软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(5):1260−1271 [doi: 10.3724/SP.J.1001.2012.04052]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

无线移动网络跨可信域的直接匿名证明方案*

杨 力[1,2+], 马建峰[1,2], 姜 奇[1]

[1](西安电子科技大学 计算机学院,陕西 西安 710071)

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

Direct Anonymous Attestation Scheme in Cross Trusted Domain for Wireless Mobile Networks

YANG Li[1,2+], MA Jiang-Feng[1,2], JIANG Qi[1]

[1](School of Computer Science and Technology, Xidian University, Xi'an 710071, China)

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

+ Corresponding author: E-mail: xdyangli@gmail.com

Yang L, Ma JF, Jiang Q. Direct anonymous attestation scheme in cross trusted domain for wireless mobile networks. *Journal of Software,* 2012,23(5):1260−1271. http://www.jos.org.cn/1000-9825/4052.htm

Abstract: Based on delegation of trusted relationship, a ross-domain direct anonymous attestation scheme for wireless mobile networks is proposed. A proxy signature is used for delegation among domains, and the direct anonymous attestation (DAA) method is used for mobile terminal authentication when a terminal roaming to another domain. The remote attestation system is security-enhanced by a key agreement. The authentication protocol is analyzed in Canetti-Krawczyk (CK) model, and the results show that the protocol is secure. Further analysis shows that this proposal can resist reply attacks and platform masquerade attacks; the scheme is effective and suitable for the mobile trusted computing platforms.

Key words: direct anonymous attestation; cross trusted domain; delegation; proxy signature; authentication

摘 要: 基于信任委托的思想,提出一种移动环境下的跨可信域的直接匿名(direct anonymous attestation,简称DAA)证明方案,采用代理签名技术和直接匿名证明方法,实现对移动终端在多可信域之间漫游时的可信计算平台认证,并在认证过程中协商会话密钥,增强了远程证明体系的安全性.利用 Canetti-Krawczyk(CK)模型对方案的认证协议的认证安全性和匿名安全性进行了形式化分析和证明.分析表明,该方案能够抵抗平台伪装攻击和重放攻击,其性能适用于无线网络环境.

关键词: 直接匿名证明;跨可信域;信任委托;代理签名;认证

中图法分类号: TP393 **文献标识码**: A

可信计算的概念与技术已被广泛接受,应用于包括台式机、笔记本及智能手机等多种设备中,以所嵌入的可信平台模块 TPM(trusted platform module)[1]为核心,为用户和平台提供安全保障.可信平台模块 TPM 具有远程证明的能力,能够响应远程验证方的请求,证明平台身份和平台完整性等可信属性.TCG(trusted computing

* 基金项目: 国家自然科学基金-广东联合基金(U1135002); 国家自然科学基金(61072066, 61100230, 61100233, 61173135); 国家科技部重大专项(2011ZX03005-002); 中央高校基本科研业务费项目(JY10000903001, K50510030003)

收稿时间: 2010-10-12; 定稿时间: 2011-04-28

group)要求在远程证明过程中有效地保护平台身份信息的隐私性,即 TPM 向验证方进行远程证明时不能暴露身份信息,也不能由验证方将多次证明信息进行关联以推断身份信息.

为了解决远程证明时平台隐私信息的保护问题,TCG 先后采用引入可信第三方隐私 CA(privacy-CA)[2]的方法和直接匿名证明(direct anonymous attestation,简称 DAA)[3]的方法.Privacy-CA 方法是 TPM 规范 V1.1b 中所采用的方法,在证明系统中引入可信第三方 Privacy-CA,Privacy-CA 作为权威的证书机构向 TPM 颁发身份证书,当 TPM 向远程验证方证明身份时出示该证书,验证方将证书返回给 Privacy-CA,并与其一同验证 TPM 的合法性.由于每次进行证明时都需要 Privacy-CA 的参与,因此它会成为整个系统的性能瓶颈和安全瓶颈.

为了弥补此缺陷,TPM 规范 V1.2 中采纳了 Brickell 等人提出的直接匿名证明方法,简称为 BCC 方案.BCC 方案基于 CL 群签名[4]和知识证明方法[5]构建,使得 TPM 在向远程验证方证明身份的同时不泄露隐私信息.在 BCC 方案中,TPM 选择私有的秘密值,通过一个安全的两方协议获得 DAA 证书,即 DAA 颁发者(DAA issuer)在其上的 CL 签名.当 TPM 向远程验证方证明身份时,利用 DAA 证书和秘密值对消息进行 DAA 签名,验证者确认此 DAA 签名,并相信 TPM 通过知识证明获得了匿名签名.

但是,TCG 规范所给出的方案仅提供了单可信域内的对 TPM 的认证,且 BCC 方案的各参与方如 DAA Issuer、验证者、TPM 及平台必须位于同一可信域,不能实现跨可信域的认证,限制了其在移动计算平台主机 Host,如笔记本、智能手机等中的应用.此外,各个不同的 TPM 厂商都设置有 DAA 颁发者,形成相对独立的可信域,不同的可信域有不同的 DAA 颁发者,不同可信域的参与者信任不同的 DAA Issuer.而在移动环境下,由于应用的需要,用户经常在家乡域与外地域之间进行漫游切换,存在漫游认证问题[6](IETF mobile IP 技术规范).一般情况下,家乡域与外地域分属不同的可信域,它们可能信任不同的 TPM 厂商指定的 DAA Issuer,跨可信域认证问题比较突出.

TCG 规范中所采用的 BCC 方案既不适用于移动环境,也不能满足跨域安全认证.在 BCC 方案中,TPM 及所在平台与验证者交互复杂且运算量大,不能应用于计算资源有限的嵌入式设备.He 等人提出了能够满足嵌入式系统的直接匿名证明方案[7],以下简称 DAA-ED 方案.该方案基于 CM 群签名方案[8]设计,缩减了 TPM 及平台与验证方的交互复杂度,简化了协议运算量,解决了资源受限环境下的 TPM 直接匿名证明问题,适用于移动计算平台等资源受限系统.但在实际用于远程证明时,该方案存在安全缺陷,不能防范平台伪装攻击和重放攻击,且不能实现跨可信域认证.基于 BCC 方案,陈小峰等人提出了基于签证证书的跨信任域的 DAA 方案[9].该跨域方案基于公钥证书设计,认证交互频繁,且需要相互证书验证,不适用于无线网络环境.Lin 等人提出 Mobile IP 下的 TPM 认证方法[10],可以实现跨认证域的 TPM 认证,但方案中引入 DAA CA 和 PKI 机制,此 DAA CA 会成为系统的性能瓶颈和安全瓶颈,存在安全隐患,且方案性能不佳.

