一种基于融合网络通用可组合安全的漫游认证协议

李亚晖 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 无线网络融合是通信业发展的趋势,其中安全问题是当前研究的关注点。针对以3G网络为核心网络,采用蓝牙、WiMAX和无线局域网为接入网络构成的融合网络中认证协议的安全和效率问题,提出了一种高效的漫游认证协议。该协议通过对无线接入网络身份进行验证,抵御了重定向攻击的行为,实现了漫游认证的密钥分发;采用局部化认证过程,减少了认证消息的传输延时,提高了认证协议的效率,并给出了在NS2环境下的性能仿真结果。通过通用可组合安全模型对新协议进行的安全性分析,证明该协议具有UC安全属性。

关键词 无线网络,认证协议,会话密钥,漫游
中图法分类号 TP309 **文献标识码** A

Universally Composable Secure Roaming Authentication Protocol for Interworking Networks

LI Ya-hui MA Jian-feng
(Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071, China)

Abstract Security problems in interworking networks have attracted much attention of researchers recently. The typical interworking networks can be constructed with the core network WCDMA and the accessing networks WiMAX and WLAN. Considering security and efficiency issues, a roaming authentication protocol based on symmetric cryptographic algorithms was proposed for that network. It verified the identity of wireless access networks to prevent the re-direction attack, and used the localized authentication mechanism to reduce the message transmission delay and improve the efficiency of reauthentication process. The efficiency of proposed protocol was simulated in NS2. By analyzing the security of the proposed protocol with universally composable(UC) model, it proves that the proposed protocol satisfies the definition of UC security defined in the UC model.

Keywords Wireless network, Authentication protocol, Session key, Roaming

随着无线通信技术迅速发展,移动通信3G与蓝牙、WLAN和WiMAX等无线网络已逐渐成为市场新技术的主流。融合移动通信3G与蓝牙、WiMAX和WLAN等无线技术,实现用户在不同的接入方式下的无缝移动,可以利用宽带网络的优势带给用户全新的宽带体验和富有吸引力的优惠资费。近期3GPP提出了3GPP-LTE(Long Term Evolution)计划[1],主要实现在系统架构上能够与其他无线网络的互联。当前3G网络的特点包括网络覆盖范围广,能够提供语音、数据和多媒体等业务,具有很强的漫游功能,但是传输速率较低。蓝牙、WiMAX和WLAN等无线网络作为局部热点范围内的无线应用网络,能够为用户提供较高的传输速率和方便的接入服务。因此,以3G网络为核心网络,将蓝牙、WiMAX和WLAN等无线网络作为3G网络在热点地区的宽带接入方式,可以构造一种高效的融合网络应用模式。本文针对以3GPP为核心网络的融合网络的漫游认证协议进行研究和分析,提出了一种适用于多种无线接入网络(Wireless Access Network, WAN)的漫游认证协议RAKE(Roaming Authentication and Key Exchange),利用对称密码算法和哈希算法进行加密保护和身份认证,减少了移动用户的资源消耗,实现了3G移动用户在不同WAN之间的快速漫游认证过程,有效地减少了移动用户漫游切换的延时。

融合网络的安全需求主要包括:(1)身份隐藏。通常目的的认证密钥交换协议可能支持身份隐藏性,但也可能不支持。很多融合网络应用都把身份隐藏性作为基础,身份隐藏性被看成是融合网络漫游认证密钥交换协议的核心要求。身份隐藏需求具有保护对等参与方身份的能力,防御网络的偷听者和主动攻击者。(2)有效性。由于融合网络移动设备的便携性特点,融合网络漫游认证密钥交换协议容易受到身份假冒攻击、中间人攻击等。(3)并发安全性。使用融合网络的安全系统几乎总是高度并发的操作。在并发条件下,攻击者能自适应地修改通信内容,并发安全性强调融合网络实体涉及的协议是复合安全的。

本文主要在以下方面进行研究。首先,在UC安全框架模型[2]中,定义了融合网络漫游认证密钥交换协议安全模型,该模型包含身份隐藏性和可组合安全性需求。其次,提出了一个身份隐藏的融合网络漫游认证密钥交换协议,该协议保

