

文章编号:1001-9081(2016)08-2231-05

doi:10.11772/j.issn.1001-9081.2016.08.2231

移动网络可信匿名认证协议

张 鑫^{1*}, 杨晓元^{1,2}, 朱率率¹

(1. 武警工程大学 电子技术系, 西安 710086; 2. 武警工程大学 信息安全管理研究所, 西安 710086)

(*通信作者电子邮箱 zhang0551xin@163.com)

摘要:针对终端接入移动网络缺乏可信性验证问题,提出一种移动网络可信匿名认证协议,移动终端在接入网络时进行身份验证和平台完整性认证。在可信网络连接架构下,给出了可信漫游认证和可信切换认证的具体步骤,在认证时利用移动终端中预存的假名和对应公私钥对实现了用户匿名隐私的保护。安全性分析表明,协议满足双向认证、强用户匿名性、不可追踪性和有条件隐私保护。协议中首次漫游认证需要2轮交互,切换认证需1轮即可完成,消息交换轮数和终端计算代价优于同类可信认证协议。

关键词:可信计算;可信网络连接;移动网络;漫游认证;可信认证

中图分类号: TP309.7 **文献标志码:**A

Trusted and anonymous authentication protocol for mobile networks

ZHANG Xin^{1*}, YANG Xiaoyuan^{1,2}, ZHU Shuaishuai¹

(1. Department of Electronic Technology, Engineering University of Armed Police Force, Xi'an Shaanxi 710086, China;

2. Institute of Information Security, Engineering University of Armed Police Force, Xi'an Shaanxi 710086, China)

Abstract: The lackness of trusted verification of mobile terminal may affect the security of mobile network. A trusted anonymous authentication protocol for mobile networks was proposed, in which both user identity and platform integrity were authenticated when the mobile terminal accesses the networks. On the basis of trusted network connection architecture, the concrete steps of trusted roaming authentication and trusted handover authentication were described in detail. The authentication used pseudonyms and the corresponding public/private keys to achieve the protection of the user anonymous privacy. The security analysis indicates that the proposed protocol meets mutual authentication, strong user anonymity, untraceability and conditional privacy preservation; moreover, the implementation of the first roaming authentication requires two rounds of communications while the handover authentication protocol just needs one round. The analytic comparisons show that the proposed protocol is efficient in terminal computation and turns of message exchange.

Key words: trusted computing; trusted network connection; mobile network; roaming authentication; trusted authentication

0 引言

无线网络技术迅速发展,移动网络变得越来越普遍。在移动网络中,由于本地网络覆盖范围有限,当用户移动到本地网络之外时,为获得通信服务,须同外地网络进行验证才能使用外地网络资源。但移动网络存在多种安全威胁,移动终端也存在软硬件被篡改(病毒感染、植入木马等)或软件存在漏洞、版本过期,不仅影响用户的信息安全,也是整个网络的安全隐患。

为了确保移动设备的安全,同时考虑到移动终端在处理器、电源容量和存储空间等的限制,可信计算组织(Trusted Computing Group, TCG)^[1]的移动电话工作组以可信平台模块(Trusted Platform Module, TPM)为基础,针对移动设备的特性进行了重新定义和修改,发布了可信移动模块(Mobile Trusted Module, MTM)规范。同时为了解决网络访问控制中存在的安全问题,TCG 还提出了将可信计算技术同网络接入

控制技术相结合的可信网络连接(Trusted Network Connect, TNC)^[2]。终端在接入网络时,首先对终端的身份进行验证,接着完整性度量层会对终端软、硬件的状态进行检查:若度量的状态满足指定的安全策略则允许终端接入网络;否则,对终端进行隔离修复,将终端的可信状态扩展到整个网络。在2011年12月,TCG 组织发布了架构指导“ARCHITECT'S GUIDE: Mobile Security Using TNC Technology”^[3],对TNC 架构下的移动安全设计方面的问题给出了指导。

TNC 架构下的移动网络接入引起了学术界的关注,文献[4]在分析可信网络连接架构存在的安全缺陷后,提出了一种可证明安全的可信网络连接模型;文献[5]提出了移动互联网下可信移动平台的接入机制,定义了移动互联网下的本地服务和跨域访问两种访问模式,运用通用组合模型对方案进行了安全性分析;文献[6]提出了一种无双线性对无证书的无线局域网(Wireless Local Area Network, WLAN) 可信接入协议,将平台身份和平台完整性验证同用户身份认证结合,

