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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 July 2012 (19.07.2012)

WIPO | PCT

(10) International Publication Number
WO 2012/096558 A1

(51) International Patent Classification:
G06F 21/00 (2006.01) *H04L 9/32* (2006.01)

(21) International Application Number:
PCT/MY2011/000168

(22) International Filing Date:
11 July 2011 (11.07.2011)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PI 2011000166 13 January 2011 (13.01.2011) MY

(71) Applicant *(for all designated States except US)*: **MIMOS BERHAD** [MY/MY]; Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MAT ISA, Mohd, Anuar** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **ROHMAD, Mohd, Saufy** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY). **ANSIRY, Zakaria, Wira, Zanoramy** [MY/MY]; Mimos Berhad, Technology Park Malaysia, 57000 Kuala Lumpur (MY).

(74) Agent: **WONG, Jan, Ping**; c/o Intellect Worldwide SDN BHD, 3.02 Menara Boustead Penang, 39, Jalan Sultan Ahmad Shah, 10050 Penang (MY).

(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, CL, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,

[Continued on next page]

(54) Title: SYSTEM AND METHOD TO PROVIDE INTEGRITY MEASUREMENT OF A MACHINE WITHOUT TPM USING TRUSTED AGENT

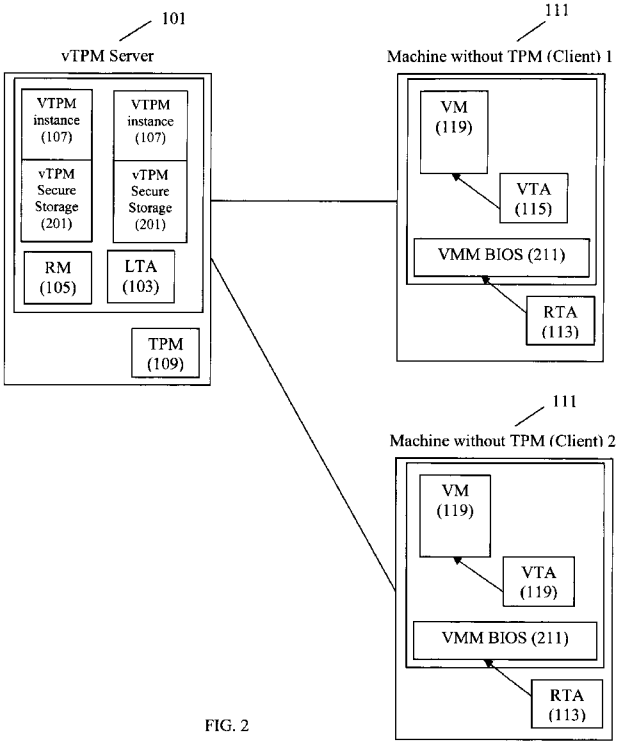

FIG. 2

(57) Abstract: The present invention relates generally to a system and method to provide integrity measurement of a machine without TPM using trusted agents, wherein said trusted agents comprise of at least one Local Trusted Agent (LTA) (103), at least one Remote Trusted Agent (RTA) (113) and at least one Virtual Machine Monitor Trusted Agent (VTA) (115) for capturing integrity measurements and thereby create a chain of trust between client machines (111) without TPM and machine with TPM.

WO 2012/096558 A1

MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *of inventorship (Rule 4.17(iv))*

Published:

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

SYSTEM AND METHOD TO PROVIDE INTEGRITY MEASUREMENT OF A MACHINE WITHOUT TPM USING TRUSTED AGENT

1. TECHNICAL FIELD OF THE INVENTION

The present invention relates generally to a system and method to provide integrity measurement of a machine without TPM using trusted agents, wherein said trusted agents comprise of at least one Local Trusted Agent (LTA), at least one Remote Trusted Agent (RTA) and at least one Virtual Machine Monitor Trusted Agent (VTA) for capturing integrity measurements and thereby create a chain of trust between client machines without TPM and machine with TPM.

2. BACKGROUND OF THE INVENTION

Trusted Platform Module (TPM) is used in machine as one of the security features to ensure trustworthy of the machine. Generally Trusted Platform Module offers facilities for the secure generation of cryptographic keys and limitation of their use as well as to authenticate hardware devices. It is capable of performing platform authentication, for example, it can be used to verify that a system seeking access is the expected system. In the absence of TPM, machine could not provide platform integrity measurement which is

used by application during attestation process and therefore may create the possibility of confidentiality violations.

