platforms and together with other technology like smartcards and biometrics also the authentication and identification of computer users.

Parallel to the PC world there is an additional computing universe, the world of embedded computing.

An embedded computing system is a special-purpose system in which the computer is completely encapsulated by the device it controls. Physically, embedded systems range from portable devices such as MP3 players, to large stationary installations like traffic lights or factory controllers.

Embedded systems are designed to do some specific task, rather than be a general-purpose computer for multiple tasks. Some also have real-time performance constraints that must be met, for reason such as safety and usability; others may have low or no performance requirements, allowing the system hardware to be simplified to reduce costs.

Due to the upcoming broad use and importance of these application in daily life, similar trust and security requirements are coming up, where the application of TC or at least the integration of a Trusted Platform Module (TPM) could increase system security and performance.

Especially Trusted Operating Systems based on virtualization and compartment technology can not only increase trust and security but also the reliability and safety by protecting computing processes as well as application kernels against negative influence or erroneous states from other parts of the total system or from external networks. This broad use of TC will allow protecting the upcoming generation of embedded systems against the whole variation of security incidents well known from the PC world.

Based on the public available standards of the Trusted Computing Group it will be shown how software modules and operating systems for all areas of trusted and secure computing in the embedded regime like mobile phones, trusted networking, and secure content management for Digital Rights Management (DRM), industrial control, automotive and a lot of similar applications will benefit from the integration of protective security and trust requirements.

2 Introduction

Industrialized societies are increasingly dependant on embedded systems that are getting more and more complex, dynamic, open, while interacting with an progressively more demanding and heterogeneous environment. As a consequence, the reliability and security of these systems have become major concerns. However, current systems provide little or no support to determine their level of dependability and trustworthiness. An increasing number of external security attacks as well as design weaknesses in operating systems, especially in the PC world, have resulted in large economical damages and as a consequence, difficulties to attain user acceptance and getting accepted by the market.

In order to allow users to place reliance in IT systems, services and especially into intelligent products based on the performance of embedded computing, their trust should stem from justified expectations rather than just “firm belief”. Generalized notions of “trust” (accepted dependence) and “trustworthiness” (measure of risk) refer to generic properties that go beyond security and relate, in this respect, strongly to the concepts of “dependence” and “dependability”.

As a follow-up to these demands, the Trusted Computing Group (TCG) [an international industrial standardization group with the membership of all major computer and software companies (currently about 130 members), www.trustedcomputinggroup.org] has defined a specification (now about 1200 pages and rising) for realizing and implementing Trusted Computing on different computing platforms. This Trusted Computing standard is already becoming the cornerstone for future PC generations as well as should also be used with other critical computing platforms like mobile phones, content management (DRM), industrial control (automotive) and much more. The TCG standard is based on a cost-optimized security kernel chip, the “Trusted Platform Module” (TPM), with which it will be possible to establish a chain of trust, which not only gives trust in the platform integrity, but also delivers a trust reference for applications and operating systems and can also support safety for critical applications.

Trust according to the TCG is defined as “Trust is the expectation that a device will behave in a particular manner for a specific purpose”. This general approach supports the efficient construction of trusted and secure systems in the whole world of electronic systems (from PCs to embedded systems) and can also include features like safety for protecting related execution assets.

The TCG standard controls and regulates only this trusted kernel element and the handling of critical data for trust and security implementation. It is independent from the processor base, as it is also Operating System agnostic. This allows on one hand, an easy and high-performing adaptation to different computing platforms like Servers and PCs and on the other hand it scales well to different embedded platforms.

3 Market relevance

Trusted computing secures and protects applications in many industrial sector(s):

- *Open Servers and PC's*
- *Mobile Chipset providers*
- *Smart-Cards and Trusted Personal Devices*
- *Consumer Electronics*
- *Professional Mobile Radio Communication*
- *Embedded systems in general*

A reference for the importance of trusted computing is the expected sales figure for the Trusted Platform Module (TPM), the central security kernel of trusted computing (TC). Every TPM in a platform enables the capabilities for trusted security and behaviour.

