ISCCF

第十九届全国信息保密学术会议
（IS2009）
论 文 集

中国计算机学会信息保密专业委员会 编

金城出版社
GOLD WALL PRESS

ISCCF

第十九届全国信息保密学术会议
(IS2009)
论 文 集

中国计算机学会信息保密专业委员会 编

金城出版社
GOLD WALL PRESS

图书在版编目（CIP）数据

第十九届全国信息保密学术会议（IS2009）论文集 / 中国计算机学会信息保密专业委员会编 . —北京：金城出版社，2009. 9

ISBN 978-7-80251-227-6

Ⅰ . 第… Ⅱ . 中… Ⅲ . 信息系统—安全技术—学术会议—文集 Ⅳ . TP309-53

中国版本图书馆 CIP 数据核字（2009）第 149922 号

第十九届全国信息保密学术会议（IS2009）论文集

作　　者	中国计算机学会信息保密专业委员会
责任编辑	王景涛　蔡传聪
开　　本	787毫米×1092毫米　1/16
印　　张	24.75
字　　数	600千字
版　　次	2009年9月第1版　2009年9月第1次印刷
印　　刷	北京金瀑印刷有限责任公司
书　　号	ISBN 978-7-80251-227-6
定　　价	80.00元

出版发行	**金城出版社** 北京市朝阳区和平街11区37号楼　邮编：100013
发 行 部	(010)84254364
编 辑 部	(010)64222699
总 编 室	(010)64228516
网　　址	http://www.jccb.com.cn
电子邮箱	jinchengchuban@163.com
法律顾问	陈鹰律师事务所　(010)64970501

前　言

第十九届全国信息保密学术会议（IS2009）于2009年9月在甘肃省敦煌市召开。经有关专家评审，从来自全国各科研开发部门、大专院校和管理部门的论文中选出61篇编入此本《第十九届全国信息保密学术会议论文集》，供信息安全保密专业人员交流。

在此向热情为本次学术年会投稿的全体作者，为此次会议召开和论文集出版提供大力支持的专家、学者以及甘肃省国家保密局、沈阳东软软件股份有限公司、联想网御科技（北京）有限公司表示感谢。

中国计算机学会

信息保密专业委员会

秘　书　组

2009年9月

目　录

面向平台的可信计算环境构造方法研究*

赵 波[1,2] 张焕国[1,2] 李 晶[1,2] 陈 璐[1,2]

武汉大学计算机学院[1]
空天信息安全与可信计算教育部重点实验室[2]

摘 要 目前可信计算已经成为信息安全领域的新潮流，对构建安全信息系统有重大指导意义。可信环境的构建是可信计算系统安全的基础，目前国内外可信计算平台产品的体系结构都是对现有通用产品的迁就和妥协，未在理论上做出证明和分析，并不是构建可信环境的最佳结构，对系统信任边界的动态扩展缺乏有效支持。

本文研究面向平台的可信计算环境构建的理论模型和关键技术。该模型将突出星型的可信环境结构特点，降低信任传递过程中的信任损耗；同时根据该模型具体设计出一种新的可信计算平台体系结构，该体系结构能够灵活地扩展信任边界；最终提出一种新的可信度量方法，支持多信任等级的可信度量。

上述研究，可以有效地解决可信环境构建、体系结构、度量方法等问题。

关键词 可信计算 环境构建 可信度量

可信计算已经成为信息安全领域的新潮流，可信计算技术是一种行之有效的信息安全技术。可信计算平台是能够提供可信计算服务的计算机软硬件系统。

可信计算组织 TCG 为此制定了一系列的技术规范，我国也在制定自己的可信计算技术标准，国内外的大多数可信计算产品都遵从 TCG 所提出的系统结构和技术路线。然而，TCG 提出的以可信平台模块 TPM 为核心搭建信任链机理，从未在理论上获得对该种体系结构的安全性和合理性的证明。

可信的计算环境非常重要，仅依靠 TCG 的信任链构造方式并不能确保整个计算环境的可信，也不符合我们的国家利益。如何构造出具有自主知识产权的面向平台的可信计算环境，正是我们所要研究的重要课题。

1 现有可信平台构造理论的问题

目前大部分可信计算平台的体系结构表现为链式结构，这种结构存在很多不足之处，主要表现在：可信计算平台作为被动设备运行：在多次逐级传递后，整个系统信任关系的

* 基金项目：国家自然科学基金（60673071）和国家 863 计划项目（2006AA01Z442，2007AA01Z411）

安全性会受到影响，信任链中的任何一个环节被攻破都可能破坏整个系统的安全；经过多层次的调用后会降低系统的工作效率；如果要增加一个系统组件（硬件或软件）或者要进行网络连接，都需要信任链的重新度量；如果信任链中的某个节点出现问题，信任根无法对问题节点做出快速反应，无法越过中间节点操作问题节点，信任根则对信任链上其他节点的控制能力较弱。