Most of the TPMs today are conforming to the Trusted Computing Groups (TCG). Consequently, a client is not able to execute the TCG enable application such as Trusted Online Banking on the machine without TPM. Furthermore, machine without the TPM could not provide privacy protection for the online application which is running in cloud computing environment because all the client information or some private information may be exposed to a third party during online transaction. Subsequently, there is high possibility of information leakage when a client is trying to access cloud infrastructure. Therefore, stringent security requirements must always be complied for workloads that share the same platform or when client is accessing to cloud infrastructure.

Nowadays, cloud service providers are making substantial efforts to secure their systems in order to minimize the threat of insider attacks as well as to reinforce the confidence of customers. However, no method or system is available to provide integrity measurement and chain of trust between machine without TPM and machine with TPM for ensuring the confidentiality and integrity of computations. Thus there is an essential need to seek for a technical solution that could secure the confidentiality and

integrity of computation, in a way that is verifiable by the customers of the service.

It would hence be extremely advantageous if the above shortcoming is alleviated by having a proactive approach to provide integrity measurement of a machine without TPM by using of trusted agents, whereby the trusted agents collect platform information and extend this information into vTPM.

3. SUMMARY OF THE INVENTION

Accordingly, it is the primary aim of the present invention to provide a system and method for integrity measurement of a machine without TPM by using of trusted agents for capturing integrity measurement.

It is yet another object of the present invention to provide a system and method for integrity measurement of a machine without TPM whereby chain of trust between machine without TPM and machine with TPM is generated.

It is yet another object of the present invention to provide a system and method for integrity measurement of a machine without TPM whereby

trusted agents are able to establish chain of trust by collecting integrity measurement from vTPM server, client machine and client virtual machine.

It is yet a further object of the present invention to provide a system and method for integrity measurement of a machine without TPM which is capable to provide privacy protection for online application running in cloud computing environment.

Yet a further object of the present invention is to provide a system and method for integrity measurement of a machine without TPM which is capable of preventing information leakage when a client is accessing to cloud infrastructure.

Other and further objects of the invention will become apparent with an understanding of the following detailed description of the invention or upon employment of the invention in practice.

According to an embodiment of the present invention there is provided,

A system to provide integrity measurement of a machine with TPM comprising:

at least a server (101);

at least a client machine (111);

characterised in that

said server is a vTPM server (101) which comprises of at least one trusted agent; said client machine (111) comprises of at least one trusted agent; said system is able to perform integrity measurement without the use of TPM in said client machines (111).

In another aspect there is provided,

A method to provide integrity measurement of a machine without TPM comprising steps of:

i. capturing integrity measurement of the vTPM server (101) by at least one Local Trusted Agent (103) and transmitting the said integrity measurement to at least one Resource Manager (105);

ii. measuring integrity measurement of client machine (111) without TPM by at least one Remote Trusted Agent (113) and transmitting said integrity measurement to at least one Resource Manager (105);

iii. measuring integrity measurement of virtual machine (119) in said client machine (111) by Virtual Machine Monitor Trusted Agent (115) and transmitting the said integrity measurement to at least one Resource Manager (105);

iv. assembling said integrity measurements from said Trusted Agent by Resource Manager (105) and utilizing the said integrity measurement as initial value for at least one vTPM instances (107).

4. BRIEF DESCRIPTION OF THE DRAWINGS

Other aspect of the present invention and their advantages will be discerned after studying the Detailed Description in conjunction with the accompanying drawings in which:

FIG. 1 shows a schematic diagram illustrating a system to provide integrity measurement of a machine without TPM.

FIG. 2 shows a schematic diagram of a system to provide integrity measurement of a machine without TPM in accordance with the preferred embodiment of the present invention.

FIG. 3 shows a flowchart of a process flow that happens between the client machine, vTPM server and its subcomponents.

5. DETAILED DESCRIPTION OF THE DRAWINGS

In the following detailed description, numerous specific details are set forth in order to provide a thorough understanding of the invention. However, it will be understood by those or ordinary skill in the art that the invention may be practised without these specific details. In other instances, well known methods, procedures and/or components have not been described in detail so as not to obscure the invention.

The invention will be more clearly understood from the following description of the embodiments thereof, given by way of example only with reference to the accompanying drawings which are not drawn to scale.

