普适计算环境下的安全访问模型

周彦伟[1,2,3],杨 波[1,2,3],张文政[2]
(1. 陕西师范大学计算机科学学院,陕西西安 710062;2. 保密通信重点实验室,四川成都 610041;
3. 中国科学院信息工程研究所信息安全国家重点实验室,北京 100093)

摘 要: 针对移动终端的普及和可信计算技术对移动终端通信模式的影响,为满足普适计算环境的安全访问需求,本文提出普适计算环境下的安全访问模型,该模型定义了普适计算环境下用户的本地注册、域内访问和域间漫游3种机制,并详细介绍了相应的工作流程. 安全性证明表明本文机制是CK安全的;分析显示本文模型在匿名性、安全性和效率上的优势,使其更加适合在普适计算环境下使用.

关键词: 普适计算环境; 安全访问模型; 跨域; CK安全模型
中图分类号: TP393.08 **文献标识码:** A **文章编号:** 0372-2112 (2017)04-0959-07
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.04.027

Security Access Model in Pervasive Computing Environment

ZHOU Yan-wei[1,2,3], YANG Bo[1,2,3], ZHANG Wen-zheng[2]
(1. *School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*;
2. *Science and Technology on Communication Security Laboratory, Chengdu, Sichuan* 610041, *China*;
3. *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

Abstract: Because of the popularity and the change of communication mode for mobile terminals and in order to meet the security access demand of pervasive computing environment, we present a security access model for pervasive computing environment which contains three kinds of access mechanisms: local service domain registration, local domain access and cross-domain access, and the specific work processes of the above access mechanisms are introduced at the same time. The security proof shows that our proposal is provably secure in the CK security model and has superiority in anonymity, security and efficiency, which make it more suitable for pervasive computing environment.

Key words: pervasive computing environment; security access model; cross-domain; CK security model

1 引言

不同的智能区域构成了开放的分布式环境——普适环境,每个智能区域都有认证服务器管理区域的资源及用户,为用户提供身份认证等服务. 在该环境中,由于用户会漫游到不同的区域,此时存在漫游过程中用户身份的认证问题. 当用户进行漫游访问时,由于不存在事先的信任关系,因此访问区域的认证服务器需联合家乡区域的认证服务器对其身份合法性进行验证;并且在跨域访问过程中,需保护用户身份、位置等隐私信息的安全性,同时要防止攻击者的跟踪、窃听等行为,因此在跨区域漫游过程中需隐藏用户的真实身份等个人隐私信息,为用户提供匿名漫游服务;因此跨域认证方案在实现安全认证和会话密钥协商的同时需满足匿名性和不可跟踪性,即访问区域的认证服务器和其他用户都无法确定跨域用户的真实身份及不同的会话源头.

由于普适环境中移动终端的存储、计算能力的局限性,使得传统漫游认证机制[1~7]无法满足普适环境对匿名性和计算开销的要求;同时用户身份的合法,并不意味着终端平台的安全可信. 然而传统的跨域漫游认证机制[1~7]仅关注用户身份的合法性,缺乏对用户所持

收稿日期:2015-08-25;修回日期:2015-11-25;责任编辑:孙瑶
基金项目:国家自然科学基金(No. 61572303, No. 61272436, No. 61402275);中国科学院信息工程研究所信息安全国家重点实验室基金(No. 2015-MS-10);保密通信重点实验室基金(No. 9140C110206140C11050);中央高校基本科研业务费专项资金(No. GK201504016);陕西师范大学优秀博士论文基金(No. X2014YB01)

终端平台的可信性验证,同时传统机制的计算开销较大,已无法满足当前普适环境对计算效率的需求.

针对普适环境下漫游认证机制的研究现状,为解决现有机制所存在的不足;同时为推广可信移动终端(Trusted Mobile Terminal,TMT)的应用,本文综合可信计算技术提出普适计算环境下的安全访问模型,具体包括本地域注册、域内访问和域间漫游 3 种机制;并基于 CK 安全模型对域间漫游机制的安全性进行了证明.

2 相关工作

2.1 普适环境下的域间漫游

域间漫游机制确保普适环境下用户能获得随时随地的接入服务,研究人员就漫游问题提出多个解决方案[1~7].通过分析现有的匿名漫游方案[1~7]发现存在下述不足:文献[1]涉及复杂的证书管理;文献[2]与文献[1]一样,无法满足用户个人隐私信息的匿名性要求.文献[3]的漫游认证时延较大;文献[5]中攻击者易对用户的通信过程进行跟踪;文献[6]无法满足域间漫游的需求;文献[7]未考虑终端平台本身的安全性.

2.2 移动终端的安全性

由于移动终端的智能化发展,其所支持的功能越来越多;由于存储信息敏感程度的不断提升,促使越来越多的用户开始注重自身隐私的安全性.可信计算理论的初衷是在终端平台上以硬件芯片为基础构建安全可信的计算平台,加强对终端平台的安全性保护.为确保移动设备信息的安全,可信计算组织发布了移动可信模块(Mobile Trusted Module,MTM)规范,意在移动终端上建立可信的安全机制来保护用户隐私信息和敏感数据的安全性;文献[8,9]详细介绍了可信计算的相关关键技术.