到稿日期:2009-02-09 返修日期:2009-04-19 本文受国家自然科学基金项目(60633020, 60573036)资助。
李亚晖(1976-),男,博士生,主要研究方向为网络安全、安全协议,E-mail: ml_0902@163.com;马建峰(1963-),男,博士生导师,主要研究方向为密码学与网络安全。

证了协议的有效性和安全开销的最小化。然后，文献[3]提出了在 WCDMA 和无线接入网络互联中进行局部化认证的需求，因而 RAKE 协议对移动用户实现了在无线接入网络中的局部化认证过程。最后，对融合网络漫游认证密钥交换协议进行了安全性证明。

1 背景知识

1.1 基于 3G-LTE 的融合网络架构

在 3GPP-LTE 演进计划中[1]，对 3G 网络的体系结构进行了调整，简化了空中接口部分的复杂度，从而使其与 WiFi 和 WiMAX 等无线网络结构类似。在核心网络部分进行了扩展，通过 S2 接口可以和其他非 3GPP 无线网络进行 IP 层的结构互联，从而提高了它利用其他宽带无线资源作为接入网络的能力，如图 1 所示。

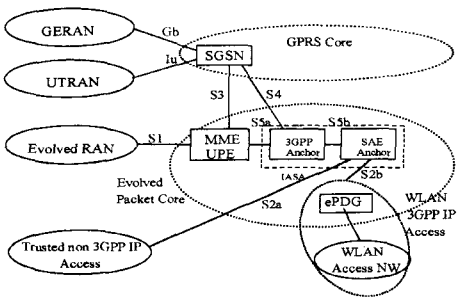

图 1 3GPP-LTE 网络体系结构

1.2 UC 安全模型

安全协议的研究一直是人们关注的话题。一般来说，安全协议研究分为两大阵营：符号逻辑观点和计算复杂性观点[4]。符号逻辑观点用简单的形式化语言和符号方法进行协议设计和推理分析，它包括 BAN 逻辑、GSP 方法、NRL 协议机等[5]。计算复杂性观点用一种计算模型和复杂性理论进行协议设计和推理分析，它包括当前流行的安全性证明 Random Oracle 模型[6]、安全多方计算模型[7,8]、Canetti-Krawczyk 模型[9,10]、通用可组合安全模型[2]等。

Bellare 等人[11]在 1998 年引入了可证明安全理论模块化的设计思想，通用可组合安全(UC 安全)是由 Canetti 提出的用于定义密码协议安全性的框架，在该框架中，定义了一个可以提供某种服务的不可攻陷的理想函数 F、虚拟参与者 $\tilde{P}$ 以及理想攻击者 S。每个虚拟参与者之间不能直接通信，理想攻击者 S 可以在任何时间攻陷任意的虚拟参与者。与此相对应，在该框架中还定义了能够实现上述特殊服务的真实协议 π、实际参与者 P 以及真实环境下的攻击者 A。在 UC 的安全框架中，利用一个环境机 Z 来模拟协议运行的整个外部环境(包括其它并行的协议、攻击者等)。Z 可以与所有的参与者($\tilde{P}$ 和 P)以及攻击者 A 和 S 直接通信，不允许直接访问理想函数 F。各个实际参与者间均可以直接通信，攻击者 A 可以控制它们之间的所有通信。也就是说，A 可以读取及篡改实际参与者间传递的任何通信内容，也可以在任何时候攻陷任何的实际参与者。通用可组合的安全框架如图 2 所示。

(1)通用可组合安全 (Universal Composable Security)：在 UC 的安全框架中，如果真实协议 π 可以在任何环境对于任何攻击者 A 都有与理想函数 F 同样的“行为”，就认为这是协议的一个安全实现。具体地说，如果对于任意的攻击者 A 和环境机 Z 而言，始终存在一个理想对手 S，使得 Z 无法区分是与虚拟参与者 $\tilde{P}$ 和 S 的交互，还是与实际参与者 P 和 A 的交互的话，就认为协议 π 安全地实现了理想函数 F 的功能(属性)。Canetti 等人证明了这个安全的定义具有一定的可组合性，并在此基础上开展了许多的工作。