Referring to FIG. 1, there is shown a schematic diagram illustrating a system to provide integrity measurement of a machine without TPM. At least a Virtual Trusted Platform Module (vTPM) server (101) and a plurality of client machines (111) is shown in FIG. 1 wherein said vTPM server (101) includes a security module comprises of at least one Local Trusted Agent (LTA) (103), at least one Resource Manager (RM) (105), at least one Virtual Trusted Platform Module (vTPM) Instance (107) and at least one Trusted

Platform Module (TPM) (109). Said client machine (111) comprises of Virtual Machine Monitor (VMM) (117) and trusted agents such as Remote Trusted Agent (RTA) (113) and Virtual Machine Monitor Trusted Agent (VTA) (115). Each of the trusted agents plays a role in collecting platform information. For example, Local Trusted Agent (LTA) (103) is used to capture the integrity measurement of the vTPM server (101), at least a Remote Trusted Agent (RTA) (113) is used to measure the integrity of client machine (111) without TPM, and Virtual Machine Monitor Trusted Agent (VTA) (115) is used to measure integrity of virtual machine (119) in said client machine (111). The trusted agents collect platform information and extend this information into vTPM.

Referring to FIG. 2, there is shown a system to provide integrity measurement of a machine without TPM in accordance with the preferred embodiment of the present invention. The system comprises of two parties, which are the client machine (111) without TPM and the vTPM server (101). The purpose of the system architecture is to provide chain of trust from the physical TPM in vTPM server (101) to the physical client machine (111) and eventually up to the virtual machine (119) in said client machine (111). Two client machines (111) without TPM are shown in FIG. 2, in which one is for Client Machine 1 and one is for Client Machine 2. A plurality of the said client machine (111) without TPM can be used in the present invention,

wherein each of the said client machine (111) comprises of at least one Remote Trusted Agent (RTA) (113), at least one Virtual Trusted Agent (VTA) (115), at least one VMM BIOS (211) and at least one virtual machine (VM) (119). Said RTA (113) in client machine (111) communicates with said LTA (103) in vTPM server (101) to establish root chain of trust in client machine (111). Said RTA (113) is first check for low level integrity value in client machine (111) such as BIOS and bootloader value. The control is then passed to virtual machine (119) and after all the value is validated and trust is established, the virtual machine (119) can utilize vTPM that created for it.

Said vTPM Server (101) comprises of at least one physical TPM (109), at least one vTPM resource manager (RM) (105), at least one Local Trusted Agent (LTA) (103) and a plurality of vTPM instance (107) with vTPM Secure Storage (201). Each of the virtual machine (119) is assigned to respective vTPM instance (107). Therefore, the number of vTPM and vTPM Secure Storage (201) contained in said vTPM server (101) is depending on the number of virtual machine which is connected to it.

In said vTPM server (101), Local Trusted Agent (LTA) (103) is used to capture the integrity measurement of the vTPM server (101). This is further comprises of at least measuring BIOS, option ROM, Memory Buffer Register (MBR), Boot Loader, CMOS Memory, PCRs Integrity Metrics and Firmware instruction. In client machine (111) without TPM, at least a Remote Trusted

Agent (RTA) (113) is used to measure the said client machine (111) without TPM. This is further comprises of at least measuring BIOS, option ROM, Memory Buffer Register (MBR), Boot Loader, CMOS Memory and Firmware instruction. In addition, Virtual Machine Monitor Trusted Agent (VTA) (115) is used to measure integrity of virtual machine (119) in said client machine (111). These integrity measurements of physical hardware components are then combined using hashing algorithm. The collected platform information by the said Trusted Agents is then transmitted as integrity measurement to the Resource Manager (RM) (105) using secure communication channel. On the vTPM server (101), said Resource Manager (RM) (105) generates a virtual Platform Configuration Registers (PCRs) value through combination of the integrity measurement using hashing algorithm to concatenate multiple integrity measurements into single digest, wherein at least these measurement consist of physical machine PCR(s), physical machine measurement of remote machine and virtual machine measurement. Resource Manager (RM) (105) assembles integrity measurement from the Trusted Agents and utilizes these integrity measurements as initial value for vTPM instances (107).