随着科学技术的发展，现在的可信计算平台正在向操作系统小、功能可裁剪添加、硬件更改方便等方面发展，所以有必要研究出一种新的可信计算环境构造体系结构，既能够避免目前链式体系结构的不足，又能充分考虑其信任边界是否能够灵活地扩展、信任损失更小等特点。

现有的基于完整性度量的方式有很多局限性，这种方式是一种静态度量，侧重于对代码完整性的控制，而对代码的安全性和可控性则很难进行判别。系统软件的多变性和复杂性会给系统带来各种不可预测的结果，这些行为哪些是安全的，哪些是不安全的，直接影响着系统的可信和软件的可信，目前仅以完整性度量的方式还不能对软件的动态性做检测，因而也就无法保证整个系统的安全。另外，完整性度量方式在软硬件升级频繁的今天，无法做到真正地应用与扩展。因此，有必要研究出一种新的、更加安全合理的可信度量方法，而且这种方法有利于构造面向平台的可信计算环境。

2 可信计算环境构造

2.1 可信的定义

目前关于可信计算的准确定义，国内外无论是学术界还是工业界还尚未形成统一的意见，不同的组织与学术流派从各自的立场出发给出了一系列的定义。在讨论“可信”的概念时，经常会看到如下几个单词：Trusted、Trustworthy、Trustable、Trusting、Trustful、Dependable。这些单词在中文中均可译成“可信”，但其含义却有所不同。我们研究的计算环境的可信是指计算环境的参与方能够确信该计算环境是可以信赖的。

根据以上分析，我们对可信计算环境定义如下：

定义 1　可信计算环境是这样一种计算系统，其初始状态是可信的，而且状态转换也符合可信规则。计算环境中的实体 E 包括证明实体和被证明实体，实体的可信级别 TL 是在可信计算环境中用来标识实体是否可以通过可信条件检查的属性，仅当一个实体达到一定可信级别时才被允许执行某些操作。

定义 2　证明实体 M 是可信核心 Mc 和证明代理 Ma1，Ma2，…，Man 组成的集合，$M = \{Mc, Ma1, Ma2, \cdots, Man\}$。

定义 3　被证明实体 R 是可信计算环境中所有资源节点的集合，每个被证明节点都隶属于一个证明实体。根据证明实体的不同，被证明实体可划分为多个子域 Ra1，Ra2，…，Ran，每个子域包含数量不等的资源节点，若某证明实体 Max 下没有资源节点，则 $Rax = \emptyset$，且任意两个子域 Rax 和 Ray 的交集为空，$Rax \cap Ray = \emptyset$，$R = Ra1 \cup Ra2 \cup \cdots \cup Ran$。

可信条件：实体 E1 可以使用实体 E2 的提供服务，当且仅当 E2 的可信级别 TLE2 达到 E1 对 E2 的期望可信级别 ETLE2，即 $TLE2 \geqslant ETLE2$。

可信定理：设系统的可信初始条件为 σ0，S 是状态转换的集合。如果 S 的每个元素都遵守可信条件，那么对于每个 i≥0，状态 σi 都是可信的。

2.2 可信环境的构造定理

构造可信定理：如果构造前后环境的可信状态没有发生改变，那么构造过程是可信的。

经过对可信计算环境的分析，我们认为可信计算环境包括三类节点：可信核心、可信代理和 资源节点。图 1 所示为星型可信环境的构造模型。将每个资源节点分配给一个可信代理。

可信核心：由硬件实现，在系统初始化时进行可信证明。在系统通过初始可信度量之后，将执行之后的启动过程，并启动多个可信代理，由可信代理执行对资源节点的可信度量过程。可信核心在系统中被认为是可信服务的，可以抵抗非物理手段攻击。

