(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
3 June 2010 (03.06.2010)

PCT

(10) International Publication Number
WO 2010/060468 A1

(51) International Patent Classification:
G06F 21/00 (2006.01) *G06F 9/445* (2006.01)
G06F 15/177 (2006.01)

(21) International Application Number:
PCT/EP2008/066205

(22) International Filing Date:
26 November 2008 (26.11.2008)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FIN-02610 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ABENDROTH, Jörg** [DE/DE]; Weidener Str. 3, 81737 München (DE). **MOELLER, Wolf-Dietrich** [DE/DE]; Elise-Aulinger-Str. 22, 81739 München (DE). **SCHÄFER, Manfred** [DE/DE]; St.-Josef-Str. 16, 85661 Forstinning (DE).

(74) Common Representative: **NOKIA SIEMENS NETWORKS OY**; COO RTP IPR, Patent Administration, 80240 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

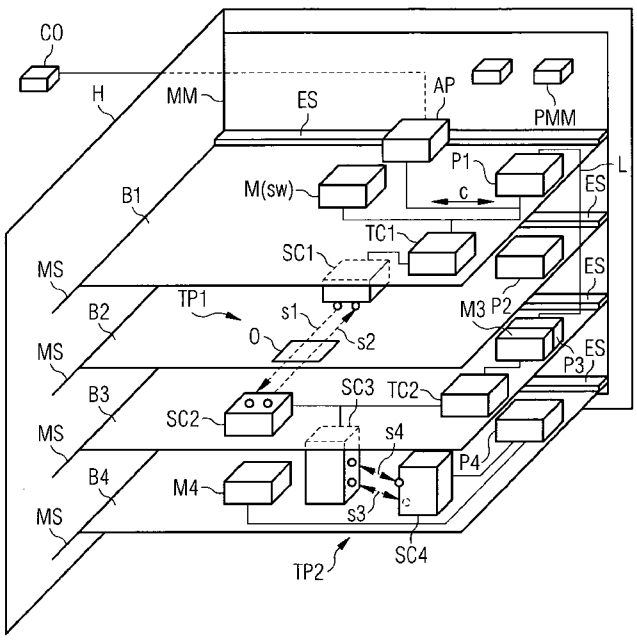
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: MULTI-MODULE SYSTEM COMPRISING A TRUSTED CONTROLLER, A MODULE OF SUCH MULTI-MODULE SYSTEM, AND A METHOD FOR CONTROLLING SUCH MULTI-MODULE SYSTEM

FIG 1



(57) Abstract: The invention regards to a multi-module system comprising a plurality of modules (B1, B2, B3, B4, MM) each having at least one processor (P1, P2, P3, P4, MMP), at least one memory (M) for storing data and/or software (sw) to be loaded into at least one of such processors (P1), a trusted controller (TC1) mounted on at least a first module (B1) of these modules and being designed for trusted booting of at least this first module (B1) or of its processor (P1), and a second access point (AP) for communication of data (c) with an outside component (CO) outside of the multi-module system. In such system the second access point is a single access point representing a single system for the outside component (CO) outside of the multi-module system, and the processors (P1, P3) of at least two of the modules (B1, B3) are only bootable under control of the trusted controller (TC1).

WO 2010/060468 A1

Multi-module system comprising a trusted controller, a module of such multi-module system, and a method for controlling such multi-module system

Technical Field

The invention regards to a multi-module system comprising a trusted controller according to pre-characterizing part of claim 1, to a module of such multi-module system, and to a method for controlling such multi-module system.

Background Art

In current TCG standards (TCG: Trusted Computing Group), mechanisms to provide system level integrity are mainly focusing on software aspects and do not provide means against hardware based attacks on module level except those directly connected with TPM implementations (TPM: Trusted Platform modules). Moreover, providing roots of trust and the notion of “transitive trust” is based on mechanisms that are specified for single processor systems physically tightly connected with associated memory or memory space. As long as any program code running in the system, including virtualisation layers and any software running on top of it, it goes through the integrity protection processes specified by TPM paradigms. Also in virtualised systems there exists only one complex boot sequence.

The MTM standard (MTM: Mobile Trusted modules) alters the standard TPM concept to include mobile device virtualisation concepts. MTM concepts introduce and support “compartmentalization” based on virtualisation of the trust principles defined with TPM and MTM usage. MTM mainly aims to

support "secure boot", i.e. with local enforcement, and certificate controlled software download in addition to some TPM capabilities like device authentication/attestation.

Part of the MTM standard are trust mechanisms supporting secure compartments where memory can be shared. The secure process-level separation of the compartments and memory is presupposed, but up to now has been out of scope of the actual MTM specification. There are limits of MTM concepts in particular because attacks at module level have been factored out. Any problem arising when separate components have to be integrity protected as a whole cannot be solved using native TCG technology. Securing of multiple separated CPU controlled components with only one TPM has not been considered so far and is not part of the TPM standards. The only solution would be to equip each module with an own TPM.

The native MTM solution is mainly suited for such a virtualised environment, where one CPU or even a multi-core CPU share the memory for all the virtualised compartments, based on one software layer for virtualisation. The need of these compartments came from the current design of some phones that have, for security reasons, independent processors for different functionality, e.g. the radio access, SIM lock, NFC, and the wish to integrate all functionality on one module having a processor/memory system to save hardware costs. Thus the standardised MTM solution does not address multiple modules, but boots.

The basic problem that remains to be solved is to create a secure link and trust chaining / transmitting between loosely coupled sub-modules and a master unit and in a reliable way to assure that chaining 'roots of trusts' is properly done and cannot be intercepted or circumvented by a potential

attacker. This apparently is very different from having the virtualisation layer loaded into memory, secured and started by a master CPU itself.

According to TCG standards there could be only one module being equipped with a TPM controller. Even if there could be used several modules, in many cases this would be not wanted, as, e.g. in bigger networks, the management and control of the single elements shall not be aware if single elements would consist of one or a multitude of modules. Thus there is no acceptable solution based on existing specified TCG mechanisms to treat such a multi-module system as one element. As with TPM it is not specified by standardization whether and how the MTM concepts easily can be transferred to multi-module environments that due to the physically decoupled memory / central processing unit may impose several security complications, e.g. unperceived change of memory content.

Putting TCG paradigms aside, mechanisms are known to provide tamper evidence or even tamper resistance. The difficulty of these mechanisms is that either they are not really efficient, e.g. simple security tapes could be easily faked, or very expensive to implement, or they do not integrate with the scope of the TCG approach.

Technical Problem

The problem envisaged is the creation of trusted environments over entire modular, cooperating systems, consisting of a number of individual components. In many situations it is required to assure that a complete compound of sensitive components is integer, i.e. none of the components should be modified or exchanged or be prone to other kinds of attacks

aiming to break security. This may also apply to the location of the modules, as e.g. some connections between modules may be secured by placing them in between the modules on positions, which are only reachable on removal of the modules from the rack. In particular, these components might be loosely coupled and not integrated on one controller altogether.

The demand for a proper co-design especially of hardware, software, mechanics, and housing is an essential factor for the entire security approach. However, in real systems the secure interfacing between hardware and software components often is not sufficiently respected. This essentially raises risks and opens chances for intruders to break defence mechanisms that in parts are well-meant and well-designed but in their entirety constitute porous security architectures.

To cope with complication arising from physical attacks against a system mechanisms are known to provide tamper evidence or tamper resistance, but the application of these to integrate with especially TCG technology has not been examined so far.

Furthermore, the problem is the creation of trusted environments over entire modular, cooperating systems, coupled by bus system, serial links or similar data link systems. There is not necessarily a shared machine code level command interface, i.e. a central processing unit on a first module directly working in memory of another module during normal operation, but should can exist for specific purposes. The individual modules shall be quite independent from each other, seen from a functional perspective, but are expected to form an entire integrity protected system altogether. The difficulty is to provide and to share reliable mechanisms to

ensure this, depending on a guess of the level of expected and to be defended attacks. The standard concept Root of Trust, as defined by the TCG, may not be well suited, as each module boots independently and it can not be said that one module controls the other.

Further, it is known that a multi-module system may comprise sensors sensing air particles and are embedded in resin to avoid an attack against its components or modules. In case of an attack, the resign layer would be destroyed and air would activate the sensors outputting an alarm. However, in such arrangement it is not possible to add further components to the multi-module system or to exchange any of the modules or components on the modules even if wished.