Referring to FIG. 3, there is shown a process flow that happens between the client machine (111), vTPM server (101) and its subcomponents. The process starts with the commencing of vTPM server (101) and Resource

Manager (105)) to receive client's request or demand and to response by providing vTPM instance. Local Trusted Agent (LTA) (103) is used to capture the integrity measurement of the vTPM server (101), at least a Remote Trusted Agent (RTA) (113) is used to measure the integrity of client machine (111) without TPM, and Virtual Machine Monitor Trusted Agent (VTA) (115) is used to measure integrity of virtual machine (119) in said client machine (111). The Trusted Agents are then independently transmitting its integrity measurement to the Resource Manager (RM) (105). Resource Manager (105) assembles integrity measurements that are obtained from the Trusted Agents and utilizes this integrity measurement as initial value for vTPM instances (107).

By having such methodology, the chain of trust, which is extended from the physical TPM in vTPM server (101) to each of the physical client machine (111) and up to the virtual machine (119) is properly established. In addition, the integrity data stored in the vTPM Secure Storage (201) is securely maintained and could not be accessed by unauthorized parties or other virtual machines (119).

While the preferred embodiment of the present invention and its advantages has been disclosed in the above Detailed Description, the invention is not limited thereto but only by the spirit and scope of the appended claim.

WHAT IS CLAIMED IS:

1. A system to provide integrity measurement of a machine without Trusted Platform Module (TPM) comprising;

at least a server (101);

at least a client machine (111);

characterised in that

said server (101) is a Virtual Trusted Platform Module (vTPM) server (101) which comprises of at least one trusted agent; said client machine (111) comprises of at least one trusted agent; said system is able to perform integrity measurement without the use of TPM in said client machine (111).

2. A system to provide integrity measurement of a machine without TPM as in Claim 1 wherein said trusted agent comprises of at least one of the following:

Local Trusted Agent (LTA) (103);

Remote Trusted Agent (RTA) (113);

Virtual Machine Monitor Trusted Agent (VTA) (115).

3. A system to provide integrity measurement of a machine without TPM as in Claim 1 or Claim 2 wherein said vTPM server (101) comprises of at least one said Local Trusted Agent (103) to capture the integrity measurement of said vTPM server (101).

4. A system to provide integrity measurement of a machine without TPM as in Claim 3 wherein said vTPM server (101) further comprises of at least one physical TPM (109), at least one vTPM Resource Manager (RM) (105) and a plurality of vTPM instance (107) with vTPM Secure Storage (201)

5. A system to provide integrity measurement of a machine without TPM as in Claim 1 or Claim 2 wherein said client machine (111) comprises of at least one said Remote Trusted Agent (113) for measuring integrity of said client machine (111) without TPM.

6. A system to provide integrity measurement of a machine without TPM as in Claim 5 wherein said client machine (111) further comprises of at least one VMM BIOS (211) and at least one virtual machine (119).

7. A system to provide integrity measurement of a machine without TPM as in Claim 5 or Claim 6 wherein said client machine (111) further comprises of at least one Virtual Machine Monitor Trusted Agent (115) for measuring integrity of said virtual machine (119) in said client machine (111).

8. A system to provide integrity measurement of a machine without TPM as in Claim 1 wherein said trusted agents transmit the captured integrity measurement to at least one Resource Manager (RM) (105) in said vTPM server (101).

9. A system to provide integrity measurement of a machine without TPM as in Claim 8 wherein said Resource Manager (105) assembles integrity measurements from the said trusted agents and utilizes the said integrity measurements as initial value for said vTPM instances (107).

10 A method to provide integrity measurement of a machine without TPM comprising steps of:

i. capturing integrity measurement of the vTPM server (101) by at least one Local Trusted Agent (103) and transmitting

the said integrity measurement to at least one Resource Manager (105);

ii. measuring integrity measurement of client machine (111) without TPM by at least one Remote Trusted Agent (113) and transmitting said integrity measurement to at least one Resource Manager (105);

iii. measuring integrity measurement of virtual machine (119) in said client machine (111) by Virtual Machine Monitor Trusted Agent (115) and transmitting the said integrity measurement to at least one Resource Manager (105);

iv. assembling said integrity measurements from said Trusted Agent by Resource Manager (105) and utilizing the said integrity measurement as initial value for at least one vTPM instances (107).

11. A method to provide integrity measurement of a machine without TPM as in Claim 10 wherein said step of capturing integrity measurement of the vTPM server (101) by Local Trusted Agent (103) further comprises of at least measuring of hardware components such as BIOS, option ROM, Memory Buffer Register

(MBR), Boot Loader, CMOS Memory, PCRs Integrity Metrics and Firmware instruction by Local Trusted Agent (103).

