可信的智能卡口令双向认证方案

杨 力，马建峰

(西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)

【摘要】提出一种基于智能卡的可信双向认证方案，使用散列函数认证身份，采用远程证明方法验证平台可信性。该方案支持安全会话密钥协商，支持用户身份匿名及口令自由更换，服务器平台证书可更新。分析表明，该方案可以抵抗针对智能卡口令认证方案的常见攻击，安全高效，满足安全设计目标。

关 键 词 双向认证； 口令； 远程证明； 智能卡； 可信计算

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.01.024

Trusted Mutual Authentication Scheme with Smart Cards and Passwords

YANG Li and MA Jian-feng

(Key Laboratory of Computer Networks and Information Security, Ministry of Education, Xidian University Xi'an 710071)

Abstract Only identities of the server and the user are authenticated in traditional smart cards based passwords authentication schemes, but whether the platform is trusted or not does not be verified, and this identity authentication cannot provide enough protection on personal information of users. A trusted mutual authentication scheme based on smart cards is proposed, in which hash functions are used to authenticate identities, and remote attestation is used to verify the platform. Analysis shows that our scheme can resist most of possible attacks and is therefore more secure and efficient for smart card applicatoins.

Key words mutual authentication; passwords; remote attestation; smart cards; trusted computing

身份认证是网络环境中最基本的安全服务。基于智能卡的口令认证方式是最普遍和便捷的身份认证机制之一，在用户远程登录服务器时被广泛采用，能够在开放网络环境中提供用户和服务器之间的认证，确保用户的合法性和服务器的正确性。智能卡口令认证方式被部署在多种不同类型的认证应用中，包括远程登录、在线银行、电子商务、安全装置激活等，提供基于智能卡和基于口令的双因素认证。自文献[1]首次提出利用智能卡和口令对用户进行认证以来，文献[2-7]又提出了许多的类似方案。用户借助智能卡，通过终端远程接入网络中的服务器，服务器通过事先协商好的秘密信息和智能卡本身，完成与用户的相互认证。认证通过后，用户向服务器提交个人信息，并接受服务器的服务。

然而，在日益复杂和开放的网络环境下，该类传统方案存在明显的不足，智能卡用户在登录服务器时只认证服务器的身份，没有验证服务器系统平台的可信性，未获知服务器是否在安全可信的状态，缺乏对用户信息的有效保护，可能造成用户个人隐私信息泄露等问题。开放的互联网环境中存在大量的非法程序和恶意软件(如各种木马程序、蠕虫病毒等)，一旦服务器未能按照约定处于某安全的配置状态，例如操作系统未安装最新系统补丁程序、存在软件安全漏洞、软件版本过期、已被恶意软件控制等，会给登录该服务器的用户造成安全危害，可能导致登录用户个人信息的泄露、请求业务的处理失败、财产的损失等。因此，有必要设计满足新的安全目标的智能卡口令认证方案，以符合互联网环境下用户远程登录认证服务器的需求。针对上述问题，文献[8]讨论了智能卡用户与可信计算终端之间的认证问题，给出了智能卡用户与所使用的可信计算终端完成相互认证的方案。利用该方案可以确保智能卡用户所使用终端平台的可信性，但仍然没有解决智能卡用户和所使用的终端作为整体登录服务器并进行可信验证的问题。

本文针对传统的智能卡口令认证方案未对服务器进行可信性验证的不足，提出一种可信环境下基

收稿日期：2009－08－09； 修回日期：2009－12－08
基金项目：国家自然科学基金(60633020, 60872041)；中央高校基本科研业务费专项资金(5Y10000903001,K50510030003)
作者简介：杨 力(1977－)，男，博士，主要从事信息安全、可信计算等方面的研究.