It is an object of the invention to provide an economic way to prevent and to detect aggressions at module level in a reliable manner and with manageable cost in a multi-module system comprising a trusted controller.

Technical Solution

This object is solved by a multi-module system comprising a trusted controller and having features according to claim 1, by a module of such multi-module system, and by a method for controlling a multi-module system comprising trusted controller and having features according to claim 12. Preferred aspects and embodiments are subject-matter of dependent claims.

Especially, there is provided a multi-module system comprising a plurality of at least two modules each having at least one processor, further comprising at least one memory for storing data and/or software to be loaded into at least

one of such processors, further comprising a trusted controller mounted on at least a first module of these modules and being designed, especially programmed for trusted booting of at least this first module or of its processor, further comprising at least a first access point for communication between the modules of the multi-module system, and further comprising a second access point for communication of data with an outside component outside of the multi-module system. In such multi-module system the second access point is a trustworthy single access point representing a single system for the outside component outside of the multi-module system, and the processors of at least two of the modules are only bootable under control of the trusted controller.

Especially, such a trusted controller can be designed as a trusted chip or a trusted software on a trusted board or module. Such controller can be embedded in a processor or software. Especially, the software to be used for trusted booting can be a boot loader. A boot loader is a software starting loading of a boot software from a trusted resource into the processor to be booted. Trustworthy highlights that there is a procedure running like expected.

The concept originally but not exclusively aims to support trusted computing technology by improvements for hardware protection. For the scope of this document a module as synonym for a component, e.g. an ASIC (application specific integrated circuit) or board, especially is defined in a logical way as one processor/memory system, where this system comprises one or a multitude of single processors accessing the same memory space. Also many processor/memory systems may be located on one physical module or board, thus a physical module may contain many “logical modules”. Also the opposite

is valid, that one processor/memory system is distributed across many modules or boards. Such system prevents physical attacks against such a system consisting of both software and hardware components, including mechanical and electrical elements.

Advantageous Effects

Especially, such multi-module system comprises a physical trusted path, an especially optical trusted path, between two of the modules, wherein each of the two modules comprise a sensor and trusting devices each of which emitting a physical trusting signal, especially optical trusting signal, to the other of the sensor and trusting devices and each of which receiving such trusting signal from the other of the sensor and trusting devices and each of which running under control of at least one of such trusted controller. Such trusted paths provide integrity of the modules especially if all modules are housed in a closed housing in a manner that there is no access possible from outside the housing.

According to a preferred embodiment the sensor and trusting devices comprises a transmitter or an encoder arranged or programmed for cryptographically protecting, especially encrypting, the trusting signal before emitting it and/or a receiver or decoder device arranged or programmed for cryptographically verifying, especially decrypting, the received trusting signal. Thus, there are provided combined cryptographic and especially optical sensor and trusting devices being hardware devices, which are controlled logically and electronically driven.

In the multi-module system there can be arranged an other module comprising an especially optical opening, wherein the

other module being arranged between the two of the modules providing the trusted path, the modules being arranged one to the other in a manner that the trusted path is directed through the opening. Thus, even the second module is protected with respect to its position, although the second module comprise no trusted controller and no sensor and trusting device, because a change of the position of the second module would move the opening and would interrupt the first trusting path.

The module and/or the sensor and trusting devices can comprise an integrated energy source, an integrated clock device and an integrated controller logic or functionality arranged or programmed for detecting an attack to the trusting path. Especially, the energy source is an energy buffer like an accumulator to provide enough energy for the other components to detecting an attack even in power-off state of the module. The integrated clock device provides a clock signal making possible running of its sensor and trusting device even if there is no external or other clock signal in the module. Therefore, the controller logic or functionality is provided even if the module is running without external power or clock signal.

Especially, the data and/or software is transferred from the memory on one of the modules to the memories and/or to the processors on the other modules via the trusting paths using the trusting signals under control of the trusted controllers and/or under control of the sensor and trusting devices.

According to an alternative or combined embodiment, the data and/or software is transferred from the memory on one of the modules, especially on the first module to the memories and/or to the processors on the other modules via the first

access points and a line or lines on a further module being arranged between the two modules.

Such a multi-module system can be arranged with a cascading arrangement of trusted controllers, a first of the trusted controllers being arranged on one of the modules, especially on the first module, a second of the trusted controllers being arranged on another of the modules, and a further of the trusted controllers being arranged on a further one of the modules, wherein the processor of the further module is only bootable under control of the second trusted controller.

Especially, the data and/or software stored in the at least one memory and to be loaded into the processors is stringently required for booting of the processors and is used for booting of the processors.

Especially, there is provided a module of such a multi-module system, wherein the module is designed as an application specific integrated circuit or a circuit board or is arranged on a circuit board to be inserted into a compartment or housing of a software controlled apparatus, especially server, base station, network element or phone. This makes possible an apparatus like a phone that having, for security reasons, a plurality of such modules or modules with each independent processors for different functionality, e.g. the radio access, SIM lock, NFC, and having integrated all functionality on one module having a processor/memory system to save hardware costs.

Such module can comprise an integrated energy source, a integrated clock device and an integrated controller logic or functionality being arranged or programmed for detecting an attack to the memory storing the data and/or software to be

loaded into at least one of such processors and/or being arranged or programmed for detecting an attack to a trusting path provided by an sensor and trusting device between the module and the other module.

Furthermore, there is provided a method for controlling a multi-module system, especially method for controlling such a multi-module system, wherein data and/or software being stored in at least one memory within the multi-module system is loaded into at least one processor, the at least one processor being a processor of processors in a plurality of at least two modules of the multi-module system each module having at least one of such processors, wherein at least this first module or its processor is booted in a trusted way by use of a trusted controller mounted on at least this first module of these modules, wherein at least a first access point is used for communication between the modules of the multi-module system, and wherein a second access point is used for communication of data with an outside component outside of the multi-module system, wherein the second access point is used as a single access point representing a single system for the outside component outside of the multi-module system, and wherein the processors of at least two of the modules are booted under control of the trusted controller.

Such method is preferred, if especially optical trusting signals are transmitted via an especially optical trusted path between two of the modules under control of sensor and trusting devices arranged on each of the two of the modules or under control of at least one of such trusted controllers. Especially, the trusting signal is cryptographically protected before emitting it via the especially optical trusted path. The data and/or software stored in the at least one memory and loaded into the processors should be

stringently required for booting of the processors and should be used for booting of the processors.

The core idea of such multi-module system is to have one of the modules acting as first module to the outside component as the single access point, representing for the outside component a single system. Especially, the first module acts for all elements used for secure boot and software integrity, e.g. as software loading server or attestation server. The especially first module having the single access point, also called master module in the following, must be equipped with a trusted controller and must perform a secure boot as usual when e.g. TCG standards are deployed. This makes possible secure boot of systems and ensures software integrity by using e.g. standards of the TCG. In particular specifications of TPM and MTM known as such are well suited. However the concept can also be seen independent of the TCG context. Thus, the solutions proposed may be applied to other purposes as well, e.g. those where software integrity is not considered or required, i.e. non TCG aware applications requiring intelligent cryptographically secured light barriers.

The selection, which of the modules of the multi-module system acts as master, is not directly coupled to the functional architecture of the multi-module system. In many cases the master module in the sense of the preferred embodiment will be also be the functional master module, but in principle it may be any of the modules, depending on security architecture of the system.

The concept integrates with frameworks to assure system integrity as e.g. given by TCG specifications and faces several classes of attacks against multi-module systems.

Complex or high-performance systems can be constructed using a multi-module solution with either the same processor on each module or with different, often application specific processors e.g. signal processors.

There is given a contribution to the "integrity problem" for systems consisting of multiple coupled modules, e.g. via bus or other communication systems. This system integrity may apply to only the physical integrity of the hardware system, but it may also extend to hardware /software co-systems, where the integrity mechanisms used for software integrity rely on the physical integrity of the underlying hardware as e.g. in TCG specifications.

Description of Drawings

An embodiment will be disclosed in more details with respect to enclosed drawing. There are shown in:

Fig. 1 components of a multi-module system having at least two modules each comprising a trusted controller for secure boot of systems and ensuring of software integrity,

Fig. 2 an algorithm showing steps of a booting program,

Fig. 3 a block diagram showing a preferred embodiment having several modules some of which serving as slave units and other of which serving as master unit or as slave- and sub-master unit, and

Fig. 4 another block diagram showing a transmitting of trusted software or data.