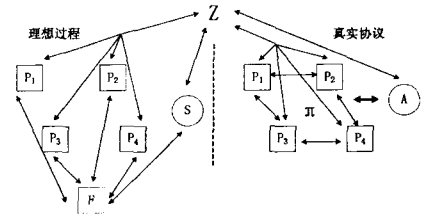

图 2 通用可组合的安全框架

(2)组合理论 (Composition Theorem)：UC 安全最重要的意义就在于可以利用已经设计好的子协议，安全地构建一个更为复杂的协议，从而实现指定的任务，并保证相应的安全属性。通常一个复杂的系统可以分解成多个子系统，每一个子系统都可以实现某个安全任务。Canetti 将这条性质定义为组合理论。组合理论可以保证通过使用已经证明是 UC 安全的子协议来构建一个更为复杂的、满足 UC 安全的密码协议。

(3)混合模型 (hybrid model)：为了描述上述理论以及形式化表述一个真实协议访问理想函数的多个副本(copy)的情况(如签名)，Canetti 引入了混合模型的概念。参与者除了在彼此之间发送信息，还可以与无限数量的理想函数 F 的副本进行交互。理想函数的副本通过会话标识 SID 来区分，发送给某一副本以及从该副本发出的所有消息都对应唯一的标识 SID。

2 漫游认证协议的描述

本文提出了以 3G 网络为核心网络的 RAKE 协议，对无线访问网络的身份验证抵御了 re-direction 攻击，对 3G 用户在无线访问网络之间的漫游切换提供了快速认证过程，有效地提高了 3G 与融合网络的接入过程的安全性和效率。本文对涉及到的 WCDMA 中的密码算法没有进行修改。在后文中计算会话密钥和消息认证码时，不再提及具体的密码算法。如图 3、图 4 和图 5 所示，流程中给出了消息发送的内容。

(1) $WAN \rightarrow UE$: *ID request*

(2) $UE \rightarrow WAN$: *ID response*, $[NAI]$

(3) $WAN \rightarrow 3G$: *ID response*, $[NAI]$

(4) $3G \rightarrow WAN$: *Auth data*, $RAND_1$, $AUTH_1$, MAC_1

(5) $WAN \rightarrow UE$: *Auth data*, $RAND_1$, $AUTH_1$, MAC_1, $Nonce_{AN}$

(6) $UE \rightarrow WAN$: *Auth data*, RES_1, $Nonce_{UE}$, $Nonce_{AN}$, U_{MAC}, MAC_1

(7) $WAN \rightarrow 3G$: *Auth data*, RES_1, $Nonce_{UE}$, $Nonce_{AN}$, U_{MAC}, MAC_1

(8) $3G \rightarrow WAN$: *Auth data*, SK_1, $\{(RAND, XRES, SK, AUTH)_i, \cdots\}$, $i>1$

(9) $WAN \rightarrow UE$: *Auth Success*

图 3 RAKE 协议的接入认证消息

(1) $WAN \rightarrow UE$: *ID request*

(2) $UE \rightarrow WAN$: *ID response*, $[NAI]$

(3) $WAN \rightarrow UE$: *Auth data*, $RAND_i$, $AUTH_i$, MAC_i, $i>1$

(4) $UE \rightarrow WAN$: *Auth data*, RES_i, MAC_i, $Token_i$, $i>1$

图 4 RAKE 协议重认证消息流程

(1)$NEW\ WAN \rightarrow UE: ID\ request, Nonce_{AN}$

(2)$UE \rightarrow NEW\ WAN: IDresponse, [NAI], Nonce_{UE}, U_{MAC}$

(3)$NEW\ WAN \rightarrow OLD\ WAN: ID\ response, [NAI], Nonce_{AN}, Nonce_{UE}, U_{MAC}$

(4)$OLD\ WAN \rightarrow NEW\ WAN: Auth\ dada, \{(RAND, XRES, SK, AUTH)_{i,\ldots}\}, i \geqslant 1$

(5)$NEW\ WAN \rightarrow UE: Auth\ data, RAND_1, AUTH_1, MAC_1$

(6)$UE \rightarrow NEW\ WAN: Auth\ data, RES_1, MAC_1$

(7)$NEW\ WAN \rightarrow UE: Auth\ Success$

图 5　RAKE 协议的漫游认证消息

说明如下：

(1)$RAND$ 是由 3G 网络产生的认证向量中的随机数，每个认证向量都会有一个新的随机数，用于计算会话密钥；

(2)$AUTH$ 是由 3G 网络产生的认证向量中的认证数据，用户实体(User Entity，UE)需要利用与 3G 网络共享的长期密钥来验证该数据的正确性；