可信代理：相当于可信计算环境定义中的证明代理，是平台的一个功能组件，用于对资源节点进行可信度量，每个可信代理管理一个或多个资源节点。

资源节点：相当于可信计算环境定义中的被证明实体。该节点可以是资源或服务的提供者或请求者，即为资源服务者或资源请求者，请求的发起及响应需符合可信规则。

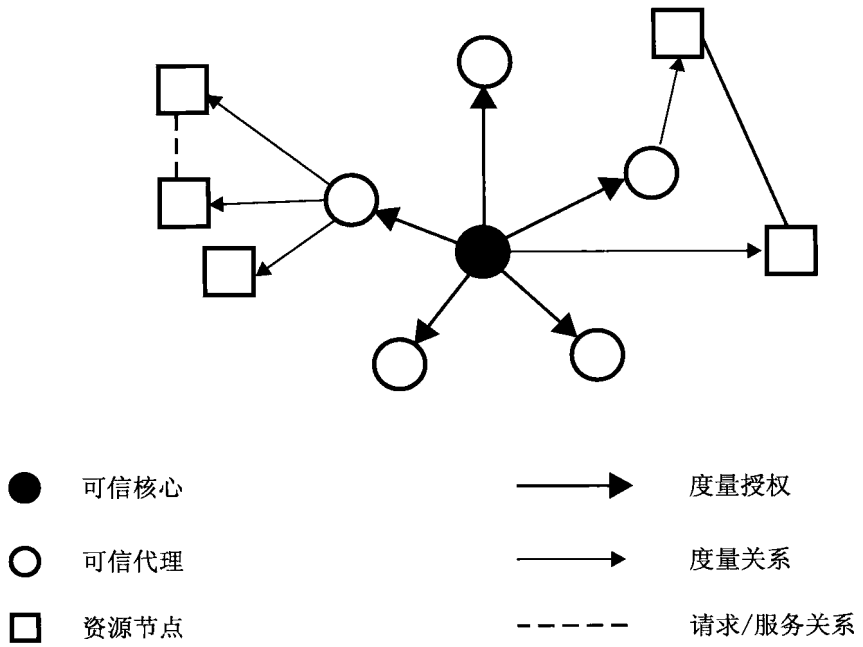

图 1 可信环境构造模型

可信核心为可信计算环境的构造提供了初始条件。如何保证初始可信，如何利用可信代理对节点进行度量，如何在构造过程中保证系统状态依然可信是本项理论研究的主要问题。

在面向平台的可信计算环境构造体系结构的研究中，依据上面描述的可信环境构造的相关角色，结合平台特点，可以把可信核心与可信计算平台中的可信硬件相对应，可信计

算平台中的其他组件与可信代理和资源节点相对应，从而得到体系结构的初步方案，该方案不仅需要满足构造可信计算环境的充分必要条件，还要给出体系结构中各个组件的描述及组件间关系。基于上述考虑，我们给出如下的定义：

定义4　一个可信计算平台可表示为一个五元组 TS = （ ID，RT，V，E，TV）。其中：ID 为可信计算平台的标识；RT（Root of Trust）表示为根节点，作为可信计算平台的可信核心；V 为节点集；E 为边集，表示节点间的信任关系；TV（Trust Value）为相应每条边的权值集合。

定义5　节点集 V 是一个有限集，V = {MD，SD}，其中，MD = {MDi，i = 1，2，…，n} 是管理域集，SD = {SDi，i = 1，2，…，m} 是资源域集。把系统中看成由各种组件组成的，不论是逻辑上的功能模块还是各种物理设备都看成是一个组件，并把这些组件分类。将以可信硬件作为可信核心，提供对平台上其他组件进行度量，具有度量功能的组件作为管理域中的元素，其他没有度量功能的组件作为资源域中的元素，即 MD 是由各种执行度量及相关管理功能的组件作为元素所组成的域的集合，SD 则是由相应的被度量的组件作为元素所组成的域的集合。

定义6　SDi 定义为一个五元组 S，S = （I，D，PS，T，NE）。其中：I 为该 S 的标识；D 为域的属性集；PS 为定义在 S 上的处理符集；T 为 S 的可信度；NS 为与该 SDi 上有过交互的节点集。

定义7　MDi 定义为一个七元组 M，M = （I，S，DM，PO，T，NO）。其中：I 为该 M 的标识；S 为 MDi 的资源域集；DM 为 M 的属性集；PM 为定义在 M 上的处理符集；T 为 M 的可信度；NM 为与该 MDi 有过交互的节点集。

定义8　同一域内元素其可信度是相同的，可以进行交互。

定义9　当不同资源域中元素需要交互时，可将一方当作服务提供者（Service Provider），另一方当作任务执行者（Task Executor），它们分别对应资源的提供方和消费方。在一次交互中，域中元素既可以属于服务方，也可以属于任务方，或者同时既属于服务方又属于任务方。根据域中元素的信任需求和评估标准，每个元素在作为服务方和作为任务方时各需要一个信任阈值 TT（ Trust Threshold）：TTservice 和 TTtask ，两者的值一般不相等。

设置信任阈值符合可信条件的要求。例如：实体 i 作为任务方，希望与 j 进行通信，只有当信任值 Ti，j > TTtask 时，实体 i 才认为 j 是可以信任的；同理，作为服务方的 j，计算得到信任值 Tj，i（ 注意与 Ti，j 相区分），只有 Tj，i > TTservice 时，j 才信任 i，愿意为其提供服务。