Mode for Invention

Fig. 1 shows components of a multi-module system comprising a housing H. The multi-module system can be a computer having a plurality of modules B1, B2, B3, B4, MM or a mobile device like a mobile phone having a plurality of components like modules which are housed in the housing H. Especially a first module B1 of these modules is designed as a master module. The modules B1, B2, B3, B4, MM shown are boards like printed circuit boards. However, other forms of modules like solid modules or ASICs can be used.

The first module B1 and a second, a third and a fourth module B2 – B4 of these modules are mounted in a fifth module MM of these modules. The fifth module MM is designed as e.g. a mother-module and comprises a plurality of first access points ES for communication between the modules. The first access points ES are designed to insert the first to the fourth module B1 – B4 and to provide an electric contact to lines L on the fifth module MM to make possible an electric connection between components of the different of the first to fourth module B1 – B4. As exemplarily shown data could be communicated from a processor P1 via such first access points ES and such line L to or from a processor P3 mounted on the third module B3. Usually there are a plurality of further lines to make possible a connection to further processors P2, P4, PMM mounted on the other modules B2, B4, MM.

According to a preferred embodiment, the housing H comprises mechanical fasteners MS to provide an additional mechanic fastening for each of the modules B1 – B4 at the housing H.

Furthermore, there is provided a second access point AP for communication with an outside component CO. The outside

component CO can be a network access point, an additional device like a hard disc or any other component or controlled device making possible communication of data c from or to the outside component CO.

To avoid a not trusted transfer of data c from or to the outside component CO, the first module B1 comprises a first trusted controller TC1. The trusted controller TC1 is designed to make possible a secure boot of the multi-module system and to ensure software integrity. Especially the trusted controller TC1 might be designed according to standards of the TCG, and in particular the specifications of TPM and MTM are well suited. Thus, the multi-module system is especially built up on the frame work as given by TCG specifications.

In addition to the first trusted controller TC1 and the second access point AP the first module B1 comprises a memory M. The memory M comprises memory space to store data and/or software sw being used by the first trusted controller TC1 on the first module B1 for secured booting of the multi-module system.

According to the preferred embodiment, the other modules B2 – B4 each comprise a memory M3, M4. The memory M4 on the fourth module B4 is designed as a memory having its own housing. The memory M3 on the third module B3 is designed as memory space within a processor housing of the processor P3 on the third module B3.

Modules B1 – B4 are booted under control of the first trusted controller TC1 on the first module B1. The first trusted controller TC1 loads the data and/or software sw into the processor P1 of the first module B1. In addition the data

and/or software sw is forwarded from the memory M on the first module B1 to the memory M3 on the third module B3 and/or into the processors P3, P2 on the third and e.g. second module B3, B2. Before any other action these processors P1 - P3 on the first to third module B1 - B3 are booted with or under control of the data and/or software sw loaded under control of the first trusted controller TC1.

The processor P4 of the fourth module B4 is booted under control of a second trusted controller TC2 on the third module B3. In other words, in a first booting cycle there are booted the first, second and third module B1 - B3 under control of the first trusted controller TC1 being a master unit on the first module B1. Thereafter, the second trusted controller TC2 being arranged as slave unit and sub-master unit on the third module B3 boots the fourth module B4 under its control. Especially the second trusted controller TC2 can forward the data and/or software sw from the memory M on the first module B1 or from its own memory M3 into the memory M4 and/or processor P4 of the fourth module B4 before its booting.

To make sure that there is a secure contact of the first to fourth module B1 - B4 one to the other via the mother-module MM there are sensor and trusting devices SC1 - SC4 arranged on the modules B1, B3, B4. Each of the sensor and trusting devices SC1 - SC4 runs under control of one of the trusted controllers TC1, TC2.

The sensor and trusting devices SC1 - SC4 comprises means, especially optical means, for sending and for receiving optical signals being trusting signals s1 - s2. A first of the sensor and trusting devices SC1 is mounted at the first module B1 and sends a first trusting signal s1 to a second of

the sensor and trusting devices SC2. The second sensor and trusting device SC2 sends a second trusting signal s2 to the first sensor and trusting device SC1. Therefore, there is a first trusting path TP1 between the first and second sensor and trusting devices SC1, SC2.

According to a preferred embodiment the trusted signals s1 – s4 are encrypted data signals. The sensor and trusting devices SC1 – SC4 runs under control of a cryptographically secured communication protocol.

The second sensor and trusting device SC2 is mounted at the third module B3 to enable the first trusting path TP1 between the first and second sensor and trusting devices SC1, SC2. There is provided an opening O or optical opening within the second module B2 enabling the transfer of light. Thus, even the second module B2 having no trusted controller is protected with respect to its position, because a change of the position of the second module B2 would move the opening O and would interrupt the first trusting path TP1.

Third and fourth sensor and trusting devices SC3, SC4 are mounted on the third and fourth module B3, B4, respectively, in a manner that a second trusting path TP2 between them is directed with at least a main extension of it parallel to an extension plane of the modules B3, B4. A third and a fourth trusting signal s3, s4 are communicated between the third and fourth sensor and trusting devices SC3, SC4 under control of a cryptographically secured communication protocol.

As shown, second module B2 can be a module without a trusted controller. However, it is preferred that every module and not only modules B1, B3, B4 running in trusted environment

should be controlled by an own trusted controller TC1, TC2 on the module B1 - B4.

According to a preferred embodiment all components, especially all modules B1 – B4, MM are housed in the housing H in a manner that there is no access possible from outside the housing H. The integrity of the modules B1 – B4, MM is given by the trusting paths TP1, TP2 and the sensor and trusting devices SC1 – SC4 running under control of the trusted controllers TC1, TC2. In such an arrangement the data and/or software sw can be transferred from the memory M on the first module B1 via the first access points ES and the line L or lines on the fifth module MM.

According to another embodiment the data and/or software sw can be transferred from the memory M to the memories M3, M4 and/or processors P3, P4 on the other modules B3, B4 via the trusting paths TP1, TP2 using the trusting signals s1, s3.

Fig. 2 shows exemplarily an algorithm for booting such multi-module system. In a first step S1 the trusted controller TC1 on the first module B1 is activated before any activation of the processor P1 of the first module B1. Thereafter, in a second step S2 the first trusted controller TC1 controls the first sensor and trusting device SC1 and activates the first sensor and trusting device SC1, the second sensor and trusting device S2 and the second trusted controller TC2 on the third module B3. Especially, the first and second trusting signals s1, s2 are encrypted signals and are used to control the first trusting path TP1 to be sure that there is no other device between the first and second sensor and trusting devices SC1, SC2 and that the modules B1, B2, B3 are not moved from their originally positions within the housing H.

In a third step S3 it is checked, whether or not the trusting signals s1, s2 are transmitted in a secured manner. If not, the transfer of the data and/or software sw is stopped in a fourth step S4. Further, the booting is stopped. Additionally or alternatively there is activated an alarm signal and/or recorded an error.

As long as the transfer of the trusting signals s1, s2 is in order, in fifth step S5 the data and/or software sw are transferred from the memory M to the first processor P1 on the first module B1 and to the third processor P3 on the third module B3 via the first access points ES and the line L or via the trusting signals s1, s2. In a sixth step S6 the processors P1, P3 are booted with or under control of the data and/or software sw.

Thereafter the processors P1 and P3 are running with the data and/or software and/or with other data and software under control of the first and second trusted controllers TC1, TC2 as long as in seventh step S7 the first trusting path TP1 is in order as shown by an eighth step S8. Otherwise in a ninth step S9 the processor or processors P1, P3 are stopped and/or an error protocol is recorded and/or an alarm is activated.

Not shown in Fig. 2 is the booting and running of the other modules B2, B4. According to a simple embodiment these modules could be booted and controlled by the first trusted controller TC1 on the first module B1 in a same manner.

According to another embodiment having cascading hierarchies, the processor P4 on the fourth module B4 is booted under control of the second trusted controller TC2 on the third module B3. Such embodiment is sketched by a block diagram of

Fig. 3. The first trusted controller TC1 on the first module B1 controls the processors via assistance of a third and a fifth trusted controller TC3, TC5 on the second and on a fifth module B2, B5. The first trusted controller TC1 is designed as a master unit for trust. The third and the fifth trusted controllers TC3, TC5 are slave units for trust on the second and fifth module B2, B5. The third module B3 comprising the second trusted controller TC2 serves as a slave unit for trust from the view of the first trusted controller TC1 on the first module B1. In addition, the second trusted controller TC2 on the third module B3 serves as a master or sub-master unit for trust with respect to a fourth trusted controller TC4 arranged on the fourth module B4 being a slave unit for trust.