(3)MAC 是每条消息的消息验证码，消息的接收者通过该消息验证码来鉴别消息的完整性；

(4)U_{MAC} 是 WAN 身份的验证码，由 UE 利用与 3G 网络共享的长期密钥计算得到。

$U_{MAC} = H(K_{3G,MS}, Nonce_{AN} || Nonce_{UE} || ID_{AN})$；

(5)$Nonce$ 是由 UE 和 WAN 产生的随机数，用于解决 WAN 身份验证码的重放攻击问题；

(6)$XRES$ 是由 3G 网络生成的认证码，用于验证 UE 的身份；

(7)RES 是由 UE 生成的认证码，它与 3G 网络计算用的 XRES 不同，用于验证 UE 的身份；

(8)SK 是由 3G 网络生成的会话密钥，发送给 WAN，用于建立 UE 和 WAN 之间的会话安全通道。

3　漫游认证协议的安全分析

3.1　协议的安全性分析

3.1.1　抗 Re-direction 攻击

在 RAKE 协议中，针对 EAP-AKA 协议可能存在的 Re-direction 攻击，在协议认证过程中间的 3 条消息中，引入了利用移动用户与 3G 网络之间共享的长期密钥对 WAN 的身份进行验证，以保证 3G 网络与用户之间对 WAN 身份的一致性。在图 3 的第 5 条和第 6 条消息中，各携带了随机数 $Nonce_{AN}$ 和 $Nonce_{UE}$，用来防止 WAN 的身份验证码的重放攻击。第 7 条消息中，WAN 将 $Nonce_{UE}$，$Nonce_{AN}$ 和 U_{MAC} 发送给 3G 网络。3G 网络接收到消息后，验证 U_{MAC} 的正确性。当 U_{MAC} 通过验证后，就表明 3G 网络与 UE 所持有的关于 WAN 的身份是相同的，从而防止 Re-direction 攻击的发生。

3.1.2　用户身份隐藏

RAKE 协议采用 3G 提供的用户临时身份技术，可以部分保护移动用户的真实身份，抵御第三方在无线信道中窃听用户的真实身份。但是，由于 3G 核心网络的临时身份体制允许接入网络无法识别临时身份时，可以要求用户发送真实身份信息，因此身份隐藏机制只能抵御被动攻击者。

3.2　协议的安全性证明

UC 模型最优秀的性质就是模块组合思想：可以单独设计子协议，只要协议满足 UC 安全，就可以进行组合，构造新的 UC 安全协议，并保证协议安全性。这里采用该安全模型来分析、证明所设计的新协议。

把新协议 π 拆分成 3 个子协议 π_1，π_2 与 π_3，其中 π_1 是 RAKE 协议的接入认证流程，π_2 是 RAKE 协议的快速重认证流程，π_3 是 RAKE 协议的漫游认证流程。本文主要证明 π_1 的安全性，π_2 与 π_3 的证明同理。那么根据通用可组合特性，π 就等价于 π_1，π_2 与 π_3 组合的安全性。

首先构造实现理想函数 F_{sig} 的协议 ρ_S：

协议参与者 P_i 与 P_j 运行基于签名算法 S 为 (gen, sig, ver) 的协议 ρ_S，进行交互。

(1)P_i 收到输入 $(signer, sid)$ 后执行算法 gen，保留的签名密钥 s 将验证密钥 v 发送给 P_j。

(2)若 P_j 需要对某消息 m 进行签名，则将 $(sign, sid, m)$ 发送给 P_i：P_i 令 $\sigma = sig(s, m)$，并将 $(signature, sid, m, \sigma)$ 发送给 P_j。

(3)若 P_j 需要对某消息 m 签名进行验证，则将 $(verify, sid, m, \sigma)$ 发送给 P_i：P_i 则输出 $(verify, sid, m, ver(v, m, \sigma))$ 给 P_j。

引理 1　S 为 (gen, sig, ver) 是文献[12]描述的签名，那么协议 ρ_S 对于静态的攻击者，在真实环境下，可以安全实现 F_{sig}，当且仅当 S 是抗击选择消息存在性伪造[2]。

