# 基于可信计算的Web单点登录方案

邱 罡[1] 张 崇[2] 周利华[1]
(西安电子科技大学CNIS教育部重点实验室 西安 710071)[1]
(南阳医学高等专科学校第一附属医院ECT室 南阳 473058)[2]

**摘 要** 为增强现有单点登录技术中用户域的安全性,在客户端平台引入可信平台模块(TPM),同时采用智能卡、口令及指纹相结合的客户端认证方案,实现了用户、客户端及智能卡间的相互认证,并保证了应用服务所提供的信息资源的安全使用。分析结果表明,该方案不要求用户与客户端预先协商信任关系,且可辨别客户端的主人和普通使用者。使用哈希函数的用户认证计算及推式平台完整性验证使得系统具有较高的运行效率。

**关键词** 可信计算,单点登录,智能卡,身份认证,模型
**中图法分类号** TP309 **文献标识码** A

## Web Single Sign-on Scheme Based on Trusted Computing

QIU Gang[1] ZHANG Chong[2] ZHOU Li-hua[1]
(The CNIS Key Laboratory of the Education Ministry, Xidian University, Xi'an 710071, China)[1]
(The First Affiliated Hospital of Nanyang Medical College, Nanyang 473058, China)[2]

**Abstract** To enhance the security of user domain in single sign-on system, the Trusted Platform Module(TPM) was introduced to ensure the terminal trustworthiness. Meanwhile a user authentication scheme combined with password, fingerprint and smartcard was adopted, which achieves the mutual identification among user, user terminal and smartcard, and ensures the usage security of the information provided by application service. The security and performance analysis shows that the user authentication can identify the owner of user terminal from the genuine operators without any pre-negotiation, computation with Hash function in user authentication and push validation attestation on user platform integrity are of high efficiency.

**Keywords** Trusted computing, Single sign-on, Smart card, Identity authentication, Model

## 1 引言

单点登录(Single Sign-on, SSO)技术是出于效率和安全性因素的考虑,将多个应用服务的用户登录系统进行统一管理,获得统一的认证功能,用户只需在网络中主动进行一次身份认证,即可获得所需访问应用系统和资源的授权,而不需要再次参与其它的身份认证过程。

有关SSO技术在Web应用中实现的方案已经有许多[1],如基于ticket的Kerberos系统[2]、基于Portal服务器的Web请求代理[3]等。以上SSO系统中保存用户的访问身份的ticket或cookie通常存放于客户端平台中,因此客户端平台的安全性至关重要。目前用户身份认证方案广泛采用的基于用户名/口令的认证方式存在着很大的安全问题。基于PIN的用户身份认证方案,由于密钥长度短且通常包含用户的个人信息,容易遭到字典攻击和穷举攻击;而单纯基于生物特征(如指纹)的身份认证方法也易遭到重放攻击。文献[4]借助智能卡通过指纹比对和动态口令验证,实现了基于口令和指纹的双因素用户身份认证方案,但指纹仅被用来产生一个无关紧要的随机数,并未和口令实现紧密结合。以上方案均未考虑以下几个问题[5]:

(1)未检验终端平台本身是否安全可信。若终端平台的操作系统、应用软件或固件等被攻击者恶意修改,用户输入的口令和指纹很容易被非法窃取。

(2)用户在认证过程中使用的敏感信息很可能被其它程序截获或重放。

(3)仅实现了终端或智能卡对用户身份的鉴别,但用户却无法认证终端和智能卡。用户很可能在不知情的状态下向非法的智能卡或终端提供自己的口令、PIN和指纹数据。

(4)缺乏智能卡和终端平台间的相互认证,将导致合法的智能卡被恶意的终端平台欺骗,或合法的终端平台被恶意的智能卡欺骗。

TCG[6]定义了一组支持可信计算的硬件和软件工业标准规范,其核心是一个可防止篡改的硬件安全模块——TPM[7]。TPM作为加密协处理器和保护密钥及秘密信息的

到稿日期:2009-10-19 返修日期:2009-12-29 本文受国家自然科学基金重点项目(60633020),河南省重点科技攻关项目(102102210432),南阳市科技攻关项目(2007G0803)资助。