为了解决无线移动网络环境下的可信计算平台跨可信域认证问题,本文基于代理签名技术所提供的信任委托机制和 DAA-ED 方案,提出移动环境下的跨可信域的直接匿名证明方案.方案中,基于代理签名的委托机制,由 DAA 颁发者利用代理签名委托可信计算平台进行域认证,采用 DAA-ED 方案所提供的 CM 群签名方法进行可信终端平台身份的直接匿名证明,给出了可信计算平台在漫游至其他可信域时,由非本地可信域验证者所进行的可信认证协议.利用 Canetti-Krawczyk(CK)模型分析了该认证协议的认证安全性与匿名安全性,结果表明,所设计的协议满足可证明安全性.进一步的实验测试与分析表明,本方案能够抵抗平台伪装攻击和重放攻击,且运算性能适用于无线网络及 Mobile IP 网络中.

本文第 1 节介绍本文的背景知识.第 2 节给出本文的跨可信域认证方案.第 3 节给出方案的认证协议并采用 CK 模型证明其安全性.第 4 节分析方案的性能,并给出方案的实验验证.第 5 节对全文进行总结.

1 背景知识

1.1 基本定义

定义 1(强 RSA 假设(strong RSA assumption)). 设 n 是 RSA 模数, $z \in Z_n^*$ 是随机元素,Flexible RSA 问题是

指找到 $e>1$ 和 $u\in Z_n^*$,使其满足 $u^e\equiv z \bmod n$.强 RSA 假设是指不存在多项式时间算法能够以不可忽略的概率解决 Flexible RSA 问题.

定义 2(DDH 假设(decisional diffie-hellman assumption)). 设 k 为安全参数,p,q 为素数,其中,q 的长度为 k 比特,且 $q|p-1$,g 是阶为 q 的群 Z_p^* 中元素,x,y,z 是从 Z_p 中均匀选择的,则对于任何的多项式时间算法,$Q_0=\{\langle p,g,g^x,g^y,g^{xy}\rangle:x,y\leftarrow^R Z_p\}$与 $Q_1=\{\langle p,g,g^x,g^y,g^z\rangle:x,y\leftarrow^R Z_p\}$的概率分布是计算不可区分的.

定义 3(CDH 假设(computational diffie-hellman assumption)). 设 k 为安全参数,p,q 为素数,其中,q 的长度为 k 比特,且 $q|p-1$,g 是阶为 q 的群 Z_p^* 中元素,x,y 是从 Z_p 中均匀选择的,则对于任何的多项式时间算法 A,$Pr[A(p,q,g,g^x,g^y)=g^{xy}]$是可忽略的.

1.2 代理签名

定义 4(代理签名)[11]. 所谓代理签名就是指在一个代理签名方案中,一个被指定的代理签名者可以代表原始签名者生成有效的签名,利用代理签名可以实现信任的委托关系.

为了更好地理解代理签名的概念,下面介绍 Mambo,Usuda 和 Okamoto 的代理签名方案[12]如下(以下简称 MUO 方案),并对其安全特性进行简单的说明.

设 p 是一个大素数,q 是 $p-1$ 的一个素因子,$g\in Z_p^*$ 是一个 q 阶生成元,参数设置全文通用.原始签名者的密钥是 $s\in_R Z_p$,相应的公钥是 $V=g^s \bmod p$.M-U-O 方案使用如下协议:

(1) 委托过程:
   (a) 代理密钥生成:原始签名者随机选择 $k\in_R Z_p$,并计算 $K=g^k \bmod p,\sigma=s+kK \bmod q$.
   (b) 代理密钥发送:原始签名者将(σ,K)通过安全信道发送给代理签名者.
   (c) 代理密钥验证:代理签名者检验等式 $g^\sigma=VK^K$ 是否成立:如果该等式成立,则(σ,K)是一个有效的代理密钥;否则拒绝接受该密钥,并要求原始签名者重新发送一个新的代理密钥,或者停止协议.

(2) 代理签名生成:当代理签名者代表原始签名者在文件 m 上签名时,它使用σ代替 s 执行普通的签名运算.于是,由代理签名者声称的关于 m 的代理签名是$(m,sig_\sigma(m),K)$.其中,$sig_\sigma(m)$表示文件 m 用密钥σ所生成的普通签名.

(3) 代理签名验证:验证者在验证代理签名时首先计算 $V'=VK^K \bmod p$,然后用 V'代替 V,使用与验证普通签名相同的验证运算就可以验证代理签名的有效性.

该方案满足可验证性、不可伪造性、可区分性、不可抵赖性、密钥依赖性、可注销性等基本安全性质.利用代理签名可以实现 DAA Issuer 签名权的委托,免去复杂的公钥证书或身份证书的签署与颁发的操作,满足移动环境跨可信域的需要.

1.3 CK模型

Bellare,Canetti 和 Krawczyk 于 1998 年引入模块化思想来分析安全协议[13],为利用可重用的模块来构造新的可证安全的密钥交换协议提供了理论基础.Canetti 和 Krawczyk 对该模型的方法进行了扩展[14],称为 Canetti-Krawczyk 模型,简称 CK 模型.CK 模型给出了会话密钥安全的定义和利用该定义分析和设计安全协议的模块化方法,CK 模型采用不可区分性方法定义安全,即若在允许的攻击能力下,攻击者不能区分协议产生的会话密钥和一个独立的随机数,则认为该协议是安全的.

在 CK 模型中定义了两种攻击模型,即理想模型 AM 和现实模型 UM[14].AM 是认证的链路模型,在该模型中,攻击者是被动的,能够调用协议运行、攻陷协议参与者(party corruption)、查询会话密钥(session key query)、暴露会话密钥(session key reveal)以及测试会话密钥(test session query).但是只能忠实地传递同一消息 1 次,不能伪造、篡改或重放来自未被攻陷的参与者的消息.UM 模型是未认证链路模型,攻击者除了能够执行 AM 模型中的所有攻击以外,还可以伪造、篡改和重放消息.

认证器是模块化方法中一个非常重要的机制,它可以确保将 AM 中安全的协议转化为 UM 中安全的协议.

定义 5[13]. 设π和π'是 n 方消息驱动协议,π运行在 AM 中,π'运行在 UM 中.如果对于任何 UM 敌手 U,存在一个 AM 敌手 A 使得 $AUTH_{A,\pi}$和 $UNAUTH_{A,\pi'}$是计算不可区分的,则称π'在 UM 中仿真π.