3 普适环境下的安全访问模型

如图 1 所示本文普适环境下安全访问模型涉及的实体包括:用户(User)、管理员(Admin)和身份认证服务器;其中 User 是请求接入的实体,终端的 MTM 安全芯片将收集平台可信度量信息,并发给身份认证服务器验证其身份合法性和平台可信性;Admin 是服务域的相关管理人员;身份认证服务器主要完成本地域中 User 的身份合法性及平台可信性的验证,为 User 签发临时身份标识,同时受理其他服务域中 User 的漫游访问请求,并对漫游用户的身份合法性及平台可信性进行验证,为合法且可信的漫游用户签发临时的漫游标识,同时负责制定本地用户的身份合法性及平台可信性验证策略,管理用户的注册信息.

根据 User 的具体工作过程,本文定义了 3 种访问机制:

(1)本地域注册. 本地域注册是指用户向本地服务器进行注册,获得相应的注册信息. User 向本地域身份认证服务器(Home Authentication Server,HS)申请注册,HS 完成 User 身份合法性及平台可信性的验证,对身份合法且平台可信的 User 签发临时身份标识 TID_U.

(2)域内访问. 域内访问是指注册完成后用户与本地域服务器进行通信的过程. User 完成本地注册后,获得 HS 签发的 TID_U,可持 TID_U 与 HS 进行通信. 图 1 中 Alice 进行域内访问.

(3)域间漫游. 域间漫游是指 User 注册完成后向其他区域申请服务的通信过程. User 完成本地注册后,请求漫游进入远程域(远程域是相对用户而言的),无需 HS 的协助,远程域身份认证服务器(Remote Authentication Server,RS)直接完成对漫游 User 的身份合法性及平台可信性验证,并为通过验证的用户签发具有时效性的漫游标识 RID_U. 图 1 中 Bob 进行域间漫游访问.

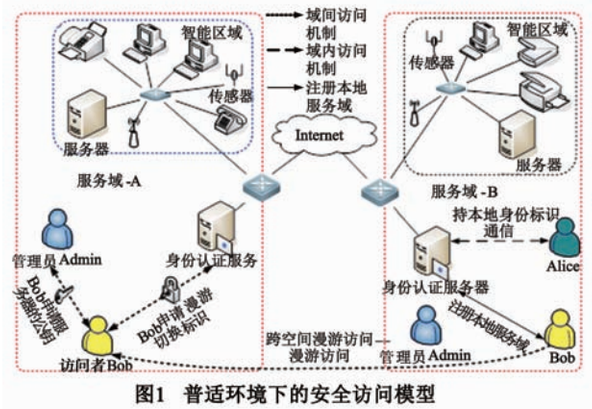

图1 普适环境下的安全访问模型

本文使用的相关变量定义如下:

ID 是身份标识或相关网络标号;TID 是 HS 为本地 User 生成的临时身份;Leg_A 是 TID 的验证标识,且初始值为 0;RID 是 RS 为漫游 User 签发的漫游临时身份;RLeg 是 RID 的验证标识,且初始值为 0;T_i 是时间戳;Z_q^* 表示小于 q 的非 0 正整数,其中 q 是大素数.

本文使用的相关运算表述如下:

双线性映射. 设 G_1,G_2 分别为阶是大素数 q 的加法循环群和乘法循环群,P 为群 G_1 的生成元. 当映射 $e:G_1 \times G_1 \rightarrow G_2$ 满足下列性质时,称 e 为双线性映射.

①双线性. 对于 $a,b \in Z_g^*$ 和 $P,Q \in G_1$,均有 $e(aP,bQ)=e(P,Q)^{ab}$ 成立.

②非退化性. 存在 $P,Q \in G_1$,使得 $e(P,Q) \neq 1_{G_2}$,其中 1_{G_2} 为 G_2 的单位元.

③可计算性. 对于 $P,Q \in G_1$,可在多项式时间内完成 $e(P,Q)$ 的计算.

同时定义 $<E,D>$ 表示对称的加/解密算法;$<\mathrm{Enc},\mathrm{Dec}>$ 表示非对称的加/解密算法;$\oplus$ 表示异或

运算;‖表示连接符.

本文使用的相关假设表述如下:

假设 1　各服务域中的认证服务器获得由普适环境管理中心签发的身份证书,证书包含公钥、管理中心的签名信息等,各认证服务器安全存储私钥防止其泄露.

假设 2　User 在交互过程中加/解密、随机数产生等操作可由安全芯片 MTM 完成.

假设 3　时钟同步机制可确保本文模型中时间戳的新鲜性.