其次，构造实现密钥交换理想函数 F_{KE} 的协议 π_1'：

(1)协议参与者 P_i 与 P_j 在混合模型 $F_{sig\text{-}hybrid}$ 中运行协议 π_1'，进行交互。

(2)若协议发起者 P_i 得到输入 (P_i, P_j, sid)，则发送初始化消息 $(signer, 0, sid)$ 给 F_{sig}；同样，若协议响应者 P_j 得到输入 (P_j, P_i, sid)，则发送 $(signer, 1, sid)$ 给 F_{sig}。

(3)P_j 选择 $n \in_R N$，发送 $(sign, 1, sid, (sid, n))$ 给 F_{sig}，F_{sig} 返回签名 σ_j，并发送 (P_j, sid, n, σ_j) 给 P_i；

(4)当 P_i 收到 (P_j, sid, n, σ_j)，则发送 $(verify, 1, sid, P_j, (sid, n), \sigma_j)$ 给 F_{sig}；如果通过验证，则 P_i 选择 $m \in_R N$，发送 $(sign, 0, sid, (sid, m))$ 给 F_{sig}，F_{sig} 返回签名 σ_i，P_i 计算 $K_{sid} = prf(K_{3G,MS}, sid, n, m)$；并发送 (P_i, sid, m, σ_i) 给 P_j；

(5)当 P_j 收到 (P_i, sid, m, σ_i)，则发送 $(verify, 0, sid, P_i, (sid, m), \sigma_i)$ 给 F_{sig}；如果通过验证，则 P_j 计算 $K_{sid} = prf(K_{3G,MS}, sid, n, m)$。

引理 2　如果消息认证码 MAC 的认证算法是安全的，则协议 π_1' 在混合模型 $F_{sig\text{-}hybrid}$ 下安全实现了 F_{KE}。

证明：构造一个理想环境下的攻击者 S(仿真器)，使得任何环境机 Z 都不能辨别它是与 H 及 π_1' 在 $F_{sig\text{-}hybrid}$ 下进行的交互，还是与 S 及 F_{KE} 在 Ideal-life 下进行的交互。即对任何环境机 Z，等式 $HYB^{F_{sig}}_{\pi_1', H, Z} \approx IDEAL_{F_{KE}, S, Z}$ 均成立。

(1)仿真器 S 的构造：S 运行一个模拟的攻击者 H，并按下面的规则进行操作：

①任何从 Z 的输入均传递给 H，任何 H 的输出将作为 S 的输出，使 Z 可以读取；

②若 S 从 F_{KE} 处收到 $(sid, P_i, P_j, role)$，则表明 P_i 发起了密钥交换，那么让 S 仿真出 F_{sig} 及 $F_{sig\text{-}hybrid}$ 下与 H 交互的协议 π'_1，并给定同样的输入。并且，S 让 H 和 P_i 按照 π'_1 的执行规则与 Z 交互；

③为了仿真 π'_1 的执行，S 可以激活 F_{sig} 得到相应的签名值 σ；S 也能计算 $k = prf(r, \cdot)$，其中 r 是 F_{KE} 给 P_i 和 P_j 的

密钥输出；

④当 π'_1 中的某个 P_i 需要产生本地输出时，如果对端 P_j 没有被攻陷，则 S 将 F_{KE} 的输出发送给 P_i；如果 P_j 已被攻陷，F_{KE} 会让 S 决定密钥，而 S 则使用 P_i 前面的输出来确定仿真的 P_i 与 P_j 的本地输出；

⑤当 H 执行攻陷 P_i 的操作，S 同样攻陷理想环境下对应的 P_i。如果 F_{KE} 已经给 P_i 发送了密钥，则 S 将得到该密钥；如果 P_i 和 P_j 均没有产生本地输出，则 S 将其内部状态传递给 H，包括它们的秘密选值；如果 P_i 或 P_j 其中一方已经产生了本地输出，则它们的秘密选值均被擦除，所以 S 直接将本地输出的密钥传递给 H。