定义 6[13]. 编译器 C 是一种算法,其输入是协议的描述,输出也是协议的描述.若一个编译器 C 对于任何的协议π,协议 $C(\pi)$在 UM 中仿真π,则这个编译器称为认证器.

定理 1[13]. 假设λ是一个 MT-认证器,也就是说,λ在 UM 中仿真了简单消息传输(MT)协议,假设 C_λ是在λ的基础上定义的一个编译器,那么可以说 C_λ是一个认证器.

MT 协议将一条消息由一个参与者发送给另一个参与者.一个协议的认证器 C_λ是若干个 MT 认证器λ的组合.如果 AM 中协议只有 1 个消息流,那么一个 MT 认证器λ就可以作为认证器 C_λ;否则,为 AM 中协议的每个消息流进行仿真的 MT 认证器λ组合在一起才能作为认证器 C_λ.

CK 模型首先在理想模型中证明协议的安全性,再利用认证器将协议转换到现实模型中.基于 CK 模型设计认证和密钥协商(AKE)协议的基本方法一般可以分为以下 4 步[15]:

(1) 设计基本协议,并证明在 AM 下是安全的;

(2) 构造认证器,并证明是一个有效的认证器;

(3) 通过认证器将基本协议转换成 UM 下的安全协议;

(4) 进行必要的重新排序、重用消息组合以优化结果协议.

2 移动环境下跨可信域 DAA 方案

给出本文的跨可信域的系统模型如图 1 所示.其中,TD_A为可信域 A;TD_B为可信域 B;$Issuer_A$为可信域 TD_A的 DAA 证书颁发者,简记为 IS_A;$Issuer_B$为可信域 TD_B的 DAA 证书颁发者,简记为 IS_B;$Host_A/TPM_A$为可信域 TD_A中的可信计算平台,简记为 HT_A;$Host_B/TPM_B$为可信域中的可信计算平台,简记为 HT_B;V_A和 V_B分别为各自可信域中的验证者.在本模型中,HT_A在本地可信域 TD_A完成加入操作.一般而言,加入操作在安全通道中进行,其安全性可以得到保证.当 TD_A中的 HT_A漫游到另外的可信域 TD_B时,由 TD_B中的验证者 V_B对其进行可信认证.

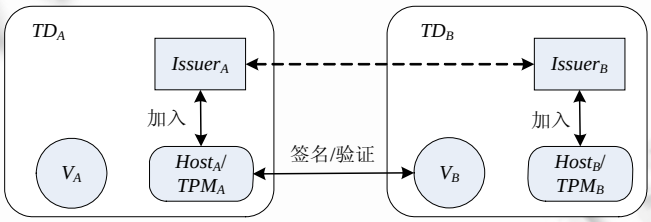

Fig.1 Cross trusted domain model

图 1 跨可信域模型

2.1 系统参数设定

DAA Issuer 选择安全参数β,以如下方式产生系统参数[7,11]:

(1) n,v,g_1,g_2.n 是一个 special RSA 模数,$n=p_1q_1$.这里,p_1 和 q_1 至少是β bits 的长度(因此 $p_1,q_1>2^\beta$),且 $p_1=2p'+1,q_1=2q'+1$,其中,p',q'均为素数.g_1是循环群 QR_n的随机生成元.选择大素数 p_2 和 q_2,且 $q_2|p_2-1$,$g_2 \in Z_{p_2}^*$ 是一个 q_2 阶生成元.选择原始签名密钥为 $x \in_R Z_{p_2-1}$,计算公钥为 $V = g_2^x \bmod p_2$ .n,V,g_1,g_2 是公开参数,通过安全的方式公布给要加入的 TPM,p_1,q_1,x 是秘密值并由 DAA Issuer 秘密保存.

(2) X,Y,α,l_c,l_s,l_b.X,Y 均为整数常量,α,l_c,l_s,l_b 是大于 1 的安全参数,满足 $Y > 2^{\alpha(l_c+l_b)+1}, X > 2Y + 2^{\alpha(l_s+l_c)+2}$.

(3) H_1,H_2.这是两个抗强碰撞的单向函数(散列函数),满足 $H_1:\{0,1\}^* \to Z_n^*, H_2:\{0,1\}^* \to \{0,1\}^{l_c}$.

2.2 加入过程

(1) 代理密钥生成及传送.Issuer 产生随机数 $k \in_R Z_{p_2-1}$, 计算 $K = g_2^k \bmod p_2$, 计算$\sigma=x+kK \bmod (p_2-1)$,计算

$\{\sigma,K\}_{PK_{EK}}$.其中,PK_{EK}为 TPM 的 EK 公钥,并发送$\{\sigma,K\}_{PK_{EK}}$给 TPM.

(2) 代理密钥验证.TPM 利用 EK 私钥解密恢复出(σ,K),验证 $g_2^{\sigma}=?VK^K \bmod p_2$ 是否成立:如果成立,则(σ,K)是有效的代理密钥;否则拒绝该密钥,并要求原始签名者重新发送合法的签名密钥,或者也可以终止协议.

(3) 加入 Issuer 群.采用与 CM 群签名中相同的加入协议,TPM 获得它的群成员身份证书即密钥对(E,s).其中,$s\in(X,X+2^{l_s})$,且 s 为素数,并满足 $E^s\equiv g_1 \bmod n$.s 为 TPM 的私钥,被 TPM 秘密保存.E 可以被 Issuer 知道,Issuer 用知识签名的方法证明(E,s)的正确性,更详细的过程参见文献[7].

2.3 认证过程

认证过程包括可信计算平台(host\TPM)对消息进行签名,以及验证者(verifier)对签名的验证,认证的目的在于确认可信计算平台的 TPM 是来自正确的 DAA Issuer 可信域,且是该可信域中合法的 TPM.在可信计算的远程证明中,TPM 的身份即代表了平台和 Host 的身份.因此,本文着重讨论对 TPM 的认证,这样也可以简化协议的设计.

2.3.1 消息签名

(1) 首先完成对 Issuer 的身份信息、公钥信息等的代理签名.

TPM 计算 $m_p=H_2(bsn_I,V)$,利用σ替代 x 执行普通的签名操作,选择随机数 $r_t\in_R Z_{p_I-1}$,计算 $R=g_2^{r_t} \bmod p_2$,计算 $S_t=r_t^{-1}(m_p-\sigma R) \bmod (p_2-1)$.其中,$bsn_I$为 Issuer 的长期名.

