

可信计算中远程自动匿名证明的研究

刘吉强¹⁾ 赵 佳¹⁾ 赵 勇^{1),2)}

¹⁾(北京交通大学计算机与信息技术学院 北京 100044)

²⁾(北京工业大学计算机学院 北京 100022)

摘 要 远程证明是可信计算的一个重要特征,目的是证明远程平台的身份或配置信息是否可信.常用的二进制证明方法不仅暴露了本地平台的配置信息,而且在现实情况中很难处理平台多样性问题.文中提出的可信计算中远程自动匿名证明方案利用环签名实现直接匿名证明,隐藏了平台的身份信息,以属性证书代替平台配置信息,可以有效防止私有信息的暴露,同时兼顾到对系统的升级和备份的可信评测.证明协议避免了使用零知识证明.分析结果显示,具有较高的实现效率.

关键词 可信计算;远程证明;自动协商;属性证书;环签名

中图法分类号 TP309

DOI号: 10.3724/SP.J.1016.2009.01304

Study of Remote Automated Anonymous Attestation in Trusted Computing

LIU Ji-Qiang¹⁾ ZHAO Jia¹⁾ ZHAO Yong^{1),2)}

¹⁾(School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044)

²⁾(College of Computer Science and Technology, Beijing University of Technology, Beijing 100022)

Abstract Remote attestation is an important attribute in trusted computing. The purpose of remote attestation is to attest the identity and configuration of remote platform. The shortcomings of popular binary attestation are not only revealing information about the configuration of platform or information, but also requiring the verifiers to know all possible “trusted” configurations of all platform as well as managing updates and patches that change the configuration. The remote automated anonymous attestation hides the identity of platform by ring signature, replaces configuration by property-based certificate, which takes good reference for updates and patches of system. The hidden certificate signed by trusted computing module and its host does not need extra zero-knowledge proof, so our scheme is very efficient in realization.

Keywords trusted computing; remote attestation; automated negotiation; property certificate; ring signature

1 引 言

可信计算技术为拥有新的安全体系结构的新一代计算平台提供了基础.可信计算技术的发起者和

主要推动者是可信计算组织(Trusted Computing Group, TCG),TCG继承了其前身可信计算平台联盟的若干规范,目标是为计算平台提供“可信”的保障.在可信计算包含的多个方面的内容中,平台之间的远程证明(remote attestation)是其中的一个重要

基本特征^[1],也是网络环境中终端相互信任的保证.在TCG规范中,通过检测远程计算平台的完整性实现证明从而取得信任.但这种证明的一个明显的不足之处是暴露了平台(包括硬件和软件)的配置信息,侵犯了终端平台的隐私性(privacy),这在隐私性保护日益受到关注的今天,无疑是影响了可信计算的发展.TCG规范中专门提出了隐私性的考虑^[1],并引入了平台身份别名——身份验证密钥(Attestation Identity Keys, AIK)来保护可信平台模块的签名密钥从而隐藏平台的身份信息,但未考虑平台状态配置信息的隐私性保护问题.近几年来,远程证明中的隐私性保护问题受到了多方的关注,如何在有效地实施远程证明的同时,保护计算平台的隐私信息不仅在理论上也在实际应用上都具有非常重要的意义.

本文提出的可信计算远程自动匿名证明(Remote Automated Anonymous Attestation, RAAA)方案的主要贡献在于:以属性证书代替平台配置信息,不仅可以有效防止隐私性的暴露,而且为系统升级和备份过程的可信检测提供了很好的思路;利用环签名实现直接匿名证明,避免了可信计算平台与可信第三方的协商过程,在提高执行效率的同时,也增强了安全性;基于可信计算模块及其宿主的联合签署的隐藏属性证书实现远程自动匿名证明,不需要额外的零知识证明,实现效率较高.

