文章编号:1001 - 9081(2006)08 - 1807 - 03

基于可信计算平台的体系结构研究与应用

肖 政[1,2],韩 英[1,2],叶 蓬[3],侯紫峰[1,3]
(1. 中国科学院 计算技术研究所,北京 100080; 2. 中国科学院 研究生院,北京 100039;
3. 联想研究院 信息安全研究室,北京 100085)
(xiaozheng@ict.ac.cn)

摘 要:介绍了可信计算平台的关键部件组成及其功能,描述了可信计算平台的特点和原理机制,以及目前可信计算平台的研究进展情况,分析了基于可信计算平台技术的应用前景和存在的问题,并对未来的趋势进行了展望。基于 863 项目"可信计算系统平台"的安全芯片研制成功,展现了可信计算的良好应用前景。

关键词:可信计算平台;身份认证;可信平台模块
中图分类号: TP309;TP393.08 **文献标识码**:A

Research and application of architecture based on trusted computing platform

XIAO Zheng[1,2], HAN Ying[1,2], YE Peng[3], HOU Zi-feng[1,3]
(1. *Institute of Computing Technology, Chinese Academy of Sciences, Beijing* 100080, *China*;
2. *Graduate School, Chinese Academy of Sciences, Beijing* 100039, *China*;
3. *Info-Security Lab, Lenovo Corporate R&D, Beijing* 100085, *China*)

Abstract: Key components and functions of trusted computing platform were introduced first. Then, its characteristics and mechanism were described. After that, an overview of the actual research state was given. At last, the future applications and problems of the technology based on the trusted computing platform were analyzed, and a prospect about its development was made. The successful application of "A Trusted Computing Platform System" funded by 863 Projects indicates that future of the trusted computing platform will be promising.

Key words: trusted computing platform; identity authentication; trusted platform module

0 引言

信息系统产生安全事故的主要原因是主机软、硬件结构存在设计漏洞,对合法的用户没有进行严格的认证和授权控制,导致资源被滥用,恶意程序利用系统弱点肆意进行破坏。

当前安全防范的重点还是放在对服务器和网络的保护上,但大多数都忽略网络终端接入者本身的安全,事实上大多数的攻击事件恰恰就是由终端不安全而引发的。如果能够从网络终端系统平台建立起安全的防护体系,把不安全因素从源头控制好,那么有望从根本上解决大多数的安全问题。

鉴于此,1999 年由 IBM、Intel、AMD、HP 和微软等许多业界巨头发起组成的可信计算组织(Trusted Computing Group, TCG)就是专注于从计算平台体系结构上增强系统安全性的。它的主要思路是在计算机的硬件平台上引入安全芯片架构,通过安全芯片和相应软件提供的安全特性来从根本上提高系统的安全性[1~4]。

本文首先介绍可信计算平台的关键部件可信平台模块(Trusted Platform Module, TPM)和可信软件协议栈(Trusted Software Stack, TSS)[5]的组成和功能,然后介绍了可信计算平台的特点和原理机制,接着介绍目前可信计算平台的研究进展情况,最后分析了基于可信计算平台技术的应用前景和存在的问题,并对未来的趋势进行了展望。

1 可信计算平台的组成

可信计算平台是指本机用户及远程交易方都信赖的平台,可以从四个方面来理解:1) 用户的身份唯一性认证,是对使用者的信任;2) 平台软硬件配置的正确性,体现了使用者对平台运行环境的信任;3) 应用程序的完整性和合法性,体现了应用程序运行的可信;4) 平台之间的可验证性,指网络环境下平台之间的相互信任。

可信计算平台中有两个重要部件,它们是可信平台模块(TPM)和可信软件协议栈(TSS)[6~8]。

1.1 TPM 的总体结构

TPM 是可信计算技术的核心,是一个含有密码运算部件和存储部件的小型片上系统。在可信计算平台上执行大部分操作都需要授权,即使你是 TPM 的所有者也不会例外,这样就提高了可信计算平台的可信任程度。

TPM 是一个带密码运算功能的安全微控制器,通过 LPC 总线与 PC 芯片集结合在一起。TPM 通过提供密钥管理和配置管理等特性,与配套的应用软件一起,主要用于完成计算平台的可靠性认证、用户身份认证和数字签名等功能。TPM 由输入和输出、密码协处理器、散列消息认证码 HMAC 引擎等组件构成。TPM 芯片首先验证当前底层固件的完整性,如正确则完成正常的系统初始化,然后由底层固件依次验证 BIOS