Fig. 4 shows the transmitting of trust by e.g. transferring the data and/or software sw from the memory in the first module B1 into the memories and/or processors in the other modules. The transmitting of trust is done in a first step from the first module B1 and its first trusted controller TC1 to the third module B3 and to another module B5 by transferring data and/or software sw into their processors or memories M3, M5. Thereafter in a second step the transmitting of trust is done from the third module B3 to the fourth module B4 by transmitting these or other trusted software or data into the memory M4 of the fourth module B4.

In any way, the outside component CO believes that there is a unique system corresponding via the second access point AP. The outside component CO is not aware that there is a multi-module system having a plurality of modules B1 - B5, which are independently controlled by their own processors P1 - P4.

Thus, according to a first aspect there is provided a multi-

component system, attack protected by trusting paths TP1, TP2 and cryptographic sensors provided by the sensor and trusting devices SC1 – SC4 running under control of the trusted controllers TC1, TC2.

The technical principle of the system with especially first and third modules B1, B3, one is kind of master unit and the others are sub-modules can easily be applied to a multi-module environment using the mechanism described for each sub-module paired with another module. Also cascading hierarchies can be built up extending the same principle.

The system in Fig. 1 consisting of several modules B1 - B4 plugged into a backbone like fifth module MM and mounted into a chassis like housing H is built is a typical configuration of many today's systems built together as a composition of printed circuit boards. Especially, the modules B1 - B4, MM are sufficiently protected by a case, by the vicinity of the modules B1 - B4, and are fixed e.g. by mechanical fasteners MS or slots and electrical contacts provided by the first access points ES at the backbone, so that an attacker is not able to unplug the components in other ways as foreseen by the system design. E.g. they should be not dragged from a slot or contacted in the wrong direction. Otherwise a component should be damaged or destroyed or at least heavily twisted or completely bent out of shape.

Fig. 1 shows each one trusting path TP1, TP2 and each two cooperating cryptographic sensors provided by the sensor and trusting devices SC1, SC2, and SC3, SC4 between two modules B1, B3, and B3, B4, respectively.

According to a preferred embodiment there are each three or more inclined trusting paths TP1 between two corresponding or

dedicated of the modules B1 - B3. Each of the trusting paths TP1 is arranged as optical spit, two between the dedicated modules B1, B3 and one at the backbone or fifth module MM fixing the modules against bowing and un-plugging. Especially, intermediate modules like second module B2 with kind of pinholes or other optical openings O passing the light also can be secured.

Alternatively or additionally there is shown a variant that may substitute one of the sensors provided by the sensor and trusting devices SC3, SC4 between the modules B3, B4 by adding some more mechanical solidity.

Especially, the sensors is a combined cryptographic and optical sensor to prevent that the component or module is removed from the plug-in position without destroying it, in order to modify electrical, electronic or any other security relevant parts of the design. It works like one ore more paths obliquely plunged through the modules B1, B3 to mechanically fix them. However, the paths are realized by pairs of electronic/optical components that operate similar to a light barrier. Light is transmitted along straight lines and can be focused to produce a beam with small diameter.

Other implementations follow the same principle. Galvanic connections in principle are possible but would ease some attacks, such as those based on unperceived elongated wires. Microwave transmission is possible provided the wavelength is that short that a small and directed beam may be generated.

The concept includes that the appliance described can be varied according to the system requirements and, in particular can be applied to fix modules B1 - B4 at the module M5 providing a motherboard or backbone.

The basic protection principle is, that the "optical trusting paths TP1, TP2" are arranged in a way that any change of the plugged-in module position is detected by loss of connectivity, i.e. the light receivers will lose 'their' transmitters.

When using simple light, i.e. a light beam without embossed information transfer e.g. as emitted by an not modulated LED or other optical unit, attacks based on mirrors or other sources of light would be possible, just simulating one of the partnered optical unit. Also, with only simple light no authenticated and secure context would be possible.

Use of mirrors can be effectively prevented by directly contacting pairs of tubes. e.g. opaque glass, metal, rubber tubes, through witch the light is sent in longitudinal axis. Any pressure from side required to get into the beam would either cause a mechanical break that could be detected and/or interruptions of the beam by the displaced tube material itself. Given the functional appliance is based on minimal tolerances this would make "elongation" attacks extremely hard.

According to the preferred embodiment, a cryptographically secured communication protocol is applied between source and sink of the trusting paths TP1, TP2, so that decoupling cannot be covered by any other means, especially protection against man-in-the-middle.

Each "optical unit" provided by the sensor and trusting devices SC1, SC2, and SC3, SC4 is controlled logically and electronically "driven" by a hardware component e.g. an trusting end point that provides some crypto functionality

like e.g. hashing or symmetric encryption and includes the end point of the optical connection together with any logic necessary. Especially, the sensor and trusting devices SC1, SC2, and SC3, SC4 each securely holds a clock unit and some authentication data, e.g. a shared secret, which is also known at trusting end point's counterpart, i.e. it is shared between source and sink.

Further, the trusting end point may be equipped with a battery/accumulator or similar device to assure that in case of attacks some rapid security actions autonomously can be taken, e.g. sending out alarms, delete secrets, log data, set internal attack flags. The trusting end point may be implemented as single controller solution e.g. ASIC or as multi-controller module, advantageously secure against tampering and unauthorized access.

It is preferred that either these trusting end points protect mechanisms as well as the secrets used and in addition are physically protected by the mounted modules themselves, or that these trusting end points send out alarm signals to the module where they are attached, which requires the connections to the module being secure enough, e.g. according to the requirements which are given by TCG for TPM controller deployment in modules, and the module being able taking appropriate action, e.g. delete secrets, or that the trusting end points just store the alarms internally if they are only used for later auditing or "proof keeping".

The trusting end points are enabled to communicate with each other via the optical or other link. The source may be, in the case of a light trusting path, any light source, which may be modulated fast enough for the expected data rate for especially repeated authentication and possibly other data

transmission, e.g. software download for boot of the sub-module. The light source may be a LED (light emitting diode), a laser diode, a fluorescent light source or other, depending on required intensity, focusing of the light beam, and modulation speed.

Especially, the trusting end points run the following protocol: First sink and source authenticate each other, e.g. by use of the shared secret or PKI (public key infrastructure) based asymmetric mechanisms, and then periodically send out messages, e.g. time stamps, sequence numbers and/or numbers used only once, based on a suited challenge & response protocol. In case an attacker interrupts this protocol by mechanical or electrical disturbances it will be detected and suited actions can be taken. Buffered energy or energy of an accumulator allows detecting of manipulations even in power-off state of the system itself.

One possible application of the optical trusting path TP1, TP2 protection is related to the realization of trusted computing mechanisms to securely provide “roots of trust” and “trust chaining” in multi-module/component environments. Solutions to provide system integrity relying on TCG mechanisms may require securely coupled components. Such coupling mechanisms in multi-module environments are not provided by TCG standards, but are needed if e.g. the root of trust residing in one module shall verify the integrity of software residing or loaded in another module. The integrity of the complete hardware system, especially made up of several modules, is ensured and realized by combining the optical trusting path TP1, TP2 concept with e.g. booting of multi-module environments. Such arrangement and procedure mainly protecting against software driven attacks will harden these mechanisms against several classes of hardware attacks

and moreover significantly eases and improves implementation. Several embodiments can be provided as exemplarily follows.

In multi-module systems requiring integrity protected and trusted computing the trusted state of the complete system depends on the fact that all hardware modules making up the system are really the intended ones and are genuine. The optical trusting paths can ensure that the correct modules make up the complete system, and that, if necessary, a certain configuration, e.g. sequence of modules ordered on the motherboard or backplane, is kept.

If the sub-modules contain fixed software in ROM, then the physical integrity of the system also ensures correct software "loaded" in the sub-component.

The optical trusting path TP1, TP2 can be implemented as the single way to impress "roots of trust" from one e.g. master component to another e.g. slave component. For instance integrity protected images, especially to be booted in a sub-component with volatile boot memory, can be transmitted through the links s1 - s4 of the optical trusting paths TP1, TP2. If it is assured that this is the only way for impressing boot images, one can be sure that this is done in the plugged-in position of all modules and thus under control of the master unit like first module B1 e.g. being equipped with a trusted controller TC1 like a TPM controller. Naturally this requires the master module to notice a successful authentication of the sub-module, and to only start transmission of software sw after successful authentication.