2 相关工作

在TCG设计规范中,证明(attestation)分为多种形式,针对平台的证明(to the platform)是其中的一种.一个平台可以通过提供与平台相关的证书如签名证书(endorsement credential)来证明平台可以被信任做出完整性度量报告.签名证书可以提供平台嵌入有合法的可信平台模块(Trusted Platform Module, TPM)的证据.但由于TPM往往和宿主平台有绑定关系,通过直接提供签名证书完成这种证明显然会泄露平台的身份信息.TCG在公布的版本1.1中使用了可信第三方(私有CA)辅助进行身份认证从而避免平台身份信息的泄露^[2]——每一个TPM拥有私有CA颁发的一个RSA密钥对,即签名密钥(Endorsement Key, EK),在TPM需要证明自己的身份时,并不直接使用EK进行签名,TPM生成另外一对RSA密钥对,即身份验证密钥(Attestation Identity Key, AIK)来完成签名,并通

过和私有CA交互确认AIK的正确性来完成身份的证明.该方案仍然存在缺点,即私有CA需要参与到每次会话中,因此需要CA始终在线.与常用的离线CA相比,一方面需要高度的可用性保障,另一方面也为CA本身的安全需求提出了更高的要求.2004年,Brickell等提出一项名为“直接匿名证明(Direct Anonymous Attestation, DAA)”的策略^[3],直接匿名证明的理论基础来自于Goldwasser等人提出的“零知识证明(Zero Knowledge Proof)”^[4],结合Chaum首先提出的群签名(group signature)等技术,使得验证者可以确认通信对方是真正的TPM宿主(host),但又不暴露对方的真实身份信息.DAA已成为TCG规范(版本1.2)的一部分^[5].尽管如此,由于DAA中运用了多次零知识证明,在实际实现上复杂度仍然较大,不具备可行性.

除了上述针对平台的证明之外,证明还包括另一种方式,即对平台环境状态的配置信息的证明,称为对平台的证明(attestation of the platform).可信平台模块TPM运用身份验证密钥AIK对受保护的配置寄存器(Platform Configuration Register, PCR)内存储的有关平台环境状态配置信息的度量值进行数字签名,平台转发该数字签名给远程请求者来提供平台完整性的度量(如图1所示^[1]).

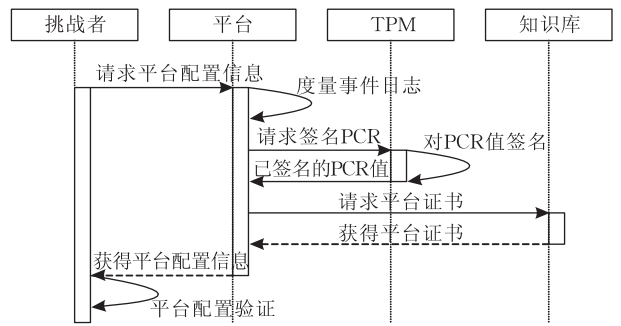


图1 证明协议

由于PCR中所存储的度量值是利用散列函数获得的二进制摘要值,因此TCG提供的这种对平台证明的方式也称为二进制证明(binary attestation).这种二进制证明方法仍然有很多缺点,一个明显的不足之处是暴露了本地平台(包括硬件和软件)的配置信息,这在一定程度上给攻击者提供了方便,使之更容易遭受各种攻击.另一个缺点是可能的平台状态信息的多样性问题,考虑到系统更新和备份问题,这在实际的分布式应用中很难实现.除了上述常用的二进制证明之外,Haldar等人提出语义远