收稿日期:2016-01-27;修回日期:2016-03-17。

基金项目:国家自然科学基金资助项目(61402530);武警工程大学基础研究基金资助项目(WJY201520)。

作者简介:张鑫(1991—),男,安徽合肥人,硕士研究生,主要研究方向:信息安全、可信计算、可信网络连接; 杨晓元(1959—),男,湖南湘潭人,教授,硕士,主要研究方向:信息安全、密码学; 朱率率(1985—),男,山东淄博人,讲师,硕士,主要研究方向:信息安全、可信计算、密码学。

并且证明了协议在 eCK (extended Canetti-Krawczyk) 模型下是安全的;文献[7]提出了可信无线匿名认证协议,对移动用户身份和终端平台可信性进行认证,认证每个阶段使用不同的密钥保证匿名性,但协议执行时外地服务器都需要在本地服务器协助下才完成漫游信息的证明;文献[8]提出了移动互联网下移动可信匿名漫游协议,外地网络通过本地为移动终端颁发的漫游证明完成认证,但用户变换漫游地时需要重新向本地服务器申请漫游证明。

针对现有文献可信漫游认证存在的不足,本文提出一种移动网络可信匿名漫游协议,分别讨论了首次漫游接入网络认证和接入点(Access Point, AP)间高效切换认证,通过移动终端中预存的假名实现用户的匿名。协议通过基于身份的密钥交换机制实现用户认证和密钥交换,利用可信计算技术完成平台的完整性验证。在漫游认证时无需借助本地服务器进行验证或使用指定漫游地的可信漫游证明,同现有的可信漫游协议相比具有更高的灵活性和实用性。

1 协议框架模型

如图 1 所示,协议在可信计算下的移动网络,主要由可信移动终端(Trusted Mobile Node, TMN)、本地验证服务器(Home Authentication Server, HAS)和外地认证服务器(Foreign Authentication Server, FAS)组成,还包括可信第三方互联网管理中心——认证中心(Certification Authority, CA)。

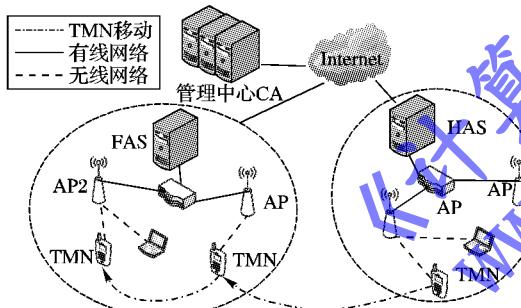


图 1 移动可信网络认证基本架构

本协议基于可信计算技术,协议中的网络接入实体 TMN 需要完成用户身份认证以及密钥协商,同时还需要认证服务器(Authentication Server, AS)(包括 HAS/FAS)完成平台的身份和完整性的验证。为简化协议,给出以下假设:

- 1) 协议中的实体具有可信平台模块;
- 2) 同传统无线网络一样,AP 和 AS 之间存在安全信道;
- 3) AS 是可信实体,控制所在整个网络并且诚实地响应每一个接入请求;
- 4) TMN 已经向隐私证书中心申请了身份认证证书 $Cert(AIK_p)$;
- 5) 本地的认证服务器 HAS 为本地注册的 TMN 建立了撤销列表,并向外提供撤销列表的查询下载服务。

本文使用的相关符号定义如下: n 为大素数; r_A 代表 A 选取的随机数, ID_A 代表 A 的身份标识, pid_i 标识用户所使用的第 i 个假名, $Cert_A$ 代表 A 的身份证书, $\langle PK_A, SK_A \rangle$ 代表 A 的一对公私钥, $\langle AIK_p, AIK_s \rangle$ 代表安全芯片(TPM 或 MTM)的身份密钥, $Cert(AIK_p)$ 代表可信计算平台的平台身份密钥(Attestation Identity Key, AIK)证书, SK_A^{-1} 代表 A 的私钥 SK_A 的求逆运算值,并且要使得用户的私钥求逆运算值与公钥的

乘积为常数,即 $SK_A^{-1}PK_A = Q$ (Q 为常数),2.1 节假名的公私钥在注册时生成,无需满足上述要求。

本文使用的相关运算定义如下: $E(K, m)$ 和 $D(K, c)$ 代表使用对称密钥进行加密/解密; $ENC(SK, m)$ 和 $DEC(PK, c)$ 分别代表使用非对称密钥进行加密/解密运算; $SIG_A(m)$ 代表 A 对消息 M 进行数字签名; $H(m)$ 代表标准散列算法。