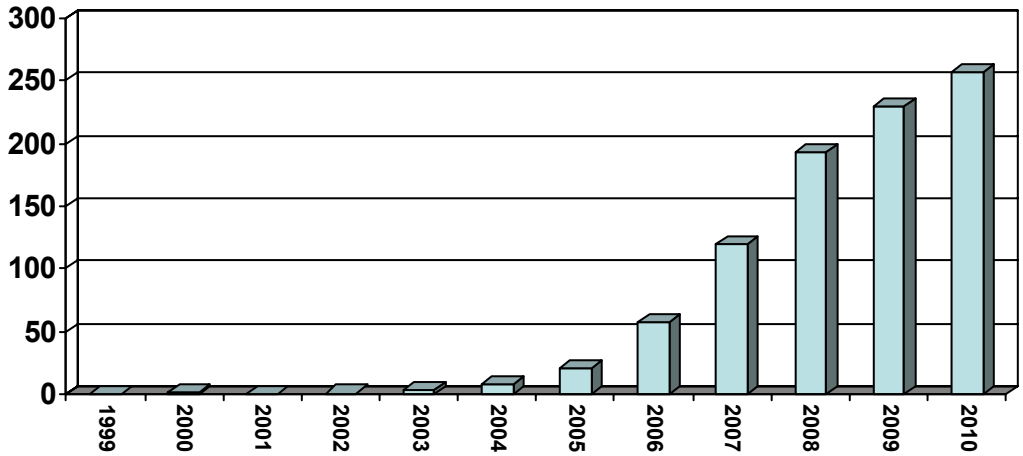

Figure 1: TPM sales evolution 1999-2010 (source IDC)

While most of the figures still are PC platforms, embedded trust will rise similarly.

According to the IDC, the number of TPMs sold in the Server/PC world should reach more than 200 million units by year 2010. This is also the number of produced PCs per year, which means that nearly every new PC will contain a TPM as a basis for future and advanced security mechanism.

Due to this broad distribution and use in the PC world, this technology is assumed to rise on an economical and scientific stable fundament and can therefore be used also for embedded platforms without too many risks.

3.1 Mobile Chip sets

According to latest ARM forecasts, the number of mobile devices should go well over 1 billion units by 2010 as shown in the figure below. The projected number of Smart Phones (3 SOC average) and Feature Phones (1, 5 SOC average), represent a big share of this market. The increasing functionality with required trusted software gives a high demand of such operating systems and applications. It can be projected that a huge proportion of these figures will include strong Trust and Security features.

Applications * ARM Estimate	TAM 2004	TAM 2010	Avg. SOCs per Product [2010]*
Smart Phones	32	255	3,0
Feature Phones	224	340	1,5
Voice Phones	384	255	1,0
Cordless Phones	256	561	1,0
Bluetooth (Headset etc.)	47	284	1,0
PDAs	10	16	2,0
Portable Media Players	40	168	1,0

Figure 2: Total Available Market Forecast

3.2 Consumer Electronics

For the consumer electronics environment the relevance of this project pivots around the trustworthiness of consumer electronics platforms. More and more consumer electronics platforms will be connected to the Internet. This increasing connectivity will enable new distribution mechanisms, but it will also increase the risks for both the devices and the content owners and distributors.

3.3 Public safety

In the public safety and professional market, the project relevance will be around the need of trustworthy security solutions for a wide range of equipment (PMR terminal, PC, server, ….) which are more and more composed of blocks and solutions coming from external and with strong need of interoperability (COTS, standard OS, portability,…). The rising «Homeland Security» market is estimated at 37 G€ in 2005 and will imply the use of wide range of secured equipment among which one very important is the PMR (mobile) market.

3.4 Road Vehicles

With more and more telematics functions for cars, trucks and the entire traffic system, trusted in-vehicle systems are a necessary requirement to enhance the safety of vehicles and passengers on European roads and to guarantee the safe operation of theses and future telematics functions and services.