在不考虑系统间信息交互的情况下，我们认为可信计算环境构建体系结构如下：

由图2 可以看出，该体系结构中 RT 作为可信根，可以确保初始状态可信。所有 MD 都由 RT 进行度量管理，MD 间的信任关系要通过 RT 建立，同一 MDi 下的 SDij 与 SDpq 间的信任是通过 MDi 建立的，而属于不同 MD 的 SDij 与 SDpq 则需要通过相应 MD 及 RT 才能建立信任。可信环境的构造是通过 RT 不断扩展 MD 构成的。

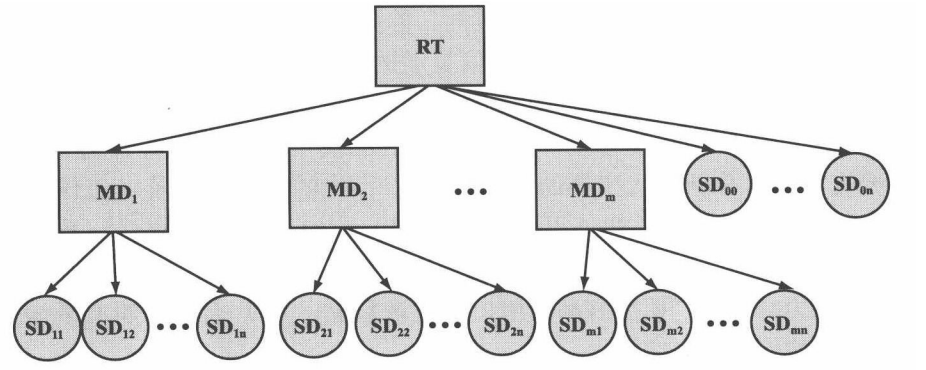

图 2　可信计算环境构造体系结构

具体到平台，可信计算环境的构成由上层安全应用软件、操作系统、硬件平台、可信硬件芯片以及 BIOS、芯片内软件系统的配合完成，这些软硬件系统构成了可信平台环境的各个结构层，我们初步设计了一个更加细化的可信环境构造的体系结构，如图 3 所示：

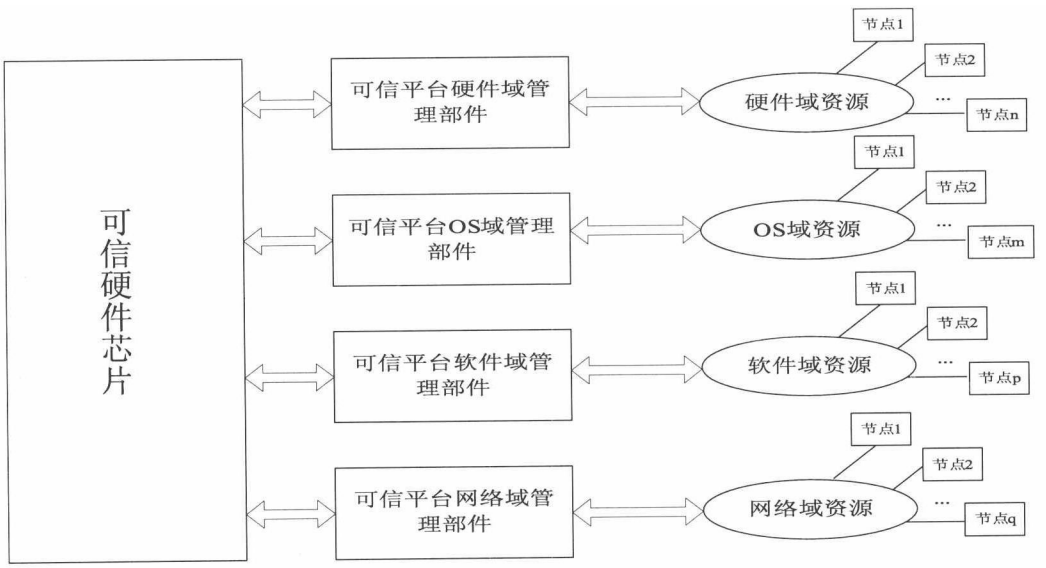

图 3　进一步细化的可信环境构造的体系结构

在图 3 中，可信硬件负责对不同域的管理部件进行度量，决定一个新的域是否能加入到系统中，而各个域管理部件能够对其下属的节点进行度量和报告，并负责节点的增加和删除。

2.3　可信度量的方法

可信度计算的准确性和适用的广泛性是衡量一个模型算法的有效标准。在可信计算环境中，对每一个组件的度量不能单纯地依靠其完整性，还需要考虑：（1）组件间的组织方式及结构；（2）组件信任关系的度量、存储和报告；（3）恶意组件出现的情况；（4）组件的添加、删除对平台状态的影响。因此，我们可以结合信任理论对度量方法进行扩展，让可信代理度量其他实体的可信度，继而由这些实体构成可信计算环境。此外，考虑