(2)仿真器 S 的有效性：假设在仿真器 S 的执行下，存在一个环境机 Z'，成功辨别与 H 及 π'_1 在 $F_{sig\text{-}hybrid}$ 下进行交互及与 S 及 F_{KE} 在 Ideal-life 下进行交互的概率不可忽略，即使 $HYB^{F_{sig}}_{\pi'_1,H,Z} \neq IDEAL_{F_{KE},S,Z}$ 成立的概率为 $1/2+\varepsilon$，且该值远远大于 $1/2$，其中 ε 表示 Z' 的辨别优势。而这与 MAC 安全假设矛盾，所以得证。

引理 3 令 π'_1 为 $F_{sig\text{-}hybrid}$ 下的协议，ρ_S 为安全实现 F_{sig} 的协议，那么对于任何攻击者 A 都存在一个攻击者 H，使得对任何环境机 Z 来说，等式 $REAL_{\pi'^{\rho_S}_1,A,Z} \approx HYB^{F_{sig}}_{\pi'_1,H,Z}$ 均成立，即，组合协议 $\pi'^{\rho_S}_1$ 安全仿真了 $F_{sig\text{-}hybrid}$ 下的 π'_1[2]。

命题 1 真实环境下组合协议 $\pi'^{\rho_S}_1$ 与协议 π'_1 等价。

证明：将混合模型 $F_{sig\text{-}hybrid}$ 下协议 π'_1 对所有理想函数 $F_{sig(sid)}$ 的访问均替换为对协议 $\rho_{S(sid)}$ 的访问，可以得出协议 $\pi'^{\rho_S}_1$ 与协议 π'_1 等价，得证。

定理 1 真实模型下的协议 π_1 安全实现了理想函数 F_{KE}，即对任何环境机 Z，等式 $REAL_{\pi_1,A,Z} \approx IDEAL_{F_{KE},S,Z}$ 均成立。

证明：由引理 1—引理 3 及命题 1 得证。

4 漫游认证协议的性能分析

3GPP 针对 3G 网络和 WLAN 已经提出了一套互联方案[13]，并为互联的安全接入设计了一个 EAP-AKA 认证协议[14]。在该互联方案中，3G 用户通过 EAP-AKA 协议可以在 WLAN 局部认证接入到 3G 网络，并利用 WLAN 高速率的网络带宽访问 Internet 资源。由于 EAP-AKA 协议在不同的访问网络之间的漫游认证过程中，必须经过移动用户的归属网络进行认证、授权和计费，因此在移动漫游时认证过程的延时会严重影响用户的移动服务。

为了进一步分析协议的性能，基于 3G-WLAN 平台对 RAKE 协议进行了性能仿真。本文采用 NS-2.26 作为仿真平台，工作在一台 PC 机(C2.66G，256M RAM)上，操作系统为 Red Hat Linux 9.0。仿真场景包含由 6 个 AP 和 10 个移动节点构成的 2 个 WLAN、1 个接入网关 WAG 以及 3GPP 的访问网络和家乡网络 AAA 服务器。每个 WLAN 和 WAG 之间以一个 10Mb 带宽、1ms 时延的链路相连，WAG 和 AAA 服务器之间以一个 100Mb 带宽、1ms 时延的链路相连，仿真场景如图 6 所示。

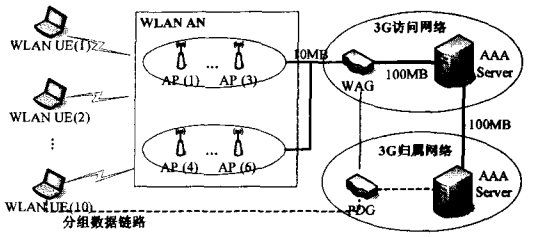

图 6 3G-WLAN 互联仿真场景

图 7、图 8 和图 9 的横坐标为认证次数；纵坐标为认证协议的执行时间，单位为秒。仿真结果表明，RAKE 协议全认证时延略大于 EAP-AKA，重认证和漫游认证的时延明显低于 EAP-AKA 协议。对于当前的无线网络，影响协议效率的最主要因素是消息传输延时。RAKE 协议虽然增加了一些传输负载，但是相对于 EAP-AKA，其平均消息传输延时减少了大约一半，提高了协议效率。