收稿日期:2006 - 02 - 13;**修订日期**:2006 - 04 - 25 **基金项目**:国家 863 计划资助项目(2004AA1Z1090;2005AA142030)

作者简介:肖政(1976 -),男,安徽巢湖人,博士研究生,主要研究方向:可信计算、网络安全管理、计算机体系结构; 韩英(1980 -),女,山东济南人,博士研究生,主要研究方向:可信计算、网络安全; 叶蓬(1976 -),男,江西南昌人,副研究员,主要研究方向:网络安全、计算机安全体系结构; 侯紫峰(1955 -),男,山西清徐人,研究员,博士生导师,主要研究方向:计算机体系结构、网络安全、可信计算.

和操作系统完整性,如正确则正常运行操作系统,否则停止运行。之后,利用 TPM 芯片内置的加密模块生成系统中各种密钥,对应用模块进行加解密,向上提供安全通信接口,以保证上层应用模块的安全。

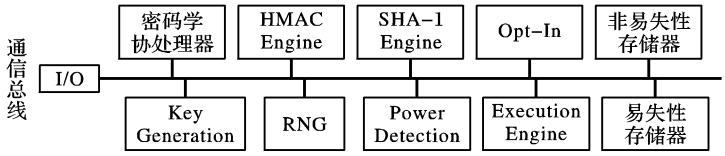

图 1 TPM 的体系结构

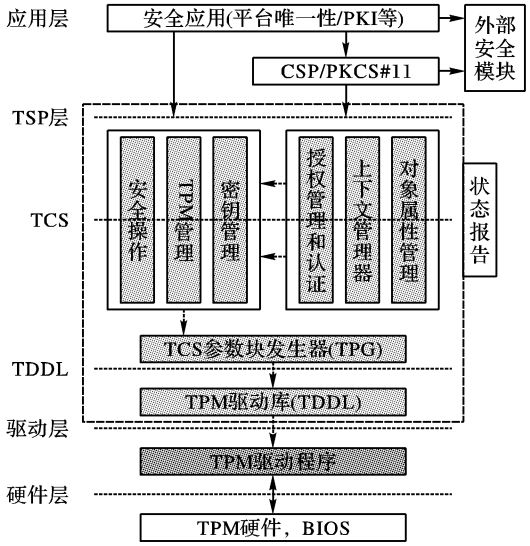

图 2 TSS 总体结构

1.2 TSS 的总体结构

TSS 是对可信计算平台提供支持的软件,它的设计目标是对使用 TPM 功能的应用程序提供一个唯一入口:提供对 TPM 的同步访问;管理 TPM 的资源;适当的时候释放 TPM 的资源等。TSS 有两部分组成,分别是 TCS(TSS core service)和 TSP(TSS service provider)。TCS 驻留在用户态,通常以系统服务形式存在,它通过 TDDLI 和 TPM 进行通信。TCS 提供了几乎所有的基本功能和复杂功能,像上下文管理、密钥管理、事件管理和审计管理等,它为 TSP 提供接口。TSP 通过 TCS 来使用 TPM 的功能。TSP 也提供了丰富的面向对象的应用接口,包括上下文管理、密钥管理和安全操作等。TSS 平台软件从结构上可以分为三层,自下至上分别为 TDDL、TCS 和 TSP,全部运行于用户模式。TSS 各部分功能如下:

1)TDDL(TPM 驱动程序库)提供两个功能,一个功能是通过提供标准接口,屏蔽各种不同安全芯片的差异。另一个功能是在用户模式和内核模式之间提供一个通信通道。

2)TCS(TSS 核心服务)是用户模式的系统进程,通常以系统服务形式存在,它通过 TDDL 与安全芯片进行通信。除提供安全芯片所具有的所有原始功能外,还提供如密钥管理等功能。通过 TCS 的接口,上层应用可以非常直接、简便地使用安全芯片提供的功能。

3)TSP(TSS 服务提供者)是用户模式的用户进程,位于 TSS 的最上层,它为应用程序提供了丰富的、面向对象的接口,使应用程序可以更加方便地利用安全芯片提供的功能构建所需要的安全特性。

2 可信计算平台的特点和原理机制

2.1 可信计算平台的特点

可信计算平台有两个主要的特点:

1)在可信计算平台上的操作必须是经过授权和认证的,任何不合法的用户都不能使用该平台进行工作。可信计算平台对用户的鉴别是与硬件中的 BIOS 相结合,通过 BIOS 提取用户的身份信息,让用户身份认证不再依赖操作系统,确保用户身份的真实性。

2)可信计算平台会对系统的一致性进行检查,平台内部各元素之间存在严密的互相认证,系统的启动从一个可信信任源开始,依次将验证 BIOS、操作系统再到应用程序,从而会形成一个信任链来保证系统平台没有被改动或攻击过。

可信计算技术的核心是基于 TPM 的安全芯片,由 TSS 配合 TPM 对可信计算平台提供支持,在它们共同作用下,可信计算平台提供基于硬件保护的安全存储和各种密码运算等功能。以 TPM 为基础,可信计算平台的可信机制主要通过三个方面来体现[9]:

1)完整性度量是获取影响平台完整性的平台特性序列的过程。任何将要获得控制权的实体,都需要先对该实体进行度量。

2)完整性存储是完整性度量和完整性报告的一个中间步骤,所有度量值形成一个序列,然后在日志中保存,并在 PCR 中保存这些序列的摘要。TPM 的保护能力也包含其他的安全功能,例如:认证报告度量的密钥、密钥管理、系统状态的密封数据等。

3)完整性度量报告是证明完整性存储内容的过程。通过报告机制来完成对平台可信性的查询,如果平台的可信环境被破坏,询问者可以拒绝与该平台交互或向该平台提供服务。

2.2 可信平台的信任链度量机制

解决平台安全问题的核心办法之一就是建立一个可信的信任链。在 TCG 系统中,由于信任根的错误行为不会被检测到,因此信任根必须是一个可信的组件。在一个可信计算系统平台上有两个根:完整性度量信任根和完整性报告信任根。图 3 是可信平台中的信任链度量机制过程图。

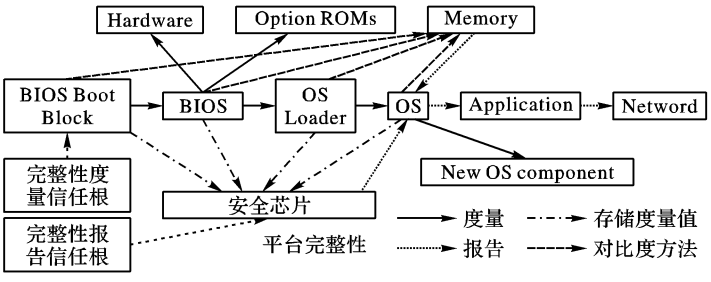

图 3 可信平台的信任链度量机制

BIOS Boot Block 为完整性度量信任根,TPM 芯片为完整性报告信任根。从平台加电开始,BIOS Boot Block 会度量 BIOS 的完整性值并将该值存储在安全芯片上,同时在自己可写的那块内存中记日志;接着 BIOS 度量 Hardware 和 ROMS,将度量得到的完整性值存在安全芯片中,在内存中记日志;接着 OS Loader 度量 OS,OS 度量应用和新的 OS 组件。当操作系统启动后,由用户决定是否继续信任这个系统平台。这样一个信任链的建立过程保证了系统平台的可信性。完整性值通常是一个哈希值,通常采用的哈希算法是 SHA1。

2.3 可信平台的身份标识机制

可信计算平台中很重要的一个概念就是 TPM 的身份,包括平台的身份,平台拥有者的身份和平台使用者的身份。不同的身份有不同的权限,而且这些身份之间也有一定关系。在 TPM 中用密钥来表示不同的身份特征,要证明一个平台的信任度量是可靠的,就需要证明该平台是具有唯一性身份的可信平台,该证明是通过密码学保证的身份标识来提供的:平台所有者的每个可信身份标识都兼顾私有性和可信性,这些身份标识是由 PKI/CA 和安全 PC 平台共同来创建。

首先由安全芯片随机产生一个公钥密码算法的密钥对,然后将其中的公开密钥通过 PKI/CA 和安全芯片功能交互后制作成可信身份标识。

这些密钥包括背书密钥 EK,它是 TPM 的唯一性密码学身份标识,唯一的标识了一个 TPM 的身份,一旦生成就会固化到安全芯片上,不允许再修改。TPM 所有者的身份是在 TPM 出厂时会给 TPM 的所有者设置一个共享秘密(口令变形),用来证明谁是 TPM 的所有者。

