文章编号: 1001 - 9081(2009)04 - 0920 - 04

可信计算发展研究

马新强[1],黄 羿[1],李丹宁[2]
(1.重庆文理学院 计算机学院,重庆 402160; 2.贵州科学院,贵阳 550001)
(lidn121@hotmail.com; mxq345@sohu.com)

摘 要:可信计算是目前信息安全技术研究的一个热点,它是在计算系统的基础上发展来的。从科学计算、容错计算到可信计算,介绍了可信计算的起源和发展,重点分析了可信计算属性、可信计算机系统和可信平台的体系结构等关键技术,并对目前可信计算的研究现状和可信软件系统存在的难点问题进行了总结。

关键词:可信计算;可信平台模块;信息安全;可信软件系统
中图分类号: TP309 **文献标志码**: A

Study on development of trusted computing

MA Xin-qiang[1], HUANG Yi[1], LI Dan-ning[2]
(1. *College of Computer Sciences, Chongqing University of Arts and Sciences, Chongqing* 402160, *China*;
2. *Guizhou Academy of Sciences, Guiyang Guizhou* 550001, *China*)

Abstract: Trusted computing is a hotspot of information security research nowadays. It is developed based on computed system. From science computing and fault-tolerant computing to trusted computing, the origin and development of trusted computing were introduced, especially its property, trusted computer system, and architecture and key components of the trusted platform module. The current research and difficult problems of trusted software system have also been summarized.

Key words: trusted computing; Trusted Platform Module (TPM); information security; trusted software system

0 引言

随着计算机各种技术的迅速发展,信息的安全却日益成为系统成败的关键要素。系统安全是整个计算机安全的基础,没有系统的安全,就谈不上建立在其上的数据库安全和其他应用软件的安全,更无法保证整个网络的安全。目前以防火墙、入侵检测和病毒防护为主的传统的信息安全技术仅仅只是从外部对企图共享信息资源的非法用户和越权访问进行封堵,以达到防止外部攻击的目的。然而对于来自于内部的安全威胁,常规的信息安全技术很难发挥其功效,无法通过现有的常规技术来防止内部人员对重要信息的泄露、窃取、篡改和破坏。传统的安全技术面临新的挑战,新型的网络计算模式不断涌现。毫无疑问,保护信息的私密性、完整性、真实性和可靠性,以提供一个可信赖的计算环境已经成为企业和消费者最优先的需求之一。以底层的计算技术和密码技术相结合的可信计算技术,由于其可以在 PC机硬件平台上引入可信平台模块架构,通过提供的安全特性来提高系统终端的安全性,保证了内部的安全[1]。目前,可信计算已成为信息安全技术研究的热点。

1 可信计算的起源和定义

1.1 计算系统

可信计算的思想源于社会。其基本思想是在计算机系统中首先建立一个信任根,再建立一条信任链,一级测量认证一级,一级信任一级,把信任关系扩大到整个计算机系统,从而确保计算机系统的可信[2]。然而最初的计算机是基于计算系统建立起来的,计算系统最基本的功能是计算精度与正确性。但是计算系统仍然存在需要很多研究的问题,其核心是大规模的科学计算。世界上大多数国家是通过大规模数值计算来进行核武器模拟,美国、日本等国已把大规模科学计算作为国家战略。大规模科学计算的根本是置信度,数值模拟的置信度是当前研究的热点之一。科学计算与可信计算密切相关,置信度 =计算机科学的可信计算 (⑤ + ④ + ③) +物理数学的可信度 (① + ② + ③),其中计算方法为核心,如图 1所示。如几何计算中的误差分析与控制,浮点表示可能导致误差。计算本身"不可信"将是可怕的事情,计算系统应该给人类带来帮助,而不是灾难!