3.1　初始化

初始化阶段主要完成认证服务器的注册及参数生成. 具体过程如下所述:

①认证服务器向管理中心注册,管理中心选择满足双线性映射 $e:G_1\times G_1\rightarrow G_2$ 条件的 q 阶循环加法群 G_1 和乘法循环群 G_2,P 是群 G_1 的一个生成元;定义抗碰撞哈希函数 $H:\{0,1\}^*\rightarrow\{0,1\}^{L_K}$,$H_1:\{0,1\}^*\rightarrow Z_q^*$,$H_2:\{0,1\}^*\rightarrow\{0,1\}^{|ID|}$ 和 $H_3:G_1\rightarrow\{0,1\}^{|ID|}$(为方便描述将 H,H_1 和 H_2 定义为对任意长度字符串的映射),其中 L_K 表示协商会话密钥的长度,|ID|为相关参与者的身份标识长度,管理中心公开系统基础参数 Params = $\{q,G_1,G_2,e,P,H,H_1,H_2,H_3\}$.

②HS 选取随机秘密数 $S_{HS}\in Z_q^*$ 作为主密钥,计算公钥 $P_{Pub}^{HS}=S_{HS}P$. HS 妥善保管主密钥 S_{HS},公开系统参数 $Params_{HS}=\{q,G_1,G_2,e,P,P_{Pub}^{HS},H,H_1,H_2,H_3\}$.

③RS 选取随机秘密数 $S_{RS}\in Z_q^*$ 作为主密钥,计算公钥 $P_{Pub}^{RS}=S_{RS}P$. RS 妥善保管主密钥 S_{RS},公开系统参数 $Params_{RS}=\{q,G_1,G_2,e,P,P_{Pub}^{RS},H,H_1,H_2,H_3\}$.

3.2　家乡域注册

User 向 HS 申请注册,完成身份合法性及平台可信性验证,并获得 HS 生成临时身份标识 TID_U.

(1)User 选取随机数 $r_U\in Z_q^*$ 后,计算 $R_U=r_UP$,用 HS 的公钥 P_{Pub}^{HS} 加密 $AIKCert_U$,$ATTCert_U$,ID_U,R_U 和 T_U 生成注册消息,其中 $AIKCert_U$ 和 $ATTCert_U$ 是安全芯片 MTM 生成的平台可信性验证信息;公钥加密确保仅有 HS 能正确解密消息,保证消息的安全性;时间戳保证消息的新鲜性.

(2)HS 基于 $AIKCert_U$ 和 $ATTCert_U$ 对平台可信性进行验证(相关关键技术详见文献[8,9]),为身份合法且平台可信的 User 分配临时身份标识 TID_U.

①计算秘密数 $S_{HS}^U=H_2(ID_U\|Num_{HS})$ 和临时身份标识 $TID_U=S_{HS}^U\oplus ID_U\oplus ID_{HS}$,其中 Num_{HS} 是 HS 选取的秘密随机数.

②选取随机秘密数 $r_{HS}\in Z_q^*$,计算 $R_{HS}=r_{HS}P$,$L=r_{HS}+f_US_{HS}$(其中 $f_U=H_1(ID_U,R_{HS},R_U)$).

③计算会话密钥 $k_1=H(r_{HS}R_U\|ID_U\|ID_{HS})$.

④在本地数据库中,为 User 建立注册信息 $Data_U=<ID_U,TID_U,S_{HS}^U,TID_U',Leg_U',Result>$,其中 $TID_U'=TID_U\oplus H_3(R_{HS})$,$Leg_U'=0\oplus H_3(R_{HS})$,Result 表示平台可信性验证结果.

HS 将 TID_U,$<L,R_{HS}>$,$Enc(S_{HS},TID_U\|Result)$ 和 T_{HS} 用私钥 S_{HS} 加密后发送给 User;私钥加密确保应答消息是由 HS 发送.

(3)User 收到应答消息后,验证应答消息的合法性及新鲜性,并计算相应的协商密钥.

①通过等式 $LP=(r_{HS}+f_US_{HS})P=R_{HS}+f_UP_{Pub}^{HS}$(其中 $f_U=H_1(ID_U\|R_{HS}\|R_U)$)验证注册应答消息 $<L,R_{HS}>$ 的正确性.

②计算会话密钥 $k_1=H(r_UR_{HS}\|ID_U\|ID_{HS})$.

③计算 $S_U=r_U+L$ 和 $R=R_U+R_{HS}$,则 User 的注册证书为 $Cert_U=<S_U,R,f_U>$,User 安全存储 $Cert_U$ 和平台可信性验证结果 $Enc(S_{HS},TID_U\|Result)$,并销毁秘密数 r_U,使其不对外泄露.

3.3　域内访问机制

如图 1 所示,Alice 获得 TID_U 后可持其与本域内服务器 HS 进行通信,HS 基于 TID_U 完成对 Alice 身份合法性及平台可信性的验证.

(1)Alice 通过下述计算生成服务请求消息.

①随机选取秘密数 $n\in Z_q^*$,计算身份证明信息 $Q_A=nS_AP$,$W_A=nR$,$V_A=nf_AP$.