于智能卡和口令的远程双向认证方案，双方身份互认证，验证服务器平台属性，安全地协商会话密钥，提供对智能卡用户和服务器的多方面安全保障，支持用户身份匿名，支持用户口令自由更换和服务器平台可信证书更新，达到所设计的安全目标。

1　背景知识

可信计算组织(trusted computing group，TCG)[9]提出的可信计算概念与技术，已被学术界和产业领域所接受，成为当前信息安全领域研究的热点[10-12]。可信计算的核心是在终端平台上嵌入可信平台模块(trusted platform module，TPM)[13]，提供密码支持和保护存储功能，为各种可信机制和安全功能提供硬件保障，并为度量和验证平台的可信属性即完整性提供基础。

TPM具有向远程验证方证明本地平台配置信息的能力，即远程证明(remote attestation，RA)，其主要过程是通过完整性验证证明平台的可信性。TPM内部有一组PCR(platform configuration register)寄存器，存储所在平台的完整性度量信息。系统加电时PCR初始化，TPM度量平台硬件和软件组件，对应的散列值被写进平台配置寄存器PCR。度量组件时，创建事件并记录在度量存储日志(stored measurement log，SML)中。PCR值和SML值一起用于向远程验证方证明平台的状态。为了确保度量值的可信，TPM使用身份证明密钥(attestation identity key，AIK)对度量值进行签名。

远程证明时，计算平台响应远程验证方的要求，采集事件记录，计算平台的PCR值并进行AIK签名；随后将签名值、事件记录及AIK证书等内容报告给验证方；验证方对提交的内容进行验证，确定远程计算平台身份及其所报告内容的真实性，依此判断平台的可信性。

2　方案的安全目标

2.1　安全目标

理想的智能卡口令认证方案应满足一定的安全设计目标，以满足应用需求和有效的抵抗针对智能卡口令认证方案的攻击。结合文献[14]和文献[15]，在可信计算环境下，本文采用的智能卡口令认证方案应达到的安全目标如下。

G1：提供双向身份认证；

G2：服务器管理员对用户口令明文未知；

G3：建立会话密钥以提供秘密通信；

G4：用户可以自由选择和更换口令；

G5：支持用户匿名登录；

G6：对服务器进行可信验证；

G7：服务器完整性证书更新。

在可信计算环境下，智能卡口令认证方案应抵御的常见攻击类型如下。

SR1：抵抗拒绝服务攻击；

SR2：抵抗重放攻击；

SR3：抵抗密钥猜测攻击；

SR4：抵抗并行会话攻击；

SR5：抵抗伪装攻击；

SR6：抵抗内部攻击；

SR7：抵抗偷窃验证者攻击；

SR8：抵抗平台假冒攻击。

2.2　符号定义

本文符号定义如表1所示。

表1　符号定义

符　号	含　义
S	服务器
U	客户端用户
ID	客户端用户身份
PW	用户U的口令
$h(\ )$	单向散列函数
$E_K(\ )$	对称加密算法
$\oplus$	按位异或运算
T	系统时间戳
AIK_{priv}	平台AIK私钥
AIK_{pub}	平台AIK公钥
$Cert_{AIK}$	平台AIK证书
$Sig\{X\}_{AIK}$	AIK签名运算
$Log(X)$	安全度量日志提取

3　可信双向认证方案

本文方案的场景模型如图1所示。客户端、服务器(TPM)、管理服务器接入Internet并可互相访问，持有智能卡的用户U先在服务器S所在机构完成注册，然后选择客户端登录，向服务器发出访问请求，服务器与用户完成双向可信认证，管理服务器提供对服务器可信证书的更新服务并允许用户查询。