程证明的方法,其基本思想是使用基于语言的可信虚拟机,通过检测运行于虚拟机上的代码的安全策略实现证明,但其可信虚拟机仍然需要二进制证明^[6]. Sadeghi 等提出的基于属性的证明(Property-Based Attestation,PBA)是一种更加有效且灵活的远程证明解决方案^[7]. 这里的属性是针对特定需要的平台行为的表现,每种属性可以对应多种平台配置信息,验证者只能获知被验证平台具有某种属性而不能知道具体的配置信息,从而避免了平台具体配置信息的直接暴露. 在此基础上 Chen 等人提出了一个基于属性证书的证明协议^[8]、属性,其对应的配置信息对应一个属性配置证书(Property-Configuration Certificates),由一个可信的第三方 CA 负责管理和发布,通过一系列复杂的交互协议达到匿名证明的目的. 这种证明协议仍然使用大量的零知识证明隐藏真实的配置信息,实现属性的证明,实现复杂度较高. 不仅如此,该方案中默认的可信第三方必须熟知所有的平台状态信息并对其进行签名,这实际上是把二进制证明中验证者的部分验证工作转移给了可信第三方,仍然没有从根本上解决平台状态信息的多样性问题.

与本文研究内容密切相关的还有自动信任协商(Automated Trust Negotiation,ATN)技术. 事实上有关 TPM 的直接匿名证明以及有关平台配置信息的证明从本质上讲都是网络环境中双方终端平台信任关系的确立问题. 证明的目的就是为了满足通信对方的需求条件,取得对方的信任. 自动信任协商(ATN)是由 IBM 的 Winsborough 等人于 2000 年首先提出^[9],目的是解决在开放的分布式网络中信任关系的自动建立问题. 自动信任协商(ATN)同样使用了基于属性的数字证书(property-based digital credentials)来模拟现实生活中的纸制证明文件^[10]. 每个属性证书都包含了证书所有者的一项或多项属性,证书发布者并不要求统一,因此并不需要一个统一的可信第三方. 在 ATN 中通过协商策略(negotiation strategy)的控制,对属性证书、访问控制策略(access control policies)进行交互披露,资源的请求方和提供方自动地建立信任关系(如图 2 所示),从而保证了敏感资源的受控访问.

有关 ATN 的研究工作仍在不断发展之中,Holt 等人^[11-12]借鉴基于身份密码系统思想,提出了隐证书(Hidden Credential)的概念,资源提供者可以任意选择解密消息的对象来保护敏感的属性、证书和资源等. Li 等人也利用数字签名、比特承诺以

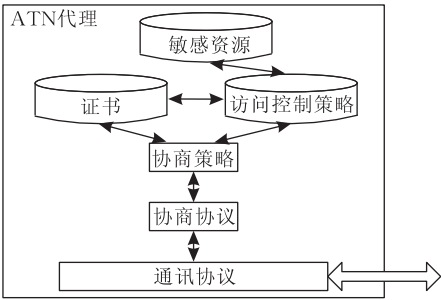


图 2 ATN 工作原理

及零知识证明等现代密码学的工具和方法提出不经意属性证书(oblivious attribute certificate)来保护敏感属性(sensitive attributes)^[13-17]. 隐证书和不经意属性证书方案都可以使资源访问者在满足了协商对方的访问控制策略时,不需要揭露自己的真实属性就可以正常访问对方资源信息,在一定程度上解决了双方循环依赖的问题. 但两者仍有一个共同的缺点是无法防止证书转移的问题,也就是说合法的证书拥有者可以把证书转移给任何第三者而资源提供者无从知晓.

3 远程自动匿名证明方案(RAAA)

网络通信中的远程证明应该首先从对方是否嵌入有 TPM 模块开始. TCG 体系中的 DAA 方案以 CL 数字签名(Camenisch and Lysyanskaya signature scheme)为基础,结合了群签名以及零知识证明等技术来完成 TPM 模块的直接匿名证明. 所采用的算法需要大量的幂运算,实现效率较低,可行性较差. 近几年发展起来的环签名方案^[18]可以由签名者自主选择环的成员,使得签名者的身份很好地隐藏在所选择的环的成员之中,并且不需要群签名中的管理者. 环签名方案在很好地符合了直接匿名证明要求的同时,由于不需要多余的零知识证明,实现效率较高. 但由于 TPM 计算能力的限制,有效地完