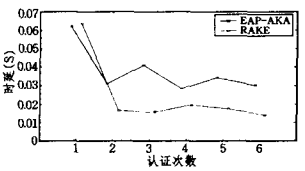

图 7 在归属网络认证的时延比较

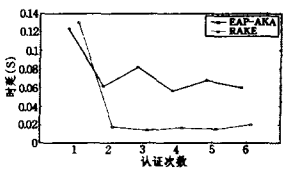

图 8 在访问网络重认证的时延比较

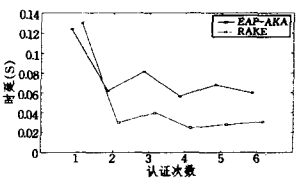

图 9 在访问网络漫游的时延比较

结束语 本文构造了一种以 3G 为核心网络的融合网络应用模式，给出了一个高效安全漫游认证协议 RAKE 的解决方案，使 3G 移动用户在无线接入网络中能够更加快捷、安全地漫游切换。由于采用对称密码算法对消息进行安全保护，节省了移动用户的资源消耗，便于移动终端使用。对无线访问网络的身份进行了验证，从而抵御了 Re-direction 攻击行为。在无线访问网络中的局部化认证，有效地减少了认证过程中消息的传送时延；在无线访问网络之间的快速漫游认证，使移动用户的漫游切换更加平滑。本文利用 UC 模型对 RAKE 协议进行了安全证明，该协议具有通用可组合安全属性。RAKE 认证协议改进了融合网络安全接入协议，具有一定的应用价值。

参 考 文 献

[1] 3GPP. TR 33.821 Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution(SAE)(Release 8)[S]. Valbonne:3GPP,2007

[2] Canetti R. Universally Composable Security: A New Paradigm for Cryptographic Protocols[C]//Proceedings of the 42nd IEEE Symposium on the FOCS. New York:IEEE Press,2001:136-145

[3] Chen Y, Hao C K. 3G and WLAN interworking security: current status and key issues[J]. International Journal of Network Security,2006,2(1):1-13

(下转第 78 页)

在隐藏信息流通道。解决方法就是采用临时强制性约束手段，将连通点对应的可读写文档禁止写操作，截断有向图之间的连通路径，则隐藏信息流通道将不再存在。

例如，对于当前用户 $s_0 \in S$ 来说，假定在时刻 t 时，新打开一个文档 d'，此时他所打开的开启文档集为 $OD(s_0)$，活动信息流图为 $AG(s_0)$。为了判别用户 s_0 的当前文档集 $OD(s_0)$ 是否安全，需要做下列分析。是否存在一个 $s \in S$，其所对应的权限信息流图 $G(s)$ 与有向图 $AG(s_0)$ 之间存在连通点 d'，并且至少存在一条连通路径。假设上述条件均满足，则表明当前活动用户的 $OD(s_0)$ 文档集是不安全的，如图 4 所示，存在隐藏信息流隐藏通道 $\langle d_0, d_1 \rangle$ 和 $\langle d_0, d_2 \rangle$。因而，在活动用户 s_0 新打开文档 d' 的同时，临时强制性约束禁止对文档 d' 的写操作，以截断有向图之间的连通路径，确保隐藏信息流通道不存在。

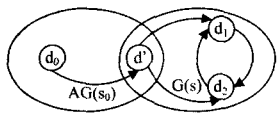

图 4　存在隐藏通道

在图 5 中，发现如果有向图 $AG(s_0)$ 与 $G(s)$ 之间仅仅存在连通点 d'，但是不存在任何连通路径，则表明当前活动用户的 $OD(s_0)$ 文档集是安全的。

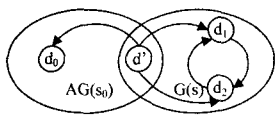

图 5　安全通道

下面给出活动信息流图 $AG(s_0)$ 隐藏信息流通道检测算法。

隐藏通道检测算法 Predict

描述：本算法依据当前活动用户 s_0 新打开的文档 d'，以及对应的活动信息流图 $AG(s_0)$，对全体用户集 S 所对应的信息流图 G 进行遍历，判断是否存在连通点 d' 并且连通路径同时存在。如果存在，遍历终止，并对连通节点文档进行强制性约束，禁止写操作。否则，说明 $OD(s_0)$ 是安全的。