2 移动可信匿名认证协议

2.1 TMN 向本地认证服务器 HAS 注册

在系统初始化阶段,可信移动终端使用自身的真实身份向 HAS 注册时,HAS 提供一系列不可链接的随机假名身份(Pseudonym ID, PID), $PID = \{pid_1, pid_2, \dots, pid_n\}$ 。HAS 将会预先给每个假名身份 $pid_i \in PID$ 公钥 pk_{pid_i} 和相应的私钥 sk_{pid_i} ,同时每个假名公钥同时绑定了到期时间(Expiration Date, EDate),公钥使用仅仅只在特定的到期时间之前有效。然后 HAS 将所有的元组 $(pid_i, pk_{pid_i}, sk_{pid_i})$ 安全地发送给 TMN。在当前的工作中,文献[9]就对预先装载长期使用假名的匿名密钥和相关证书的存储空间进行了详细定量的研究。当前工作^[9]对预先装载长期使用的密钥和相关证书的存储空间进行了详细的定量研究,本文的认证协议中使用了短期命名池,其存储开销在合理范围。

假名 pid_i 的公钥 pk_{pid_i} 和私钥 sk_{pid_i} 通过以下具体步骤生成:

1) HAS 初始化。令 G 为一个 q 阶的循环加法群, G_T 为一个 q 阶的循环乘法群;令 P 为 G 的一个任意的生成器,且 $\hat{e}: G \times G \rightarrow G_T$ 为双线性映射。HAS 选择一个随机数 $s \in \mathbf{Z}_q^*$ 作为主密钥, $P_{pub} = sP$ 为公钥;另外选择两个安全的散列函数 H_1 和 H_2 ,其中 $H_1: \{0,1\}^* \rightarrow G, H_2: \{0,1\}^* \rightarrow \mathbf{Z}_q^*$ 。

2) HAS 对每个 PID 计算 $H_1(pid_i)$ 作为 pid_i 的公钥, $sH_1(pid_i)$ 作为其私钥。

3) HAS 公开发布本地的注册用户使用的参数 $params_{HAS} : \{G, G_T, q, P, P_{pub}, H_1, H_2\}$ 。

2.2 TMN 同外地认证服务器 FAS 接入认证

外地访问服务器代理 FAS 的接入点 AP 进行周期性声明服务存在性的广播。当 TMN 在 AP 的直接通信范围内时,向 FAS 提出接入网络申请:

1) 当 FAS 收到一个接入请求消息,FAS 生成随机数 $r_{FAS} \in \mathbf{Z}_q^*$, sid 为会话标识,时间戳 Ts 用于抵御重放攻击,随机数 $Nonce$ 用于保证消息的新鲜性。

$FAS \rightarrow AP: sid, ID_{AP}, ID_{FAS}, r_{FAS}, Nonce;$

2) AP 收到 FAS 的消息,AP 选择秘密随机数 r_{AP} ,计算 $D_{AP} = (r_{AP} + sk_{AP})pk_{TMN}$ 用于同 TMN 之间生成共享密钥,向 TMN 发送消息。

$AP \rightarrow TMN: sid, ID_{AP}, ID_{FAS}, r_{FAS}, D_{AP}, Nonce;$

3) TMN 选择一个未使用的假名身份 pid_i ,作为自己的身份。

① TMN 使用假名私钥 sk_{pid_i} 和消息 $M_i = (sid \parallel pid_i \parallel ID_{HAS} \parallel ID_{AP} \parallel ID_{FAS} \parallel Ts \parallel Nonce)$ 计算签名 $\sigma_i = H_2(M_i) \cdot sH_1(pid_i)$ 。

② TMN 选取秘密随机数 r_{TMN} ,计算 $D_{TMN} = (r_{TMN} +$

$sk_{TMN})pk_{AP}$, 计算同 AP 之间的共享密钥 $K_{(TMN,AP)} = sk_{TMN}^{-1}(r_{TMN} + sk_{TMN})D_{AP}$ 。

③调用 TPM 指令 TPM_PcrRead() 获取平台配置寄存器值 PCRs 值, 从 TPM 中读取证明身份密钥 AIK_s, 调用 TPM_Quote() 对 PCRs 进行签名 $SIG_{TPM}(PCRs \parallel r_{FAS}) = ENC(AIK_s, PCRs \parallel r_{FAS})$, 生成平台完整性验证信息, SML (Store Measurement Log) 为度量日志。

④利用 FAS 的公钥 pk_{FAS} 进行加密 $C = ENC(pk_{FAS}, PIV)$, 其中 $PIV = SML \parallel PCRs \parallel Cert(AIK_p) \parallel SIG_{TPM}(PCRs, r_{FAS}) \parallel pid_i$ 。