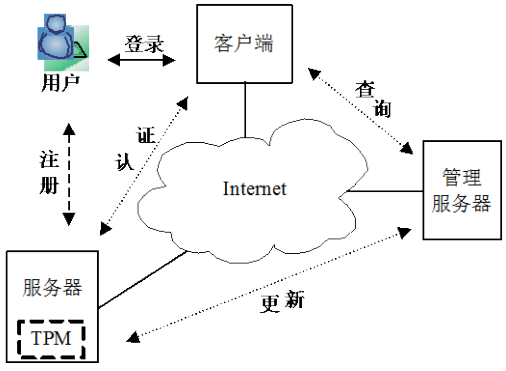


图1　方案场景模型

用户利用持有的智能卡请求对服务器的访问，方案实施过程包含注册、登录认证和认证更新3个阶段。根据文献[8]，本文假定用户所使用的终端平台是可信的，即服务器不验证用户终端平台的可信性。

3.1 注册阶段

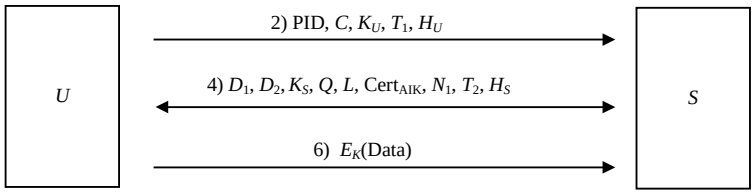
用户首先需要成为系统的合法注册用户，注册过程包括用户向服务器发送注册请求和服务器签发注册信息给用户，具体步骤如下：

1) 当用户U向服务器S请求注册时，U任意选择一个身份ID和口令PW，计算h(PW)，发送ID、h(PW)给服务器S。

2) 服务器S收到注册请求消息后，计算PID=$h(x,$ ID)，$I=h(\mathrm{Cert_{AIK}})$，$B=\mathrm{PID}\ \ h(\mathrm{PW})\ \ I$。其中，$x$为$S$随机挑选的秘密数，为安全考虑应大于100 bit，$\mathrm{Cert_{AIK}}$为S的平台完整性证书。S选择大素数p及$g\in\mathrm{GF}(p)$，选择随机数N_0，S通过安全信道签发PID、B、I、N_0、p、g给U作为注册信息。

3.2 登录认证阶段

当用户U在远程终端上利用签发的智能卡向服务器请求服务时，其登录认证过程如图2所示。



1)计算：$C=h(B\oplus h(\mathrm{PW})\oplus N_0\oplus T_1)$；

$K_U=g^a \bmod p$； $H_U=h(\mathrm{PID}, C, K_U, T_1)$

5) 验证：T_2; H_S; D_2; I; PCR_S

计算：$N_1= D_1\oplus h(\mathrm{PID}\oplus N_0\oplus I\oplus T_2)$;

$K_{US}=(K_S)^a=(g^b)^a \bmod p$

3) 验证：T_1; H_U; C

计算：$D_1=h(\mathrm{PID}\oplus N_0\oplus I\oplus T_2)\oplus N_1$;

$D_2=h(D_1\oplus T_2)$； $K_S=g^b \bmod p$;

$K_{US}=(K_U)^b=(g^a)^b \bmod p$;

$\mathrm{PCR}_S=\mathrm{SHA1}(\mathrm{PCR}_0\|\ldots\|\mathrm{PCR}_N)$;

$Q=\mathrm{Sig}\{\mathrm{PCR}_S, h(K_S, N_1)\}_{\mathrm{AIK}}$;

$L=\mathrm{Log(SML)}$;

$H_S=h(D_1, D_2, K_S, Q, L, \mathrm{Cert_{AIK}}, N_1, T_2)$

图2 登录认证过程

1) 用户U将智能卡接入终端设备，输入用户身份ID和口令PW，智能卡首先验证ID和PW的有效性，即验证ID的合法性与h(PW)的正确性；验证通过后，计算$C=h(B\oplus h(\mathrm{PW})\ \ N_0\oplus T_1)$，其中$T_1$为本地时间戳。用户$U$随机产生秘密数$a$，计算$K_U=g^a \bmod p$、$H_U=h(\mathrm{PID},C,K_U,T_1)$，发送消息PID、$C$、$K_U$、$T_1$、$H_U$给服务器$S$。