邱 罡 博士生,讲师,主要研究方向为网络信息安全,E-mail:qiugang7780@163.com;张 崇 工程师,主要研究方向为电子技术;周利华 教授,博士生导师,主要研究方向为计算机网络安全理论与技术等。

保护存储装置，同时被用来度量和报告平台的完整性信息，并且不会受到平台使用者或其上运行的软件的威胁。在 TCG 公布标准所提出的对用户的认证及授权协议中[6]，终端平台主人(Owner)与可信平台模块(TPM)共享一个 20 字节的机密信息——授权数据(AuthData)，通过挑战/应答的方式来实现相互认证。授权数据由用户口令作为外部种子经过 Hash 运算归一化处理后的 Hash 值，并存储在终端平台上。此类方案虽然实现了用户和 TPM 间的双向认证，但仍未能摆脱基于口令的认证方式的脆弱性。

文献[8]以 OSAP 为例，对可信平台的用户认证协议进行了改进，提出了基于可信计算平台的结合口令和智能卡的双因素用户认证方案。用户通过向智能卡提供 PIN 码，在卡内计算共享的认证信息 AuthData，实现了智能卡与 TPM 之间的相互认证，但此方案的薄弱环节仍在于用户与智能卡间的 PIN 码。文献[9]在 SSO 中引入可信计算技术，该方案仅在系统终端远程证明可信的基础上讨论了对服务提供方信息的保护，并未提到用户身份的验证。

本文在单点登录系统中引入可信计算技术以提高客户端平台的安全性，并结合智能卡和指纹识别的用户认证方案，以提高整个系统的安全性。

## 2 可信计算技术

### 2.1 平台完整性度量

平台完整性度量包括对构成平台的硬件和软件部分分阶段的度量和存储。完整性度量通常分为两种类型：TCG 的可信引导以及在可信引导基础上的其它完整性度量。

当系统加电运行时，初始引导代码(如 BIOS 引导块)在将控制权传递给下一个组件之前对其进行度量，并将度量值存入 TPM。接下来的每个软件组件都要进行度量，并保存度量结果，直到装入整个操作系统。BIOS 引导模块及 TPM 被称作核心根(Core Root of Trust for Measurement，CRTM)，可信计算平台的可信性建立在以 TPM 为信任根和从信任根开始的信任链之上。每一个度量都使用 SHA-1 哈希算法对组件的二进制映像进行度量，并将度量结果存入 TPM 中的平台配置寄存器(Platform Configuration Registers，PCR)。

### 2.2 平台完整性报告

TCG 标准中定义的平台完整性报告(或远程证明)机制，用于向挑战方报告存储在 PCR 中的完整性度量值是以可靠方式存储的。在证明过程中 TPM 对 PCR 值和附加的数据(如来自挑战方防止重放攻击的随机数)使用私钥签名，并传给挑战方。证明是一项受保护的原子操作，不能被恶意软件伪造。平台也可以在证明中发送附加信息，如完整性度量日志，其中包括平台中加载并被 TPM 度量过的组件列表，以及这些组件是如何构成的。

远程挑战方通过验证带有 AIK 证书的签名，并将完整性度量值与本地收集的参照度量日志进行对比来验证证明。攻破的系统可以修改度量日志，但其不能改变受 TPM 保护的度量结果与修改过的日志匹配，因此通过和签过名的度量结果对照来验证度量日志，即可发现伪造操作。

## 3 系统组成

如图 1 所示，基于可信计算平台的单点登录系统主要包括可信客户端 TC、生物特征读取设备(Biometric Reader，BR)、智能卡 SC、认证服务器 AUS、完整性验证服务器 IVS 和应用服务器 AS 等几个部分。