TMN→AP: $M_i, \sigma_i, C, D_{TMN}$;

4) AP 收到消息后执行以下验证操作:

①检查时间戳 Ts , 以抵御重放攻击; 根据 ID_{HAS} 得到 HAS 事先发送的参数 $params_{HAS}$, 来验证 $\hat{e}(\sigma_i, P) = \hat{e}(H_2(M_i) \cdot H_1(pid_i), P_{pub})$ 是否成立, 从而检查签名 σ_i 是否有效。

②AP 计算同 TMN 的共享密钥 $K_{(AP,TMN)} = sk_{AP}^{-1}(r_{AP} + sk_{AP})D_{TMN}$ 。

AP→FAS: $sid, pid_i, ID_{HAS}, ID_{AP}, Nonce, C$;

5) FAS 收到来自 AP 的消息后进行如下操作:

①检查 pid_i 是否在撤销假名散列列表 (Revocation List, RL) 中, 检查 pid_i 服务到期时间。为了保证撤销列表中的用户前向匿名性, 本地网络代理 HAS 将撤销用户的未过期假名进行散列变换, 得到 $HPID = \{H_2(pid_j), H_2(pid_{j+1}), \dots, H_2(pid_n)\}$ 。外地验证服务器 FAS 在检查 pid_i 是否被撤销时, 将收到的 pid_i 进行散列变换 $H_2(pid_i)$, 再同收到的撤销列表中的 $HPID$ 进行匹配。若匹配成功则使用假名 pid_i 的用户已被撤销, 拒绝该连接; 否则通过撤销验证。

②验证通过后, 使用自身私钥解密 $PIV = DEC(sk_{FAS}, C)$, 获得平台可信性验证消息。利用 AIK_p 验证 $SIG_{TPM}(PCRs, r_{FAS})$, 获得 SML、PCRs。

③FAS 根据终端平台的可信验证策略, 验证平台的状态是否满足。若不满足则拒绝 TMN 的接入; 若满足生成可信证明 $Tproof = E(K_{FAS}, M_{proof})$, $M_{proof} = ID_{HAS} \parallel ID_{FAS} \parallel Hash(pid_i) \parallel EDate' \parallel N$ 。其中: $EDate'$ 为 FAS 设定的可信证明有效期, N 为 FAS 颁发给 pid_i 可信证明序列号。

FAS→AP: $sid, pid_i, ID_{AP}, Tproof$;

6) AP 收到消息后, 产生验证码 $Aut = H_2(K_{(AP,TMN)} \parallel sid \parallel pid_i \parallel ID_{AP} \parallel Ts' \parallel Nonce)$ 和 $Tproof$, 发送给 TMN。

AP→TMN: $sid, pid_i, ID_{AP}, Ts', Nonce, Aut, Tproof$;

TMN 检查时间戳 Ts' , 产生验证码 $Ver = H_2(K_{(TMN,AP)} \parallel sid \parallel pid_i \parallel ID_{AP} \parallel Ts' \parallel Nonce)$, 将其与 Aut 进行比较。若 Ver 与 Aut 相等, 则 TMN 确定 AP 是合法并且建立了会话密钥 $K_{(TMN,AP)}$; 否则, 拒绝该连接。

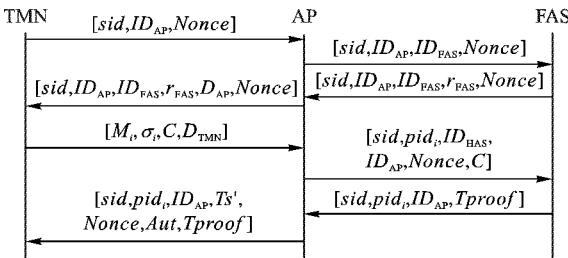


图 2 TMN 首次接入认证

2.3 TMN 在 FAS 下的 AP 间高效切换

TMN 向同一 FAS 下的 AP2 进行切换认证:

1) TMN 选择一个未使用的假名身份 pid_j 作为自己的身份。TMN 使用私钥 sk_{pid_j} 和消息 $M_j = (sid \parallel pid_j \parallel ID_{HAS} \parallel ID_{AP2} \parallel ID_{FAS} \parallel Ts \parallel Nonce)$ 计算签名 $\sigma_j = H_2(M_j) \cdot sH_1(pid_j)$ 。接着, TMN 选取秘密随机数 r'_{TMN} , 计算 $D_{TMN} = (r'_{TMN} + sk_{TMN})pk_{AP2}$ 。