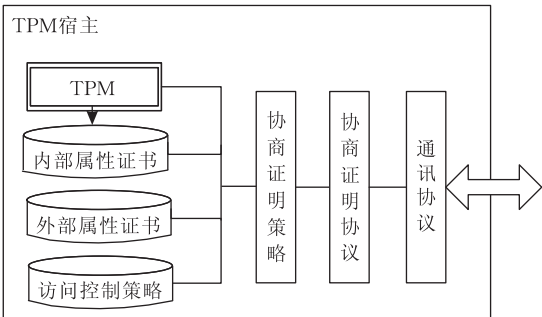


图 3 基于 TPM 和属性证书的自动协商证明

成完整的直接匿名证明需要 TPM 宿主的参与辅助,因此必须根据 TPM 的特性修改常规的环签名方案使得 TPM 宿主和 TPM 可以联合生成签名但又不暴露私有性. 基于 TPM 的自动协商证明工作原理如图 3 所示.

3.1 TPM 签名

采用环签名方案实现远程证明将在保持匿名性的前提下提高证明的实现效率. 本节遵循当前 TPM 的设计规范^[4], 并使用文献[18]中的环签名方案.

设 f, g 分别是加密解密函数, 即对于明文消息 m 和密文消息 c , $c = f(m)$, $m = g(c)$. 按照 TPM 的设计规范^[4], 每个 TPM 拥有一个 RSA 密钥对 EK , 当 TPM 宿主需要向验证者证明自己是合法的 TPM 拥有者时, TPM 宿主选择 $t-1$ 个其它的 TPM 与自身嵌入的 TPM 形成环(实际上只需要其他 TPM 的公钥信息, 可以通过 TPM 的公钥证书获得), 把自己的身份隐藏在环中, 设环中成员 TPM 的公钥分别为 P_1, P_2, \dots, P_t (其中包含自身拥有的 TPM, 设其序号为 s), 选择待签名信息 m , TPM 及其宿主联合生成环签名 $TPMSign(m) = (P_1, P_2, \dots, P_t; v; x_1, x_2, \dots, x_t)$. 其中非关键数据的生成和计算, 如散列函数值 $k = H(m, P_1, P_2, \dots, P_t)$ 、初始值 v 和随机数序列 $x_1, \dots, x_{s-1}, x_{s+1}, \dots, x_t$ 以及 $y_i = f(x_i)$, $i \neq s$ 可以由 TPM 宿主完成, $x_s = g(y_s)$ 必须由 TPM 完成, 环方程 $C_{k,v}(y_1, y_2, \dots, y_t) = v$ 沿用文献[18]中的环方程. 验证签名的阶段和环签名一致, 验证者只能验证该签名是由环中某成员生成的, 但无法知道具体的签名者身份. 很显然, 上述匿名证明的计算复杂度直接与所选择的环的大小有关, TPM 宿主可以根据自己的隐私性保护需求, 自主地选择隐藏身份的环的大小以及成员组成.

3.2 属性证书

针对现有的二进制证明方法暴露了平台具体配置信息的问题, 本文采用类似于自动信任协商中的属性证书的技术, 把多种平台配置具有的共同属性准确地抽象成属性证书. 一种属性 P 对应多种平台配置信息 $C_i^{(P)}$, $i \in I$. 例如, 是否支持应用隔离、是否具有病毒防护能力、病毒库是否最新等等都可以作为一种属性, 而且, 即使是不同生产厂商, 只要其产品能够提供上述属性, 其配置就是合理的. 我们根据属性证书的签发者不同, 将属性证书分为两类, 即内部属性证书和外部属性证书.

定义 1. 由可信第三方(trusted third party)签发的证书称为外部属性证书(outer property

certificate).

定义 1 中的可信第三方并不限定于一个特定的第三方, 外部属性证书的目的在于说明某种(可以是多种)特定的平台配置信息具有某种属性. 证书的签发者可以是相关平台软硬件的生产商, 例如杀毒软件的病毒库版本的更新日期可以由防毒软件生产厂商签发, 而是否安装了杀毒软件可以由权威认证部门认证的多种防毒软件为标准, 并以该部门签发的证书为依据等等.