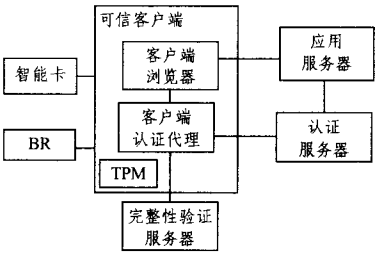


图 1 系统结构图

用户先向系统管理员申请智能卡进行注册，用户的智能卡信息存储在认证服务器端用户的身份鉴别信息表中，服务器采取加密手段保障信息表的安全性。认证服务器接收客户端认证代理提交的用户身份证书，与其内部保存的用户身份鉴别信息表进行对比，验证用户身份；完整性验证服务器用于客户端平台的完整性验证，提供完整性验证报告；应用服务器向用户提供所需的服务。

客户端采用智能卡结合可信 BR 的用户身份认证方式，同时使用 LCD 亮起指示平台认证状态错误，LED 指示平台是否可信。智能卡具有公钥密码运算功能，其中存储用户证书和敏感信息，如认证参数、指纹模板 $F_u$ 的哈希值。其中认证参数包括用户接入网络时需要的参数以及用户与终端进行认证的参数$(U,V,W)$。$U,V,W$ 的具体计算方法见式(1)－式(3)。其中，$PW$ 为用户口令，$h(x)$表示计算 $x$ 的 Hash 值。

$$U=h(ID_u||PW) \tag{1}$$

$$V=h(PW)\oplus h(F_u) \tag{2}$$

$$W=U\oplus h(ID_u||F_u) \tag{3}$$

TPM 中存储着自己的私钥 $SK_{TPM}$、证书 $Cert(TPM)$、与 BR 共享的密钥 $K_{BT}$、其它模块的完整性向量值以及用于标示终端平台所有者的 $x_{TO}=h(h(PW_{TO})\oplus h(F_{TO}))$。

## 4 系统工作流程

为简化描述，在认证阶段将可信终端与 TPM 看作一个整体。整个系统的工作流程分为智能卡、用户和终端平台的相互认证过程以及用户请求应用服务过程。系统加电后在 TPM 监控下引导到可信状态，然后用户插入智能卡进行平台验证。

### 4.1 客户端用户身份认证

1)SC→TC/TPM：$r_1$，$ID_s$，$D_1$

智能卡 SC 向可信终端 TC 发出随机数 $r_1$、智能卡标志 $ID_s$、平台验证请求 $D_1$。

2)TC/TPM→IVS：$r_2$，$Cert_{TPM}$，$PCR$，$Sign_{TPM}$，$D_2$

$Sign_{TPM}=Sign(SK_{TPM},r_1||r_2||ID_{TPM}||PCR)$

TC 生成随机数 $r_2$，并将平台证书 $Cert_{TPM}$、平台配置寄存器值 PCR、使用 TPM 私钥签名的平台证明 $Sign_{TPM}$以及平台验证请求 $D_2$ 发送给完整性验证服务器 IVS，请求获得证明证书。$Sign(k,x)$表示使用 $k$ 的私钥对 $x$ 进行签名。

3)IVS→TC/TPM：$E(PK_{TPM},r_2||Cred_{TC})$

完整性验证服务器对终端平台进行验证后，返回使用 TPM 公钥加密的验证结果证书 $Cred_{TC}$。$E(k,x)$表示使用密钥 $k$ 对 $x$ 进行加密。

4)TC/TPM→SC:$E(PK_{SC},r_1||ID_{SC}||ID_{TPM}||Cred)$

$Sign(SK_{TPM},r_1||ID_x||ID_{TPM}||Cred)$

终端平台将完整性验证报告返回智能卡,由智能卡判断平台状态是否符合完整预期;如果验证成功,可通过 LED 指示灯指示并进入下面的用户认证阶段;否则通过 LCD 指示平台认证出错。