(2) 对于消息 M,TPM 执行以下步骤完成 DAA 签名:

(a) Host 产生随机数 $b\in_R[Y-2^{l_b},Y+2^{l_b}]$,TPM 产生随机数 $t_1\in_R \pm\{0,1\}^{\alpha(l_s+l_c)}$,$t_2\in_R \pm\{0,1\}^{\alpha(l_b+l_c)}$.

(b) Host 计算 $T_1=E^b \bmod n=g_1^{s^{-1}b} \bmod n$,$T_2=g_1^b \bmod n$.

TPM 计算 $d_1=T_1^{t_1} \bmod n$,Host 计算 $d_2=g_1^{t_2} \bmod n$.

(c) 随后,Host 计算 $c=H_2(g_1\|T_1\|T_2\|d_1\|d_2\|m_p\|R\|S_t\|K\|M)$;

TPM 计算 $w_1=t_1-c(s-X)$,Host 计算 $w_2=t_2-c(b-Y)$.

(3) TPM 利用验证者的公钥 PK_V 对消息(m_p,R,S_t,K)进行加密,即计算 $Enc_{PK_V}(m_p,R,S_t,K)$,发送消息$(Enc_{PK_V}(m_p,R,S_t,K),c,w_1,w_2,T_1,T_2)$给验证者 Verifier.

2.3.2 消息验证

(1) 收到可信计算平台发送来的消息后,验证者 Verifier 首先验证 TPM/Host 所提供的 Issuer 的信息的正确性.由于 bsn_I,V 是公开参数,因此假设 Verifier 已经知道了该 TPM 的可信域参数.

(a) 收到消息后,利用私钥 SK_V 对消息 $Enc_{PK_V}(m_p,R,S_t,K)$ 解密,得到(m_p,R,S_t,K).

(b) 验证 $m_p=H_1(bsn_I,V)$是否成立.

(c) 计算 $V'\equiv VK^K \bmod p_2$,计算 $g_2^{m_p}=R^{S_t}V' \bmod p_2$ 是否满足.

(d) Verifier 将已有的 Issuer 可信域信息与收到的信息相比较,不正确则终止协议.

(2) 然后验证签名的正确性.Verifier 利用收到的消息重新计算 c 值,即计算:

$$c'=H_2(g_1\|T_1\|T_2\|T_1^{w_1-cX}T_2^c\|g^{w_2-cY}T_2^c\|m_p\|R\|S_t\|K\|M).$$

当且仅当 $c=c'$, $w_1\in\pm\{0,1\}^{\alpha(l_s+l_c)+1}$, $w_2\in\pm\{0,1\}^{\alpha(l_b+l_c)+1}$ 同时成立时,接受此签名.

2.4 假冒TPM的检测

(1) 虽然 TPM 是防篡改的,但是在某些极端的情况下也可能被攻陷,其密钥可能泄露.因此,Verifier 应该能够识别来自假冒 TPM 的证明请求.为了做到这点,被攻陷的 TPM 的秘密值(EK,E,s)应在撤销列表中被公布.对于撤销列表中的密钥对(E,s),Verifier 检查 $T_1^s=?T_2 \bmod n$.如果此等式成立,则该请求来自被撤销的 TPM.随后,Verifier 向 DAA Issuer 提供该 TPM 的密钥对信息.

(2) 假冒的 Issuer 可信域信息也要被检测,即检测假冒的代理签名密钥对.在本方案中,如果 Issuer 在向 TPM 发送(σ,K)时将 K 与 TPM 的身份绑定在一起,当 Issuer 看到已被攻陷的 TPM 的消息时,可以通过 K 识别 TPM 的身份,同时注销该 TPM 拥有的代理签名密钥σ,就可以"广播"(此消息由 Issuer 签名)消息,宣布 K 不再有效,从而 TPM 生成的所有代理签名随之失效.该被攻陷的 TPM 同时被清除出 Issuer 可信域.同时,该消息被返回 Verifier 以更新撤销列表中的信息,(EK,E,s)被更新为(σ,K,EK,E,s).该消息既可以用来检测被攻陷的 TPM 可信域的信息,又可以用来检测被攻陷的 TPM 签名信息.

3 远程证明协议安全性证明

利用上述方案,构建如图 1 所示的面向应用、直接匿名、跨可信域的远程证明认证协议,并在 CK 模型下证明该认证协议的安全性.

3.1 认证安全性分析

3.1.1 AM 中的跨可信域 DAA 协议

给出 AM 中 SK 安全的跨可信域 DAA 协议如图 2 所示.

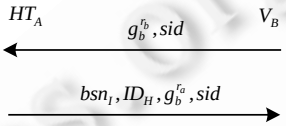

Fig.2 Authentication protocol in AM

图 2 AM 中的认证协议

HT_A 与 V_B 需要经过一轮消息交互实现会话密钥的协商,在 AM 中,由于敌手不能对消息进行伪造、篡改和重放,只能真实地转发合法参与者产生的消息,所以协议是安全的.该认证协议的简要过程如下:

(1) V_B 选择消息 K_B,sid 给 HT_A,其中,$K_B = g_v^{r_b} \bmod n_v$,$g_v,n_v$ 由 V_B 选定用于会话密钥协商,r_b 是 V_B 选择的秘密私钥,sid 是会话标识.

(2) 收到消息后,HT_A 进行相应的计算并发送消息 bsn_I,ID_H,K_A,sid 给 V_B,其中,$K_A = g_v^{r_a} \bmod n_v$,$r_a$ 是 HT_A 选择的秘密私钥.

(3) V_B 计算后返回确认消息 ACK,sid 给 HT_A.

在上述交互过程中,HT_A 与 V_B 基于两方的 DH 密钥交换协议来完成会话密钥的协商,基于 DDH 假设该协议已被 Canetti 和 Krawczyk[14]证明在 AM 中是 SK 安全的,因此本文所设计的 AM 中的跨可信域 DAA 协议也是 SK 安全的.

3.1.2 UM 中的跨可信域 DAA 认证协议

在 CK 模型中,需要仿真 AM 协议的每个消息流,所采用的 MT 认证器组合在一起就构成了完整的协议认证器.本文采用基于数字签名和随机数的 MT 认证器[13],如图 3 所示.

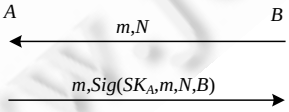

Fig.3 MT authenticator based on signature and random numbers

图 3 基于数字签名和随机数的 MT 认证器

采用基于数字签名和随机数的 MT 认证器与基于 MAC 的认证器一起仿真消息流,达到对 HT_A 和 V_B 的身份认证,完整的认证器由若干 MT 认证器组合而成.由于所采用的认证器是可证安全的,基于数字签名的 MT 认

证器的安全证明见文献[13],因此由定理 1 可知,所构造的认证器也是安全的.