TMN→AP2: $M_j, \sigma_j, D_{TMN}, Tproof$;

2) AP2 收到消息后执行以下验证操作, 检查时间戳 Ts , 以抵御重放攻击, AP2 根据 ID_{HAS} 得到 HAS 事先发送的 $params_{HAS}$, 验证 σ_j 。

AP2→FAS: $sid, pid_j, ID_{HAS}, Nonce, Tproof$;

3) FAS 收到消息后检查 pid_j 的 $EDate$ 是否到期, 使用 pid_j 假名的用户是否被撤销, 可信证明 $Tproof$ 的有效性。若未通过, 拒绝该连接, 否则发送消息。

FAS→AP2: sid, pid_j, ID_{AP2} ;

4) AP2 收到消息后选择秘密随机数 r'_{AP2} , 再计算 $D_{AP2} = (r'_{AP2} + sk_{AP2})pk_{TMN}$, 共享密钥 $K_{(AP2,TMN)} = sk_{AP2}^{-1}(r'_{AP2} + sk_{AP2})D_{TMN}$ 和验证码 $Aut = H_2(K_{(AP2,TMN)} \parallel sid \parallel pid_j \parallel ID_{AP2} \parallel Ts' \parallel Nonce)$ 。

AP2→TMN: $sid, pid_j, D_{AP2}, Ts', Aut$;

5) TMN 收到消息验证时间戳, 计算共享密钥 $K_{(TMN,AP2)} = sk_{TMN}^{-1}(r'_{TMN} + sk_{TMN})D_{AP2}$, 生成 $Ver = H_2(K_{(TMN,AP2)} \parallel sid \parallel pid_j \parallel ID_{AP2} \parallel Ts' \parallel Nonce)$, 若与 Aut 相同, 则 TMN 确定 FAS 是合法并且建立了会话密钥 $K_{(TMN,AP)}$, 否则拒绝该连接。

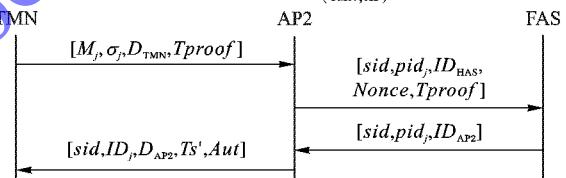


图 3 TMN 切换到 AP2

3 协议分析

3.1 协议安全性

在协议中 TMN 首次访问外地网络时实现了双向的身份认证。AP 对 TMN 的认证使用公钥算法, AP 验证签名 $\sigma_i = H_2(M_i) \cdot sH_1(pid_i)$ 是基于随机身份的签名, 通过检查 $\hat{e}(\sigma_i, P) = \hat{e}(H_2(M_i) \cdot H_1(pid_i), P_{pub})$ 是否成立, 完成 AP 对 TMN 的验证。具体验证过程如下:

$$\begin{aligned} \hat{e}(\sigma_i, P) &= \hat{e}(H_2(M_i) \cdot sH_1(pid_i), P) = \\ &\hat{e}(H_2(M_i) \cdot H_1(pid_i), sP) = \\ &\hat{e}(H_2(M_i) \cdot H_1(pid_i), P_{pub}) \end{aligned}$$

因为只有在认证服务器 HAS 才保存秘密数 $s \in \mathbb{Z}_q^*$, 敌手无法通过公开参数 $params_{HAS}$ 计算出 TMN 的私钥 $sH_1(pid_i)$, 因此敌手无法伪造合法签名, TMN 对 AP 的验证类似。敌手无法获得 AP 的私钥生成共享密钥, 则无法伪造合法的验证码 Aut 。在通信的过程中, 对主要消息进行散列值运算保证消息的完整性, 同时采用了时间戳和随机数保证消息的新鲜性并防止重放攻击。

协议中双方完成身份合法性和平台可信性验证的同时, 完成了会话密钥的协商。正确性如下:

$$K_{(AP,TMN)} = sk_{AP}^{-1}(r_{AP} + sk_{AP})D_{TMN} =$$

$$\begin{aligned} sk_{AP}^{-1}(r_{AP} + sk_{AP})(r_{TMN} + sk_{TMN})pk_{AP} = \\ (r_{AP} + sk_{AP})(r_{TMN} + sk_{TMN})Q \end{aligned}$$