到可能出现的恶意实体，在计算实体可信度时，除了计算其信誉度外，还要通过分析其历史行为引入隐含不确定性的风险值作为对信誉度的追加。因此在对实体进行度量的方案中，可信性的度量是平衡风险和信任因素的结果。具体思路如下：

在对节点的可信性进行度量时，我们利用信任模型的思想，并要遵循如下原则：（1）系统要有能力区分新加入实体的好坏；（2）行为的时效性，若一实体长期表现很好但突然表现变坏，系统必须能够很快识别；（3）抵御攻击的鲁棒性，系统必须能够防止实体操纵信任系统；（4）算法简洁和适当透明度，因为待处理证据集庞大且普适计算等设备计算能力有限，透明度有利于用户信任该系统；（5）合成逻辑必须满足交换率和结合律，并尽量保持信息完整性。

根据上面的信任系统的设计原则，我们认为节点可信度是由信誉值和风险值两部分组成。

定义10　用T_{ij}表示节点i对节点j的可信度，R_e和R_i分别表示节点j的信誉值和风险值，α和β分别是两者的权重，则节点j的可信度为：

$$T_{ij}=\alpha R_e-\beta R_i,\qquad 0\leqslant\alpha,\ \beta\leqslant 1$$

α和β的取值依据请求节点i对被评价节点j交互的乐观程度，对j的行为及交互结果越乐观，则选择合适的α和β值使得$\frac{\alpha}{\beta}$越大，使可信度受风险的影响小些；相反，对j的行为越悲观，则$\frac{\alpha}{\beta}$越小，可信度对风险值越敏感。

（1）信誉度计算

在研究节点的信誉度时，可以在信任中引入不确定性因素，借助主观逻辑中结构化符号对信任关系进行建模，并引入证据空间和观念空间的概念来描述和度量信任关系。主观逻辑采用事实空间定义人类对某件事情发生的主观判断，包含了对某件事情发生的不确定性判断，其主观逻辑算子主要包括合并（cojunction）、合意（consensus）和推荐（recommendation）。但主观逻辑描述可信度时没有考虑到时间衰减的影响，也没有考虑不同权值的信任合成及恶意节点出现的情况。所以我们在利用主观逻辑对信任建模时，除了定义一组主观逻辑运算子进行可信度的推导和综合计算，还要引入衰减算子计算时间衰减对信任值的影响，并利用证据理论考虑不同权值的信任合成。

（2）风险计算

在已有的基于推荐的信任模型中，只是单纯考虑了信誉值。这种模型普遍存在的问题是，在感知节点失常行为时缺乏灵敏性，因为其需要时间来对节点的评价逐渐降低。风险的引入有两方面的作用，一方面对风险的考虑可看作是对节点不良行为的惩罚，当交互记录中良好居多时，则风险值小，反映在可信度上即受风险的影响小，反之则对节点信誉值追加较大的风险值，从而比单纯依赖信誉计算出的可信度低；另一方面，可以作为识别恶意节点的有效手段，因为风险来自于交互历史中失败、损失发生的记录，风险值决定其频度及恶劣程度，而恶意节点的交互记录中，失败和损失的频度及恶劣程度大，风险就大，风险值能够被用作预测其未来行为的有力参考。

在实际解决方案中，由于节点动态行为引起的不确定性给可信度的计算带来了难度，我们可以借鉴信息熵理论在处理不确定问题上独有的优势来定义置信度，以便较准确地量化节点的

风险值。具体来说，通常风险总是由危险、损失等不利后果造成。假设造成该不利后果的可能性有 n 个，体现在其直接交互所得的值上为，其中 $f(i)$，确定其为恶意节点的值为 $f(E)$。

定义 11　风险的量化为 $R_{isk}=\frac{\sum_{i=1}^{n}f(i)H(\rho_i)}{f(E)}$，其中 $H(\rho_i)=-\rho_i\log\rho_i$ 为 $i(i=1,2,\cdots,E,\cdots\cdots,n)$ 的熵，ρ_i 为 i 情况的置信度，满足条件 $0\leq\rho_i\leq1$，$\sum_{i=1}^{n}\rho_i=1$。

综上所述，该可信度量方案可以按（1）确定度量路径，找到计算可信度的路径；（2）确定各种路径的可信度并行组合计算方法的优化；（3）用主观逻辑和风险评估理论相结合进行可信度的推算。所以以图 9 的可信计算环境构建模型为基础的度量体系中，RT 是信任根，也是度量根，所有的管理域节点由进行可信度量，而则用于度量其下属资源域中节点的可信度，其度量方法如上所述。当资源域内的节点想与节点进行通信时，节点向相应的管理域发出通信请求，由管理域返回节点的可信值来决定是否继续通信；同样，当新加入一节点时，若节点是管理域内节点则由度量后加入，若节点是资源域内节点，则由相应管理域度量后加入。