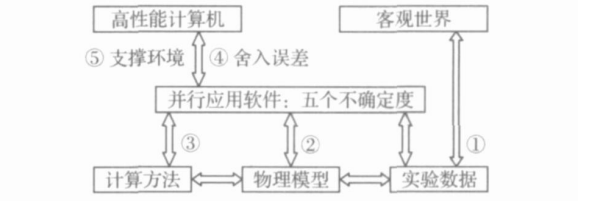

图 1 置信度

可信计算的发展与容错计算密切相关。容错计算的研究与发展应该以 1971年召开第一届国际容错计算会议 (FTCS1-1)为起点[3]。从 1975年开始,商业化的容错机推向市场。到九十年代,软件容错的问题被提了出来,进而发展到网络容错。差不多同期,安德逊 (J. P. Anderson)首次提出可信系统 (Trusted System)的概念。较早期学者对可信系统研究主要集中在硬件设备和运行于其上的软件的安全和可靠性。此时的可信计算实际上是一种可靠计算 (Dependable computing)

收稿日期: 2008 - 10 - 06;**修回日期**: 2008 - 12 - 01。 **基金项目**:国家自然科学基金资助项目 (90718009);贵州省高新技术发展及产业化项目 (20085014);重庆文理学院校内科研重点项目 (Z2008SJ15; Y2007SJ43)。

作者简介:马新强 (1979 -),男,山东鱼台人,讲师,硕士,CCF会员 (E200009253M),主要研究方向:可信计算、信息安全; 黄羿 (1976 -),女,重庆人,讲师,硕士,主要研究方向:可信计算、信息安全、信息检索; 李丹宁 (1961 -),男,贵州贵阳人,副研究员,博士,主要研究方向:信息安全、信息检索、数字地球。

的概念,与容错计算(fault-tolerant computing)领域的研究密切相关。Dependable Computing概念是美国电机电子工程师学会会士(IEEE Fellow)阿维泽尼斯(A. Avizienis)教授 1995年在 FTCS-15上提出的。

1.2 可信计算的定义

1.2.1 可信

在定义可信计算之前,首先应明确可信的概念。"如果一个实体的行为总是以预期的方式达到既定目标,那么它是可信的"(An entity can be trusted if it always behaves in the expected manner for the intended purpose)[4]。这个定义将可信计算和当前的安全技术分开:可信强调行为结果可预期,但并不等于行为是安全的,这是两个不同的概念[5]。根据英特尔的密码与信息安全专家大卫.格劳洛克(David Grawrock)的说法,如果你知道你的电脑中有病毒,这些病毒会在什么时候发作,了解会产生怎样的后果,同时病毒也确实是这么运行的,那么这台电脑就是可信的。

1.2.2 可信计算

对于可信计算并没有统一的定义。ISO/IEC15408标准定义为:一个可信的组件、操作或过程的行为在任意操作条件下是可预测的,并能很好地抵抗应用程序软件、病毒以及一定物理干扰所造成的破坏[6]。它强调行为的可预测性,能抵抗各种破坏,达到预期的目标。

文献[7]认为可信是指:计算机系统所提供的服务是可靠的、可用的,信息和行为上是安全的。相对应的可信计算平台是能够提供可信计算服务的计算机软硬件实体,它能够提供系统的可靠性、可用性、信息和行为的安全性。

学术界把可信计算(Dependable Computing)定义为"系统提供可信赖的计算服务的能力,而这种可信赖性是可以验证的[8]"。即你必须用某种方法来验证你的系统是可信赖的,这是很困难的。众所周知,法律对于人有所谓"无罪认定原则",就是说,除非有证据证明某人有罪,否则他就是无罪的。而对于可信系统,执行的是"有错认定原则",那就是说,用户可以对系统设计者和制造者说,除非你有足够的证据证明你的系统是可信的,否则我就认为你的系统是不可信的。例如,对于一个软件,如果开发者没有足够的理由说明它是正确的,用户就认为它是有错误的。这个要求对系统设计者和制造者来说,是个难题,需要可信计算技术来提供。而且,可信性必须成为可以衡量和验证的性能。

可信计算并没有形成统一的定义,正如 19世纪政论家 Walter Bagehot在谈到什么是"民族"时曾这样说:你要是不问,我们都知道它是什么,但要马上对它做出解释或给个定义,却做不到。

简单地定义可信计算为:计算系统应计算准确,功能正确而完备,具有容错能力与可抵御外部干扰;可信≈可靠+安全。主要体现系统的"可信性",计算系统的"可信"是一个目标,"可信计算"研究是一个系统工程。