12. A method to provide integrity measurement of a machine without TPM as in Claim 10 wherein said step of measuring client machine (111) without TPM by Remote Trusted Agent (113) further comprises of at least measuring hardware components such as BIOS, option ROM, Memory Buffer Register (MBR), Boot Loader, CMOS Memory and Firmware instruction by Remote Trusted Agent (113).

13. A method to provide integrity measurement of a machine without TPM as in Claim 11 or Claim 12 further comprises of concatenating the integrity measurements of hardware components using hashing algorithm and then transferring the said integrity measurements to the Resource Manager (105) using secure communication channel.

14. A method to provide integrity measurement of a machine without TPM as in Claim 10 wherein said Resource Manager (105) generates a virtual Platform Configuration Registers (PCRs) value through a combination of the integrity measurements from LTA (103) and RTA (113) using hashing algorithm, wherein at least the said measurement comprises of physical machine PCR(s), physical

machine measurement of remote machine and virtual machine measurement.

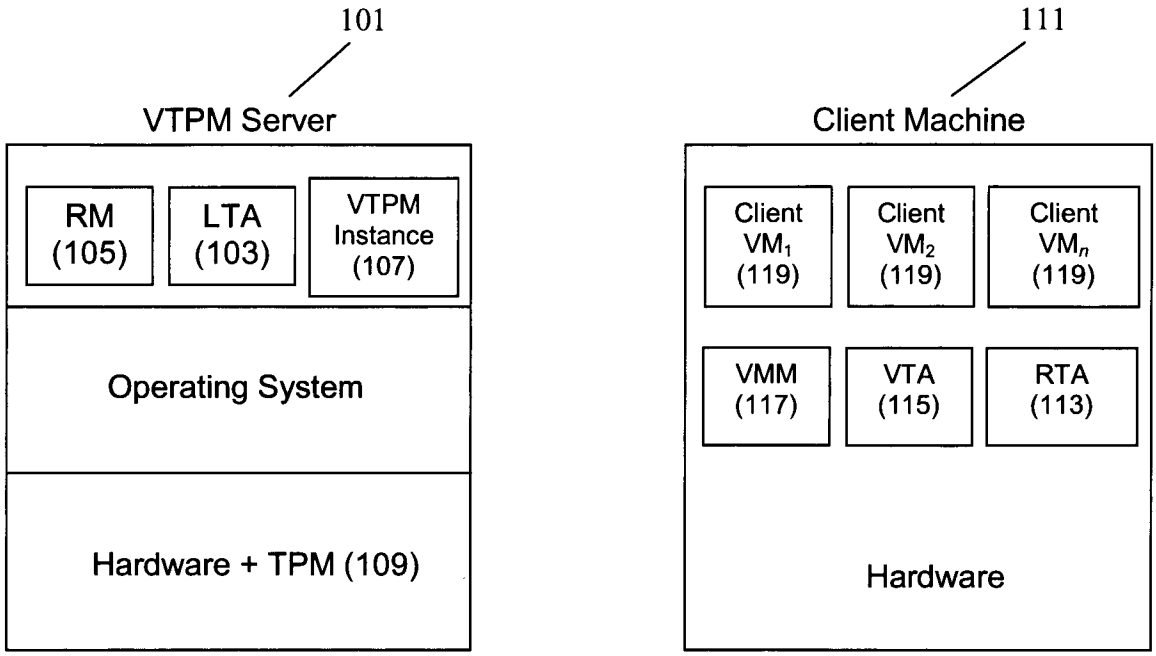
101
VTPM Server
RM (105)
LTA (103)
VTPM Instance (107)
Operating System
Hardware + TPM (109)
111
Client Machine
Client VM1 (119)
Client VM2 (119)
Client VMn (119)
VMM (117)
VTA (115)
RTA (113)
Hardware