由于平台和应用多种多样, 平台/应用的配置信息复杂多变, 并且应用之间的关系错综复杂, 以现有的二进制证明方法来确定配置信息存在很多不足之处. 即使采用基于属性的远程证明方法, 外部属性抽象也是一件很困难的任务, 平台/应用的可信性相互依赖, 一个应用的运行状态可能被另一个应用的状态所影响, 因此为了证明某一应用的当前配置是否满足某种属性, 必须同时证明平台上的其它应用是否可信, 这在实际操作中很难实行. 实际上, 系统中的任何应用一般都可以独立完成, 除了必需的输入外, 并不需要来自其它应用的信息流. 属性抽象以应用间的隔离为基础, 消除上述应用间“牵一发而动全身”的依赖关系, 使之更有利于可信度量.

定义 2. 由 TPM 和 TPM 宿主联合签发的证书称为内部属性证书(inner property certificate).

内部属性证书的目的在于说明当前平台具有某种属性. TPM 的签名用来保证平台配置的真实性, 因此在签发内部属性证书时, TPM 的参与必不可少. 内部属性证书涉及到 TPM 的签名以及平台的配置信息, 所以隐私性保护是最重要的一个问题. 假设属性值 P 对应多种平台配置 C_1, C_2, \dots, C_t , 有关配置信息 C_r ($1 \leq r \leq t$) 的内部属性证书采用由 TPM 签发的隐证书的方式. 考虑到 TPM 的现有结构, 采用如下形式的隐证书结构方案: TPM A 选择一个 RSA 加密算法的模数 n_A 和公私钥对 (e_A, d_A) 、私有信息 x_A 以及 $\mathbf{Z}_{n_A}^*$ 中的高阶元 g_A . TPM 提取存放于对应 PCR 中的配置信息摘要值 C_r ($1 \leq r \leq t$), 联合 TPM 宿主计算属性隐藏值 $y_A = (g_A^{x_A} - H(P, C_1, C_2, \dots, C_t))^{d_A} \bmod n_A$, 并对公共参数 n_A 和 g_A 、公钥 e_A 以及属性隐藏值 y_A 签名得到 $TPMSign(n_A, g_A, e_A, y_A)$. 属性 P 对应的内部属性证书中包括公共参数 n_A 和 g_A 、公钥 e_A 、属性值 P 、属性隐藏值 $y_A = (g_A^{x_A} - H(P, C_1, C_2, \dots, C_t))^{d_A} \bmod n_A$ 以及 TPM 的签名.

3.3 基于 TPM 及属性证书的远程自动协商证明

TCG 设计规范中对平台的证明,一般是由挑战者发起对平台配置信息的请求,并在获得相应配置信息以及签名之后验证是否符合要求.事实上,从安全的角度出发,平台不应该对任何挑战都去响应并提供自身的配置信息,从验证目的考虑,可分为如下两种情形:推(Push)式证明和拉(Pull)式证明.

定义 3. 平台 A 为了向平台 B 发送信息,保证所发送的信息不含有危害性的代码,主动向对方证明自己身份的方式称为推式证明方式.

定义 4. 平台 A 希望访问平台 B 的资源 R,需要提供相应的身份证明使之符合对方的访问控制策略的方式称为拉式证明方式.

针对这两种情形,结合自动信任协商中现有的协商策略和协商协议,我们采用两种方案来实现远程自动协商证明协议.这两种方案在证书签发和签名阶段完全相同,但是在交互验证阶段有所不同,因为在拉式证明中还需要平台 B 将平台 A 请求的资源 R 加密后发送给平台 A.

3.3.1 参数初始化阶段

设平台 A、B 是要进行远程自动协商证明的双方.外部属性证书中属性 P 对应多种平台配置 C_1, C_2, \dots, C_t .