2 可信计算关键技术

2.1 可信属性

"可信计算"属性主要从四个方面来理解:1)用户的身份认证,这是对使用者的信任;2)平台软硬件配置的正确性,这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。但其属性基本应包含"可靠性、安全性、完整性、保密性、可用性、可预测性、生存性、互操作性和可控性等"。"可信"与不同的对象联系在一起,会产生不同的理解。例如:可信终端、可信网络和可信软件等。依据对象的不同,某些属性要求也会相对突出一些。

2.2 可信计算机系统

信任根和信任链是可信计算平台的关键技术[2]。一个可信计算机系统由可信根、可信硬件平台、可信操作系统、可信数据库系统和可信应用系统组成,如图 2所示。信任链是通过构建一个信任根,从信任根开始到硬件平台、操作系统、数据库系统,再到应用,一级认证一级,一级信任一级,从而把这种信任扩展到整个计算机系统。其中信任根的可信性由物理安全和管理安全确保。

图 2　可信计算机系统

2.3 可信平台体系结构

可信平台是以可信平台模块(Trusted Platform Module, TPM)为核心,把 CPU、操作系统、应用软件和网络基础设备融合为一体的完整体系结构。一个典型的 PC平台上的体系结构主要可以分为三层:可信平台模块(Trusted Platform Module, TPM)、可信软件栈(Trusted Software Stack, TSS)和应用软件[4],如图 3所示[5]。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,并提供对 TPM的同步访问管理。TSS平台软件从结构上可以分为四层,自下至上分别为 TPM驱动程序库(TPM Device Driver Library, TDDL)、可信软件栈核心服务(TSS Core Services, TCS)和可信服务提供者(Trusted Service Provider, TSP),全部运行于用户模式和运行于内核态的 TPM驱动程序(TPM Device Driver, TDD)。

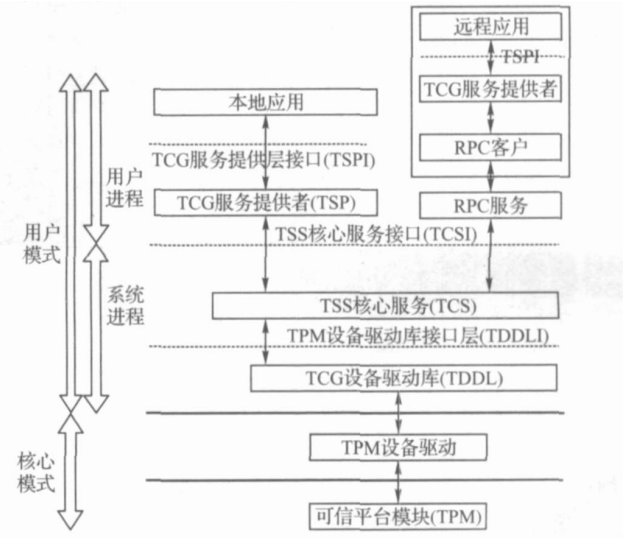

图 3　可信平台体系结构

2.3.1 TDDL

TDDL是用户模式和内核模式之间的过渡,功能是通过提供标准接口,屏蔽各种不同 TPM的差异。

2.3.2 TCS

TCS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 TPM进行通信。除提供 TPM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 TPM提供的功能。

2.3.3 TSP

TSP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。

3 可信计算的研究现状

3.1 国内外研究发展

可信计算的出现最早可以追溯到上世纪八十年代。1983年美国国防部国家计算机安全中心制定了橘皮书《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteria, TCSEC)[9],在 TCSEC中第一次提出可信计算机和可信计算基(Trusted Computing Base, TCB)的概念,并把 TCB作为系统安全的基础。随后又相继推出了可信数据库解释 TDI(Trusted Database Interpretation)[10]和可信网络解释 TNI(Trusted Network Interpretation)[11]作为补充。由于可信计算机评价准则系列是在早期 BLP模型[12]的基础上提出的,具有一定的局限性。它们主要考虑了信息的保密性,缺乏完整性、真实性控制;强调了系统安全性的评价,却没有给出达到这种安全性的系统结构和技术路线。