②随机选取秘密数 $r_A^i\in Z_q^*$,计算 $R_A^i=r_A^iP$,计算临时身份标识 $TID_A^i=TID_A^{i-1}\oplus H_3(R_{HS}^{i-1})\oplus H_3(R_A^i)$,其中 TID_A^{i-1} 是 Alice 在第 $i-1$ 次域内访问时生成的临时身份标识,R_{HS}^{i-1} 是 Alice 在第 $i-1$ 次域内访问时 HS 生成的密钥协商参数,$TID_A^0=TID_A$.

③计算 $Sig_A=r_A^i+nS_Uh_A$(其中 $h_A=H_1(TID_A^i\|R_A^i)$)后,Alice 产生时间戳,将消息 TID_A^i,Sig_A,$E(k_{A,HS}^{i-1},TID_A^i\|R_A^i)$,$Enc(S_{HS},TID_U\|Result)$,$T_A^i$ 和 $<Q_A,W_A,V_A>$ 用 P_{Pub}^{HS} 加密发送给 HS.

(2)HS 用私钥 S_{HS} 解密消息,验证消息的完整性及时戳的新鲜性后,完成对 Alice 的身份合法性及平台可信验证.

①通过等式 $e(Q_A,P)=e(W_A,P)e(V_A,P_{Pub}^{HS})$ 验证身份证明信息 $<Q_A,W_A,V_A>$ 的合法性.

②使用密钥 $k_{A,HS}^{i-1}$ 解密消息 $E(k_{A,HS}^{i-1},TID_A^i\|R_A^i)$,通过等式 $Sig_AP=R_A^i+h_AQ_A$(其中 $h_A=H_1(TID_A^i\|R_A^i)$)验证密钥协商参数 R_A^i 的正确性.

③通过索引 $TID_A^i\oplus H_3(R_A^i)$ 查找本地数据库中 Alice 的相关注册信息 Leg_A',基于等式 $ID_A=TID_A^i\oplus H_3(R_A^i)\oplus Leg_A'\oplus S_{HS}^A\oplus ID_{HS}$ 验证 Alice 临时身份 TID_A^i 所

对应真实身份的合法性.

④选取秘密数 $r_{HS}^i \in Z_q^*$,计算 $R_{HS}^i = r_{HS}^i P$,并更新会话密钥 $k_{A,HS}^i = H(r_{HS}^i R_A^i \| ID_U \| ID_{HS})$和注册信息 $TID_A' = TID_A^i \oplus H_3(R_{HS}^i)$, $Leg'_A = Leg_A' \oplus H_3(R_{HS}^i) \oplus H_3(R_A^i)$.

⑤基于 $Enc(S_{HS}, TID_A \| Result)$可获知 Alice 平台的可信性结果,根据等式 $TID_A = TID_A^i \oplus H_3(R_A^i) \oplus Leg'_A$ 验证授权身份与持有者身份的一致性.

HS 将消息 $E(k_{A,HS}^i, TID_A^i \| R_{HS}^i)$, R_{HS}^i和 T_{HS}^i用 S_{HS}加密后发送给 Alice.

(3) Alice 更新与 HS 间的协商会话密钥 $k_{A,HS}^i = H(r_A^i R_{HS}^i \| ID_U \| ID_{HS})$,解密消息 $E(k_{A,HS}^i, TID_A^i \| R_{HS}^i)$并验证应答消息的正确性.

3.4 域间漫游

如图 1 所示,用户 Bob 漫游进入其他服务域,并向管理员申请获知认证服务器 RS 的公钥,Bob 与 RS 建立连接并申请漫游标识;RS 无需 HS 的协助直接完成对 Bob 的身份合法性及平台可信性验证.

(1) Bob 通过下述计算生成域间漫游消息.

①随机选取秘密数 $m \in Z_q^*$,计算身份证明信息 $Q_B = mS_B P$, $W_B = mR$, $V_B = mf_B P$.

②随机选取秘密数 $r_B \in Z_q^*$,计算 $R_B = r_B P$,计算 $Sig_B = r_B + mS_B h_B$(其中 $h_B = H_1(TID_B \| R_B)$).

将消息 R_B, ID_{HS}, ID_{RS}, $Enc(S_{HS}, TID_B \| Result)$, $<Q_B, W_B, V_B>$, TID_B 和 T_B 用 P_{Pub}^{RS}加密后发给 RS.

(2) RS 解密请求消息,并验证消息的完整性及时戳的新鲜性,防止重放攻击的发生. RS 通过下述操作完成对漫游用户 Bob 的合法性验证.

①通过等式 $e(Q_B, P) = e(W_B, P)e(V_B, P_{Pub}^{HS})$验证漫游身份证明信息 $<Q_B, W_B, V_B>$的合法性.

② 通过等式 $Sig_B P = (r_B + mS_B h_B)P = R_B + h_B Q_B$(其中 $h_B = H_1(TID_B \| R_B)$)验证密钥协商参数 R_B 的正确性.