FIG. 1

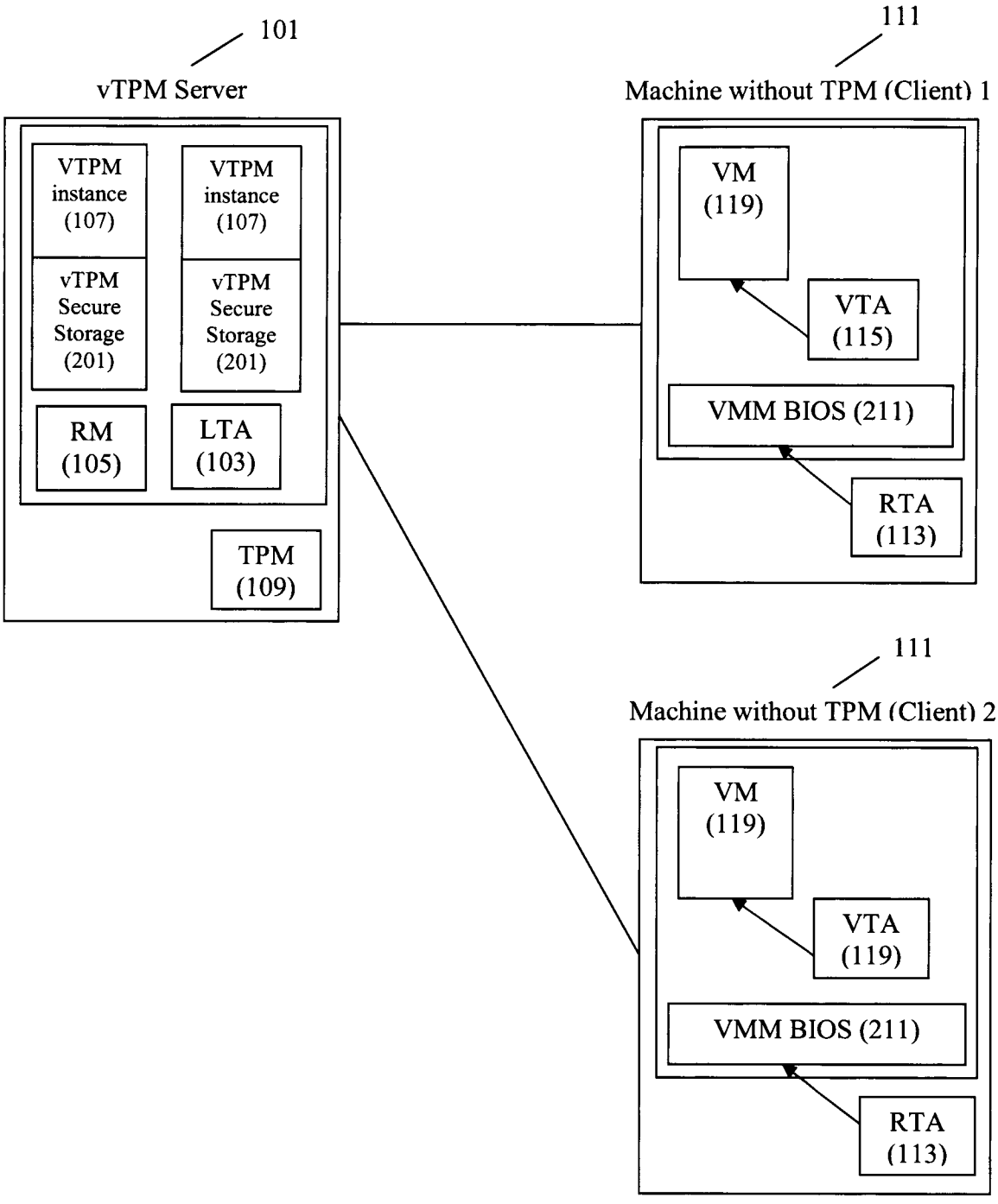
101
vTPM Server
VTPM instance (107)
VTPM instance (107)
vTPM Secure Storage (201)
vTPM Secure Storage (201)
RM (105)
LTA (103)
TPM (109)
111
Machine without TPM (Client) 1
VM (119)
VTA (115)
VMM BIOS (211)
RTA (113)
111
Machine without TPM (Client) 2
VM (119)
VTA (119)
VMM BIOS (211)
RTA (113)