2.4 可信平台的安全存储机制

基于 TPM 的安全芯片还有一个重要功能是密钥或关键安全参数的安全存储,有效地克服了传统安全解决方案的致命缺陷,即存储在硬盘的密钥数据易被盗取或破坏。TPM 是采用硬件保护存储通过专门的硬件存储块来存储用户的秘密信息,如文件加密密钥、鉴别密钥等。硬件保护使得通过加密的秘密信息只能在拥有相应密钥的专有存储块中才能被解密。

TPM 中以树型结构来保护密钥数据和关系,即由父密钥全程负责其子密钥的生命周期管理,包括存储加密保护和使用授权,实现了一个用于保护存储的密钥层次其根是 SRK (Storage Root Key),每层中的密钥都被其上一层的密钥加密。

3 可信计算平台的研究情况

Microsoft 与 Intel 公司携手合作,共同打造基于可信计算平台的下一代安全计算机系统。微软提出的是下一代 Longhorn 操作系统中的 NGSCB (Next-Generation Secure Computing Base)技术,Intel 提出的是集成在处理器/芯片组内的 LaGrande 技术。

3.1 Microsoft NGSCB 技术

NGSCB 是下一代 Windows 操作系统 Longhorn 的基本安全组件和安全平台。它通过软硬结合的方式保证系统不受入侵或破坏,从而在数据安全、个人隐私及系统完整性等方面给用户提供了一个具有高安全强度的运行环境,这个环境可提供应用程序、外围硬件、内存与存储设备、输入输出系统的安全连接,相当于在软件与硬件之间建立了一个过滤网,任何要在执行的代码提交给硬件处理前都必须经过 NGSCB 的审核,这样就可以保护系统免受黑客恶意代码的攻击。

NGSCB 的关联组件功能上像一个 OS 微内核,管理整个系统的可信代码,执行用户的选择。为了安全可信的计算环境,微软为 NGSCB 增加了“Nexus”工作模式。Nexus 模块与安全芯片配合进行编码运算,在计算机内部形成另外一个系统空间作为软件系统与硬件系统的沟通媒介。标准分区和保护分区是相互隔离的,而受保护的程序就在保护分区内运行,在该区域所运行的程序以一种“安全代理”的形态出现。在该区域内,所有运行中的软件及数据都处于严密的保护状态下,包括密封的存储、受保护的执行、受保护的 I/O 等,而相应的加密操作是由一个“安全支持部件”的芯片来完成的,这样就有效避免了其他程序的窥视和攻击。

3.2 Intel LaGrande 技术

LaGrande 技术通过硬件将内存页面、存储系统、输入/输出过程严密地保护起来,当与可支持 LaGrande/NGSCB 技术的操作系统和应用程序相互配合时,LaGrande 机制就可以在硬件层面上直接保护电脑系统中数据的机密和完整性。

与 NGSCB 的标准模式和安全模式对应,LaGrande 也提供了标准和受保护两个运行环境。要实现上述安全保护功能,除了操作系统支持外,关键还在于包括处理器、芯片组、键盘/鼠标和显示输出等硬件的支持。

具有 LaGrande 功能的处理器可执行更安全的程序运行指令,来创建多重运行环境和分区,让标准分区与被保护的分区可以同时存在并相互隔离,受保护的程序就在保护分区内运行。

计算域安全管理器在 LT 模块的功能支撑下,为操作系统和应用程序提供运行环境安全隔离服务,以控制应用程序通过驱动程序直接获取另一应用程序的资源访问权限。

LaGrande 同时创建一条安全的信息传输途径,经由该途径传输的数据经过加密处理,同时对保护分区内存储的数据预先进行硬件加密处理,这样即便黑客窃取到这些数据,也无法在其他硬件平台上将它正常解密,这样保证了数据存储的安全。

4 应用前景和存在的问题

基于可信计算平台规范的产品和系统能够在硬件中存储密钥、数字证书、口令和数据,保护数字身份标识,在系统和网络之间提供相互认证,对金融和其他交易提供不可抵赖的数字签名,可以保护在线电子商务,电子政务,预防病毒、蠕虫和其他恶意攻击,为电子商务之类的系统应用奠定有效的安全信用基础,具有很好的应用前景。