当且仅当上述验证都通过时,RS 接受 Bob 的域间漫游申请,认为 Bob 是在 HS 处已完成注册的身份合法且平台可信的漫游用户.

③选取随机数 $r_{RS} \in Z_q^*$,计算 $R_{RS} = r_{RS} P$,生成临时漫游标识 $RID_{Bob} = TID_{Bob} \oplus ID_{RS} \oplus H_3(R_{RS})$.

④基于消息 $Enc(S_{HS}, TID_B \| Result)$可获知 Bob 平台的可信性验证结果,根据 TID_B 验证与 Bob 身份的一致性,同时可进一步确认 Bob 是在 HS 处注册的合法用户;在本地数据库中为 Bob 建立漫游认证信息库 $<TID_B, Result, RID_B, RLeg_B, Time, Length>$,其中 $RID_B = TID_B \oplus H_3(R_{RS})$, $RLeg_B = 0 \oplus H_3(R_{RS})$, Time 是漫游临时标识的签发时间, Length 是有效期.

⑤计算会话密钥 $k_{B,RS} = H(r_{RS} R_B \| ID_{Bob} \| ID_{RS})$后, RS 将 TID_B, RID_B, R_{RS}, $E(k_{B,RS}, RID_{Bob})$和 T_{RS}用 S_{RS}加密后发给 Bob.

(3) Bob 计算与 RS 间的会话密钥 $k_{B,RS} = H_1(r_B R_{RS} \| ID_{Bob} \| ID_{RS})$,并解密 $E(k_{B,RS}, RID_{Bob})$验证临时漫游标识 RID_{Bob}的正确性.

3.5 重复漫游机制

当 Bob 获得漫游临时标识 RID_{Bob}后,在其有效期内可持其向 RS 申请多次漫游服务,Bob 第 i 次的漫游申请过程如下所述:

(1) Bob 选取秘密数 $r_B^i \in Z_q^*$,计算 $R_B^i = r_B^i P$,更新临时漫游标识 $RID_B^i = RID_B^{i-1} \oplus H_3(R_{RS}^{i-1} \oplus H_3(R_B^i))$,其中 RID_B^{i-1} 为第 $i-1$ 次漫游时 Bob 的漫游标识, R_{RS}^{i-1}是第 $i-1$ 次漫游时 RS 产生的密钥参数. Bob 将消息 RID_B^i, R_B^i和 T_B^i用 P_{Pub}^{RS}加密后发送给 RS.

(2) RS 基于漫游注册信息验证 RID_B^i 的真实性.

①以 $RID_B^i \oplus H_3(R_B^i)$为索引,检索数据库中的相关记录信息 $RLeg_B$,并计算 $TID_B' = RID_B^i \oplus RLeg_B$,验证记录信息 TID_B 是否与 TID_B' 相等;

②根据 RID_B^i 的有效期、颁发时间等信息验证 RID_B^i 在当前时间是否有效;

③选取秘密数 $r_{RS}^i \in Z_q^*$,计算 $R_{RS}^i = r_{RS}^i P$,更新与 Bob 间的会话密钥 $k_{B,RS}^i = H(r_{RS}^i R_B^i \| ID_{Bob} \| ID_{RS})$.

④更新漫游认证信息,即 $RID_B = RID_B \oplus H_3(R_{RS}^i)$, $RLeg_B = RLeg_B \oplus H_3(R_{RS}^i) \oplus H_3(R_B^i)$.

RS 将 RID_B^i, R_{RS}^i, $E(k_{B,RS}^i, RID_B^i)$和 T_{RS}用 S_{RS}加密后发给 Bob.

(3) Bob 计算与 RS 间的会话密钥 $k_{B,RS}^i = H(r_B^i R_{RS}^i \| ID_{Bob} \| ID_{RS})$,解密 $E(k_{B,RS}^i, RID_B^i)$并验证临时漫游标识 RID_B^i 的正确性.

4 安全性证明

以本文域间漫游机制为例,在 CK 安全模型下对其安全性进行证明,文献[10~13]对 CK 安全模型的理想模型 AM、现实模型 UM 及会话密钥安全等基本定义进行了详细介绍.

4.1 困难性假设

判定性 Diffie-Hellman(DDH)问题. 设 G 为阶是大素数 q 的循环群, P 为群 G 的生成元;对于元组 (aP, bP, abP)和 (aP, bP, cP),其中 $a, b, c \in Z_q^*$ 且未知,DDH 问题的目标是判断 $abP = cP$. 任意概率多项式时间算法 $\mathcal{A}$ 成功求解 DDH 问题的概率 $Adv^{CDH}(\mathcal{A}) = |Pr[\mathcal{A}(aP, bP, abP) = 1] - Pr[\mathcal{A}(aP, bP, cP) = 1]|$是可忽略的.

4.2 AM 中的域间漫游机制

为简化协议证明过程,将本文域间漫游过程抽象

描述为协议 φ,协议 φ 描述如下:

(1)漫游请求. User 在注册阶段获得临时身份标识 TID_U;选取用于密钥协商的随机秘密数 r_U,并向 RS 发送漫游请求.