5)SC→TC/TPM:$r_3,E(PK_{TPM},O||P||Q||ID_{SC})$

$$O=h(U||r_3) \tag{4}$$

$$P=U\oplus h(r_3||ID_{TPM}) \tag{5}$$

$$Q=h(V||r_3) \tag{6}$$

智能卡 SC 生成随机数 $r_3$,并计算 $O,P,Q$,使用 TPM 公钥加密后向可信终端 TC 发送,进行用户认证。

6)TC/TPM→SC:$M_T,r_4$

客户端接收到 $E(PK_{TPM},O||P||Q||ID_{SC})$进行解密,并根据用户输入的口令 $PW'$和指纹 $Fu'$计算 $U'=P\oplus h(r_3||ID_{TPM})$,$O'=h(U'||r_3)$。若 $O=O'$,则现在用户为普通用户,否则停止认证;然后,在 TPM 中计算 $x'=h(h(PW')\oplus h(F'))$,若 $x'=x_{TO}$,则智能卡的持有者是平台的真正属主。通过上述步骤可信平台不仅认证了智能卡是合法的,同时认证了用户是合法普通用户或是平台属主。

TPM 计算 $M_T=h(ID_u||F'_u)\oplus r_4$ 发送到智能卡,由智能卡对平台进行认证。

7)智能卡计算 $U'=M_T\oplus r_4\oplus W$,如果 $U'=U$,则平台认证通过。

### 4.2 Web 服务请求流程

用户与平台之间的相互认证通过后,用户即可向应用服务器 AS 发出访问请求,获取所需资源。考虑到用户认证方式的兼容性[1],本文采用图 2 所示的代理认证结构,认证流程描述如下:

1)AS 首先向作为认证中心和信任证明方的认证服务器进行注册,更新其服务模块签名,同时认证服务器也可验证 AS 的合法性,以防止假冒 AS 发起的钓鱼攻击。

2—3)用户向认证服务器请求进行服务身份的确认。认证服务器可为用户分配用于此次会话的临时身份,便于匿名服务,同时便于权限的统一分配管理。认证服务器返回用户身份 $ID_{user}$ 及用户信任证书 $Cred_{user}$。

4)用户使用 $ID_{user}$ 发起服务请求。

5)AS 向用户发出平台完整性证明挑战请求,并附带随机数 $r$。

6)客户端平台生成用于加密完整性度量结果的会话密钥。

7)TPM 发起对客户端平台的完整性度量。

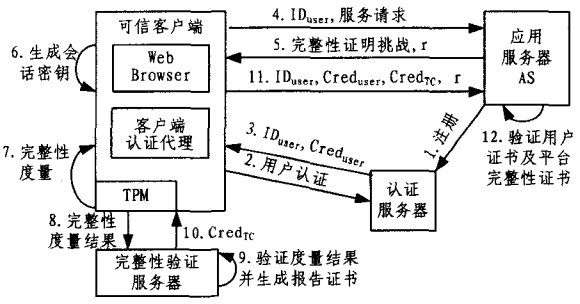


图 2 Web 访问认证流程

8)客户端认证代理将客户端的 PCR 值及存储度量日志 SML 发送到完整性验证服务器进行验证。

9—10)完整性验证服务器根据度量结果生成度量信任证书 $Cred_{TC}$ 并发送到客户端认证代理。

11)客户端响应应用服务器 AS 的用户及平台验证请求,将用户 $ID$、平台信任证书 $Cred_{TC}$、用户信任证书 $Cred_{user}$ 及随机数 $r$ 使用会话密钥加密返回 AS。

12)AS 验证用户和平台证书后,如果平台状态可信,则根据用户的身份提供相应的服务响应。

## 5 系统安全及性能分析

### 5.1 系统安全性分析

1)三方认证。本方案在可信平台的框架下,实现了用户、智能卡和可信平台之间的双向认证,确保了用户口令和指纹数据在认证过程中的安全性,强化了用户对可信平台或智能卡中数据的访问控制,并减少了智能卡遗失或可信平台被攻破所造成的数据泄漏的危害。