In case the system integrity is based and relying on flashed-in boot images such embodiment protects against removing and re-flashing with unchecked software.

The trusting end point can also be equipped with some functionality to support detection of memory manipulations on sub-components or sub-modules in particular on those that have no "own" trusted xb. In such embodiment it may take over the "verification" of sub-modules memory content and report it to the master module or unit. The trusting end point continuously checks the memory. The memory should be either empty before boot or filled with the boot images provided by the master unit. The trusting end point is aware of what the master module is doing and stores some values in internal registers. Especially, there are stored memory addresses and hashes over loaded images. If the measurements taken by the trusting end point fail, as a possible reaction the trusting end point interrupts the beam to propagate the faults to partnered trusting end points and steers the associated sub-module processor into halt state. Thus, both the master module or unit as well as the sub-module can react on memory-level manipulations.

Such embodiments provide several advantages as follows.

There is provided efficient and economic protection against HW tampering, especially removing, shifting or unplugging components from correct position, both, online and offline with respect to power. Tamper evidence mechanism and light-weight tamper proof mechanisms can be implemented. In particular mechanisms such as "security tapes" stuck over cases and caps do not provide active defence responses, as provided by e.g. logging or clearing of secrets.

In combination with a mechanically securely packed system intrusions are made quite complicated.

Embodiments can provide significant implementation improvements for system integrity protection concepts in well-designed multi-module environments. Implanting of "roots of trust" and software in general can be defended against most critical hardware attacks like e.g. memory flashing.

If other direct connections than the optical trusting paths TP1, TP2 exist, e.g. between adjacent modules, and if the mechanical structure of the modules B1 – B4, MM allows access to such links L only by removing the modules, then also the integrity of such links L is ensured and also the confidentiality, if mechanically secured against access.

Preferred absence of electrical interfaces exclude galvanic and magnetic manipulations or eavesdropping of inter-module links and communications. Thus, secure transmissions for any other purpose between subcomponents or sub-modules are enabled as well. Several intermediate modules only equipped with pinholes also can be secured depending of exact security requirements.

Mutual identification and authentication of sub-components prevents from exchanging or cloning of security relevant parts of a system.

A second main aspect being of relevance as such, too, is booting of multi-module systems built on trusted technology like TCG technology.

According to a preferred embodiment, software integrity protection is provided such that a multi-module system can be

handled like a single system from the outside component CO. One of the modules acts to the outside for all elements used for secure boot and software integrity, e.g. software loading server or attestation server, as the single second access point AP, representing for the outside component CO a single system. A single access point module like the first module B1, called master module in the following, is equipped with a trusted controller TC1, e.g. a TPM controller, and performs a secure boot as usual when e.g. TCG standards are deployed. The selection, which of the modules B1 – B4 of the multi-module system acts as master, is not directly coupled to the functional architecture of the multi-module system. In many cases the master module in the sense of the preferred embodiment will be also be the functional master module, but in principle it may be any of the modules B1 – B4, depending on security architecture of the system.

The master module B1 may report the platform status of the complete system either in a transparent form i.e. the attestation server has no knowledge of the single modules in the system, or the master module B1 includes integrity measures for each module B2 – B4 or sub-groups of modules B2 – B4 according to the differentiation needs of the attestation server.

The other modules B2 – B4, which do not directly interact with the outside component CO are called slave modules. This structure can be accomplished in two different ways as described in the following.

There are several optional features for the system structure. Some of the slave modules of a system are treated according to the first solution having one trusted controller TC1 on each board, while the others are treated according to the

second solution having one trusted controller TC2 for the whole system of sub-boards B4 depending on it. The principles of this invention are applied in a tree structure, where each "upper node" represents a master module B1 for the modules B2 - B4 that are located below him in the tree.

Some slave modules of a system must be not included into this trusted or TCG based security architecture, if the overall security requirements of the system do not require trusted boot and/or software integrity for the functionality executed by these particular modules.

Some modules B1 - B4 are independent modules and visible from the outside as such as known as such from the state of the art description, while other modules of the same system are handled according to a preferred embodiment.

A further generalisation of the concept is that not only "naked" modules may be handled according to the preferred embodiment. Also for networks of complete elements, e.g. networks of cell phones, PDAs (Personal Digital Assistant) or PCs, ad-hoc or in fixed configuration (PC: Personal Computer), one element may take the master role, acting as master with respect to the other elements, and acting as reporting instance to an attestation server.

One embodiment shown in Fig. 1 or 3 is to equip all slave modules B2 - B5 with trusted controllers TC2 - TC5 and treat them for their own boot as separated trusted systems. On boot the master module B1, equipped with e.g. a TPM trusted controller TC1 first boots into a secure state, attests it to the network if necessary and then itself runs attestations for all the loosely coupled slave modules B2, B3, B5 that themselves are equipped with "own" TPM units or trusted

controllers TC2, TC3, TC5. Here the master module B1 represents the challenging server for the slave modules B2, B3, B5, and, in this role, should be able to check the reference values as reported by the slave units securely.

For remote attestation to some external component CO or server the master module B1 includes the slave attestations or alternatively the result of slave attestations as "passed/failed" into its own PCR state (PCR: Platform Configuration Register), which is then reported. Internally all slave modules B2 - B5 still act as if they were independent TCG-secured systems, and only the master module B1 must be aware of its slaves. Still the outside component CO sees the complete system as one system only, and is not aware of the structure inside the system. This solution seems to be quite "secure" as each module B1 - B5 has its own 'roots of trust' and is capable to run the TCG defined processes rather independently from each other.

According to another embodiment partly shown in Fig. 1 there is only one trusted controller TC1 in whole system. Here it is assumed that one module B1 being a trusted master unit exists that is equipped with e.g. a TPM controller.

The essential problem to be solved is reliable transmission of "roots of trust" provided by the master unit like first Module B1 to the sub-modules B2 - B4. Here we focus on roots of trust for measurement/verification and roots of trust for reporting, i.e. aiming to assure system integrity during boot. Establishing a secure environment partially should also solve other related problems e.g. transmitting of TPM-stored secrets to trusted sub-modules.

The basic principle is that trust chaining is done using the master unit i.e. the first module B1 equipped with the trusted controller TC1 securely booting as the first instance and then providing / controlling the software sw load process of the slave modules B2 – B4. The software layers to be transmitted/loaded into the slave modules B2 – B4 are checked and secured by the master module at the first place and then securely handed over.

The transfer of the software sw to the slave modules B2 – B4 must be such that the processor or processors, e.g. in case of multiple core processors, of each slave module B2 – B4 does not start normal operation before the software sw to be executed is loaded into the module memory M3, M4.

In addition to the requirements valid for software sw written for systems using TPM mechanisms for protection, the software sw of the slave modules B2 – B4 should be written such that no other program code may be loaded during runtime of the slave module B2 – B4. Alternatively the software sw loaded securely by action of the master module B1 must contain a root of trust for verification of further loaded modules B2 – B4. Then also the software loaded additionally is tied to the trust chain rooted in the trusted controller of the master module B1.

In line with the TCG specification, second main aspect does not necessarily handle physical security, resilience to physical attacks, of the system. Similar to TCG specifications, where e.g. attacks on module level are assumed to be excluded by suitable system design, it is assumed that appropriate measures are taken against physical access, e.g. against swapping of slave modules in case the slave module does not contain e.g. a TPM controller.

An embodiment according to some aspects of Fig. 1 or 3 comprises a plurality of modules B1 – B4, B5, one of which represents the master or first module B1. Advantageously this first module B1 is the module, which also controls the communication to the outside world with e.g. software download server or remote attestation server. The other modules B2 – B4, B5 are slave modules B2 – B4, B5, having connections of different kinds to the master module B1, to the outside and between them.

For the solution having one trusted controller TC1, TC2 per module B1 – B5, there are no particular requirements on the connections between the modules B1 – B5, as each module B1 – B5 boots separately in a secure way. After boot of the master module B1, the master module B1 checks the slave modules B2 – B5 after their boot by remote attestation. Depending on the needs of the system, the master module B1 may act on the attestation results differently:

If only remote attestation is necessary, the master module B1 must include the results of the remote attestations of the slave modules B2 – B5 into its own reporting values, and thus report the state of the whole system when challenged for a remote attestation by an outside server.