2) 服务器S收到消息后，首先验证时间戳T_1，检查$T_1'-T_1\leqslant\Delta T$是否成立，其中$T_1'$为服务器当前时戳，$\Delta T$为合法的通信延迟。若成立，则计算$H_U'=h(\mathrm{PID},C,K_U,T_1)$，判断$H_U'$与原值$H_U$是否一致，以验证$U$所发送消息的完整性；若通过，则继续验证用户$U$的身份，即验证PID和$C$的正确性。计算$C'=h(\mathrm{PID}\ \ N_0\oplus I\oplus T_1)$，判断$C'$与原值$C$是否相等，若相等，则服务器$S$确定$U$为该系统的合法用户。

服务器S计算$D_1=h(\mathrm{PID}\ \ N_0\oplus I\oplus T_2)\ \ N_1$、$D_2=h(D_1\oplus T_2)$，其中$T_2$为$S$产生的时间戳；随机产生秘密数$b$，计算$K_S=g^b \bmod p$；利用收到的$U$的密钥计算双方会话密钥$K_{US}=(K_U)^b=(g^a)^b \bmod p$；接着，$S$利用TPM芯片加载平台的AIK私钥$\mathrm{AIK_{priv}}$，计算服务器的平台完整性校验值$\mathrm{PCR}_S$，即$\mathrm{PCR}_S=\mathrm{SHA1}(\mathrm{PCR}_0\|\mathrm{PCR}_1\|\cdots\|\mathrm{PCR}_N)$，并进行AIK签名，即计算引用值$Q=\mathrm{Sig}\{\mathrm{PCR}_S,h(K_S,N_1)\}_{\mathrm{AIK}}$，其中$N_1$为$S$挑选的随机数，加载平台安全度量日志$L=\mathrm{Log(SML)}$。服务器$S$计算所发送消息的散列值$H_S=h(D_1,D_2,K_S,Q,L,\mathrm{Cert_{AIK}},N_1,T_2)$，发送消息$D_1$、$D_2$、$K_S$、$Q$、$L$、$\mathrm{Cert_{AIK}}$、$N_1$、$T_2$、$H_S$给用户$U$。

3) 用户U收到消息后，首先验证时间戳T_2的正确性，检查$T_2'-T_2\leqslant\Delta T$是否成立，其中$T_2'$为用户终端当前时戳，若成立则验证消息是否被篡改，即计算$H_S'=h(D_1,D_2,K_S,Q,L,\mathrm{Cert_{AIK}},N_1,T_2)$，判断$H_S'$与原值$H_S$是否一致，若一致，则说明消息未被篡改。随后，利用收到的消息计算秘密随机数N_1，即$N_1=D_1\oplus h(\mathrm{PID}\ \ N_0\oplus I\oplus T_2)$，并保留$N_1$作为下一次登录服务器时使用。计算$D_2'=h(D_1\oplus T_2)$，验证$D_2'$是否与原值$D_2$相等，验证$\mathrm{Cert_{AIK}}$，即计算$I'=h(\mathrm{Cert_{AIK}})$并与原值比较是否相等。若以上验证都通过，则用户$U$确定服务器$S$的身份。

用户U验证服务器平台的完整性，以确保服务器系统配置信息是否符合安全策略，即判断服务器

状态是否可信。首先，利用AIK证书$\mathrm{Cert_{AIK}}$中服务器的AIK公钥$\mathrm{AIK_{pub}}$对Q值进行解密，得到服务器平台PCR_S值和$h(K_S,N_1)$，可再次验证K_S和N_1的正确性。接着，利用L中的存储值重新计算$\mathrm{PCR}'_S = \mathrm{SHA1}(\mathrm{PCR}_0 \| \mathrm{PCR}_1 \| \cdots \| \mathrm{PCR}_N)$，验证$\mathrm{PCR}'_S$与$\mathrm{PCR}_S$是否一致，若一致，服务器平台完整性获得验证。随后，用户U利用收到的服务器S的密钥计算双方会话密钥$K_{US}=(K_S)^a=(g^b)^a \bmod p$。