1999年 10月,由 Compaq、HP、IBM、Intel和 Microsoft牵头组织成立了可信计算平台联盟(Trusted Computing Platform Alliance, TCPA),2003年 TCPA改组为可信计算组织(Trusted Computing Group, TCG),现有 200多家公司参加。2002年 1月,微软比尔·盖茨提出了可信计算(Trustworthy Computing)[13];2003年,美国计算研究协会提出了可信计算研究的任务;欧洲于 2006年 1月启动了名为"开放式可信计算(Open Trusted Computing)"的研究计划[14]。表明在国际上出现了可信计算的高潮期,这一阶段不仅考虑信息的秘密性,更强调了信息的真实性和完整性,而且更加产业化和更具广泛性。

我国可信计算研究起步较晚,但在技术研究与产品开发方面,有一定的积累。在安全芯片、可信安全主机、安全操作系统和可信计算平台应用等方面都先后开展了大量的研究工作。上世纪九十年代,因军队的特殊要求,我军开发了 PC机的安全防护系统,实现了可信防护,其结构、功能与 TCP类同。2000年,武汉瑞达公司开始可信安全计算机的研发工作,于 2004年推出具有自主知识产权的可信计算机产品,通过了国密局主持的鉴定[15]。目前已展开了省级党政机要系统的应用试点工作。联想公司和中科院计算所也较早开展了安全芯片和安全计算机的研究工作。2003年,联想公司安全芯片的研发工作在国密办立项,2005年 4月完成了安全芯片的研制,安全主机产品计划在 2005年内推出,其安全芯片和可信 PC平台已通过国密局主持的鉴定。2006年 3月,联想公司正式加入国际可信计算组织,成为核心成员。兆日公司是我国较早开展 TPM芯片研究工作的企业。2005年 4月,推出符合可信计算组织技术标准的 TPM安全芯片,并已经开展了与长城、同方等多家主流品牌电脑厂商的合作;其安全芯片已通过国密局主持的鉴定[16]。2007年,贵州科学院与加拿大阿尔百特大学联合开始"可信内容管理系统"的研究。以上表明我国也已进入可信计算的发展期。

国家"十一五"规划和"863计划"中,把"可信安全计算平台研究"列入重点支持方向,并有较大规模的投入与扶植。国家发改委、信息产业部在"十一五"发展规划中也作为发展重点。尤其是何积丰院士领导的国家自然科学基金委员会颁布的"可信软件基础研究"重大研究计划项目,将进一步推动我国可信计算的研究发展。

3.2 可信计算研究内容现状

可信计算研究涵盖多个学科领域:计算机科学与技术通信、数学、管理科学、复杂系统科学、社会学与心理学、法律和政治等。现在可信计算研究主要有五个方面:理论和体系结构、核心关键技术、综合试验平台、应用和度量标准。

1)可信计算理论和体系结构。

由于可信计算概念来自于工程技术发展,到目前为止还没有一个统一的科学严谨的定义,基础理论模型还未建立,现有的体系结构还是从工程实施上来构建,缺乏科学严密性。但在理论研究上,已受到国际社会的重视,如:IEEE组织于 2004年开办了 IEEE Transactions on Dependable and Secure Computing杂志,专门刊发可信计算研究论文。主要包含:可信计算的基础理论模型[17]、可信计算的体系结构研究、可信软件和可信计算的安全保障。

2)可信计算关键技术。

可信计算的关键技术涵盖了芯片、终端、网络和软件等信息系统组件,通过运用这些核心关键技术,最终实现保护应用资产安全的目的。可信芯片:可信计算的安全基础是可信芯片,需要设计特殊的 CPU和安全保护电路,内嵌高性能的加密算法、数字签名、散列函数和随机发生器等,是可信计算研究中体现国家主权控制和竞争能力的核心。可信终端:把 CPU、操作系统、应用可信软件以及网络设备融为一体的基础设备,是构成可信体系的基础装备。可信网络[18]:主要研究可信网络的体系结构、可信网络协议层次、可信网络的控制模型、机制与方法、可信操作系统、可信软件、可信软件工程技术[19]和可信数据库等。