If the system provides means for enabling/disabling e.g. connections or operation of the slave modules B2 – B5, then the master module B1 may enable slave modules B2 – B5 which passed the remote attestation or disable slave modules B2 – B5 which failed attestation.

For a solution having one trusted controller in the whole system or having a trusted controller not on every of the

modules, the software of the slave modules B2 – B5 should be loaded from the master module B1 to the slave modules B2 – B5 before the processors P2 – P4 on the slave modules B2 – B5 starts their normal execution.

According to a first way the slave module is coupled to the master module B1 with a special bus, which is only activated during boot. The memory space of the slave module B2 – B5 is mapped into the address space of the master module B1 for the download process. After finishing of the download or at least after establishing a secure local root of trust in the slave module, e.g. an MTM engine, the connection is cut, and the slave module starts the execution autonomously.

According to a second way the slave module is coupled to the master module by Direct Memory Access (DMA) with a DMA controller. In particular if the DMA controller is controlled by the master processor P1 on master / first module B1, the loading of the slave memory happens under direct control of the first module B1.

According to a third way the slave module has a memory or program part of the memory, which only can be written from the master module like e.g. a flash EPROM (Erasable Programmable Read Only Memory). Then the master module may load the program, i.e. re-flash the EPROM, at any convenient time, and perform the integrity check of this flashed software especially using its own security mechanisms at flash time. In this case the slave module can boot without any intervention from the master module B1, as the EPROM can only be changed by the especially TCG-secured master module, which ensures an integrity protected program at any time.

As in this case the loading of the program code to the slave module is not done necessarily at each boot, the master module B1 has to provide some persistent secure indication of the successful loading of the relevant slave module. As PCR values in the trusted controller TC1 of the master module B1 are reset on each boot, this indication cannot be stored in PCRs, but e.g. in some data stored using the secure storage facilities of the trusted controller TC1 on the master module B1. A possible mechanism is to store the hash of the slave program code in a data structure secured by the TPM controller, e.g. encrypted with seal and wrap-to-PCR, and to use this data on subsequent boot processes of the system instead of calculating the hash from the loaded slave program code.

The slave module B2 - B4, B5 is coupled to the master module B1 via serial link or other connection not giving direct access to slave module memory M3, M4, M5. The actual loading of software sw from this link into memory M3, M4, M5 is done by means which are not changeable by loading or other software means, and thus may be checked for correctness e.g. at production time.

This may be some small logic which is either implemented in hardware or controlled by some software which is firmly stored on the module, e.g. in ROM (Read Only Memory). Also the processor of the slave module may accomplish this loading job, if the program executed for this loading is stored in a secure location, e.g. some special memory space on the processor controller which is one-time programmable only, and this location is accessed on every boot.

For completeness it should be mentioned that a slave module might also contain unalterable memory only for program code,

thus not necessitating any online check of software integrity after boot. Here the integrity check can be done beforehand, e.g. at production time.

Such embodiments provide assurance of software integrity for the entire multi-module systems. There is possible management of remote attestation, wherein network sees only one module instead of a multitude of modules. In addition, the configuration and number of modules of a network element may change from release to release, which is hidden from the network by the invention.

Even if there is only one module with trust like TPM necessary, but still the whole system is covered by security mechanisms. In such case there is no need to adapt all perhaps existing modules to trusted usage. Further, it is possible to deploy a module as slave module, if the processor or bus structure makes deployment of trusted controllers impossible or very hard.

List of reference signs:

AP	second access point for communication with outside component
B1	first module designed as master module
B2	second module
B3	third module
B4	fourth module
CO	outside component
c	data from or to outside component
ES	first access points for communication between the modules
H	housing
L	line on fifth module
MM	fifth module designed as mother module
M	memory on first module
M3	memory on third module
M4	memory on fourth module
M5	memory on fifth module
MS	mechanical fasteners
O	optical opening
P1	processor on first module
P2	processor on second module
P3	processor on third module
P4	processor on fourth module
PMM	processor on fifth module
SC1	first sensor and trusting device
SC2	second sensor and trusting device
SC3	third sensor and trusting device
SC4	fourth sensor and trusting device
sw	data and/or software
s1	first trusting signal
s2	second trusting signal
s3	third trusting signal
s4	fourth trusting signal

TC1 first trusted controller on first module
TC2 second trusted controller on third module
TC3 third trusted controller on third module
TC4 fourth trusted controller on third module
TC5 fifth trusted controller on third module
TP1 first trusting path
TP2 second trusting path

CLAIMS

1. Multi-module system comprising
- a plurality of at least two modules (B1, B2, B3, B4, MM) each having at least one processor (P1, P2, P3, P4, MMP),
- at least one memory (M) for storing data and/or software (sw) to be loaded into at least one of such processors (P1),
- a trusted controller (TC1) mounted on at least a first module (B1) of these modules (P1, P2, P3, P4, MMP) and being designed for trusted booting of at least this first module (B1) or of its processor (P1),
- at least a first access point (ES) for communication between the modules (P1, P2, P3, P4, MMP) of the multi-module system, and
- a second access point (AP) for communication of data (c) with an outside component (CO) outside of the multi-module system, **characterized in that**
- the second access point (AP) is a single trustworthy access point representing a single system for the outside component (CO) outside of the multi-module system, and
- the processors (P1, P3) of at least two of the modules (B1, B3) are only bootable under control of the trusted controller (TC1).

2. Multi-module system according to claim 1 comprising a physical, especially optical trusted path (TP1; TP2) between two of the modules (B1 – B3; B3 - B4), wherein each of the two modules (B1 – B3; B3 - B4) comprise a sensor and trusting devices (SC1, SC2; SC3, SC4) each of which emitting a physical trusting signal, especially optical trusting signal (s1, s2; s3, s4) to the other of the sensor and trusting devices (SC2, SC1; SC4, SC3) and each of which receiving such trusting signal (s1, s2; s3, s4) from the other of the sensor and trusting devices (SC1, SC2; SC3, SC4) and each of which

running at least during booting under control of at least one of such trusted controllers (TC1, TC2).

3. Multi-module system according to claim 2, wherein the sensor and trusting devices (SC1, SC2; SC3, SC4) comprises an transmitter or encoder arranged or programmed for cryptographically protecting, especially encrypting, the trusting signal (s1, s2; s3, s4) before emitting it and/or a receiver or decoder device arranged or programmed for cryptographically verifying, especially decrypting, the received trusting signal (s1, s2; s3, s4).

4. Multi-module system according to claim 2 or 3 having another module (B2) comprising an especially optical opening (O) and being arranged between the two of the modules (B1 - B3) providing the trusted path (TP1), the modules (B1 - B3) being arranged one to the other in a manner that the trusted path (TP1) is directed through the opening (O).

5. Multi-module system according to any of claims 2 or 4, wherein the module and/or the sensor and trusting devices (SC1, SC2; SC3, SC4) comprises an integrated energy source, a integrated clock device and an integrated controller logic or functionality arranged or programmed for detecting an attack to the trusting path (TP1, TP2).

6. Multi-module system according to any of claims 2 to 5, wherein the data and/or software (sw) is transferred from the memory (M) on one of the modules (B1; B3) to the memories (M3, M4) and/or to the processors (P3; P4) on the other modules (B3; B4) via the trusting paths (TP1; TP2) using the trusting signals (s1, s3) under control of the the trusted controllers (TC1; TC2) and/or under control of the sensor and trusting devices (SC1, SC2; SC3, SC4).

7. Multi-module system according to any of the preceding claims, wherein the data and/or software (sw) is transferred from the memory (M) on one of the modules, especially on the first module (B1) to the memories (M3) and/or to the processors (P3) on the other modules (B3) via the first access points (ES) and a line (L) or lines on a further module (MM) being arranged between the two modules (B1, B3).

8. Multi-module system according to any of the preceding claims having a cascading arrangement of trusted controllers (TC1, TC2, TC4), a first of the trusted controllers (TC1) being arranged on one of the modules, especially on the first module (B1), a second of the trusted controllers (TC2) being arranged on another of the modules (B3), and a further of the trusted controllers (TC4) being arranged on a further one of the modules (B4), wherein the processor (P4) of the further module (B4) is only bootable under control of the second trusted controller (TC3).

9. Multi-module system according to any of the preceding claims, wherein the data and/or software (sw) stored in the at least one memory (M) and to be loaded into the processors (P1 - P4) is stringently required for booting of the processors (P1 - P4) and is used for booting of the processors (P1 - P4).