输入：当前用户的活动信息流图 $AG(s_0)$，用户集 S 的各信息流图 G。

输出：$OD(s_0)$ 的动态约束条件。

1) for 所有 s∈S

1.1) if $V(G(s)) \cap \{d'\} \neq \emptyset$ then

1.2.1) for 遍历有向图 $AG(s_0)$ 和 $G(s)$ 中各节点

1.2.1.1) If $\langle d_0, d' \rangle \in E(AG(s_0))$，其中 $d_0 \in V(AG(s_0))$ and $\langle d', d_1 \rangle \in E(G(s))$，其中 $d_1 \in V(G(s))$ and $SC(d_0) \leqslant SC(d_1)$ then //存在隐藏信息流通道

1.2.1.1.1) 临时禁止 (s_0, d', w) 写权限，在关闭后恢复相关权限；//动态约束条件

1.2.1.1.2) 跳出 for 循环，遍历终止；

结束语　由于文档是企业组织信息资产的重要组成部分，为了预防内部威胁，防止内部滥用事件的发生，提出了一个针对文档信息流的多级安全策略模型，来保障企业组织中的信息资产。该模型不仅可以和其他安全策略混合使用，添加相关静态约束规则，而且，它将随着企业操作环境的上下文，对信息流通道进行动态约束，屏蔽相关的隐藏信息流通道，以保障文档操作环境的安全。

但是考虑到内部威胁的复杂性，在未来的研究中，有必要引入已知的各种内部威胁模式，作为该多级安全策略的一种强有力的补充，进行进一步的修订和完善。

参 考 文 献

[1] 王辉，刘淑芬. 一种可扩展的 Insider Threat 预测模型[J]. 计算机学报，2006，29：1346-1355

[2] Bell K，LaPadula L J. Secure computer systems：Unified exposition and multics interpretation[R]. MTR22997. MITRE Corporation，1976

[3] Denning D. A Lattice Model of Secure Information Flow [J]. Communications of the ACM，1976，19：236-243

[4] Brewer D，Nash M. The Chinese Wall security policy[C]//Proceedings of the IEEE Symposium on Research in Security and Privacy. Los Alamitos，CA：IEEE Computer Society Press，1989：206-214

[5] Pramanik S，Sankaranarayanan V，Upadhyaya S. Security Policies to Mitigate Insider Threat in the Document Control Domain [C]//Proceedings of the 20th Annual Computer Security Applications Conference. 2004

(上接第 50 页)

[4] Abadi M. Reconciling two views of cryptography[J]. Journal of Cryptology，2002，5(2)：103-227

[5] Mao Wenbo. Modern Cryptography：Theory and Practice[M]. Prentice-Hall，PTR，2004

[6] Bellare M. Random Oracles are Practical：a Paradigm for designing efficient protocols[C]//First ACM Conference on Computer and Communications Security. New York：ACM Press，1993：62-73

[7] Beaver D. Foundations of secure interactive computing [C]// Joan Feigenbaum：Advances in Cryptology-Crypto'91. Lecture Notes in Computer Science. Berlin：Springer-Verlag，1991：377-391

[8] Yao C. Protocols for secure computations (extended abstract) [C]//23rd Annual Symposium on Foundations of Computer Science. 160-164

[9] Canetti R. Analysis of key exchange protocols and their use for building secure channels[C]//Eurocrypt'01. 2001

[10] Canetti R. Security Analysis of IKE's Signature-based Key Exchange Protocol[C]//Advances in Cryptology- Crypto 2002

[11] Bellare M，Canetti R，Krawczyk H. A Modular Approach to the Design and Analysis of Authentication and Key-exchange Protocols[C]//Proc. of the 30th Annual Symp. on the Theory of Computing. New York：ACM Press，1998：419-428

[12] Goldwasser S，Micali S，Rivest R. A Digital Signature Scheme Secure Against Adaptive Chosen-message Attacks[J]. SIAM Journal on Computing，1998，17(2)：281-308

[13] 3GPP. TS 22.934 Feasibility Study on 3GPP System to Wireless Local Area Network (WLAN) interworking (Release 6)[S]. Valbonne：3GPP TSG SA，2003

[14] 3GPP. TS 33.234 Wireless Local Network(WLAN) Interworking Security[S]. Valbonne：3GPP，2005