TPM A 基于 RSA 密码算法,选择两个互异的大素数 p_A, q_A , $n_A = p_A q_A$, e_A 与 $(p_A - 1)(q_A - 1)$ 互素,且 $e_A d_A = 1 \bmod (p_A - 1)(q_A - 1)$,公共参数 g_A 为 $\mathbf{Z}_{n_A}^*$ 中的高阶元.公钥分别为 (e_A, n_A) 和 (d_A, n_A) ; $H()$, $H_1()$ 为两个抗碰撞的散列函数.

3.3.2 签名阶段

TPM A 随机选择一个私有信息 x_A ,提取存放于对应 PCR 中的配置信息摘要值 $C_r (1 \leq r \leq t)$,联合 TPM 宿主计算属性隐藏值 $y_A = (g_A^{x_A} - H(P, C_1, C_2, \dots, C_t))^{d_A} \bmod n_A$.此时,TPM A 要签名的信息为 $m = (n_A, g_A, e_A, y_A)$.

设签名环由 t 个 TPM 组成,对应公钥分别是 P_1, P_2, \dots, P_t (包括自身 TPM,设序号为 s).TPM A 宿主计算散列值 $k = H(m, P_1, P_2, \dots, P_t)$,随机选择初始值 v 和随机数序列 $x_1, \dots, x_{s-1}, x_{s+1}, \dots, x_t$,计算出 $y_i = f(x_i), i \neq s$.

TPM A 选择环方程如式(1)所示:

$$C_{k,v}(y_1, y_2, \dots, y_t) = E_k(y_t \oplus E_k(y_{t-1} \oplus E_k(\dots \oplus E_k(y_1 \oplus v) \dots))) = v \tag{1}$$

其中, $E_k()$ 为对称加密算法(可采用 TPM 规范中推

荐的候选对称加密算法 AES^[4]), $k = H(m, P_1, P_2, \dots, P_t)$ 为对称加密算法的密钥, \oplus 为逐比特异或运算. TPM A 根据环方程(1)计算出

$y_s = E_k(y_{s-1} \oplus E_k(y_{s-2} \oplus E_k(\dots \oplus E_k(y_1 \oplus v) \dots))) \oplus D_k(y_{s+1} \oplus D_k(y_{s+2} \oplus D_k(\dots \oplus D_k(y_t \oplus D_k(v)) \dots)))$, 其中, $D_k()$ 为相应的对称解密算法,然后再利用私有密钥计算出 $x_s = g(y_s)$.

此时 TPM A 联合其宿主主机完成了签名,并将信息 $m = (n_A, g_A, e_A, y_A)$ 和签名 $TPMSign(n_A, g_A, e_A, y_A)$ 发送给平台 B.

3.3.3 交互验证阶段

推式证明中,平台 B 在收到平台 A 发送的消息及 TPM 签发的属性证书后,首先验证签名是否合法,若不合法则丢弃收到的消息,反之则随机选择私有信息 x_B ,计算 $k_1 = H_1((y_A^{e_A} + H(P, C_1, C_2, \dots, C_t))^{x_B})$ 并发送 $g_A^{x_B}$ 给平台 A. TPM A 与宿主主机合作计算并返还 $k_2 = H_1((g_A^{x_B})^{x_A})$ 给对方,平台 B 通过验证 $k_1 = k_2$ 来确定对方是否具有属性 P.

拉式证明更接近于自动信任协商下的不经意属性证书方案.平台 B 在收到平台 A 发送的由 TPM 签发的隐藏属性证书后,仍然首先验证签名是否合法,然后在签名合法时再随机选择私有信息 x_B ,计算 $k_1 = H_1((y_A^{e_A} + H(P, C_1, C_2, \dots, C_t))^{x_B})$,并发送 $g_A^{x_B}$ 以及用密钥 k_1 加密的资源 R 给平台 A, TPM 与宿主平台联合计算 $k_2 = H_1((g_A^{x_B})^{x_A})$,并利用 k_2 解密获得资源 R.