2)用户三因素认证。用户通过插入本人的智能卡并且正确地输入口令和指纹,才可以通过所有的认证。缺少任何一个因素,用户都不能够使用客户端平台或智能卡。

3)口令与指纹存储与计算的安全性。智能卡用户的身份信息、口令和指纹模板通过 Hash 函数紧密地联系在一起,并借助智能卡、TPM 和 Hash 函数的安全特性,弥补了单纯口令或指纹认证方案的脆弱性。攻击者即使获取了智能卡中的信息,也无法得到智能卡所有者的信息。由于 TPM 和智能卡不直接存储用户原始信息,且指纹和口令信息在各个接口与相应实体生成的随机数将一起加密传送,因此指纹和口令自身的机密性、新鲜性和完整性得到了保证。在用户输入口令和指纹之前对平台的完整性验证保证了用户信息在录入、存储、通信和计算过程中的安全性都大大提高。

4)平台完整性的安全保证。客户端平台通过平台完整性证明,减少了其上存在病毒等恶意程序攻击的可能,为用户身份信息和应用服务资源的安全提供了保证。

5)"推"式的证明方式。在智能卡和 AS 验证终端的完整性时,终端平台将证明信息以推的方式发送给完整性验证服务器 IVS。根据来自挑战者的请求,终端平台将 IVS 颁发的证书发送给挑战者智能卡或 AS。这种证明方式中,终端平台不需要向智能卡或 AS 揭示自己的平台信息,从而保护了平台配置的隐私;智能卡或 AS 无需验证终端平台配置的能力[10]。

### 5.2 系统性能分析

本文中客户端对用户的身份认证采用 TPM 离线认证,减少了对认证中心的依赖。用户、智能卡和 TPM 相互认证使用一次性信息交换,减少了认证过程中的信息流量。三方认证过程中的计算主要以 Hash 和 XOR 计算为主,具有较快的运算速度。基于"推"式平台完整性证明使得客户端在切换到不同应用服务器时,在一定有效期内可以使用已经得到的平台完整性证书,不需要再次请求完整性验证服务器进行完整性证明,提高了证明的效率。

**结束语** 本文提出了基于可信计算的 Web 单点登录系统,其中融合了 PKI 证书、认证代理及可信计算技术,实现了

(下转第 156 页)

TCIA 可以用于描述和验证构件系统设计阶段构件交互的情况。如前面的例子所示，TCIA 可以描述复合构件系统的行为和时间约束信息，根据描述的信息，可以方便地验证系统的安全性、实时性及其它可信特性。

**结束语** 本文介绍了构件实时交互行为的形式化建模方法，分析了构件交互行为建模的两类方法及优缺点，提出了时间构件交互自动机的相关概念，给出了时间构件交互自动机的组合、验证方法。时间构件交互自动机结合了进程代数与自动机的优点，既能够详细描述构件交互情况，又能够清楚地描述构件系统的体系结构信息和实时信息，便于对系统进行描述和验证。我们将进一步开展构件实时行为形式化验证等相关技术的研究和实用工具的开发实现。

## 参 考 文 献


[1] Vasu A, Mubarak M. A component model for trustworthy real-time reactive systems development [C] // Formal Aspects of Component Software(FACS'07). Sophia-Antipolis, France: ENTCS, Elsevier, Sept 2007: 1-15

[2] Crnkovic I, Larsson M. Building reliable component-based software systems [M]. Norwood, MA: Artech House Publishers, 2002: 3-21

[3] Moller A, Akerholm M, Fredriksson J, et al. Evaluation of component technologies with respect to industrial requirements [C] // Proceedings of the 30th EUROMICRO Conference (EUROMICRO'04). Los Alamitos, CA, USA: IEEE Computer Society, 2004: 56-63

[4] Hatcliff J, Deng W, Dwyer M, et al. Cadena: An integrated development, analysis, and verification environment for component-based systems [C] // Lecture Notes in Computer Science. Berlin / Heidelberg: Springer, Volume 2984/2004, 2004: 160-164

[5] 杨芙清，梅宏，吕建，等. 浅论软件技术发展[J]. 电子学报，2002，30(12A)：1901-1906

[6] Plasil F, Visnovsky S. Behavior Protocols for Software Components [J]. IEEE Transactions on Software Engineering, 2002, 28 (11): 1056-1076

[7] Allen R, Garlan D. A Formal Basis for Architectural Connection [J]. ACM Transactions on Software Engineering and Methodology, 1997, 6(3): 213-249