FIG. 2

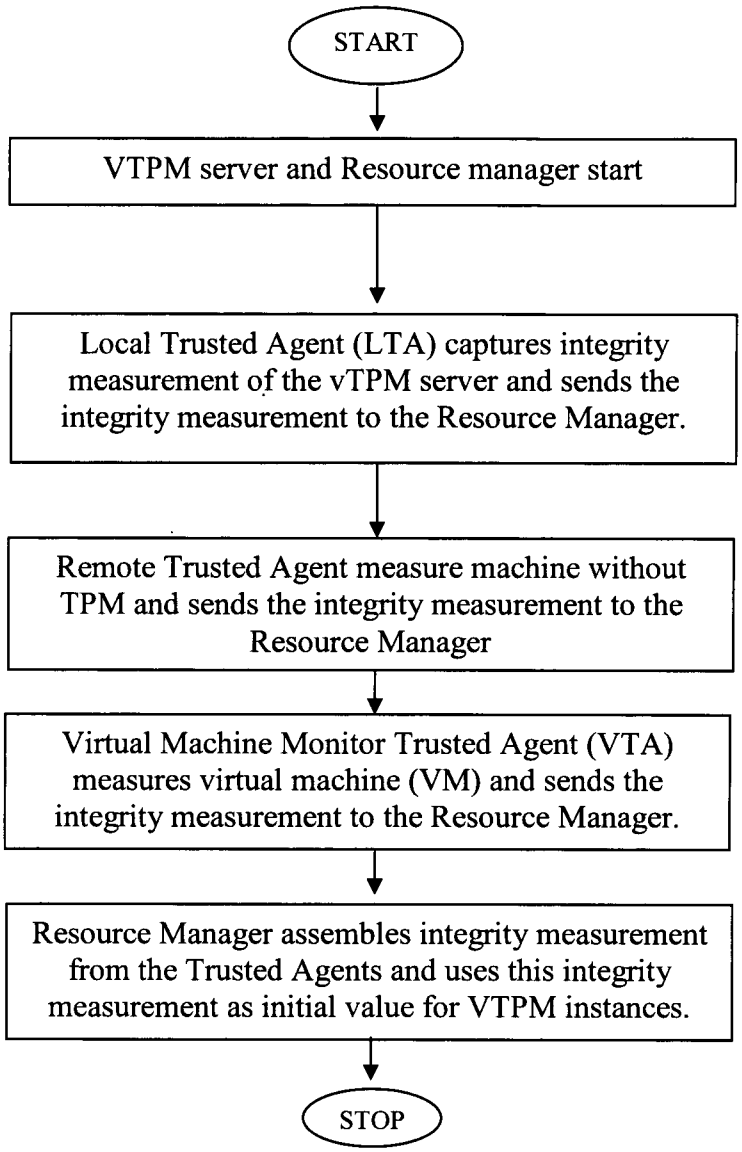
START
VTPM server and Resource manager start
Local Trusted Agent (LTA) captures integrity measurement of the vTPM server and sends the integrity measurement to the Resource Manager.
Remote Trusted Agent measure machine without TPM and sends the integrity measurement to the Resource Manager
Virtual Machine Monitor Trusted Agent (VTA) measures virtual machine (VM) and sends the integrity measurement to the Resource Manager.
Resource Manager assembles integrity measurement from the Trusted Agents and uses this integrity measurement as initial value for VTPM instances.
STOP

FIG. 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/MY2011/000168

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.

G06F 21/00 (2006.01) ***H04L 9/32*** (2006.01)

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)

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 practicable, search terms used)
WPI, EPODOC, Google Patents & Keywords (trusted, platform, module, virtual, agent, integrity, measurement, authentication, cryptology, encryption, behaviour, vTPM, TPM, cloud computing, attest) and like terms

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/0020781 A1 (SCARLATA et al) 26 January 2006 See [abstract, para 0005, para 0006, para 0007, para 0013, para 0015, para 0016, para 0017, para 0019, para 0021, para 0022, para 0023, para 0026, para 0027, para 0029, para 0030, para 0031, para 0034, para 0037, para 0060, fig 1, fig 2]	1 - 14
A	US 2009/0307487 A1 (MOVVA et al) 10 December 2009 See Whole Document	

☐ 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 application or patent 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
21 October 2011	26 OCTOBER 2011
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. +61 2 6283 7999	Authorized officer **XAVIER SIMON** AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : +61 2 6283 2623

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/MY2011/000168

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	2006020781	CN	1997955	EP	1759261	JP	2008500651
		US	7590867	WO	2006011943		
US	2009307487	CN	101473329	EP	2013808	JP	2009534749
		KR	20080112404	KR	20090006876	WO	2007124091

Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.

END OF ANNEX