3)可信计算综合试验平台。

构建可信计算的综合试验支撑环境,建立可信系统开发平台,研究网络环境下多源数据的同化、整合和可信处理,网络环境中的可信数据服务,可信 XML数据库,可信网络服务工程,可信操作系统等,对可信计算的核心关键技术研究成果在试验平台上进行测试和验证。

4)可信计算应用示范。

选择经济社会领域的重大关键应用,开展可信计算应用示范,促进可信计算研究成果的推广和产业化,切实增强我国在可信计算领域的综合实力和国际竞争力。示范应用研究举例:电子商务可信计算环境、电子政务可信计算环境、航空航天信息可信计算环境和海洋信息可信计算环境等。

5)可信计算(软件)度量标准。

可信计算国家标准关系到国家信息安全和经济利益。谁掌握了可信计算标准的制定权,谁的技术就可能成为标准,谁就将拥有市场和产业的主动权和控制权。要实现与国外接轨,重要的是把我国的可信标准融入国际标准,而不是照抄国外标准。可信计算标准研究要先立足国内,再争取成为国际标准,在世界上占一席之地。

4 可信软件系统存在的难点问题

从可信计算开始研究到目前状况,主要从硬件的角度强调可靠性、可信性等,轻视了软件系统的可信性。"可信计

算 研究是一个系统工程,不仅包含硬件,更有软件的可信性。目前,硬件的可靠性越来越高,而软件因其复杂度剧增而趋于失控。早期的一份计算机系统失效源的统计数据,如表1所示。目前据统计,90%以上对计算机网络系统的攻击利用了软件的缺陷。2002年 6月 28日,美国商务部的国家标准技术研究所 (National Institute of Standards and Technology, NIST)发表了有关软件缺陷的损失调查报告,报告表示,"据推测,由于软件缺陷而引起的损失额每年高达 595亿美元。这一数字相当于美国国内生产总值的 0.6% "。随着软件在社会生活中的广泛应用,特别是各种嵌入式软件在各种智能电器中的应用,软件缺陷造成的损失将会更大。

表 1　计算机系统失效源的统计表

系统	数据发表年份	硬件 /%	软件 /%	维护 /%	操作 /%	环境 /%
AT&TESS	1978	20	15	/	65	/
Tandem	1985	18	26	25	17	14
Bellcore	1986	26	30	/	44	/
Tandem	1987	19	43	13	13	12

可信计算环境至关重要,封闭环境中有一些安全攸关计算系统,只需要可靠性保证,但这类系统具有较高的显示度。开放环境是技术发展的趋势和主流,广泛互连、并行处理、资源竞争、潜在冲突和恶意攻击等都是在开放环境中普遍存在的。计算系统必须在开放环境中接受考验。用一句话来概括"可信计算研究 ":开放环境中软件系统可信度量及构造方法。在开放环境下,可信软件系统急需解决的几个难题:

1)能否构造软件系统的"可信 "?

需求分析、形式化、分析推理、自动程序生成和软件工程等,硬件体系结构、容错技术、密码与安全等方面的配合;可信软件问题的根本解决有待形式理论与形式方法研究的突破。

2)可信的几个重要属性能否量化、分级?

计算系统是一个产品,应该有 (也必须有)度量标准;计算系统都或多或少存在缺陷,有的能够发现,有的难以发现;有的即使能发现也不一定能排除 (人力物力时间有限);有的致命、有的无大碍;能否分级和量化指标?

3)如何把"试凑性 测试变为"理性 测试?

测试是最后一关,也是最重要的一关,在有限的资源之下,如何有效测试、发现问题?状态空间爆炸,难以遍历;缺少真实的测试环境;需要研究测试形式化的方法;还需要建立一个适于形式化测试的工具环境。能否把测试问题前移?能否变为构造性问题?

4)能否建立软件系统的动力学模型与分析方法?

软件系统 (或计算系统)是一个客观存在,其构建过程遵循严格的逻辑,不存在模糊性、随机性和不确定性,只有规模复杂性;与其他领域相比,我们对软件的动力学特性的理解极不成熟,暂无物理规律可循,也无"安全系数 "可言;而计算过程是一个复杂的动力学过程,能否把逻辑序列、分布、并行、交互和事件驱动等混杂起来,构造软件系统动力学?