It's a fact that the share of embedded electronics and more precisely embedded software in the automotive environment is growing. In 2006, the electronic embedded system will represent at least 25% of the total cost of a car and more than 35% for a high-end model

The emergence of automotive embedded networks such as LIN, CAN, TTP/C, FlexRay, MOST, IDB-1394 and the growing number of ECUs in the vehicle with new functionalities such as Flash loader, Security Modules, etc. lead to the increase of complexity and requirements on the reliability in the different vehicle domains (power train, chassis, body and telematics/multimedia).

But the increasing embedded systems lead also to the feasibility to introduce new and innovative safety and non-safety applications to increase the safety in European road traffic, to enhance the convenience of the drivers and to enable entirely new business models to strengthen the national and European economies.

A prerequisite for these new market opportunities for vehicle manufacturers, suppliers and telematics service providers is the establishment of trust in the embedded systems and applications. Trust in the way to protect the vehicle e.g., against "adjustment" of mileage counters or the "SW-tuning" of the engine control but also trust in the secure communication from the vehicle with the outside world (V2X communication). Trusted Embedded Computing will therefore lower costs by protecting embedded systems from costly malicious security attacks and accidental errors, and also enables and drives entirely new business models.

3.5 Mobile

Mobile Trusted Computing Platforms are not available yet. The current work performed in TCG/MPWG indicates that TC will play a major role in mobile applications. Our developments (Mobile TPM, integrated DRM and protection against SW attacks) will become available by the last year of the project (2009) and will be completely in-line with the market demand, as requested by the new emerging applications (DRM and Mobile TV protection - requesting a secure channel, Liberty Alliance/3GPP inter-working, mobile Payment and Ticketing- requiring trusted transaction execution).

3.6 Trustable terminal market

Mobile phones lead the market and will represent the highest volumes for the next few years. However other devices such as home gateways (broadband internet access devices), multimedia devices (set top boxes, audio and video personal players), and automotive embedded devices represent the fastest growing segments.

Despite the huge growth in mobile phone subscriber numbers over the past years (over 1, 5 billion in June 2004 with 648 million mobile phone units shipments in 2004; according to IDC) the mobile phone shipments should continue to expand during the next years according to Jon Peddie Research and reach about 800 million units in 2008.

3.7 Trust, a market criteria for acceptance

Trust and confidence are key factors to transform electronic market places into effective environments to do e-business and e-activities. To achieve trust and confidence requires not only security technologies but also, and even more importantly, the technical and organizational frameworks and infrastructures that make the deployment of these technologies viable and consistent.

While there are some similarities between above environments, there are special needs and constraints that have to be taken into account. The main difference is the availability of resources – while a server platform has practically unlimited computing power and network connectivity, some platforms may be even more restricted than a cellular phone.

Another important issue is the dependability of the platform. While a PC or a cellular phone may safely shut down or block part of the functionality if the platform is under attack, an industrial controller or a car may need to keep operating and only shut down if a safe state is reached.

4 Technological state-of-the-art

Each of us frequently uses information technology systems for professional or private purposes, and we tend to assume that these systems behave the way we expect them to. For software in particular, we assume that we can control actions performed by IT systems of our own. However, we do not have a reason to take the trustworthiness of our IT systems for granted (as each one of us recognizes from time to time).

We expect our systems to be reliable and resilient to attacks, that private data is protected and kept confidential. Until recently, security was tried to be achieved by additions such as encryption or anti-virus software that were made into a weak operating system.

Unfortunately the ever increasing complexity of IT has led to a regime of automated patch management that is beyond the users' comprehension, and our trust is on trial on a daily basis due to viruses, worms, spy- and malware that can remotely control our computers.

Software components can be modified by third parties that are neither known nor trusted by the owners and users of computer platforms. Applications can be tricked into displaying behavior not intended by their implementers and innocuous programs can often be coerced into raising their privileges, which may result in subverting the system configuration and altering its policy. Much internal damage can arise from unauthorized data access and leakage, which may lead to system degradation over time. Eventually, this also sheds doubt on the legal validity of electronic interactions performed with external parties.