将上述 MT 认证器应用于 AM 中协议的消息流仿真可得到 UM 中的跨可信域 DAA 协议.由于所构造的认证协议认证器是可证安全的,从而根据 CK 模型方法自动编译得到的 UM 中的认证协议也是可证安全的.然后应用文献[14]的方法优化 UM 中的协议,得到最终的认证协议(如图 4 所示),并且文献[14]在 CK 模型下已证明该优化过程不影响协议的安全性.因此,如图 4 所示的 UM 中认证协议是可证安全的.

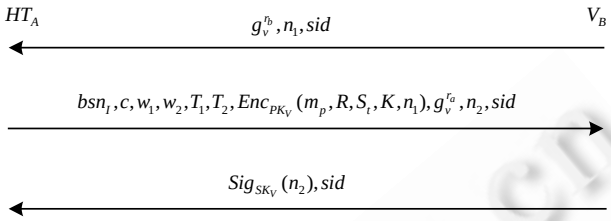

Fig.4 Authentication protocol in UM

图 4 UM 中的认证协议

UM 中的跨可信域 DAA 协议的认证过程解释如下:

(1) 验证者 V_B 选择秘密数 r_b 作为私钥,计算 $K_B = g_v^{r_b} \bmod n_v$,其中,$g_v$,$n_v$ 是验证者选定的公开参数,选择随机数 n_1,发送消息 K_B,n_1,sid 给可信平台 HT_A.

(2) 收到 V_B 的消息后,HT_A 选择秘密数 r_a,计算密钥 $K_A = g_v^{r_a} \bmod n_v$,计算会话密钥 $K_{AB} = (g_v^{r_b})^{r_a} \bmod n_v$.随后计算 m_p=H_2(bsn_I,V),利用σ代替 x 执行普通的签名操作,选择随机数 $r_t \in_R Z_{p_1-1}$,计算 $R = g_2^{r_t} \bmod p_2$,计算 $S_t = r_t^{-1}(m_p - \sigma R) \bmod (p_2 - 1)$,计算 $Enc_{PK_V}(m_p, R, S_t, K, n_1)$.

随后,HT_A 令 M=(K_A||n_1),选择随机数 n_2,计算相应的消息签名,其过程是:

- 产生随机数 $b \in_R [Y - 2^{l_b}, Y + 2^{l_b}]$,$t_1 \in_R \pm\{0,1\}^{\alpha(l_s + l_c)}$ 和随机数 $t_2 \in_R \pm\{0,1\}^{\alpha(l_b + l_c)}$.
- 并且计算 T_1=$E^b \bmod n$,$T_2 = g_1^b \bmod n$;计算 $d_1 = T_1^{t_1} \bmod n$,$d_2 = g_1^{t_2} \bmod n$.
- 最后计算 c=H_2(g_1||T_1||T_2||d_1||d_2||m_p||R||S_t||K||M),w_1=t_1−c(s−X),w_2=t_2−c(b−Y).
- 发送消息 $bsn_I, c, w_1, w_2, T_1, T_2, Enc_{PK_V}(m_p, R, S_t, K, n_1), g_v^{r_a}, n_2, sid$ 给验证者 V_B.

(3) V_B 收到消息并进行验证:首先,利用私钥 SK_V 对消息 $Enc_{PK_V}(m_p, R, S_t, K, n_1)$ 解密,得到(m_p,R,S_t,K,n_1),并验证代理签名消息的正确性,验证 n_1 是否正确,验证 m_p=H_1(bsn_I,V)是否成立,计算 $V' \equiv VK^K \bmod p_2$,$g_2^{m_p} = R^{S_t} V' \bmod p_2$ 是否满足.

然后验证 DAA 签名消息的正确性,利用收到的消息重新计算 c 值,即计算:

$$c' = H_2(g_1 \| T_1 \| T_2 \| T_1^{w_1 - cX} T_2^c \| g^{w_2 - cY} T_2^c \| m_p \| R \| S_t \| K \| M).$$

当且仅当 c=c',$w_1 \in \pm\{0,1\}^{\alpha(l_s + l_c)+1}$,$w_2 \in \pm\{0,1\}^{\alpha(l_b + l_c)+1}$ 同时成立时,验证者接受此签名.随后,利用私钥 SK_V 对 n_2 进行签名,即计算 $Sig_{SK_V}(n_2)$,最后发送消息 $Sig_{SK_V}(n_2), sid$ 给 HT_A,完成相互认证和密钥协商.

3.2 匿名安全性分析

3.2.1 匿名安全性定义

为了便于描述,设 l 为系统安全参数,$HT_A(l) = \{HT_{A1}, HT_{A2}, ..., HT_{AQ_1}(l)\}$ 为所有 HT_A 的集合,$HT_B(l)$=$\{HT_{B1}$, $HT_{B2}, \ldots, HT_{BQ_2}(l)\}$ 为所有 V_B 的集合,其中,$Q_1(l)$,$Q_2(l)$为多项式.HT_{Ai},V_{Bj} 是参与方的身份,并且 $1 \leqslant i \leqslant Q_1(l)$,$1 \leqslant j \leqslant Q_2(l)$.

在分析过程中,匿名性攻击者模型采用 UM 模型.为了分析协议的匿名性,参考文献[16]进行匿名游戏的设计.该游戏的执行者是仿真器 S,S 将敌手 A 作为子程序激活运行.该游戏详细过程如下:

(1) S 建立系统,其中的参与方为 $HT_A(l)$中的 HT_A 和 $V_B(l)$中的 V_B.

(2) S 运行 A 并回答 A 的所有询问.

(3) A 可以激活系统中的任意参与方和进行询问,从而在这些参与方之上运行认证协议.

(4) A 从所有的系统参与方中选择两个 $HT_A,HT_{Ai},HT_{Aj}\in HT_A(l)$和一个 $V_B,V_B\in V_B(l)$.

(5) A 向 S 发送测试询问,输入为(HT_{Ai},HT_{Aj},V_B).

(6) S 仿真认证协议的两个运行过程:一个的参与方是 HT_{Ai} 和 V_B,另一个的参与方是 HT_{Aj} 和 V_B.同时,S 更新每个参与方的状态信息.S 随机选择 $b\leftarrow^R\{0,1\}$,如果 b=0,则返回 HT_{Ai} 的仿真脚本给 A;否则,返回 HT_{Aj} 的仿真脚本.

(7) 接收到测试询问的响应后,A 还可以继续发起所有允许的攻击,以及激活参与方来运行协议.