但是它也同样面临许多挑战,例如在数字版权保护方面,在 DRM 监控下,用户使用的所有文件都得经过硬件级的验证以鉴别合法性,这样就不可以自由地使用未经授权的软件,如从网络上免费下载的 MP3 音乐,电影等,而这种模式损害了开源软件的作用,所以平衡共享和版权问题是一个亟待解决的问题。另外在隐私泄漏和保护,基于 TPM 的可信计算平台在硬件平台中嵌入唯一身份证明,提供了基于 PKI 的用户身份鉴别,这样非法的操作将被禁止或者记录,但同时在网络上发生的任何访问动作都能准确定位动作发起者的身份,从而也损害了用户的隐私保护,另外被信任的应用有可能滥用所收集到的用户信息,可能导致隐私的泄漏。同时系统根据被签名软硬件的信任关系来对用户行为的进行控制,这样导致用户无法按照自己的意愿实施特定的控制策略,给用户的使用带来局限性。

5 结语

当前对可信计算平台的研究和应用正处于急速发展期。基于 863 项目"数字证书 SoC 芯片"和“可信计算系统平台”,完全符合 TCG 标准的联想“恒智”安全芯片已经成功问世,国内其他的厂商也大力地推进可信计算技术。经过几年的摸索和探讨,取得了很大的进展,但要解决的问题也很多。就上节提到的问题,目前提出的解决方案有:

(下转第 1812 页)

定理 2[4] 对于最多不超过 k 个叛逆者构造的盗版解码器,二分查找黑盒子追踪算法能以 $1-\varepsilon$ 的概率识别至少一个叛逆者,其中 ε 是可以忽略的。

对于改进方案的安全性而言,下面定理成立:

定理 3 对于改进方案的安全性而言,至少同文献[4]一样安全。

证明 首先,改进方案的公钥完全同文献[4]一样。其次,改进方案的分组头中只比文献[4]多出一个元素 $h'=g^{r_{t_c}}$,由于离散对数问题的困难性,显然不能由 $h'=g^{r_{t_c}}$ 得到服务参数 t_c。用户 u 从上述解密步骤1)中只能得到 $h^{f_i(u)}$,但却不能得到 $f_i(u)$;而文献[4]中用户 u 可直接拥有 $f_i(u)$。最后,用户 u 拥有对服务 c 的服务密钥 $g_i(u,\alpha_u)$,但是从 $g_i(u,\alpha_u)=f_i(u)+t_c\alpha_u$ 中不能直接得到 $f_i(u)$,因为用户 u 并不知道 t_c;事实上,最多不超过 k 个叛逆者合谋也不能破解 $f_i(u)$(因为由 k 个叛逆者合谋组成的 k 个方程中含有 $k+1$ 个未知数),证毕。

若用户 u 在执行 OPE 协议时使用的 α_u 与发给 DS 的签字中所含的 α_u 不同,则用户 u 不能通过 DS 的验证(2.3 小节3))。用户 u 的密钥 (i,u,α_u) 中的 α_u 和服务密钥 $g_i(u,\alpha_u)$ 只有自己知道,因此当DS追踪到 u 是叛逆者时,用户 u 无法抵赖,DS的利益得到了保障。同样,DS不知道用户 u 密钥中的 α_u 和服务密钥 $g_i(u,\alpha_u)$,因此 DS 无法陷害无辜用户 u,用户 u 的利益也得到了保障。

4 性能比较

表1中 $O(\cdot)$ 表示时间复杂度,n 为所有用户数,k 为在一次合谋中最大的叛逆者人数(即合谋门限),$|M|$ 表示整数 M 的比特位长,p 和 q 为大素数且 $q\mid p-1$,$l=4(d+1)k+3d$,其中 d 是一个整数且满足 Y 的长度小于等于 $d(k+1)+k$,Y 指一个被撤销的用户集合,这些用户与一个或多个未被撤销的用户在他们的每一个子集中共存[4]。

从表1可以看出,文献[4]和改进方案均支持灵活撤销用户的功能;文献[4]和改进方案的黑盒追踪效率和公钥长度相同,分别为 $O(\log n)$ 和 $(2k+2)|p|$;文献[4]的密文长度和密钥长度比改进方案稍短;改进方案提供多服务,但文献[4]不提供;改进方案是非对称方案,但文献[4]不是。考虑到多服务、非对称(防止叛逆者抵赖)的重要性,从总体性能上来看,改进方案要好于文献[4]。