同样可得 $K_{(TMN, AP)} = (r_{AP} + sk_{AP})(r_{TMN} + sk_{TMN})Q$, 因此会话密钥正确性成立。会话密钥由双方选择的秘密随机数 r_{AP} 和 r_{TMN} 共同决定,任何一方无法单独伪造合法密钥, r_{AP} 和 r_{TMN} 分别由 TMN 和 AP 安全保存, FAS 也无法获得 TMN 与 AP 间的共享密钥,秘密随机数 r_{AP} 和 r_{TMN} 由每次接入认证时才生成,保证了会话密钥的新鲜性。

3.2 用户匿名性

协议中交互的消息中使用预存的一系列不可链接的假名 pid_i , 未出现用户的真实身份;并且不同的移动终端使用的假名是不同的,其他用户无法获得。TMN 使用假名加密传输给 HAS, 实现了用户真实身份对 HAS 的匿名性,即使假名遭到泄露,攻击者也无法获得用户的真实身份,也无法将截获的假名同其他通信过程进行关联。用户多次访问网络都是使用不同的假名,具有不可跟踪性。

由于撤销列表 RL 是由被撤销用户假名的散列值构成 $HID = \{H_2(pid_1), H_2(pid_2), \dots, H_2(pid_n)\}$ 。FAS 进行检查时将收到的假名先进行散列变化 $H_2 = (pid_i)$, 再同列表进行匹配。由于散列函数的单向性,FAS 仅能判断收到的假名是否在撤销列表中,而无法获得撤销用户的所有假名信息。

由于本地认证服务器 HAS 存储了用户所有的假名信息,在紧急情况下 HAS 可以向法律权威报告用户所有假名,则用户的隐私信息(身份、位置等)将不具有匿名性,因此协议满足有条件的隐私保护。

3.3 平台可信性

在认证服务器安全可靠的情况下,TMN 平台的软硬件配置信息不会泄露给网络之中的其他合法用户,也不会泄露给 AP,有效保护了平台的有效隐私性。终端首次接入外地网络时,TMN 向 AP 发送了用 AIK_p 签名 $PCRs$ 值、 AIK 证书以及度量日志 SML ,以证明平台的完整性。TMN 使用 AIK_p 对 $PCRs$ 值和 FAS 传输过来的随机值 r_{FAS} 进行签名,利用 r_{FAS} 保证了平台配置信息的新鲜性;平台配置信息使用了 FAS 的公钥进行加密,避免了平台配置信息被 AP 或其他用户获知,保证了 TMN 的匿名性。当 TMN 在 AP 间进行切换时,使用 FAS 颁发的可信证明 $Tproof$ 进行验证,由于可信证明 $Tproof$ 是由 FAS 的对称密钥加密而来,使得 AP 或其他用户无法将其与 TMN 之前所使用的身份绑定,保证了切换时用户的匿名性不被破坏。

3.4 抗平台替换攻击

文献[4]中指出可信网络接入架构中存在平台替换攻击,本文方案是抗平台替换攻击的。用户 A 和用户 B 都是合法用户,A 控制可信平台 PA,B 控制不可信平台 PB。若 B 通过非法手段获取了用户 A 的平台验证信息,向验证服务器申请验证。因 A 的验证信息中封装了其临时假名身份 pid_i ,而 B 无法获得假名身份的公私钥信息。所以用户 B 无法利用用户 A 的平台验证信息证明其身份合法性和平台可信性。

3.5 接入认证灵活性

传统的移动用户漫游认证方案中,部分采用三方(终端、本地服务器、外地服务器)漫游结构^[10-11],验证时需要本地服务器参与,可能存在连接失败或本地服务器单点登录失败。而两方(终端、外地服务器)漫游协议则通常使用一些复杂的密码技术(例如:组签名^[12]),给用户和外地服务器带来了较

高的计算开销。在本文协议中,用户在外地网络进行身份验证和可信验证时,使用预存的假名 $PID = \{pid_1, pid_2, \dots, pid_n\}$ 及其公私钥对进行匿名通信。本地服务器 HAS 事先已发送公共参数 $params_{HAS}$, FAS 便可以利用 $params_{HAS}$ 对来自 HAS 的漫游用户进行独立验证。因此 FAS 无需同 HAS 进行通信交互,减少了通信延迟及验证服务器负担。本文协议中的用户也无需使用复杂密码技术或者向 HAS 申请文献[8]中的指定漫游目的地的漫游证明,使得用户漫游更加自主和便捷。