4 安全性分析

RAAA 方案中的 TPM 签名即是文献[18]中基于 RSA 的环签名,因此其安全性等同于基于 RSA 的环签名方案,同时也具有了环签名的特性:(1) 无需管理中心来生成签名,无需其他成员合作;(2) 验证签名者不能分辨出环成员中哪一位代表成员签名,但确信是环中某一位成员签名;(3) 签名者可以在未经其他成员同意下代表他所属的任意环签名;(4) 每一位环成员在签名时可以使用不同的算法.由于以上环签名的特点,因而很好地隐藏了平台身份;(5) 签名不可伪造.

在远程匿名证明中,外部属性证书中的属性 P 对应多种平台配置 C_1, C_2, \dots, C_t ,从而平台的真实属性 C_r 被很好地掩盖在属性值 P 中,验证方只能获

得属性值 P 而无法判断出该 TPM A 的具体平台配置是哪一种,所以平台配置信息也被隐藏了起来.同时是由 TPM 提取存放于对应 PCR 中的配置信息摘要值 $C_r(1 \leq r \leq t)$,并由 TPM 随机选择一个私有信息 x_A 、计算属性隐藏值 $y_A = (g_A^{x_A} - H(P, C_1, C_2, \dots, C_t))^{d_A} \bmod n_A$ 以及签名最终值,因此平台无法绕开 TPM 生成伪造的平台配置值.

5 效率分析

在 RAAA 方案中,主要用到的计算有指数(Exponential)运算、散列(Hash)运算和对称密钥加密(Symmetrical Encryption)运算.我们用 E 代表指数运算, H 代表散列运算, SC 代表对称加密运算对算法效率进行分析(见表 1).

表 1 RAAA 效率分析

阶段名称		计算方	运算次数		
			E	H	SC
签名阶段		A	$t+2$	2	t
交互验证	推式证明	B	3	2	
		A	1	1	
	拉式证明	B	3	2	1
		A	1	1	1

表 1 中可以看到在 RAAA 中的以上 3 种运算的次数除变量 t 外均为常数项,而 t 的大小与 TPM A 选择的环的大小有关,所以在选择的环大小合适的情况下,RAAA 具有较高的效率.

6 结 论

本文提出的可信计算远程自动匿名证明方案以属性证书代替平台配置信息有效防止隐私性的暴露,满足了系统升级和备份过程的可信检测要求;基于可信计算模块及其宿主的联合签署的隐藏属性证书和环签名实现远程直接匿名证明,无需私有 CA 的参与,不仅利用环签名的特点隐藏了平台身份,而且隐证书能够隐藏平台配置,在提高执行效率的同时,也增强了安全性.然而如何描述平台属性值,如何准确抽象出外部属性证书仍然是我们今后面临的具有挑战性的问题.

参 考 文 献

[1] Trusted Computing Group. TCG specification architecture overview, Specification 1.4, 2007

[2] Trusted Computing Group. Trusted computing platform alliance (TCPA) main specification, Version 1.1a. Republished as Trusted Computing Group (TCG) main specification, Version 1.1b, 2001

[3] Goldwasser S, Micali S, Racko C. The knowledge complexity of interactive proofs. SIAM Journal on Computing, 1989, 18(1): 186-208

[4] Trusted Computing Group. TPM main specification, main specification Version 1.2 revision 94, 2006

[5] Brickell E, Camenisch J, Chen L. Direct anonymous attestation//Proceedings of the 11th ACM Conference on Computer and Communications Security. Washington, DC, USA, 2004: 132-145

[6] Haldar V, Chandra D, Franz M. Semantic remote attestation: A virtual machine directed approach to trusted computing. School of Information and Computer Science, University of California, California: Technical Report No.03-20, 2003

