第 35 卷 第 6 期 计 算 机 工 程 2009 年 3 月
Vol.35 No.6 Computer Engineering March 2009
·安全技术· 文章编号：1000—3428(2009)06—0186—02 文献标识码：A 中图分类号：TP309.2

一种新的可信计算平台匿名认证方案

王尚平，丁如意，张亚玲，王晓峰，解康乐
(西安理工大学理学院数学系，西安 710054)

摘 要：研究可信计算平台的匿名认证方案，分析现有方案的优缺点，利用零知识证明思想，提出一个新的可信计算平台的匿名认证方案。新方案中 TPM 平台向验证者匿名认证其真实合法性，无需可信第三方的参与。与其他方案相比，该方案的认证效率更高，且在强 RSA 假设和判定性 Diffie-Hellman 假设及随机预言模型下满足不可伪造性、匿名性和撤销性。

关键词：隐私；不可伪造性；可信计算平台

New Anonymous Authentication Scheme for Trusted Computing Platform

WANG Shang-ping, DING Ru-yi, ZHANG Ya-ling, WANG Xiao-feng, XIE Kang-le
(Department of Mathematics, Faculty of Sciences, Xi'an University of Technology, Xi'an 710054)

【Abstract】 The anonymous authentication schemes for Trusted Computing Platform(TCP) is studied in this paper, the advantages and disadvantages of the subsistent authentication schemes for TCP are analyzed. A new anonymous authentication scheme for TCP is proposed by using the method of zero-knowledge proof. The validity of a TPM platform is proved anonymously, and there is no trusted third party to participate in the authentication schemes. The new scheme has higher efficiency than others and satisfies forgery-resistance, anonymity and revocation under strong RSA assumption and Diffie-Hellman assumption in the random model.

【Key words】 privacy; forgery-resistance; Trusted Computing Platform(TCP)

1 概述

随着计算机科学技术的迅猛发展，社会已经进入以数字化、网络化、信息化为特征的信息时代，信息安全成为人们关注的焦点。据统计，绝大多数的信息安全事件都是由于计算机体系结构存在安全隐患和操作系统不安全所引起的。传统的防火墙、入侵检测和病毒防范只能在系统外部被动地抵抗攻击，并不能在根本上解决系统的安全问题。因此，只有从信息系统的软硬件底层采取安全措施，才能有效确保整个信息系统的安全。

可信计算技术由此应运而生，在 30 多年的研究过程中，可信计算的含义不断地拓展，由侧重于硬件的可靠性、可用性到针对硬件平台、软件系统、服务的综合可信，适应了 Internet 应用不断拓展的发展需要。可信计算平台(Trusted Computing Platform, TPM)是能够提供可信计算服务的计算机软硬件实体。它与密码学芯片整合在一起，以密码技术为支持，以安全操作系统为核心，提供系统的可靠性、可用性和信息安全性，实现了许多和 TPM 的特点有关的安全，如安全导入、封装式的存储、软件完整性证实、更安全的在线业务活动和在线电子交易等。

2 研究现状

2.1 问题的提出

TPM 的设计和生产方式很特殊，所有其他的远程服务器都相信来自这个 TPM 的一些密码学计算结果。TPM 的配置涉及到核心数据(用户隐私)的保密问题。在一次事务处理过程中，TPM 的用户与一个验证者交互，验证者想要确信用户确实使用了包含一个可信任硬件模块的平台，即验证者想要认证用户的 TPM。但是，用户要保护他的隐私，因此，就要求验证者只能知道他使用了一个 TPM，但不知道具体是哪一个，即 TPM 须在不暴露其真实身份的情况下向验证者证明其合法性，这就是匿名认证的思想。

2.2 相关方案

2001 年，TCG 采用了基于可信第三方 PrivCA 的匿名认证方案[1]。方案涉及 3 个实体：PrivCA, TPM，验证者(Verifier)。方案的认证思想是：每个 TPM 都生成一个 RSA 密钥对 EK。PrivCA 知道所有合法 TPM 的 EK 的公钥。当一个 TPM 需要向一个验证者证明自己的合法性时，再生成一个 RSA 密钥对 AIK，将 AIK 的公钥和 EK 的公钥给 PrivCA。PrivCA 将检查在其 EK 列表中是否能找到该 EK，如果找到了，就对该 AIK 签发一个证书并用 EK 加密，只有拥有该 EK 私钥的 TPM 才能解密该证书。TPM 通过证书向验证者证明自己。该方案有 2 种方法检测无效 TPM：

