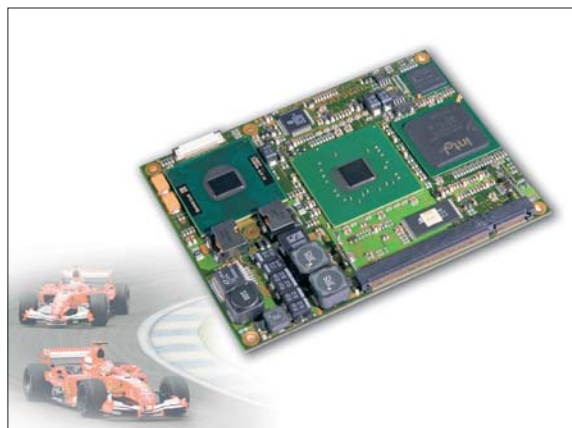


Intellectual property protection technologies for Computer-on-Modules

by Konrad Löckler, MSC

The following article shows the latest technologies for IP protection, implemented on a COM Express module using the Intel Core 2 Duo processor and a Phoenix TrustedCore BIOS.



COM Express module
CXB-CD945

■ Today the embedded computer world is more and more confronted with problems that are well known by users of home and office computers. They have to struggle with attacks from the networks every day and companies also have to invest a lot for protection of their intellectual property. In the past manufacturers of complex machines using embedded computer technology had to implement proprietary solutions in order to achieve the necessary protection against damage or theft of their IP. This always caused high costs and long development cycles. From now on standardized solutions in the areas of COMs (computer-on-modules) bring relief from these problems and even a better protection.

COM products conquered the Embedded PC market during the past five years mainly in the form of ETX modules and set here new standards, which were not conceivable in former times in this width. At present a technology change from parallel busses and interfaces to serial interfaces is taking place within this area. COM Express modules begin to flow into new designs as successors of the ETX products. The CXB-CD945 (see box) represents the highest level of security currently available in Intel architecture based computer designs. With its new CSS (core system software) platform “TrustedCore” Phoenix has enhanced the BIOS further to a crucial component within the so-

called chain-of-trust, a closed chain of software routines, which guarantees the integrity and authenticity of a system from switching on the PC until the application software starts. For this purpose TrustedCore contains a software module “StrongROM”, which makes the necessary security services available in a protected storage area. These services include functions such as encrypting and hashing algorithms (AES, RSA, SHA-1), a random-number generator, signature verification and a secured key administration. At boot time StrongROM is loaded from flash into a blocked area of the SMM memory, a protected storage area, which can be accessed neither by application software nor by the operating system. Thus it is guaranteed that this code cannot be read out or changed.

In terms of a unique and unambiguous device identification StrongROM’s “Device Master Key” (DMK) is a very interesting function. The DMK provides a unique device identification either within the network or for local application programs written accordingly. Using this DMK prevents in a simple manner that copied software from being operated on other devices except the one it is intended for. This key is stored in a safe storage place (“Secure Storage”) either in CMOS memory or inside the BIOS flash device. In both cases it is guaranteed that this memory is accessible only by the BIOS and only for a short time immediately after switching power on. In order

to close the “chain-of-trust” beyond the TrustedCore BIOS it is necessary to secure the further steps of the booting process also. Calling the INT 19h routine within the BIOS usually hands over control to the master-boot-record (MBR), the first sector of the fixed disk.

The MBR then looks for the boot sector on the “active” partition and that again loads the actual boot loader of the respective operating system. In a secured system all these steps have to be protected as well and any change must be recognized. For this purpose the INT 19h module within the TrustedCore code may contain the MBR authentication module, which examines both the MBR and the boot sector for integrity. Depending upon the configuration and capabilities of the operating system also parts of the operating system can be examined by using the optional ESM (Extended Security Module), which can be integrated into the boot procedure. Thus any gap up to the complete take-over of control by the operating system is closed. If one of the secured modules in this chain was manipulated, the operating system will stop execution and thus prevent any misuse of the device by malicious software. The MBR authentication module can be used on ATA drives or on USB flash drives formatted like a hard disk. Within particularly sensitive areas the presence of a TPM chip is frequently demanded. In MSC’s COM Express module In-

fineon's TPM SLB9635TT1.2 was implemented. Combined with the Phoenix TrustedCore BIOS this TPM brings the maximum security possible at present into the device and it already fulfils the requirements of the latest Microsoft operating system Windows Vista. The TPM is connected over the LPC bus. It contains an efficient 16-bit microcontroller among other things like an encryption unit (RSA with up to 2048 bits key length, SHA-1 hash algorithms), non-volatile memory and a random-number generator. These hardware-supported functions are merged seamlessly into the TrustedCore BIOS and thus complete MSC's security concept optimizing performance and security on the embedded computer module. If necessary, the TrustedCore BIOS platform can be extended using Phoenix's PBA module. Thus the identification of the system user is accomplished at the very beginning of the boot procedure – at a time when the fixed disk possibly is still locked by a special password. This authentication then automatically leads to the unlocking of the fixed disk. Subsequently, the credential already verified by the BIOS is passed on to the operating system by means of the Microsoft GINA protocol, which then allows Windows to boot without further login query. Thus user authentication procedure is necessary

only once and is accomplished at the beginning of the boot sequence bringing an additional contribution to overall system security. There are different methods for proofing the user's identity. Besides the conventional password input using a keyboard, a SmartCard, a USB stick (Smart token) or a finger print sensor can be supported. Phoenix's PBA software is offered in different languages allowing the user to choose the respective national language for the authentication query. Of course, tampering of the BIOS code within the flash would be fatal for the security of the overall system. To prevent this and to provide a way for maintenance updates of the BIOS at the end-customer at the same time the update procedure itself had to be secured, too. The protected TrustedCore BIOS contains a mechanism that allows an update only with a digitally signed update file. The update Tool "SecureFlash" uses the safety functions of StrongROM to verify the validity of the update file. By this it prevents inadvertent overwriting of the current BIOS code, programming of the wrong firmware and - above all - malicious manipulations of the TrustedCore BIOS by hackers or BIOS viruses. The safety functions implemented in the COM Express module are completed by additionally available API interfaces, development tools

and programs provided by Phoenix Technologies, which can accelerate the development of a safe embedded solution substantially. "Trust Connector" makes a clear, unambiguous connection between the device and the application program. Based on the device master key (DMK) mentioned earlier, the execution of the application software is bound to the device having the correct DMK. This can be guaranteed locally or in the network. This kind of device authentication prevents any copying of high-quality software solutions onto other devices as well as access of unauthorised devices to computers in the network. With "Security SDK" Phoenix offers an extensive collection of APIs for developing protected software. "Recover pro", a product for automatic backup of data, programs and operating system into a secured area on the fixed disk can increase reliability further on both stationary and mobile embedded devices. More and more industrial automation, medical technology or casino gaming applications have to be regarded as endangered besides the classical domains like e-commerce, banking etc. Since financial damage through illegal copies of complete devices constantly increases in the course of globalization, in more and more applications the degree of protection can never be high enough. ■