Today typical computing platforms (from PCs to embedded systems) lack mostly all type of protection or trust. Instead of integrating security into the OS kernel of a computer, standard unsafe OS kernels are used, which are then tried to be protected by several skins or layers of protection SW (like Virus scanners, Firewalls and similar). However these external protection mechanisms are barely protective enough against today's threats. Mostly they are dedicated to specific attacks or threats and therefore new upcoming dangers always find a way through the hull. As it is well known from existing security research, real tight protection can only be reached by a seamless integration of the security module and kernel into the core functionality. Also conventional storage and processing of data is regularly done on open memory, which can easily be attacked and altered even by other SW modules. As we know already from high trusted systems, only a separated and protected hardware security kernel (e.g. a guarded and shielded chip) gives enough prevention against these threats.

Also existing security applications are mostly only dedicated to the encryption or digital signing of data with unhardened software tools. A well known example is the increasing attacks on home banking security. Today's secure home banking packages are either fitted out with high security smart cards, which are used for signing the transaction process or use more conventional authentication tools for security like PIN/TAN authentication. Typical attacks are therefore not against high level smart cards or protected TANs (which would be too much of a hurdle) but for the soft targets. They change the computing host software by viruses or protection holes and exploit then the data or protection mechanisms with a piece of SW with fully different functionalities and features.

The same can be observed at attacks with manipulated identity of system parts like phishing (with the utilization of human weakness) or manipulating of machine certifications in untrusted storage locations (where the machines weakness is the matter).

What we need for the upcoming generation of secure systems is not only encryption of data links, secure key and certificate storage and safe authentication of the partners and machines during an transaction, but far more a reliable and protected platform with a proof of platform integrity and resulting from this trust into the correctness of the complete host system.

4.1 Technological Innovation for trusted operating systems for embedded use

In response to these problems, the before mentioned Trusted Computing Group has defined a standard for trusted computing elements and building blocks for all types of computing .platforms. However this standard does not define how a complete OS or computing system can be fitted with trust and protection. It is therefore the task of the OS or system developer, to integrate these measures wisely and carefully into his system.

Embedded Trusted Computing aims at increasing the security of and the trust in the Operating System (OS) and the supportive peripheral modules. This begins at the very lowest level of the platform, with the controlled loading of an operating system and goes on level by level. The procedure is verified after each level by using data integrity measurements. If this is done without errors, we know that we have a correctly loaded OS, in which the functions and different parts of the system (e.g. drivers) can be verified at run time.

(i) Kernel element of this layered verification process will be based on **a hardware root of trust.** This is a tamperproof security hardware module (like a high security smart card chip which is directly mounted to the motherboard, to support the integrity checks mentioned above, as well as the secure storage of keys and other data in a protected chip. This chip is referred to as 'Trusted Platform Module' (TPM) and is the central security

kernel. This hardware has been specified by the Trusted Computing Group (TCG) and is commercially available for PC motherboard structures and deployed in a large scale.

(ii) It is accompanied by a special security enhanced platform processor (CPU) and peripherals architecture that removes some well-known security architecture deficits. This includes mechanisms for policing memory access (including DMA, Direct Memory Access) as well as novel features supporting privileged execution and interception. These features are prerequisites for separating sensitive parts of the OS kernel (The new Pentium for PCs as well as ARMs Trustzone processors for embedded are typical examples. We will use them within the project).

(iii) On the Top of this configuration the trusted OS has the obligation to handle all these security building blocks and hardware capabilities to protect not only its own correctness, but also the integrity of the applications and the whole system. The OS should support the contract-based security verification in order to trust new applications or updates to be uploaded without manual interaction.

Published by:
Infineon Technologies AG
St.-Martin-Strasse 53
81669 Munich, Germany
Phone: +49-89-234-80000
www.infineon.com/TPM
security.chipcards.ics@infineon.com