4) 服务器S验证了用户U的合法身份，同时用户U验证了服务器S的合法身份，且确认了服务器S的平台完整性，服务器接受用户的合法接入请求并向其提供服务，交互数据由密钥K_{US}加密保护。

3.3　认证更新阶段

认证更新阶段包括用户对口令的更换和服务器对平台证书的更新。

1) 用户口令更换。用户可以方便地对口令进行更换，不需要与服务器在线交互。其过程如下：用户选择新的口令PW′，计算$B_1=\mathrm{PID} \oplus h(\mathrm{PW}')$并在智能卡里用$B_1$将$B$替换。用户再次登录服务器时，可利用新口令和$N_1$值生成新的服务请求消息。

2) 服务器平台证书更新。可信计算环境下，TPM会成为攻击者的攻击对象，一旦被攻陷，平台的可信性将无法保证。服务器的更新主要是对平台AIK证书的更新，通过权威的可信第3方如管理服务器，公告已被攻陷的TPM，用户在注册或登录认证之前查询管理服务器，获取该服务器新的平台证书。具体方法如下：服务器利用新的平台证书$\mathrm{Cert}'_{\mathrm{AIK}}$替换旧的平台证书，重新计算$I=h(\mathrm{Cert}'_{\mathrm{AIK}})$提交给管理服务器并通知用户，完成对$I$的更新。

4　方案分析

4.1　安全目标实现

本文方案提供了用户与服务器间的双向认证，允许用户自由地更换口令，且不需要与服务器进行在线交互；允许服务器对平台证书的及时更新，满足G1、G4和G7。用户以匿名身份PID请求登录，认证过程中服务器S和用户U利用已知的参数p、g，通过DH密钥交换协议完成双方会话密钥K_{US}的协商且具有前项保密性，满足G3和G5。方案对其他安全目标的满足情况分析如下：

1) 注册阶段，用户U提交ID和h(PW)给服务器S，其中PW由用户选择，消息中不包含明文形式的PW，且$h(\ )$具有强单向性；在登录认证阶段，通过对C的计算，用户没有直接传送口令明文PW或h(PW)；在口令更换阶段，用户自主选择新的口令PW′，在不需要服务器的参与下，用B_1替换B完成对口令的更换。整个过程中服务器管理员都不能获得用户的口令明文PW，即用户口令不会直接泄露给服务器管理员，满足G2。

2) 登录认证阶段，用户U验证服务器身份的同时，验证服务器的平台信息Q、L、$\mathrm{Cert_{AIK}}$，其中L和Q中的PCR_S值是服务器的TPM，由可信根度量开始计算所得，代表了服务器平台完整性，Q值经过AIK签名与$\mathrm{Cert_{AIK}}$一起代表了服务器平台身份，对它们的正确验证证明服务器平台的可信性，满足G6。

4.2　抵抗常见攻击

1) 在该方案中，用户需要提供正确的ID和口令PW，并通过智能卡的合法性验证后，才可以向服务器提出访问请求；若攻击者首先不能通过智能卡的验证，也就不能向服务器发起拒绝服务攻击。方案可以抵抗拒绝服务攻击，满足SR1。在登录认证阶段，用户U向服务器发送的消息中包含时间戳T_1，时间戳的采用可以有效地防范消息重放攻击，满足SR2。