在该度量方案中，必须要考虑和研究以下几个关键问题：

（1）算法自适应设计：目前所有的算法都假定信任具有传递性，而信任的传递算法及信任传递的迭代次数即信息在传递多少次后信任值将没有意义在这些方面的问题都需要加以解决。

（2）系统各节点可信度的初始值设计：目前在研究可信性传递的算法中很少有提及可信值的初始化方法，而平台系统可信环境的构建必须保证其初始环境可信，所以，对于系统各节点的初始值以及对系统新加入节点可信度的初始值都要根据平台特点进行设计。

（3）可信度的进化计算：可信度是一定时期的产物，要从辩证发展的观点看待节点可信度，所以要将以前的可信度和现在的可信度进行加权，双方的比例需要实验来确定。

3　利用可信环境构造理论的可信 PDA 设备

由武汉大学研制的可信 PDA 是上述可信计算环境构造方法的具体实现，其基本结构如图 4 所示。在充分分析星型信任关系与链式信任关系的优劣之后，我们提出一种星型的信任管理模型。该模型采用多域方式进行组织，每个子域的度量代理只对可信根负责，由子域的度量代理管理度量相应域中的组件，这样就强化了可信硬件信任根的作用，信任关系不在信任代理间传递，使信任链大大缩短，这样可以避免：在可信平台的信任链传递过程中，若使用链式结构，在各层可信代理之间，层层传递信任关系，会由于对平台系统的多层控制权转移，导致的信任强度减弱。

星型的集中信任管理方式，能够避免链式信任管理方式在安全性和可灵活扩展性方面的不足。同时，可信平台也向着小型化、功能多样化、需求灵活化等方向发展，也对信任链的灵活扩展提出了需求。可信 PDA 模型中，可信硬件芯片在整个体系结构中处于主导地位，能够对各个域模块进行可信度量和存储，并且便于不同域和组件的加入，因此具有可灵活扩展信任边界的特性。这种灵活、安全的管理不光指上一特点中的方便不同域和组件的加入，其次在遇到信任链中某些节点出问题的时候还可以方便管理，可以有一系列规则来判断应该采取的措施，不管是断开节点，还是允许其在某一定范围内继续运行，都很容易实施。

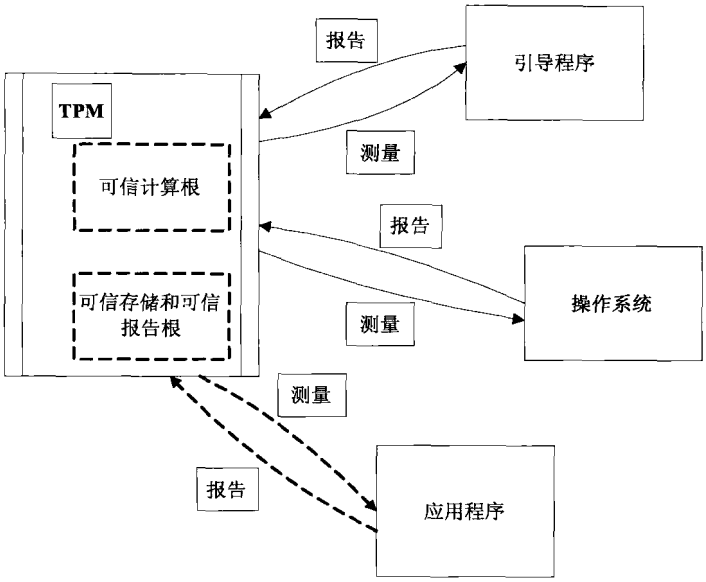

图 4　可信 PDA 的信任链结构

通过上述工程实践证明，可信计算环境的构造方法是可行的。下一步，将继续在此模型下研究可信网络连接（TNC）等技术在此框架下的实现。

参　考　文　献

[1] R. Yahalom, B. Klein, and T. Beth. Trust relationships in secure systems – a distributed authentication perspective. In RSP: IEEE Computer Society Symposium on Research in Security and Privacy, pages 150 ~ 164, 1993

[2] T. Beth, M. Borcherding, B. Klein. Valuation of trust in open networks. In Proceedings of the European Symposium on Research in Computer Security, pages 3 ~ 18, Brighton, UK, Springer – Verlag. 1994