5　结语

目前可信计算已经成为世界信息安全领域的一个新热点,然而就目前的可信计算理论而言,可信计算的研究还仅仅停留在硬件平台标准上,而且对于可信计算平台中信任量度的具体方法,可信程度的具体评估目前也没有统一的标准,尤其是对软件系统的可信性,还存在较多难点。可信计算机与普通计算机相比,安全性大大提高,但可信计算机也不是百分之百安全。并不是所有人对可信计算的普及都持乐观态度。剑桥大学的 Ross Anderson教授就对可信计算提出了不同的看法[20]。他担心可信平台芯片以及相关技术有可能成为垄断寡头们分割未来产业的手段。教授的担心是有道理的,也许我们在憧憬着未来可信计算技术的同时也应该多从本国的产业角度出发筹划未来。

志谢　在本课题的研究过程中特别得到华东师范大学的何积丰院士、加拿大阿尔百特大学袁立言终身教授和贵州科学院张明义研究员的指导,特此感谢。

参考文献:

[1] 靳蓓蓓,张仕斌. 可信计算平台及其研究现状 [J]. 长春大学学报, 2007, 14(2): 45 - 49.

[2] 张焕国,罗捷,金刚,等. 可信计算研究进展 [J]. 武汉大学学报:理学版, 2006, 52(5): 513 - 518.

[3] 闵应骅. 前进中的可信计算 [J]. 中国传媒科技, 2005, 26(9): 50 - 52.

[4] Trusted Computing Group. TCG specification architecture overview [EB/OL]. (2005 - 03 - 01) [2008 - 09 - 10]. https://WWW.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf.

[5] 张 晋,桂文明,苏涤生,等. 从终端到网络的可信计算技术 [J]. 信息技术快报, 2006, 4(2): 21 - 34.

[6] PEARSON S. Trusted computing platform, the next security solution [R]. Bristol UK: HP Laboratories, 2002.

[7] 沈昌祥,张焕国,冯登国,等. 信息安全综述 [J]. 中国科学:E辑 信息科学, 2007, 37(2): 129 - 150.

[8] AVIZIENIS A, LAPRIE J C, RANDELL B, *et al*. Basic concepts and taxonomy of dependable and secure computing [J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11 - 33.

[9] Department of Defense Computer Security Center. Department of defense trusted computer system evaluation criteria [S]. Washington, D C, USA: DOD, 1985.

[10] National Computer Security Center. Trusted database management system interpretation, NCSC-TG-021 [S]. Washington, D C, USA: DOD, 1991.

[11] National Computer Security Center. Trusted network interpretation of the trusted computer system evaluation criteria, NCSC-TG-005 [S]. Washington, D C, USA: DOD, 1987.

[12] BELL D E, LAPADULA L J. Secure computer systems: Mathematical foundations, MTR-2547 [R]. MITRE Corporation, 1973.

[13] Microsoft. Trusted platform module services in windows longhorn [EB/OL]. (2005 - 04 - 25) [2008 - 08 - 20]. http://www.microsoft.com/resources/ngscb/.

[14] The Open Trusted Computing (OpenTC) consortium. General activities of OpenTC [EB/OL]. [2008 - 09 - 01]. http://www.opentc.net/activities/.

[15] 张焕国,毋国庆,覃中平,等. 一种新型安全计算机 [J]. 武汉大学学报:理学版, 2004, 50(S1): 1 - 6.

[16] 兆日科技. 兆日 TPM安全芯片 (SSX35)和解决方案 [EB/OL]. [2008 - 09 - 25]. http://www.sinosun.com.cn.

[17] 唐文,陈钟. 基于模糊集合理论的主观信任管理模型研究 [J]. 软件学报, 2003, 14(8): 1401 - 1408.

[18] 林闯, 彭雪海. 可信网络研究 [J]. 计算机学报, 2005, 28(5): 751 - 758.

[19] 陈火旺,王戟,董威. 高可信软件工程技术 [J]. 电子学报, 2003, 31(12A): 1933 - 1938.

[20] ANDERSON R. Trusted computing frequently asked questions [EB/OL]. [2008 - 08 - 26]. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html