10. Module (B1, B3, B4) of a multi-module system according to any preceding claim, wherein the module (B1 - B4) is designed as an application specific integrated circuit or a circuit board or is arranged on a circuit board to be inserted into a compartment or housing (H) of a software controlled apparatus, especially server, base station, network element or phone.

11. Module according to claim 10, comprising an integrated energy source, a integrated clock device and an integrated controller logic or functionality
- being arranged or programmed for detecting an attack to the memory (M) storing the data and/or software (sw) to be loaded into at least one of such processors (P1)
- and/or being arranged or programmed for detecting an attack to a trusting path (TP1, TP2) provided by an sensor and trusting device (SC1, SC2; SC3, SC4) between the module (B1) and the other module (B3).

12. Method for controlling a multi-module system, especially method for controlling a multi-module system according to any preceding claim, wherein
- data and/or software (sw) being stored in at least one memory (M) within the multi-module system is loaded into at least one processor (P1), the at least one processor (P1) being a processor of processors (P1, P2, P3, P4, MMP) in a plurality of at least two modules (B1, B2, B3, B4, MM) of the multi-module system each module (B1, B2, B3, B4, MM) having at least one of such processors (P1, P2, P3, P4, MMP),
- at least this first module (B1) or its processor (P1) is booted in a trusted way by use of a trusted controller (TC1) mounted on at least this first module (B1) of these modules (P1, P2, P3, P4, MMP),
- at least a first access point (ES) is used for communication between the modules (P1, P2, P3, P4, MMP) of the multi-module system, and
- a second access point (AP) is used for communication of data (c) with an outside component (CO) outside of the multi-module system, **characterized in that**
- the second access point (AP) is used as a single access point representing a single system for the outside component

(CO) outside of the multi-module system, and
- the processors (P1, P3) of at least two of the modules (B1, B3) are booted under control of the trusted controller (TC1).

13. Method according to claim 12, wherein trusting signals (s1, s2; s3, s4) are transmitted via an especially optical trusted path (TP1; TP2) between two of the modules (B1 – B3; B3 - B4) under control of sensor and trusting devices (SC1, SC2; SC3, SC4) arranged on each of the two of the modules (B1 – B3; B3 - B4) or under control of at least one of such trusted controllers (TC1, TC2).

14. Method according to claim 13, wherein the trusting signal (s1, s2; s3, s4) is cryptographically protected before emitting it via the especially optical trusted path (TP1; TP2).

15. Method according to any of claims 12 to 14, wherein the data and/or software (sw) stored in the at least one memory (M) and loaded into the processors (P1 – P4) is stringently required for booting of the processors (P1 – P4) and is used for booting of the processors (P1 – P4).

FIG 1

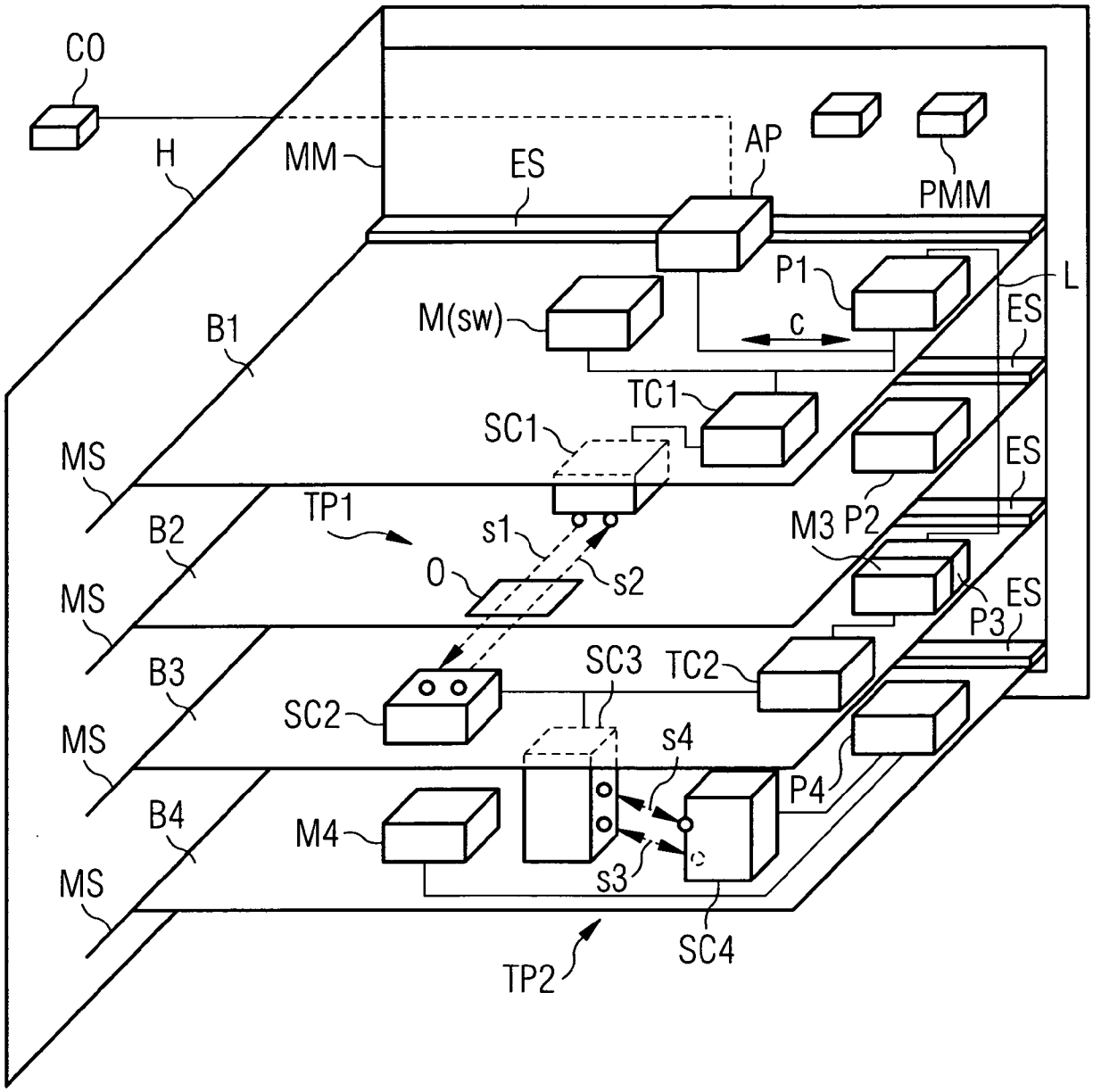

C0
H
MM
ES
AP
PMM
P1
L
M(sw)
c
ES
B1
TC1
SC1
MS
ES
TP1
B2
s1
M3 P2
O
s2
MS
ES
P3
B3
SC3
TC2
SC2
MS
s4
P4
B4
M4
s3
MS
SC4
TP2