表1 改进方案与文献[4]的性能比较

方案	服务性质	方案性质	灵活撤销	黑盒追踪效率	公钥长度	密文长度	密钥长度
Matsushita 方案	单服务	对称	支持	$O(\log n)$	$(2k+2)\|p\|$	$(l+2)\|p\|$	$\|q\|$
改进方案	多服务	非对称	支持	$O(\log n)$	$(2k+2)\|p\|$	$(l+3)\|p\|$	$2\|q\|$

参考文献:

[1] CHOR B, FIAT A, NAOR M. Tracing Traitors[A]. Advances in Cryptology - CRYPT'94[C]. Berlin: Springer-Verlag, 1994, 257 - 270.

[2] TZENG W-G, TZENG Z-J. A Public-Key Traitor Tracing Scheme with Revocation Using Dynamic Shares[A]. PKC 2001[C]. Berlin: Springer-Verlag, 2001. 207 - 224.

[3] 马华,曹正文. 基于 RSA 加密算法的叛逆者追踪方案[J]. 西安电子科技大学学报, 2004,31(4):611 - 613.

[4] MATSUSHITA T. A Flexibly Revocable Key-Distribution Scheme for Efficient Black-Box Tracing[J]. IEICE Transactions on Fundamentals, 2005, E88-A(4):1055 - 1062.

[5] PFITZMANN B. Trials of Traced Traitors[A]. Information Hiding'96 [C]. Berlin: Springer-Verlag, 1996. 49 - 64.

[6] KUROSAWA K, DESMEDT Y. Optimum Traitor Tracing and Asymmetric Schemes[A]. Proceedings of Eurocrypt98[C]. Berlin: Springer-Verlag, 1998. 145 - 157.

[7] KIAYIAS A, YUNG M. Breaking and Repairing Asymmetric Public-Key Traitor tracing[A]. ACM Workshop on DRM2002[C]. Berlin: Springer-Verlag, 2003. 32 - 50.

[8] 李勇,杨波. 一种高效非对称的动态公钥叛逆者追踪方案[J]. 西安电子科技大学学报(自然科学版), 2003,30(3):394 - 398.

[9] NAOR M, PINKAS B. Oblivious Transfer and Polynomial Evaluation [A]. Proceedings of STOC'99[C]. Atlanta: ACM, 1999. 245 - 254.

(上接第 1809 页)

在解决数字版权保护方面要建立一个信任的机制,这要求系统的基础架构能够允许提供者与用户保持相互的信任,控制策略最终应由双方共同达成,维护双方的权益。

在解决隐私方面提出了 Properly-based Attestation 协议和采用组签名策略,为不暴露平台的根秘密性,提出如零知识证明,组密钥分配等相关的认证技术,使可信计算平台能在不暴露用户隐私的前提下完成认证过程,达到保护用户隐私的目的。

在对用户的使用局限性方面,系统的控制策略应当能够由用户定制,使得用户对系统有更多的控制权利。

未来可信计算平台的研究将主要集中在以下几个方向:1)以工业化方式从计算平台体系结构上解决安全性问题;2)增强计算平台的可信性和为应用层安全创建更可靠的安全根基;3)在网络环境中建立有效的信任关系,并对这种信任关系进行有效的管理。

参考文献:

[1] TPM Main Part1 Design Principles Specification Version 1.2 52 Draft[Z]. 2003.

[2] TPM Main Part2 TPM Structures Specification Version 1.2 57 Draft [Z]. 2003.

[3] TPM Main Part3 Commands Specification Version 1.2 Revision 57 Draft[Z]. 2003.

[4] TPM Specification Part4 TPM Conformance Specification Version 1.2 Draft[Z]. 2003.

[5] TCG Software Stack Specification Version 1.10 RC 10A[Z]. 2003.

[6] TCG Infrastructure Committee Reference Architecture for Integrity Information Interoperability, revision 0.07 Draft[Z]. 2004.

[7] TCG TNC Architecture for Interoperability Specification Ver 1.0 0.16 Draft[Z]. 2004.

[8] IBM Research Report, the role of TPM in enterprise security[Z]. 2004.

[9] TCG Infrastructure Working Group. Use Cases Summary. Draft. Version 0.1[EB/OL]. https://www.Trusted-computinggroup.org/downloads, 2004 - 03 - 07.