(8) A 输出一个比特 b',作为对 b 的猜测,运行终止.

在上述游戏中,如果 HT_{Ai},HT_{Aj} 和 V_B 均未被攻陷,并且 A 输出了正确的比特 b',使得 $b'=b$,则称攻击者 A 获胜,攻击者 A 获胜的优势定义为 $Adv_{\pi,A}(l)=|Pr[A \text{ wins the game}]-1/2|$.

定义 7. 如果在安全参数足够大的情况下,对任意多项式时间攻击者 A,其优势 $Adv_{\pi,A}(l)$都是可忽略的,那么称协议满足匿名安全性,包括平台身份机密性与不可连接性.

3.2.2 匿名性和不可跟踪性分析

定理 2. 如果对称加密算法 $Enc()$是 CCA 安全的,并且 CDH 问题是困难的,那么 $Adv_{\pi,A}(l)$是可忽略的.

证明:如果协议不满足匿名性,也就是说,攻击者 A 能够以不可忽略 $v(l)$的优势获胜,那么我们可以构造攻击者 D,使得 D 能够以不可忽略的概率攻破 $Enc()$或破解 CDH 问题.

简单描述一下攻击者 D 的攻击过程:首先,D 适应性地选择密文以询问解密预言机.然后,D 选择两个不同的消息 msg_0 和 msg_1,并向游戏仿真者询问密文.仿真器随机选择 $b\leftarrow^R\{0,1\}$,并返回密文 $C=Enc_k(msg_b)$.接收到密文 C 后,D 适应性地选择除 C 之外的密文询问解密预言机,最后输出 b'作为对 b 的猜测.

现在构造该攻击者 D 来仿真游戏,其中,D 扮演 A 的仿真器:

(1) 首先,D 选择并创建 HT_A 集合 $HT_A(l)$和 V_B 集合 $V_B(l)$.然后,D 对 $HT_A(l)$中的 HT_A 和 $V_B(l)$中的 V_B 进行初始化,为每个 HT_A 和 V_B 分配随机选自集合$\{0,1\}^l$的共享密钥.

(2) D 将 A 作为子程序激活运行,回答 A 的所有询问,仿真协议运行中参与方激活的所有响应,并且将认证协议的输出消息返回给 A.

如果 A 在测试询问中未选择 V_B,D 随机选择 b'作为输出结果,并终止.

在测试询问中,如果 A 选择 V_B,D 构造并返回协议运行脚本,构造过程为:首先,D 随机选择共享密钥,构造两个等长的消息 msg_0 和 msg_1,其中,$msg_0=\{n_1,Enc_i,sid,HT_{Ai}\}$,$msg_1=\{n_1,Enc_j,sid,HT_{Aj}\}$.随后,将消息 msg_0,msg_1 作为输入询问 CCA 安全仿真器.该仿真器返回 g_v^r 和密文 C,并且满足 $C=Enc(msg_b)$, $K_{AB}=g_v^{rx}$. 然后,D 分别构造消息 $message_1,message_2$ 和 $message_3$.其中,$message_1=\{K_B,n_1,sid\}$,$message_2=\{bsn_I,c,w_1,w_2,T_1,T_2,K_A,C,n_2,sid\}$,$message_3=\{Sig_{SK_V}(n_2),sid\}$.

D 将 $message_1,message_2$ 和 $message_3$ 作为测试询问的应答.之后,D 继续执行游戏,回答 A 的所有询问并仿真协议运行中参与方激活的所有响应.当 A 输出 b'作为对 b 的猜测时,D 输出 b'并终止.

设 E 为 A 在测试询问中选择 V_B 的事件.由于 V_B 是从 $V_B(l)$中均匀地随机选择而来,因而 $Pr[E]=1/Q_2(l)$,因此可以得到:

$$Pr[A \text{ guess } b \text{ correctly}]=(1/2+v(l))Pr[E]+1/2(1-Pr[E])=1/2+v(l)/Q_2(l),$$

并且不可忽略,得证. □

下面再讨论 D 对 b 猜测正确的情况,D 可以通过下面 3 种方式猜对 b:

(1) D 通过自适应地询问 $Enc()$的解密预言机来获得选择的密文对应的明文,根据这些知识对密文 C 进行猜测.

(2) D 可以通过 g_v^r 和 g_v^x 来计算 $K=g_v^{rx}$, 并对密文 C 解密来获得 msg_b.

(3) D 以完全随机的方式猜测 b,猜对的概率为 1/2.

假定对于情况(1),D 猜对的概率为 $Adv_{\pi,Enc}$;对于情况(2),D 猜对的概率为 $Adv_{\pi,CDH}$.于是有,

$$Adv_{\pi,Enc}+Adv_{\pi,CDH}\geqslant Pr[D \text{ guess } b \text{ correctly}]-1/2=Adv_{\pi,A}(l)/Q_2(l).$$

根据假定,$Adv_{\pi,A}(l)$是不可忽略的,于是 $Adv_{\pi,Enc}$ 和 $Adv_{\pi,CDH}$ 至少有 1 个是不可忽略的,从而我们构造了一个区分器 D,能够攻破加密算法 $Enc()$,或者能够解决 CDH 问题.

因此,由定义 7 和定理 2 可知,该认证协议满足匿名性和不可连接性,并且验证者只能验证到 HT_A 来自合法的可信域 TD_A,而不能确定其真实身份,具有直接匿名性.

3.3 安全性分析

3.3.1 抗伪装攻击分析

为了防止针对本方案可信计算平台的伪装攻击,在 TPM 的签名中包含有与验证方协商会话密钥 K_{AB} 的计算.如果攻击者实施伪装攻击,在平台身份直接匿名证明的情况下,只有真实参与证明过程的可信终端平台才知道协商的会话密钥 K_{AB},因此可以阻止这种攻击.另外,认证完成后的会话消息将由密钥 K_{AB} 加密保护,攻击者同样不能进行平台伪装攻击.即使攻击者获得了认证协议中的某次会话消息,但每次由 HT_A 提供不同的密钥 K_A,并与 V_B 协商出不同的会话密钥,且密钥 K_A 由 HT_A 进行签名保护,显然,这时如果攻击者伪造 c 值,将不能被 V_B 正确验证.

3.3.2 抗重放攻击分析

同样地,针对本方案的重放攻击也会失败.假设攻击者截获了认证协议中的某次会话消息,但方案的认证协议中 HT_A 每次提供不同的密钥 K_A 与 V_B 进行密钥协商并得到不同的会话密钥 K_{AB},且 HT_A 对密钥 K_A 进行签名保护.由于 DAA 机制中密钥的保密性,攻击者不能仿冒 HT_A 完成此签名运算,因此所计算得到的 c 值无法通过 V_B 的验证.另外,方案认证协议的交互消息中引入了随机数 n_1 和 n_2,且随机数 n_1 由会话密钥进行加密保护,也能够阻止重放攻击的发生.