2) 口令猜测攻击包括在线口令猜测攻击和离线口令猜测攻击。用户使用智能卡时，需要提交正确的ID和PW，攻击者只有成功猜测ID和PW，才能假冒合法用户。针对本文方案的在线口令猜测攻击可以通过限制用户单位时间段内的登录次数来阻止。用户在网络中传输的消息中不包含口令PW的明文形式，攻击者只能截获用户与服务器交互过程中的部分数据并保存后，发动离线猜测攻击。在注册阶段，服务器发给用户的签发信息是经过安全信道传输的，可以阻止攻击者对信息的非法截获。假设攻击者截获了图2的步骤2)的消息PID、C、T_1，其中$\mathrm{PID}=h(x,\mathrm{ID})$，$C=h(B \oplus h(\mathrm{PW}) \| N_0 \oplus T_1)$，更进一步有$C=h(\mathrm{PID} \| h(\mathrm{PW}) \| N_0 \oplus T_1)$，PID中包含服务器的秘密值$x$，消息中没有包含口令信息，$N_0$为注册阶段服务器通过安全信道签发给用户的秘密值，因此攻击者无法通过所截获的消息猜测出用户的口令信息，可以抵御攻击者对用户口令的离线猜测，满足SR3。

3) 在并行会话攻击中，由于不知道用户的口令PW，攻击者想要伪装成合法用户，同样需要利用用户和服务器之间通信时遗漏的信息伪造合法用户的登录消息。攻击者从交互的会话消息中不能获得关于用户口令PW的任何信息，只能利用在用户登录认证过程中窃听到的消息产生和伪造合法的登录认证信息。图2的步骤2)中，用户发送给服务器的消息中

包含K_U和时间戳T_1；步骤4)中，服务器回复给用户的消息中包含K_S、Q和时间戳T_2及秘密值N_1，K_U和K_S提供双方进行会话密钥协商，消息Q是服务器对平台信息PCR和$h(K_S, N_1)$的AIK签名。该签名不可伪造，使得攻击者不能利用截获到的消息完成对另一方的回放，可以有效地防范并行会话攻击。另外，时间戳的使用加强了对该种攻击的防范。因此，该方案可以抵抗并行会话攻击，满足SR4。

4) 如果攻击者伪装成合法用户登录系统，在用户接入终端设备的登录阶段，攻击者不能提供正确的ID和PW，伪装攻击失败。假设攻击者截获了图2的步骤2)中的全部消息，并通过重放伪装合法用户，攻击者猜测及计算C值，即$C_g=h(\text{PID}\quad N_0' \oplus I \oplus T_1)$，其中$I$为攻击者提前已知，$N_0'$为攻击者对$N_0$的猜测。显然，攻击者的猜测值$C_g$无法通过步骤3)中对$C$的验证，伪装攻击失败。假设攻击者具有强计算能力，并通过离线字典攻击成功地猜测了N_0，此时攻击者可以提供正确地C值；但是，由于攻击者不知道用户U的秘密值a，不能在后续步骤中与服务器正确的协商会话密钥K_{US}，伪装攻击失败。假设攻击者截获了图2的步骤4)的消息，并通过重放伪装服务器，同样由于攻击者不知道服务器S的秘密值b，不能在后续步骤中完成与用户U的会话密钥协商，伪装攻击失败。因此，该方案可以抵抗伪装攻击，满足SR5。

5) 服务器不需要存储用户口令和验证表，服务器掌握着秘密值x，除了用户自己，其他人不能修改用户口令PW，该特性可阻止验证者偷窃攻击和修改攻击。在注册阶段，服务器管理员可以对用户的口令信息h(PW)进行离线字典猜测以推测用户口令PW。方案无法阻止该种形式的攻击，但一般情况下服务器会把用户注册信息加密保护，除服务器管理员外的其他内部人员均不能轻易获知用户注册信息。在后阶段的通信中，PW没有直接参与运算。因此，内部人员都不能得到用户口令PW，无法冒充合法用户U登录服务器。该方案可以防范内部攻击，满足SR6和SR7。