[3] Jameel H, Hung LX, Kalim U, Asjjad A, Lee SY, Lee YK. A trust model for ubiquitous systems based on vectors of trust values. In: Proc. of the 7th IEEE Int'l Symp. on Multimedia. Washington: IEEE Computer Society Press, 2005. 674679

[4] A. Josang. A subjective metric of authentication. In ESORICS: European Symposium on Research in Computer Security. LNCS, Springer – Verlag, 1998

[5] A. Josang, S. J. Knapskog. A metric for trusted systems. In: Global IT Security. Wien: Austrian Computer Society, pages 541 ~ 549, 1998

[6] G. Shafer. A Mathematical Theory of Evidence. Princeton University Press, 1976

[7] S. Weeks. Understanding Trust Management Systems, IEEE, 2001

[8] IBM PCI Cryptographic Coprocessor. http://www – 03. ibm. com/security/cryptocards/ pcicc/overview. shtml, 20070331

[9] IBM Coprocessor First to Earn Highest Security Validation. http://www – 03. ibm. com/ press/us/en/pressrelease/2347. wss, 20070331

[10] ARM, TrustZone Technology Overview. http://www. arm. com/products/esd/ trustzone_home. html, 20070331

[11] Tiago Alves, Don Felton. TrustZone: Integrated Hardware and Software Security Enabling Trusted Computing in Embedded Systems. July 2004. http://www. arm. com/pdfs/TZ%20Whitepaper. pdf, 20070331

[12] T. Halfhill. ARM Dons Armor: TrustZone Security Extensions Strengthen ARMv6 Architecture. Microprocessor

Report 8/25/03 ~ 01, August 2003

[13] David Lie, XOM. http://www - vlsi. stanford. edu/ ~ lie/xom. htm, 20070331

[14] David Lie, C. Thekkath, M. Mitchell et al. Architecture Support of Copy and Tamper Resistant Software. Proceedings of the 9th International Conference on Architecture Support for Programming Languages and Operating System - ASPLOS - IX, 2000: 168 ~ 177

[15] A. Carroll, M. Juarez, J. Polk, and T. Leininger. Microsoft Palladium: A business overview. http://www. microsoft. com/PressPass/features/2002/jul02/0724palladiumwp. asp, August 2002

[16] Microsoft, Microsoft Next - Generation Secure Computing Base: An Overview, http://www. microsoft. com/resource/ngscb/ngscb_overview. mspx, April 2003

[17] P. England, B. Lampson, J. Manferdelli, et al. A Trusted Open Platform. IEEE Computer, Vol. 36, No. 7, pages 55 ~ 62, 2003

[18] Bennet S. Yee. Using Secure Coprocessors. PhD thesis, Carnegie Mellon University, May 1994

[19] William. A. Arbaugh, D. J. Farber, and J. M. Smith. A Secure and Reliable Bootstrap Architecture. Proceedings of IEEE Computer Society Conference on Security and Privacy. IEEE, 1997: 65 ~ 71

[20] Reiner Sailer, Xiaolan Zhang, Trent Jaeger, Leendert van Doorn. Design and Implementation of a TCG - based Integrity Measurement Architecture. USENIX Security Symposium 2004: 223 ~ 238

[21] 沈昌祥，张焕国，冯登国，曹珍富，黄继武．信息安全综述．中国科学 E 辑：信息科学 2007 年第 37 卷第 2 期：1 ~ 22, 2007

[22] 张焕国，刘玉珍，余发江等．一种新型嵌入式安全模块．武汉大学学报（理学版）Vol. 50 No. S1, 2004: 007 ~ 011，第一届中国可信计算和信息安全学术会议（CTCIS'04），武汉，中国，2006. 10

[23] 余萍，马晓星，吕建，陶先平．一种面向动态软件体系结构的在线演化方法[J]．软件学报，2006, (06)

[24] 陈军．可信平台模块安全性分析与应用[D]．中国科学院研究生院(计算技术研究所). 2006

可信计算中基于属性的认证协议改进方案

赵一鸣　沈为君

复旦大学软件学院

摘　要　可信计算中认证协议是十分关键的，直接关系着可信平台的安全性和健壮性。一般认证协议完全依赖平台系统配置，应用范围较广，然而面对平台的软件和系统频繁升级时等情况，一般认证协议就会失效，而基于属性的认证协议能够解决这一问题。本文分析了基于属性的认证协议可能存在的攻击和安全隐患，给出了基于属性的认证协议改进方案，通过使用不可锻造零知识协议，提交协议和盲签名体制，使得协议具有较好的安全性，弥补了现有协议的不足。

关键词　零知识协议　可信计算　不可锻造性　基于属性的认证协议

1　引　言

认证协议中挑战者要求平台向其证明平台配置是可信的，平台和挑战者需要进行交互式认证协议，证明平台所具有的计算机配置是安全的。可信计算中认证协议包括一般认证协议和基于属性的认证协议。