3.6 性能分析

由于移动网络中终端计算能力有限,终端不能有过多的计算开销。协议执行效率主要用协议中终端完成的各种计算来衡量,包括指数运算、散列运算、对称加解密、公钥加解密和消息交换轮数。本文分别对终端 CPU 和 TPM 的计算开销进行了分析。本文的协议的效率比照了文献[7]和文献[8]方案在进行网络接入认证时终端的运算量。从表 1 可以得到,移动终端平台 CPU 执行了一次散列运算、两次非对称加解密运算,消息的交换轮数为两轮。这些运算只需要较小的计算量,对移动终端产生影响较小。与文献[7-8]的方案相比,本文协议中终端的计算量有优势。

表 1 协议性能分析

终端运算量	文献[7] 方案		文献[8] 方案		本文协议 漫游认证		本文协议 切换	
	CPU	TPM	CPU	TPM	CPU	TPM	CPU	TPM
散列运算次数	1	2	2	0	1	0	1	0
对称加密次数	2	0	0	0	0	0	0	0
对称解密次数	1	0	0	0	0	0	0	0
非对称 加解密次数	0	2	3	0	1	1	1	0
消息交换轮数 (TMN-FAS/ FAS-HAS)	1/1		2/0		2/0		1/0	

批验证:接入点 AP 收到 TMN 访问请求,需要验证该消息的签名 σ_i ,采用了双线性配对,计算负担大。但 AP 可以采用批验证方式缩短多个用户签名验证时间,提高验证效率,验证条签名的计算开销为 n 次点乘和两次配对操作。若有 n 个 TMN 发送验证消息 $\langle M_1, \sigma_1 \rangle, \langle M_2, \sigma_2 \rangle, \dots, \langle M_n, \sigma_n \rangle$, 若 $\hat{e}\left(\sum_{i=1}^n \sigma_i, P\right) = \hat{e}\left(\sum_{i=1}^n H_2(M_i) \cdot H_1(pid_i), P_{pub}\right)$ 成立,则验证成功,过程如下:

$$\begin{aligned} \hat{e}\left(\sum_{i=1}^n \sigma_i, P\right) &= \hat{e}\left(\sum_{i=1}^n H_2(M_i) \cdot sH_1(pid_i), P\right) = \\ &\hat{e}\left(\sum_{i=1}^n H_2(M_i) \cdot H_1(pid_i), sP\right) = \\ &\hat{e}\left(\sum_{i=1}^n H_2(M_i) \cdot H_1(pid_i), P_{pub}\right) \end{aligned}$$

4 结语

传统漫游、切换协议无法满足平台的可信认证需求,本文提出一种移动网络可信匿名认证协议。以可信网络连接 TNC 架构为基础,用户在进行漫游访问或 AP 间切换认证时,将用户身份认证同平台可信性认证结合起来,实现了高效的可信

接入。终端使用预存的假名保护用户的匿名性,假名与用户真实身份没有关联,保证了用户的身份和位置等信息机密性和有条件的隐私保护,分析表明协议计算开销相比现有协议减少并且接入认证更加灵活、自主。本文漫游认证协议在可信移动互联网中完成终端可信认证,增加了安全性。但终端负载有所增加,同时对无可信平台模块的终端和传统网络环境下的兼容性、扩展性问题,还需要进一步探讨和研究。

参考文献:

- [1] Trust Computing Group. TPM main part 1: design principles specification, version 1.2 revision 62 [S]. Geneva: International Organization for Standardization (IOS), 2009.
- [2] Trust Computing Group. TCG trusted network connect architecture for interoperability specification version 1.4 [EB/OL]. (2009-05-18) [20015-11-18]. <http://www.trustedcomputinggroup.org>.
- [3] Trust Computing Group. Architect's guide: mobile security using TNC technology [EB/OL]. (2011-12-29) [2015-10-18]. <http://www.trustedcomputinggroup.org/developers/mobile>.
- [4] 马卓,马建峰,李兴华,等.可证明安全的可信网络连接协议模型[J].计算机学报,2011,34(9):1669–1678. (MA Z, MA J F, LI X H, et al. Provable security model for trusted network connect protocol [J]. Chinese Journal of Computers, 2011, 34(9): 1669 – 1678.)
- [5] 吴振强,周彦伟,乔子芮.移动互联网下可信移动平台接入机制[J].通信学报,2011,31(10):158–169. (WU Z Q, ZHOU Y W, QIAO Z R. Access mechanism of TMP under mobile network [J]. Journal on Communications, 2011, 31(10): 158 – 169.)
- [6] 马卓,张俊伟,马建峰,等.可证明安全的无双线性对无证书可信接入认证协议[J].计算机研究与发展,2014,51(2):325–333. (MA Z, ZHANG J W, MA J F, et al. Provably secure certificateless trusted access protocol for WLAN without pairing [J]. Journal of Computer Research and Development, 2014, 51(2): 325 – 333.)
- [7] 杨力,马建峰,朱建明.可信的匿名无线认证协议[J].通信学报,2009,30(9):29–35. (YANG L, MA J F, ZHU J M. Trusted and anonymous authentication scheme for wireless networks [J]. Journal on Communications, 2009, 30(9): 29 – 35.)
- [8] 周彦伟,杨波,张文政.可证安全的移动互联网可信匿名漫游协议[J].计算机学报,2015,38(4):733–748. (ZHOU Y W, YANG B, ZHANG W Z. Provable secure trusted and anonymous roaming protocol for mobile Internet [J]. Chinese Journal of Computers, 2015, 38(4): 733 – 748.)
- [9] RAYA M, HUBAUX J-P. Securing vehicular Ad Hoc networks[J]. Journal of Computer Security — Special Issue on Security of Ad-hoc and Sensor Networks, 2007, 15(1): 39 – 68.
- [10] 侯惠芳,季新生,刘光强.异构无线网络中基于标识的匿名认证协议[J].通信学报,2011,32(5):153–161. (HOU H F, JI X S, LIU G Q. Identity-based anonymity authentication protocol in the heterogeneous wireless network [J]. Journal on Communications, 2011, 32(5): 153 – 161.)
- [11] 侯惠芳,刘光强,季新生,等.基于公钥的可证明安全的异构无线网络认证方案[J].电子与信息学报,2009,31(10):2385–2391. (HOU H F, LIU G Q, JI X S, et al. Provable security authentication scheme based on public key for heterogeneous wireless network [J]. Journal of Electronics & Information Technology, 2009, 31(10): 2385 – 2391.)
- [12] YANG C, HUANG Q, WONG D S, et al. Universal authentication protocols for anonymous wireless communications [J]. IEEE Transactions on Wireless Communications, 2010, 9(1):168 – 174.

Background

This work is partially supported by the National Natural Science Foundation of China (61402530), the Basic Research Foundation of Engineering University of Armed Police Force (WJY201520).

ZHANG Xin, born in 1991, M. S. candidate. His research interests include information security, trusted computing, trusted network connect.

YANG Xiaoyuan, born in 1959, M. S., professor. His research interests include information security, cryptology.

ZHU Shuaishuai, born in 1985, M. S., lecturer. His research interests include information security, trusted computing, cryptology.

(上接第2230页)

- [12] DENG H, WU Q H, QIN B, et al. Asymmetric cross-cryptosystem re-encryption applicable to efficient and secure mobile access to outsourced data [C]// Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. New York: ACM, 2015: 393 – 404.
- [13] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts [C]// Proceedings of the 20th USENIX Conference on Security. Berkeley: USENIX Association, 2011: 34.
- [14] MATSUO T. Proxy re-encryption systems for identity-based encryption [C]// Proceedings of the First International Conference on Pairing-Based Cryptography, LNCS 4575. Berlin: Springer, 2007: 247 – 267.
- [15] LUO S, HU J B, CHEN Z. Ciphertext policy attribute-based proxy re-encryption [C]// Proceedings of the 12th International Conference on Information and Communications Security, LNCS 6476. Berlin: Springer, 2010: 401 – 415.
- [16] SHAO J, LU R X, LIN X D. Fine-grained data sharing in cloud computing for mobile devices [C]// Proceedings of the 2015 IEEE Conference on Computer Communications. Piscataway, NJ: IEEE,

2015: 2677 – 2685.

- [17] LYNN B. The Stanford pairing based cryptography library [EB/OL]. [2015-11-20]. <http://crypto.stanford.edu/pbc>.

Background

This work is partially supported by the National Natural Science Foundation of China (61272492, 61572521), the Natural Science Foundation of Shaanxi Province (2014JM8300), the Basic Research Program of Engineering University of Chinese People's Armed Police (WJY201422, WJY201523).

HAO Wei, born in 1990, M. S. candidate. His research interests include identity-based proxy re-encryption.

YANG Xiaoyuan, born in 1959, M. S., professor. His research interests include cryptography, information security.

WANG Xu'an, born in 1981, Ph. D. candidate, associate professor. His research interests include cryptography, information security.

ZHANG Yingnan, born in 1990, Ph. D. candidate. His research interests include information hiding.

WU Liqiang, born in 1986, M. S., lecturer. His research interests include lattice-based cryptography, provable security.