4 性能与实验分析

4.1 性能分析

文献[9,10]中的方案均基于 BCC 方案构建,很明显,其方案的总计算代价要比本文方案高出很多.但在移动环境中,移动计算平台的计算资源有限,运算量成为衡量认证协议性能的重要因素,因此分析时仅考虑终端与认证者之间的认证协议的计算代价.将本文方案与文献[9,10]中方案的运算量进行分析对比,分别计算移动平台中的 Host 与 TPM 的运算量,其结果见表 1.其中,EX 表示模指数运算,M 表示乘法运算,SE 表示对称加密运算,SD 表示对称解密运算,AE 表示非对称加密运算,AD 表示非对称解密运算,H 表示散列运算.

Table 1 Comparison on computation

表 1 运算量对比

名称	可信计算平台		验证者计算量
	Host 计算量	TPM 计算量	
Chen[9]	28EX+15M+2H	16EX+16M+4H	37EX+30M+2H
Liu[10]	14EX+25M+1AE+1H	8EX+8M+2H	23EX+1AD+5M+4H
本文方案	5EX+1AE+2M+1SE+2H	2EX+3M	6EX+1DE+4M+2SD+1H

与对比方案相比,无论是可信计算平台或者验证者,其计算量都有显著减少.尤其是移动终端平台,对于最耗时的模指数运算,本文方案的 CPU 仅为文献[9]中方案的 1/5 左右,仅为文献[10]中方案的 1/3 左右.且与文献[9,10]中的方案相比,本文方案验证者的计算量也显著减少.虽然与文献[9]中的方案相比,本方案中可信计算平台 Host 与验证者方面各增加了一次非对称加密运算与非对称解密运算,但并不影响方案的整体性能.另外,就消息长度而言,本方案不需要复杂的公钥证书及相应的验证操作,相比而言所需的安全参数也比较少,因此消息长度明显缩短,有利于无线网络环境的应用.

4.2 实验分析

4.2.1 实验场景

针对本文所设计的方案及认证协议,在无线局域网环境下设计和实现跨可信域的可信认证实验系统,进一步分析其性能.该实验系统的场景如图 5 所示.

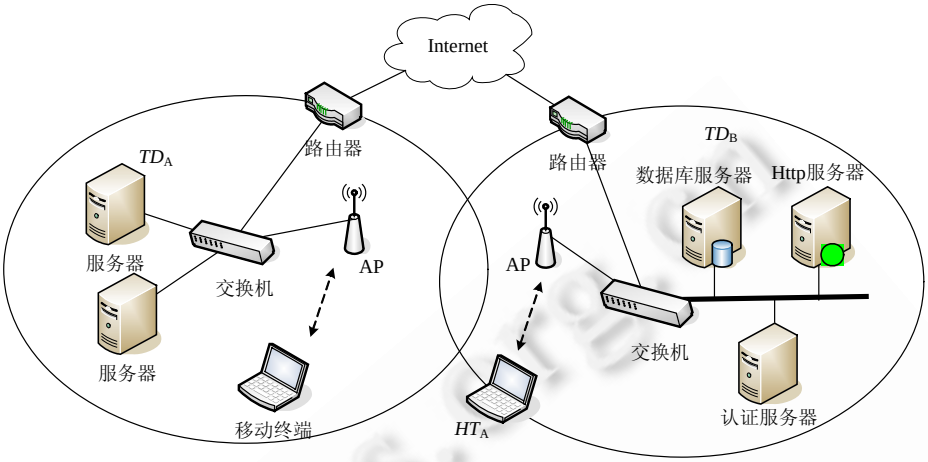

Fig.5 Experimental scenario

图 5 实验场景

在该跨域场景中,当移动终端 HT_A 漫游至可信域 TD_B 并访问可信域 TD_B 的 Http 服务器时,由该可信域中的认证服务器对其进行可信认证.在可信域 TD_B 中,组成被访问的无线网络系统的硬件设备及其主要配置见表 2.

Table 2 System configuration

表 2 系统配置

名称	型号
服务器	IBM think centre
移动终端	IBM think pad X60
接入点 AP	Cisco AIR-AP1242AG-C-K9
交换机	ZTE ZXR10 3928
路由器	Cisco 2800

基于实现和实验测试的方便性与灵活性考虑,结合无线局域网络环境,利用 TPM 芯片模拟器软件 TPM Emulator[17]实现本文的可信系统功能,包括移动平台的可信启动与平台认证等功能.TPM Emulator 是一个通过软件来虚拟硬件设备的相应功能,且基于 TCG 的 TPM 标准规范构建,能够如实地实现 TPM 的功能,该模拟器的最新版本可以实现 TPM 标准中 95%以上的功能.

4.2.2 实验实施及结果分析

在图 5 所示的实验场景中对方案进行实现及测试.实现时采用松耦合的接入认证策略,将认证分为两个阶段:用户认证阶段与平台认证阶段.移动用户进行接入访问时首先进行用户身份认证,用户认证采用 IEEE 802.1x 的 EAP-LEAP 认证架构来完成,其认证时间算入总的认证时延中;然后进行平台身份认证,平台认证采用本方案的跨域认证系统所提供的认证方法来完成,其时延为总时延的另一部分.在实验中设计了两种类型的测试.一类测试是移动终端漫游至 TD_B 并进行接入认证时,由 TD_B 的认证服务器对其进行直接的可信认证.在此测试中,移动终端 HT_A 漫游至 TD_B 中进行访问请求时,由认证服务器直接利用本方案所实现的可信认证系统进行可信认证.另一类测试是当移动终端请求 TD_B 中的 Http 服务时,重定向至认证服务器进行可信认证.在此测试中,移动终端 HT_A 请求登录 TD_B 中的 Http 服务器,例如请求高安全级的 Web 服务,此时按照安全策略的设定由服务

器将其重定向至可信认证服务器进行可信认证,且通过后再允许接入 Http 服务器.实验时,对每种认证均进行多次测试,然后计算其平均值.具体的实验结果是:直接的可信接入认证时延为 62.5ms,访问 Http 服务器时的重定向可信认证时延为 83.2ms.实验结果如图 6 所示.