[8] Reed G M, Roscoe A W. A timed model for communicating sequential processes [J]. Theoretical Computer Science, 1988, 58 (13): 249-261

[9] Magee J, Kramer J, Giannakopoulou D. Behaviour analysis of software architectures [C] // Donohoe P. editor. Proceedings of the 1st Working IFIP Conference on Software Architecture (WICSA1). San Antonio, Texas, USA: Kluwer Academic Pub, 1999: 35-50

[10] Alur R, Dill D L. A theory of timed automata [J]. Theoretical Computer Science, 1994, 126(2): 183-235

[11] de Alfaro L, Henzinger T A. Interface automata [C] // Proceedings of the Ninth Annual Symposium on Foundations of Software Engineering (FSE). ACM Press, 2001: 109-120

[12] de Alfaro L, Henzinger T A, Stoelinga M. Timed Interfaces [C] // Proceedings of the Second International Workshop on Embedded Software. LNCS 2491. Springer-Verlag, Berlin: SprinRer Verlag, 2002: 108-122

[13] Brim L, Cerna I, Varekova P, et al. Component-interaction automata as a verification-oriented component-based system specification [J]. ACM SIGSOFT Software Engineering Notes, 2006, 31(2): 1-8

[14] Varekova P, Zimmerova B. Component-interaction automata for specification and verification of component interactions [C] // IFM 2005 Doctoral Symposium on Integrated Formal Methods. Eindhoven, The Netherlands: Technische Universiteit Eindhoven, 2005: 71-75

[15] Zimmerova B, Varekova P, Benes N, et al. The Common Component Modeling Example: Comparing Software Component Models [C] // Component-Interaction Automata Approach (CoIn). LNCS, Springer-Verlag, August 2008, 5153: 146-176


(上接第 123 页)

用户、智能卡和 TC/TPM 间的相互认证，保证了用户使用平台的合法性和终端平台的完整性，有效地保护了信息的使用安全。新方案采用离线式用户认证，有效地提高了认证效率，在实现了用户身份的统一管理和认证的同时，降低了用户支持管理的复杂度。本文仅对单域的单点登录进行了研究，下一步的研究工作将考虑跨域单点登录方案的实施，以及跨域方案中用户访问的匿名实现。

## 参 考 文 献


[1] 黄琛，李忠献，杨义先，等. 一种新的兼容多种身份认证方式的 Web 单点登录方案[J]. 北京邮电大学学报，2006，29(5)：130-134

[2] Jason G. Single sign-on for your Web applications with Apache and Kerberos [EB/OL]. http://www.onlamp.com/pub/a/onlamp/2003/09/11/kerberos.html, 2008-10-22

[3] Dunne C. Build and implement a single sign-on solution [EB/OL]. http://www-106.ibm.com/developerworks/Web/library/wasinglesign/30, 2008-09-15

[4] Lin C H, Lai Y Y. A flexible biometrics remote user authentication scheme [J]. Computer Standards & Interfaces, 2004, 27 (1): 19-23

[5] Zheng Y, He D K, Yu W C, et al. Trusted computing-based security architecture for 4G mobile networks [C] // Proceedings of the IEEE Conference PDCAT. Dalian, China, 2005: 251-255

[6] Trusted Computing Group. TCG specification architecture overview [EB/OL]. https:// www.trustedcomputinggroup.org, 2008-11-25

[7] Trusted Computing Group. TPM main part 1 design principles [EB/OL]. https://www.trusted-computinggroup.org, 2008-12-11

[8] George P. User authentication with smart cards in trusted computing architecture [C] // Proceedings of the International Conference on Security and Management. Las Vegas, Nevada, USA, 2004: 25-31

[9] Pashalidis A, Mitchell C J. Single sign - on using trusted platforms [C] // Information Security. LNCS 2851. Berlin: Springer, 2003: 54-68

[10] Yoshihama S, Ebringer T, Nakamura M, et al. WS-attestation: efficient and fine-grained remote attestation on Web services [C] // Proceedings of the International Conference on Web Services. Florida: IEEE Press, 2005: 10-17