(2)漫游响应. RS 收到 User 的漫游申请后,首先验证消息的完整性及时戳的有效性,通过 TID_U 的合法性完成对 User 身份合法性及平台可信性的验证;选取用于密钥协商的随机秘密数 r_{RS},根据相应的验证结果 RS 发送漫游响应消息给 User.

定理 1　若 DDH 问题是困难的,且非对称加密、对称加密等算法均安全且难解时,漫游协议 φ 在 AM 中是会话密钥安全的.

证明　(1)在协议 φ 交互过程中,由于消息参与者没有被敌手攻陷,协议执行完毕时,User 和 RS 得到没有篡改的秘密随机数 $R_{US}=r_UP$ 和 $R_{RS}=r_{RS}P$,计算的会话密钥均为 $k=H(r_{RS}r_UP \parallel ID_U \parallel ID_{RS})$. 因此协议满足会话密钥安全的相关性质.

(2)假设在 AM 中存在一个敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 成功猜测会话密钥询问的应答是真实密钥还是随机值,那么存在输入为元组 (aP,bP,abP) 和 (aP,bP,cP) 的算法 $\mathcal{B}$,通过与敌手 $\mathcal{A}$ 的交互,能以不可忽略的优势解决 DDH 问题.

设猜测游戏的交互过程中敌手 $\mathcal{A}$ 发起会话的轮数为 L. 具体算法 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 间的交互过程如下:

①$\mathcal{B}$ 选择随机数 $J\in[1,L]$;

②$\mathcal{B}$ 调用敌手 $\mathcal{A}$ 完成域间漫游机制的模拟,发送公共参数 Params 给 $\mathcal{A}$;

③在第 J 次会话中,输入(User,RS,aP,bP,cP),调用 User 和 RS 间的会话,设 User 向 RS 发送(User,aP,ID_U);

④RS 收到(User,aP,ID_U)后,向 User 发送(RS,bP,ID_{RS});

⑤如果 User 选择会话(User,RS,J)作为最后一次测试会话,那么 $\mathcal{B}$ 向 $\mathcal{A}$ 提供 $k=H(cP,ID_U,ID_{RS})$ 作为会话密钥的询问应答;

⑥如果会话(User,RS,J)没有暴露,或者选择第 J 轮会话之外的某一次会话作为最后一次测试会话,或者 $\mathcal{A}$ 没有选择测试会话就终止了,那么 $\mathcal{A}$ 随机输出 $b\leftarrow\{0,1\}$($b=1$ 表示 k 是真实密钥,$b=0$ 表示 k 是随机值),然后终止;

⑦如果 $\mathcal{A}$ 终止并输出比特 b,那么 $\mathcal{B}$ 终止并也输出比特 $b'(b'=b)$(其中 $b'=1$ 表示 $cP=abP$,$b'=0$ 表示 $cP\neq abP$).

根据 $\mathcal{A}$ 的测试会话是否与算法 $\mathcal{B}$ 选择的一致,分两种情况讨论:

I. 敌手 $\mathcal{A}$ 选择的测试会话和随机选择的会话相同.

测试会话中,若 $\mathcal{B}$ 的输入元组满足 $cP=abP$,则给 $\mathcal{A}$ 的询问应答就是 User 和 RS 在会话 J 中的真实会话密钥;如果 $\mathcal{B}$ 的输入元组满足 $cP\neq abP$,则会话密钥的询问应答是随机的. 若 $\mathcal{A}$ 能以 $\frac{1}{2}+\varepsilon$(其中 ε 是不可忽略的)的概率猜对会话密钥的应答是真实值还是随机值,则算法 $\mathcal{B}$ 同样能以 $\frac{1}{2}+\varepsilon$ 的概率解决 DDH 问题.

II. 敌手 $\mathcal{A}$ 的第 J 次会话没有被选作测试会话.

此时,敌手 $\mathcal{A}$ 通常输出一个随机比特,然后结束会话;则 $\mathcal{A}$ 猜对会话密钥分布的概率是 $\frac{1}{2}$.

令事件 ε' 表示敌手 $\mathcal{A}$ 选择的测试会话恰好是第 J 次会话,即 $\Pr[\varepsilon']=\frac{1}{L}$.

若敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 猜对会话密钥询问应答是真实密钥还是随机值,则有:

$$\Pr[\mathcal{A}\text{猜测成功}]=\left(\frac{1}{2}+\varepsilon\right)\Pr[\varepsilon']+\frac{1}{2}(1-\Pr[\varepsilon'])=\frac{1}{2}+\frac{\varepsilon}{L}$$

由于算法 $\mathcal{B}$ 将敌手 $\mathcal{A}$ 作为子程序运行,即 $\Pr[\mathcal{B}$ 猜测成功$]\geqslant\Pr[\mathcal{A}$ 猜测成功$]$,则算法 $\mathcal{B}$ 能以不可忽略的优势解决 DDH 问题. 因此,协议 φ 满足会话密钥安全的相关性质.