6) 可信计算环境下，存在一种针对远程证明协议的攻击即平台假冒攻击[16]。假设攻击者控制着一台可信服务器和一台恶意服务器，攻击者可以将这两台服务器联合起来发起对用户的假冒攻击，即将恶意服务器假冒成可信服务器从而欺骗用户。该案中，在服务器对用户终端的远程证明过程中，时间戳T_2的采用使得攻击者不能利用恶意服务器重放可信服务器回复给用户的消息。同时，在用户与服务器进行会话密钥协商过程中，利用AIK私钥对K_S和N_1的散列值进行签名，而攻击者不掌握服务器平台的AIK私钥AIK_{priv}，因此无法完成签名。该方案有效地防止了攻击者对服务器平台信息的假冒，可以防范平台假冒攻击，满足SR8。

4.3 性能分析

1) 安全性能。在达到安全目标与抵抗常见攻击方面，该方案与其他智能卡口令认证方案进行对比分析，结果如表2和表3所示。其中，Y表示达到或满足，N表示未达到或不满足，“—”表示不涉及。

表2 安全目标分析

	G1	G2	G3	G4	G5	G6	G7
文献[2]	Y	Y	N	Y	N	N	—
文献[3]	Y	Y	N	Y	Y	N	—
文献[4]	Y	Y	Y	Y	N	N	—
文献[5]	Y	Y	Y	Y	N	N	—
文献[6]	Y	Y	Y	Y	Y	N	—
文献[7]	N	Y	Y	Y	Y	N	—
本文的方案	Y	Y	Y	Y	Y	Y	Y

表3 抵抗常见攻击

	SR1	SR2	SR3	SR4	SR5	SR6	SR7	SR8
文献[2]	Y	Y	Y	N	Y	N	Y	N
文献[3]	Y	Y	Y	N	Y	Y	Y	N
文献[4]	N	Y	Y	N	Y	Y	Y	N
文献[5]	Y	Y	Y	N	Y	Y	Y	N
文献[6]	Y	Y	Y	N	Y	Y	Y	N
文献[7]	Y	Y	Y	Y	Y	Y	Y	N
本文的方案	Y	Y	Y	Y	Y	Y	Y	Y

本文方案除达到了传统智能卡口令认证方案的安全目标之外，还增加了对服务器平台的可信性验证，增强了方案的安全性能和对攻击的抵抗能力，能够更好地保障智能卡用户免受恶意服务器的潜在危害。从表2数据中可以看出，与已有方案比较，本文方案能够达到更多的安全目标。从表3数据中可以看出，本文方案在抵抗常见的安全攻击方面也具有明显的优势。

2) 计算性能。方案的计算时间复杂度适量，满足可信计算环境的认证需求。给出计算时间符号如下，t_{h}表示执行一次散列运算的时间，t_{xor}表示执行一次异或运算的时间，t_{ek}表示执行一次对称加密和解密操作的时间，t_{exp}表示执行一次模指数运算的时间，t_{sig}表示执行一次签名运算的时间，t_{pk}表示执行一次公钥加解密运算的时间，t_{PCR}表示计算平台PCR值的时间，t_{log}表示平台安全度量日志的加载时间。

分析可知，本文方案总的计算时间复杂性为$17t_{\text{h}}+19t_{\text{xor}}+4t_{\text{exp}}+1t_{\text{sig}}+1t_{\text{pk}}+2t_{\text{PCR}}+1t_{\text{Log}}$，其中，注册

阶段$3t_h+2t_{xor}$，登录认证阶段$12t_h+15t_{xor}+4t_{exp}+1t_{sig}+1t_{pk}+2t_{PCR}+1t_{Log}$，更新阶段$2t_h+2t_{xor}$。在该方案中，服务器的TPM芯片作为独立的计算单元可完成部分计算。分析可知，由CPU完成的计算量为$17t_h+19t_{xor}+4t_{exp}+1t_{pk}+1t_{PCR}$，由TPM完成的计算量为$1t_{sig}+1t_{PCR}+1t_{Log}$，其中$t_{PCR}$和$t_{Log}$可以由TPM通过预计算取得，在时间复杂度上对方案不产生影响。