[7] Sadeghi A, Stubble C. Property-based attestation for computing platforms: Caring about properties, not mechanisms//Proceedings of the 2004 New Security Paradigms Workshop. Virginia Beach, VA, USA, 2004: 67-77

[8] Chen L, Landfermann R, Lohr H, Rohe M, Sadeghi A, Stubble C. A protocol for property-based attestation//Proceedings of the 1st ACM Workshop on Scalable Trusted Computing (STC'06). Alexandria, Virginia, USA, 2006: 7-16

[9] Winsborough W H, Seamons K, Jones V. Automated trust negotiation//Proceedings of the DARPA Information survivability Conference and Exposition. SC, USA, 2000, Volume 1: 88-102

[10] Bina E, Jones V, McCool R, Winslett M. Secure access to data over the internet//Proceedings of the 3rd International Conference on Parallel and Distributed Information Systems. Austin, Texas, USA, 1994: 99-112

[11] Holt J, Bradshaw R, Seamons K, Orman H. Hidden credentials//Proceedings of the 2003 ACM Workshop on Privacy in the Electronic Society. Washington DC, 2008: 1-8

[12] Bradshaw R, Holt J, Seamons K. Concealing complex policies with hidden credentials//Proceedings of the 11th ACM Conference on Computer and Communications Security. Washington, DC, USA, 2004: 146-157

[13] Winsborough W H, Li N. Protecting sensitive attributes in automated trust negotiation//Proceedings of the ACM Workshop on Privacy in the Electronic Society. Washington, DC, USA, 2002: 41-51

[14] Li J, Li N, Winsborough W H. Automated trust negotiation using cryptographic credentials//Proceedings of the 12th ACM Conference on Computer and Communications Security. Alexandria, Virginia, USA, 2005: 46-57

[15] Li N, Du W, Boneh D. Oblivious signature-based envelope//Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing (PODC). Boston, Massachusetts, 2003: 182-189

[16] Li J, Li N. OACerts: Oblivious attribute certificates. Dependable and Secure Computing, 2006, 4(3): 340-352

[17] Li J, Li N. Policy-hiding access control in open environment//Proceedings of the 24th Annual ACM Symposium on Principles of Distributed Computing (PODC). Las Vegas,

NV, USA, 2005: 29-38

[18] Rivest R L, Shamir A, Tauman Y. How to leak a secret//Advances in Cryptology-Asiacrypt 2001. LNCS 2248. Berlin: Springer, 2001: 552-565



LIU Ji-Qiang, born in 1973, Ph.D., associate professor. His research interests include trusted computing, applied cryptography, security protocol etc.

ZHAO Jia, born in 1980, Ph.D., lecturer. Her research interest is trusted computing.

ZHAO Yong, born in 1980, Ph.D., lecturer. His research interest is trusted computing.

Background

This work is supported by the National High Technology Research and Development Program (863 Program) of China (grant No. 2007AA01Z177 and No. 2007AA01Z410), the National Basic Research Program (973 Program) of China (grant No. 2007CB307101), and also supported by Program for Changjiang Scholars and Innovative Research Team in University (No. IRT0707).

The projects are involved in the key technology of trusted chain. Remote attestation is one of the fundamental trusted platform features. A terminal platform can attest to its description of characteristics to a remote party to guarantee the trustworthiness and freshness. TCG developed a solution using a trusted third party (Privacy CA), and then gave another solution which calls Direct Anonymous Attestation

(DAA) to avoid of revealing the private information, but various of exponential operations in the DAA protocol make it not efficient enough. Moreover, it also needs negotiations between the issuer of the TPM and the platform in the join stage of DAA. The authors proposes a remote automated anonymous attestation protocol based on ring signature in this paper. The remote automated anonymous attestation hides the identity of platform, replaces configuration by property-based certificate, which takes good reference for updates and patches of system. Furthermore, the attestation protocol does not need the third party and extra zero-knowledge proof, which makes it very efficient in realization. This new protocol will present a useful method for the remote attestation.