(1)如果 EK 私钥被泄露，PrivCA 可以计算出对应的公钥，将其从有效 EK 列表中删除；

(2)如果 PrivCA 收到过多使用同一个 EK 的请求，拒绝这些请求。

基金项目：国家自然科学基金资助项目(60873268)；教育部科学技术研究基金资助重点项目(208139)；陕西省自然科学基础研究计划基金资助项目(2006F37)

作者简介：王尚平(1963－)，男，博士，主研方向：密码理论；丁如意，硕士；张亚玲、王晓峰，博士；解康乐，硕士

收稿日期：2008-08-24 **E-mail：**spwang@mail.xaut.edu.cn

然而，该方法具有一个显而易见的缺点，PrivCA 需要参与到每一个事务中，成为一个瓶颈。如果 PrivCA 和验证者串通，或 PrivCA 的事务记录通过其他方式泄露给了验证者，验证者仍旧能够识别出是哪一个 TPM，很明显，这并不是一个令人满意的解决方法。

TCG 公布了 TPM v1.2，直接采纳了 Brickell 等人提出的直接匿名认证方案[2]。该方案吸取了群签名、身份托管和证书系统的技术精髓。方案中的 TPM 在 PrivCA 的帮助下直接向远程的服务器证实它的真实性。方案涉及 4 个实体：证书签发者(Issuer)，TPM，TPM 所在的主机平台(HOST)，验证者。2 个协议为加入协议(Join)和签名协议(Sign)。Join 协议是签发者和(TPM, HOST)对之间交互的协议。协议中 TPM 创建一个 DAA 秘密密钥 privDK，使用 EK 向签发者标识自己。如果 Join 过程成功，Issuer 将向 TPM 和 HOST 签发 DAA 证书 certDK。Sign 协议是验证者和(TPM, HOST)对之间交互的协议，在协议中，TPM 创建一个 AIK，使用 privDK 和 certDK 对该 AIK 的公钥签名，并向 Verifier 证明其合法性。Verifier 可使用 IKEY 来核验签名是否合法。如果验证通过，则向 TPM 提供服务。方案也有 2 种方法检测无效 TPM：(1)对于所有已知的源于无效 TPM 的 f，通过比较 N_V 和 ζ^f；(2)是否已经看到同一个 N_V 太多次。

该方案解决了上一方案中的瓶颈问题，但在隐私保护上显得较为薄弱。因为验证者拥有基于 N_V 做分析的机会。

文献[3]提出一个用于可信计算平台 TPM 的简单高效匿名认证方案。该方案在制造商生产 TPM 时直接注入 2 组密钥，一组是标识 TPM 合法身份的唯一的识别码(EK)，另一组专门用来做匿名验证(AAK)，它类似于 EK，在生产过程中产生。生产商和所有的 TPM 构成一个群。生产商控制群主管密钥，TPM 控制它们的匿名认证密钥。方案涉及 3 个实体：制造商(Manufacturer(群主管))，TPM，验证者。2 个协议为加入协议 Join 和签名协议 Sign。Join 协议是制造商和 TPM 对之间交互的协议，负责 TPM 作为群成员的加入。Sign 协议是验证者和 TPM 对之间交互的协议。TPM 利用一定区间上的知识签名、区间上的离散对数知识、不同基下 2 个离散对数相等的知识和 2 个离散对数互素的知识，向验证者匿名认证了其真实合法性。该方案不仅实现了直接匿名认证，无需 PrivCA 的参与，而且可以有效地鉴别无效 TPM，但认证效率仍有进一步提升的空间。

本文通过结合文献[4]中的一般化零知识证明思想，提出一个更加完善的匿名认证方案。该方案不仅优化了匿名认证密钥生成算法，提高了认证效率，而且在随机域模型下是安全的。

3 匿名认证方案

匿名认证的主要思想是：通过一定区间上的零知识证明，证明 T_2 在基 T_1 下的离散对数 s 在特定的区间，且 (E,s) 是一个有效的密钥对。

3.1 系统参数

管理员生成系统参数 $(n,p,q,p',q',g,\alpha,l,l_c,X)$，其中，$n$ 是一个安全的 RSA 模数，$n=pq$；$p=2p'+1$；$q=2q'+1$；p,q,p',q' 都是大素数；QR_n 是模 n 下的二次剩余群；g 是 QR_n 的一个生成元；α,l,l_c 是大于 1 的安全参数；X 是一个常量，且 $X>2^{\alpha(l+l_c)+1}$；n, g 是公共参数；p,q,p',q' 由管理员秘密保存。