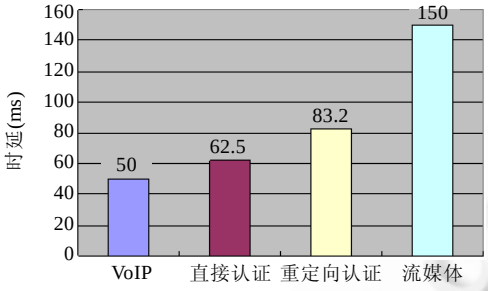

Fig.6 Authentication delay of the cross trusted domain system

图 6 跨可信域系统认证时延

目前,无线网络环境下基于移动设备的应用越来越丰富,除了传统的语音、数据业务以外,还包括 VoIP、移动 TV、视频会议、网络游戏等业务.对于这些业务来说,数据的端到端时延是影响用户体验的重要参数.例如,VoIP 延迟不能超过 50ms,流媒体应用延迟不能超过 150ms[18].从图 6 可以看出,本方案的直接可信认证时延和 Http 服务访问时延略高于 VoIP 的时延界限,但都明显优于流媒体的认证时延上限.

对此,我们分析如下:一方面,流媒体的应用在很大程度上需要依靠可信计算技术来帮助进行 DRM 管理[19],其应用需求比较明显,而 VoIP 在此方面的应用需求尚不突出;另一方面,本文方案的认证时延仍有很大的改进空间,例如可以采取紧耦合的认证方式,将用户身份认证与平台可信认证结合在一个认证过程中去完成,这将会在一定程度上节省认证时间.另外,由于本文所实现的实验系统中采用了软件模拟器的方法,在实际的应用环境中可采用实体 TPM 芯片完成可信认证功能,能够加速相关的密码学运算,进一步缩短认证时延,提高远程证明的效率.因此总体来看,本文方案满足无线移动网络的可信认证需求.

5 结束语

针对 TCG 的直接匿名证明方案不能实现跨域可信认证的不足,本文提出了移动环境下的跨可信域的直接匿名证明方案,并结合应用场景给出相应的远程证明认证协议.所设计的方案基于代理签名的委托机制,由 DAA 颁发者利用代理签名委托可信计算平台进行域认证,采用基于 CM 群签名的方法进行可信终端平台身份的直接匿名证明.采用 CK 模型分析了方案中认证协议的认证安全性与匿名安全性,达到可证明安全.分析表明,该方案能够抵抗平台伪装攻击和重放攻击,其性能适用于无线网络.

References:

[1] Trusted Computing Group. TCG specification architecture overview. 2007. http://www.trustedcomputinggroup.org

[2] Trusted Computing Group. Trusted computing platform alliance (TCPA) main specification version 1.1b. 2001. http://www.trustedcomputinggroup.org

[3] Brichell E, Camenisch J, Chen LQ. Direct anonymous attestation. In: Proc. of the 11th ACM Conf. on Computer and Communications Security. New York, 2004. 132−145. [doi: 10.1145/1030083.1030103]

[4] Camenisch J, Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials. In: Yung M, ed. Advances in Cryptology—CRYPTO 2002. LNCS 2442, Springer-Verlag, 2002. 61−76. [doi: 10.1007/3-540-45708-9_5]

[5] Camenisch J, Stadler M. Efficient group signature schemes for large groups. In: Kaliski B, ed. Advances in Cryptology—CRYPTO'97. LNCS 1296, Springer-Verlag, 1997. 410−424. [doi: 10.1007/BFb0052252]

[6] Perkins C. IP mobility support. RFC 2002, 1996. http://www.ietf.org/rfc/rfc2002.txt

[7] Ge H, Tate SR. A direct anonymous attestation scheme for embedded devices. In: Okamoto T, Wang X eds. Proc. of the PKC 2007. LNCS 4450, Heidelberg: Springer-Verlag, 2007. 16−30. [doi: 10.1007/978-3-540-71677-8_2]

[8] Camenisch J, Michels M. A group signature scheme based on an RSA-variants. Technical Report, RS-98-27, University of Aarhus, 1998.

[9] Chen XF, Feng DG. A direct anonymous attestation scheme in multi-domain environment. Chinese Journal of Computers, 2008, 31(7):1122−1130 (in Chinese with English abstract).

[10] Liu JS, Dai GZ, Li Y. A TPM authentication scheme for mobile IP. In: Proc. of the Int'l Conf. on Computational Intelligence and Security Workshops (CISW 2007). 2007. 721−724. [doi: 10.1109/CISW.2007.4425596]

[11] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation. In: Proc. of the 3rd ACM Conf. on Computer and Communications Security. ACM Press, 1996. 48−57. [doi: 10.1145/238168.238185]

[12] Mambo M, Usuda K, Okamoto E. Proxy signatures: Delegation of the power to sign messages. IEICE Trans. on Fundam, 1996, E79-A(9):1338−1354.

[13] Bellare M, Canetti R, Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols. In: Proc. of the 30th ACM Symp. on Theory of Computing. Dallas, 1998. 419−428. [doi: 10.1145/276698.276854]

[14] Canetti R, Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels. In: Pfitzmann B, ed. Advances in Cryptology—EUROCRYPT 2001. LNCS 2045, Springer-Verlag, 2001. 453−474.

[15] Tin YST, Boyd C, Nieto JG. Provably secure key exchange: An engineering approach. In: Proc. of the Australasian Information Security Workshop (AISW 2003). Australasian, 2003. 97−104.

[16] Yang GM, Wong DS, Deng XT. Formal security definition and efficient construction for roaming with a privacy-preserving extension. Journal of Universal Computer Science, 2008,14(3):441−462. [doi: 10.3217/jucs-014-03-0441]

[17] Mario S. Software-Based TPM emulator for linux. 2010. https://developer.berlios.de/projects/tpm-emulator/

[18] Mishra A, Shin M, Arbaugh W. An empirical analysis of the IEEE 802.11 MAC layer handoff process. ACM SIGCOMM Computer Communications Review, 2003,33(2):93−102. [doi: 10.1145/956981.956990]

[19] Erickson JS. Fair use, DRM and trusted computing. Communications of the ACM, 2003,46(4):34−39. [doi: 10.1145/641205.641228]

附中文参考文献:

[9] 陈小峰,冯登国.一种多信任域内的直接匿名证明方案.计算机学报,2008,31(7):1122−1130.

杨力(1977－),男,陕西乾县人,博士,副教授,CCF 高级会员,主要研究领域为密码学,可信计算,无线网络安全.

马建峰(1963－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为密码学,信息安全,安全协议工程.

姜奇(1983－),男,博士,讲师,CCF 会员,主要研究领域为安全协议分析,无线网络安全.