一般认证协议指的就是遵循 TCG 标准的认证机制，使用平台配置 S_0 作为基础来判断平台是否可信。但是这样的协议存在以下不足：第一，如果挑战者（如数字内容提供者）想要强制实现对于一个平台（如消费者的平台）的访问控制规则，在实际情况下，很难验证每个平台配置的可信性；第二，一个诸如内容提供商和大型操作系统生产商相互勾结，可以根据其自身利益，排斥可信平台的配置信息；第三，一般认证协议的接收者或者是观察者可以从特定平台的配置中获取额外信息，而攻击者不需要很复杂的计算就能进行平台分析，使得对于平台的攻击更加容易；第四，一般的认证协议为了保证在系统升级和备份后，能够保证认证协议继续成功执行，需要把秘密信息包括内容、文档等都封装到系统配置里面去，这样秘密信息就不可访问；第五，TCG 硬件提供的封装机制将加密内容和特定系统绑定起来，系统升级或者安装补丁会改变 PCR 寄存器的值，使得加密内容不能再访问。为了解决一般认证协议中的上述缺陷，文献［1］在 2003 年提出了基于属性的认证协议。

基于属性的认证协议是基于平台提供的属性，它满足某一特定需求（如安全性的需求，平台是否有内在的机制去实现隐私访问规则）的行为抽象成一种属性 P。因此，具有

不同组件和不同配置的可信平台能够满足具体的属性。基于属性的认证协议的核心在于定义一个关于平台配置 S_0 和特定属性 P 的二元关系，来表示 S_0 满足属性 P。文献［1］中提出的若干基于属性的认证方案，存在明显的安全隐患，即签名者可以获得平台的配置信息，平台配置信息存在泄露的可能，为了把这种可能性降到最低，提高安全性和实用性，本文提出了一个基于属性的认证协议改进方案。

本文结构安排如下：第 1 节是引言；第 2 节描述了基于属性认证协议所要用到的预备知识；第 3 节分析了现有基于属性认证协议中存在的不足，提出了基于属性的认证协议改进思路和改进方案；第 4 节给出了对于改进方案的安全性和效率分析；最后在第 5 节对本文进行了总结和展望。

2 预备知识

Goldwasser，Micali 和 Rackoff 提出了零知识[2]概念，零知识协议[3]是交互式证明系统，满足完整性、完备性和零知识性。不可锻造零知识[4]是指如果攻击者能够使验证者接受证明，允许攻击者和任意数量证明者交互，存在一个知识抽取器，能够成功地将证据从攻击者处抽取出来。

可信计算规范中定义的 7 种密钥类型如下：

（1）签名密钥（Signing Key）：非对称密钥，用于应用数据和信息签名。

（2）存储密钥（SK - Storage Key）：非对称密钥，用于对数据或其他密钥进行加密。存储根密钥（SRK - Storage Root Key）是存储密钥的一个特例。

（3）平台身份认证密钥（AIK - Attestation Identity Key）：专用于对 TPM 产生的数据（如 TPM 功能、PCR 寄存器的值等）进行签名的不可迁移的密钥。可信计算中认证协议使用 AIK 密钥对，因此必须保证 AIK 密钥对的安全性。

（4）签署密钥（EK - Endorsement Key）：平台的不可迁移的解密密钥。在确立平台所有者时，用于解密所有者的授权数据和与产生 AIK 相关的数据。签署密钥从不用作数据加密和签名。签署密钥是可信计算的核心，必须保证其隐私性。

（5）绑定密钥（Binding Key）：用于加密小规模数据（如对称密钥），这些数据将在另一个 TPM 平台上进行解密。

（6）继承密钥：在 TPM 外部生成，在用于签名和加密的时候输入到 TPM 中，继承密钥是可以迁移的。

（7）验证密钥：用于保护引用 TPM 完成的传输会话的对称密钥。

TCG 定义了五类证书，每类都被用于为特定操作提供必要的信息。证书的种类包括：签署证书（Endorsement Credential），符合性证书（Conformance Credential），平台证书（Platform Credential），认证证书（Validation Credential），身份认证证书（Identity or AIK Credential）。

每个 TPM 会产生 RSA 密钥对成为签署密钥对（EK）和认证密钥对（AIK）。

签署公钥（EK - pub）[8]和签署私钥（EK - pri）[8]是可信平台的安全核心。认证公钥（AIK - pub）[8]和认证私钥（AIK - pri）[8]进行认证。可信第三方私钥（TTP - pri）[8]是其私有的，可信第三方公钥（TTP - pub）[8]是公开的。PCR（Platform Configuration Register）