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,User 和 RS 得到没有篡改的身份合法性及平台可信性验证信息,并协商安全的会话密钥,所以协议 φ 在 AM 中是安全的.

4.3　UM 中的域间漫游机制

将基于时间戳的签名认证器 $\lambda_{Sig,T}$(安全性证明详见文献[13])和基于身份的匿名认证器 $\lambda_{Enc,TID,T}$(安全性及匿名性证明详见文献[12])应用于本文 AM 中的协议;在对协议可证安全性不影响的前提下,隐藏 User 的身份标识信息,实现 User 身份标识的匿名性,使攻击者无法获得 User 真实有效的身份信息.

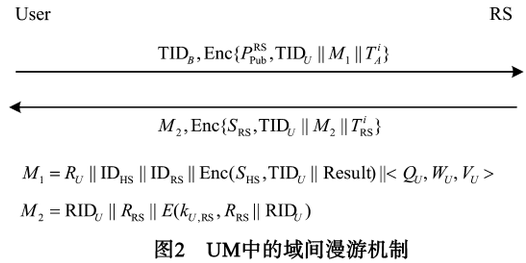

图2　UM中的域间漫游机制

定理 2 若 DDH 问题是困难的,且非对称加密算法、对称加密算法安全且难解时,漫游协议 φ 在 UM 中是安全的.

证明 如图 2 所示,运用基于时间戳的签名认证器 $\lambda_{\mathrm{Sig},T}$和基于身份的匿名认证器 $\lambda_{\mathrm{Enc,TID},T}$把协议 φ 直接转化为 UM 中会话密钥安全的安全漫游协议. 由于协议证明过程中所采用的签名认证器 $\lambda_{\mathrm{Sig},T}$ 和匿名认证器 $\lambda_{\mathrm{Enc,TID},T}$是可证安全的,根据 CK 安全模型自动编译得到 UM 中的漫游协议 φ 是可证安全的.

5 性能分析

5.1 计算效率

本文域间漫游机制包含 2 种不同的认证过程,分别为首次认证和重复认证,其中首次认证是指 User 首次向 RS 申请漫游服务;重复认证是指在 User 获得漫游标识 RID_U 后,持 RID_U 申请漫游服务. 本节将本文机制与传统漫游机制[14~17]就运算开销和认证特点进行比较,比较结果如表 1 所示.

表 1 仅对计算量较大操作(如加密,解密,指数等)进行了统计. 由表 1 可知,本文模型中 User 的计算量远小于文献[14,15]中相关方案的计算量;文献[16,17]的计算效率较高,却存在通信时延较高的不足;由于本文机制无需 HS 的协助,RS 直接对 User 的身份合法性和平台可信性进行验证,并且未使用计算量较大的指数运算,因此本文协议在未增加 RS 计算负载的基础下,减少模型的消息交互次数,降低了通信时延,提高了执行效率.

表 1 运算开销及认证模型比较(其中"—"表示方案未采用相关运算)

运算	首次认证	重复认证	文献[17]	文献[16]	文献[15]	文献[14]
对称加解密(User/RS/HS)	0/1/0	—	—	—	2/2/5	1/1/1
非对称加解密(User/RS/HS)	2/1/0	1/1/0	—	—	—	2/1/1
指数运算 (User/ RS/ HS)	—	—	—	—	—	—
群中的乘法运算 (User/RS/ HS)	—	—	2/2/0	—	2/2/0	—
信息交换次数(User-RS/ RS-HS)	2/0	2/0	3/2	4/4	2/2	3/2
认证特点	**直接认证** 无需 HS 的协助,RS 直接完成对漫游用户 User 的合法性验证		**间接认证** RS 需在 HS 的协助下完成对漫游用户 User 的合法性验证			

5.2 通信效率

域间漫游阶段,无需 HS 的协助 RS 可直接完成漫游用户 User 的身份合法性及平台可信性验证. 因此 User 与 RS 间通过 1 轮消息交互即可完成漫游申请,时延远远低于其他传统漫游方案[14~17],降低了漫游过程的通信负载和切换时延,同时有效减少漫游 User 的身份认证次数,防止 RS 和 HS 成为瓶颈;并且在重复漫游认证阶段实现 User 高效、快捷的安全漫游.

6 结束语

本文提出普适计算环境下的安全访问模型,User 申请漫游服务时,RS 无需 HS 的协助直接完成对 User 的身份合法性及平台可信性验证,采用临时身份实现用户的匿名性保护,不仅使远程网络和攻击者无法获知用户的真实身份,保护了用户身份等隐私信息的机密性;同时攻击者无法将截获的临时身份与已有的通信信息相关联,确保了用户身份和位置等隐私信息的不可跟踪性,有效防止攻击者针对用户实施跟踪、窃听等攻击行为.

下一步将继续优化本文机制,以提高实用性;同时根据现有的成果[16,17],进一步提高本文机制的计算效率.