FIG 2

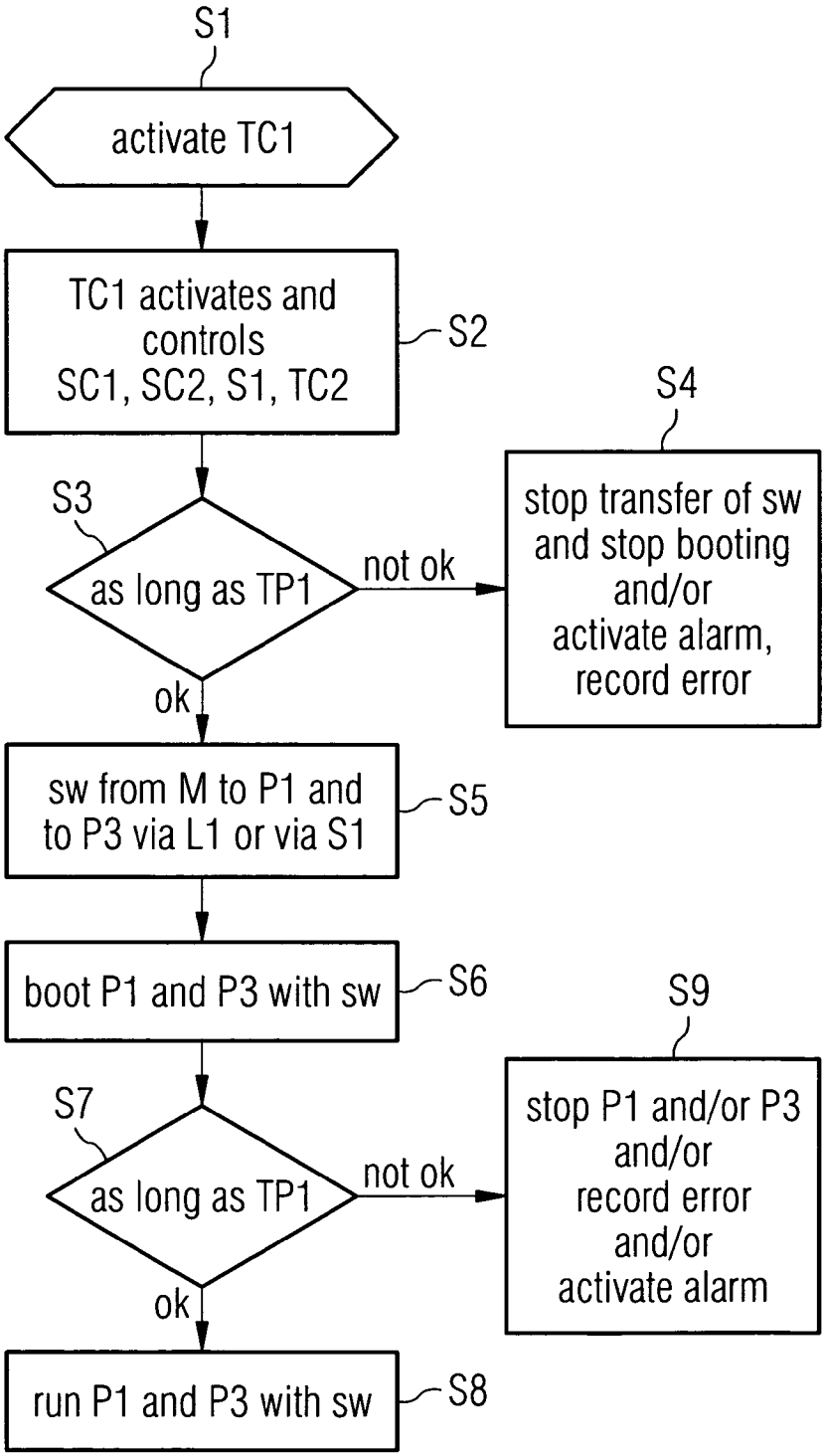

S1
activate TC1
TC1 activates and controls SC1, SC2, S1, TC2
S2
S3
as long as TP1
not ok
S4
stop transfer of sw and stop booting and/or activate alarm, record error
ok
sw from M to P1 and to P3 via L1 or via S1
S5
boot P1 and P3 with sw
S6
S7
as long as TP1
not ok
S9
stop P1 and/or P3 and/or record error and/or activate alarm
ok
run P1 and P3 with sw
S8

FIG 3

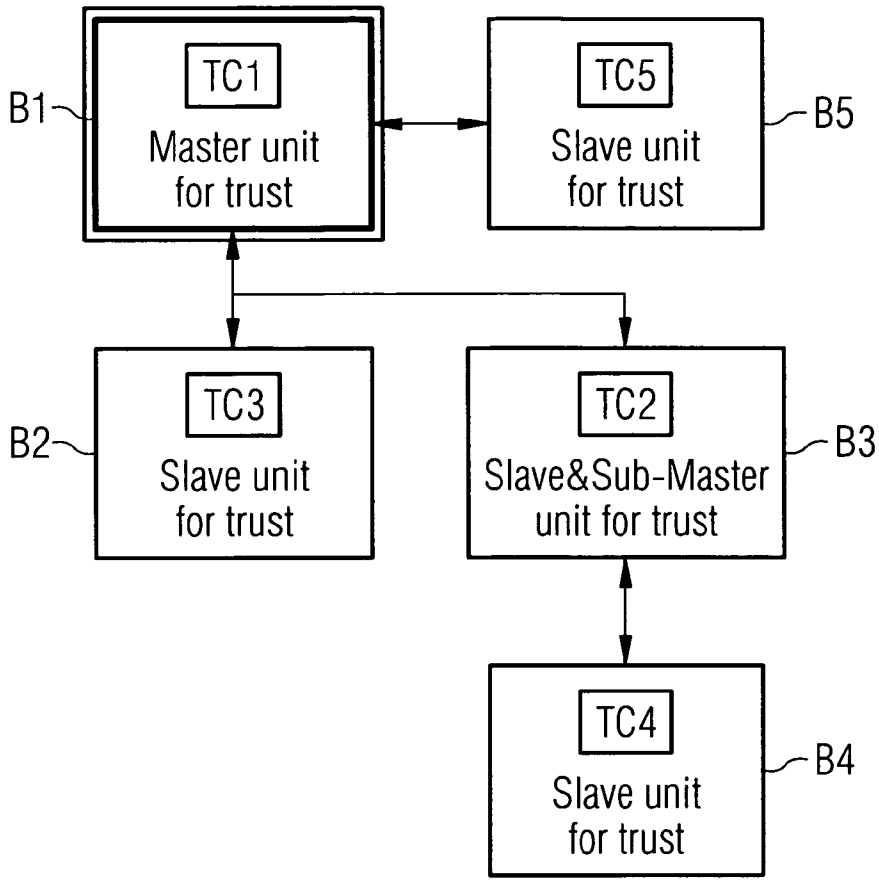
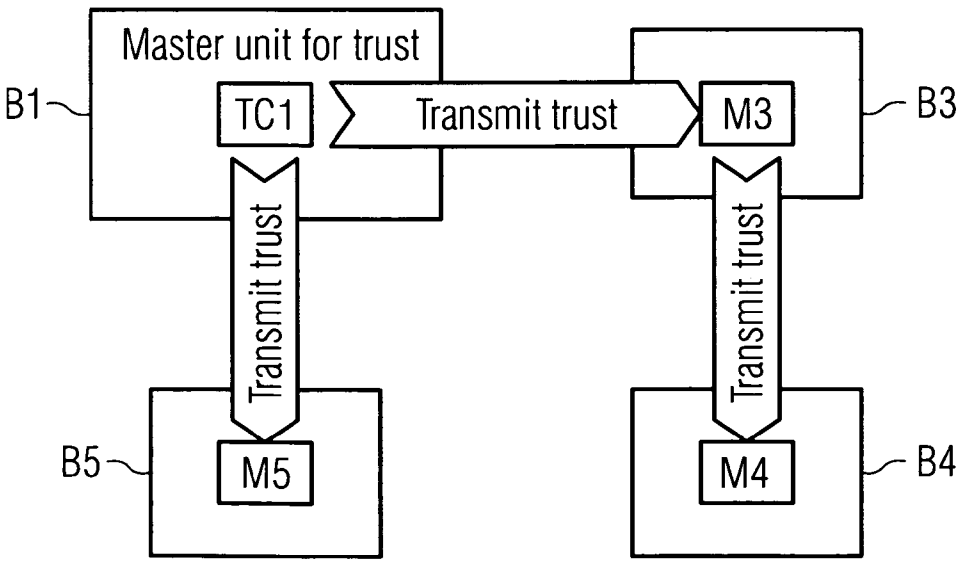

TC1
Master unit for trust
B1
TC5
Slave unit for trust
B5
TC3
Slave unit for trust
B2
TC2
Slave&Sub-Master unit for trust
B3
TC4
Slave unit for trust
B4

FIG 4


Master unit for trust
B1
TC1
Transmit trust
M3
B3
Transmit trust
Transmit trust
B5
M5
M4
B4

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2008/066205

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 G06F15/177 G06F9/445

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2007/113088 A1 (VOLP MARCUS [DE]) 17 May 2007 (2007-05-17) the whole document	1,7-12, 15 2-6,13, 14
Y	US 2005/010818 A1 (PAFF JOHN E [US] ET AL) 13 January 2005 (2005-01-13) the whole document	2-6,13, 14
A	US 2007/179907 A1 (WARIS HEIKKI [FI]) 2 August 2007 (2007-08-02) the whole document	1-15

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 August 2009	01/09/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Mäenpää, Jari

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2008/066205

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007113088 A1	17-05-2007	EP 1687717 A1	09-08-2006
		FR 2862397 A1	20-05-2005
		WO 2005050442 A1	02-06-2005
US 2005010818 A1	13-01-2005	CN 1584863 A	23-02-2005
		EP 1496418 A2	12-01-2005
		JP 2005032252 A	03-02-2005
		KR 20050006070 A	15-01-2005
US 2007179907 A1	02-08-2007	NONE	