3.2 匿名认证密钥(AAK)的生成

AAK 的生成是在 TPM 的生产过程中完成的，该过程可视为 TPM 作为群成员加入群签名组，该群的签名不具备匿名撤销性。

管理员将 $p'q'$ 通过安全信道传给 TPM 中的一个安全部件(Secure Unit, SU)。SU 负责生成 AAK 和计算匿名认证所需信息，且外界无法干涉其计算和获得内部信息(包括 TPM)。

SU 选择的一个随机素数 $s\in\left[X-2^l,X+2^l\right]$，计算

$$E=g^{s^{-1}}(\bmod n)$$

其中，s^{-1} 是 s 在模 $|QR_n|=p'q'$ 下的逆；SU 将 (E,s) 输出给 TPM。TPM 保存 (E,s)，这里 (E,s) 就是 TPM 的 AAK。

注意：SU 只能生成一次 AAK，且秘密保存 $p'q'$。

3.3 匿名认证协议

证明者 TPM(Alice)向验证者(Bob)匿名零知识证明她知道一个有效的匿名认证密钥 (E,s)，其中，s 在一个特定区间 $[X-2^l,X+2^l]$。

Step1 SU 任选一个素数 $k>X+2^{\alpha(l+l_c)}$，并计算：

$$T_1=E^{k^{-1}}(\bmod n),\quad T_2=g^{k^{-1}}(\bmod n)$$

其中，k^{-1} 是 k 在 $p'q'$ 下的逆，将 (T_1,T_2,k) 输出给 Alice。Alice 任选 2 个随机数 $t_1,t_2\in\pm\{0,1\}^{\alpha(l+l_c)}$，计算：

$$T_3=T_1^{t_1}(\bmod n),\quad T_4=T_2^{t_2}(\bmod n)$$

Alice 向 Bob 发送 (T_1,T_2,T_3,T_4)。

Step2 Bob 任选 1 个随机数 $c\in\{0,1\}^{l_c}$，并发送给 Alice。

Step3 Alice 核实 $c\in\{0,1\}^{l_c}$，并计算：

$$w_1=t_1-c(s-X),\quad w_2=t_2-c(k-X)$$

其中，$w_1\in\pm\{0,1\}^{\alpha(l+l_c)+1}$，并且向 Bob 发送 w_1,w_2。

Step4 Bob 核实 $w_1\in\pm\{0,1\}^{\alpha(l+l_c)+1}$ 并验证：

$$T_1^{w_1-cX}T_2^c\stackrel{?}{=}T_3(\bmod n) \tag{1}$$

$$T_2^{w_2-cX}g^c\stackrel{?}{=}T_4(\bmod n) \tag{2}$$

如果等式成立，且满足下文撤消性，则式(1)说明了 $T_2=T_1^s(\bmod n)$；式(2)说明了 $g=T_2^k(\bmod n)$，且有：

(1) $g=T_2^k=(T_1^s)^k=(T_1^k)^s(\bmod n)$，根据下文的不可伪造性，Alice 知道匿名认证密钥 $(E(=T_1^k(\bmod n)),s)$。

(2)因为 $T_1=E^{k^{-1}}(\bmod n)$，所以 T_1 是 QR_n 的一个元素，同理 T_2 也是 QR_n 的一个元素，且它们不是 QR_n 的生成元的概率，可忽略不计。

(3)由式(1)可知，Alice 向 Bob 证明了 Alice 知道 T_2 在基 T_1 下的离散对数 s 在特定区间 $[X-2^{\alpha(l+l_c)},X+2^{\alpha(l+l_c)}]$。

文献[4]可将该协议转换为一个非交互的“知识签名”方案，且在随机预言模型下是安全的[5]。

3.4 协议分析

本文所提方案满足不可伪造性、匿名性和撤销性。

(1)不可伪造性(forgery-resistance)：攻击者不能通过 1 组密钥对来计算出新的有效 (E,s)，因为如果存在 1 个概率多项式时间算法能通过 1 组密钥对 $(s_1,E_1),(s_2,E_2),\cdots,(s_k,E_k)$，以不可忽略的概率找到 1 个新的有效密钥 (E,s)，满足 $E^s=g(\bmod n)$，$s\neq s_i$，$1\le i\le k$，则可构造一个算法以不可忽略的概率解决 Flexible RSA 问题。即在基于强 RSA 假设下，本方案满足不可伪造性。详见文献[3]。

(下转第 191 页)