参考文献

[1] Leed G, Kang S I, Seo D H, et al. Authentication for single/multidomain in ubiquitous computing using attribute certification[A]. International Conference on Computational Science and Its Applications[C]. Glasgow, UK: Springer Berlin Heidelberg, 2006. 326 – 335.

[2] Yao L, Wang L, Kong X W, et al. An inter-domain authentication scheme for pervasive computing environment[J]. Computers and Mathematics with Applications, 2010, 59(2): 811 – 821.

[3] Chan Y Y, Fleissner S. Single sign-on and key establishment for ubiquitous smart envionments[A]. International Conference on Computational Science and Its Applications[C]. Glasgow, UK: Springer Berlin Heidelberg, 2006. 406 – 415.

[4] Forne J, Hinarejos F, Marin A, et al. Pervasive authentication and authorization infrastructures for mobile users[J]. Computers & Security, 2010, 29(4): 501-514.

[5] 罗长远,霍士伟,邢洪智. 普适环境中基于身份的跨域认证方案[J]. 通信学报,2011,32(9):111 – 115.
Luo Chang-yuan, Huo Shi-wei, Xing Hong-zhi. Identity-based cross-domain authentication scheme in pervasive

computing environments[J]. Journal on Communications, 2011,32(9):111 – 115. (in Chinese)

[6] Alomair B, Poovendran R. Efficient authentication for mobile and pervasive computing[J]. IEEE Transactions on Mobile Computing,2014,13(3):469 – 481.

[7] Mcheick H, Deladiennee L, Wajnberg M, et al. Universal connector framework for pervasive computing using cloud technologies[J]. Procedia Computer Science,2014,34:141 – 148.

[8] 徐明迪,张焕国,张帆,等. 可信系统信任链研究综述[J]. 电子学报,2014,42(10):2024 – 2031.
Xu Ming-di, Zhang Huan-guo, Zhang Fan, et al. Survey on chain of trust of trusted system[J]. Acta Electronica Sinica,2014,42(10):2024 – 2031. (in Chinese)

[9] 谭良,陈菊,周明天. 可信终端动态运行环境的可信证据收集机制[J]. 电子学报,2013,41(1):77 – 85.
Tan Liang, Chen Ju, Zhou Ming-tian. Trustworthiness evidence collection mechanism of running dynamic environment of trusted terminal[J]. Acta Electronica Sinica,2013, 41(1):77 – 85. (in Chinese)

[10] 李兴华,马建峰,马卓. 可信计算环境下的 Canetti-Krawczyk 模型[J]. 电子学报,2009,37(1):7 – 12.
Li Xing-hua, Ma Jian-feng, Ma Zhuo. The Canetti-Krawczyk model under the trusted computation[J]. Acta Electronica Sinica,2009,37(1):7 – 12. (in Chinese)

[11] Jiang Chun-lin, Jia Wei-jia, Gu Ke, et al. Anonymous authentication without home server in mobile roaming networks[J]. Chinese Journal of Electronics,2013,22(2): 382 – 386.

[12] 姜奇,马建峰,李光松,等. 基于 WAPI 的 WLAN 与 3G 网络安全融合[J]. 计算机学报,2010,33(9):1675-1685.
Jiang Qi, Ma Jiang-feng, Li Guang-song, et al. Security integration of WAPI based WLAN and 3G[J]. Chinese Journal of Computers,2010,33(9):1675-1685. (in Chinese)

[13] Tin Y S T, Vasanta H, Boyd C. Protocols with security proofs for mobile applications[A]. Proceedings of the ACISP 2004[C]. Sydney, Australia: Springer Berlin Heidelberg,2004. 358 – 369.

[14] 侯惠芳,季新生,刘光强. 异构无线网络中基于标示的匿名认证协议[J]. 通信学报,2011,32(5):153 – 161.
Hou Hui-fang, Ji xin-sheng, Liu Guang-qiang. Identity-based anonymity authentication protocol in the heterogrnrous wireless network[J]. Journal on Communications,2011,32(5):153 – 161. (in Chinese)

[15] Zhang G, Fan D, Zhang Y, et al. A privacy preserving authentication scheme for roaming services in global mobility networks[J]. Security and Communication Networks (Published online in Wiley Online Library),2015. DOI: 10.1002/sec.1209.

[16] Chang C C, Lee C Y, Chiu Y C. Enhanced authentication scheme with anonymity for roaming service in global mobility networks[J]. Computer Communications,2009, 32(4):611 – 618.

[17] Mun H, Han K, Lee Y S, et al. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks[J]. Mathematical and Computer Modelling,2012,55(1):214 – 222.

作者简介

周彦伟　男,1986 年生于甘肃通渭,陕西师范大学计算机科学学院博士生. 研究方向为无线通信技术、匿名通信技术、密码学.
E-mail:zhouyanwei1986@163.com

杨　波(通信作者)　男,1963 年生于陕西富平,教授、博士生导师,陕西省"百人计划"特聘教授. 研究方向为密码学、信息安全.
E-mail:byang@snnu.edu.cn