与其他已有方案相比，在对服务器的可信性进行验证时，用户终端增加的计算时间为$1t_{pk}+1t_h+1t_{PCR}$，其中PCR值的验证只需若干次散列运算，所增加的时间复杂度不影响用户平台的性能和方案的整体性能。$1t_{pk}$用于完成对Q的解密，Q值是对PCR和$h(K_S,N_1)$的AIK签名，其中PCR长度为160 bit，$h(K_S,N_1)$一般不超过256 bit，对它们进行加解密所需时间在可允许范围内，增加的时间复杂度提供了对服务器平台的可信验证和对方案安全性的增强。

5 结　论

本文提出一种新的可信计算环境下的智能卡口令认证方案，提供服务器与用户相互身份认证的同时，验证服务器平台的可信性。该方案满足建议的设计目标，与已有方案比较安全性更高，安全功能更全面，可为用户提供更安全的服务。但是，该方案的使用需要服务器处在可信计算环境中，因此，将进一步关注可信服务器与普通服务器共存环境中的可信认证问题及可信服务器环境的构建问题，如利用可信虚拟机，实现可信服务器的方法等。

参　考　文　献

[1] LAMPORT L. Password authentication with insecure communication[J]. Communications of the ACM, 1981, 24: 770-772.

[2] CHIEN H Y, JAN J K, TSENG Y M. An efficient and practical solution to remote authentication: smart card[J]. Computers & Security, 2002, 21(4): 372-375.

[3] KU W C, CHEN S M. Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards[J]. IEEE Trans on Consumer Electronics, 2004, 50(1): 204-207.

[4] YOON E J, YOO K Y. Drawbacks of Liao et al's password authentication scheme[C]//International Conference on Next Generation Web Services Practices. [S.l.]: [s.n.], 2006.

[5] LIAO I E, LEE C C, HWANG M S. A password authentication scheme over insecure networks[J]. Journal of Computer and System Sciences, 2006, 72(4): 727-740.

[6] YANG G, WONG D S, WANG H, et al. Two-factor mutual authentication based on smart cards and passwords[J]. Journal of Computer and System Sciences, 2008, 74(7): 1160-1172.

[7] KUMAR M. A secure remote user authentication scheme with smart cards[EB/OL]. [2009-03-02]. http://eprint.iacr.org/2008/331.

[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: [s.n.], 2004.

[9] Trusted Computing Group. TCG specification architecture overview[EB/OL]. [2009-03-02]. http://www.Trusted computing group. org.

[10] REHBOCKA S, HUNT R. Trustworthy clients: Extending TNC to web-based environments[J]. Computer Communications, 2009, 32(5): 1006-1013.

[11] SHEN C X, ZHANG H G, FENG D G, et al. Survey of information security[J]. Science in China (Information Science), 2007, 50(3): 273-298.

[12] 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.
ZHANG Huan-guo, LUO Jie, JIN Gang, et al. Development of trusted computing research[J]. Journal of Wuhan University (Natural Science Edition), 2006, 52(5): 513-518.

[13] Trusted Computing Group. TPM main specifications —Part 1 design principles[EB/OL]. [2009-03-02]. http://www.trustedcomputinggroup.org.

[14] CHUN L L, HWANG T L. A password authentication scheme with secure password updating[J]. Computers & Security, 2003, 22(1): 68-72.

[15] TSAI C S, LEE C C, HWANG M S. Password authentication schemes: current status and key issues[J]. International Journal of Network Security, 2006, 3(2): 101-115.

[16] STUMPF F, TAFRESCHI O, RODER P, et al. A robust integrity reporting protocol for remote attestation [C]//Proceedings of the Second Workshop on Advances in Trusted Computing (WATC'06 Fall). Tokyo, Japan: [s.n.], 2006.

编　辑　税　红