移动网络中的独立式安全管理系统

董雨果,刘勤让,赵昭灵,邬江兴
(郑州信息工程大学,国家数字交换系统工程技术研究中心,河南郑州 450002)

摘 要: 本文提出一种适用于移动网络的安全管理系统,由于访问网络能够独立地对漫游用户进行认证,所以称该系统为独立式安全管理(ISM). 基于 ISM 设计一种漫游用户的认证协议,通过对协议的比较分析可以看出,相对于其它安全管理系统,ISM 的突出优点是安全责任划分清晰、认证效率高.

关键词: 移动网络; 认证; 漫游; 安全管理; 数字签名
中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2003) 02-0255-04

Independent Security Management for the Mobile Network

DONG Yu-guo, LIU Qin-rang, ZHAO Zhao-ling, WU Jiang-xing
(NDSC, Information Engineering University, Zhengzhou, Henan 450002, China)

Abstract: This paper proposes a new security management system for the mobile network, which uses the asymmetric cryptosystems to authenticate the mobile users. As the visited network can authenticate the user independently in roaming, the system is called independent security management (ISM). An authentication protocol based upon ISM is given. As shown in our analysis, the greatest advantage of ISM over other security managements is that the security responsibility is made clear and the authentication procedure is more efficient.

Key words: mobile network; authentication; roaming; security management; digital signature

1 引言

近年来,全世界对个人通信系统的需求迅猛增加. 为了更好的支持全球移动性,归属网络(登记网络)以及漫游网络(访问网络)必须提供漫游服务,这种能够提供漫游服务的网络就是移动网络. 随着第三代移动通信系统的出现,通信的移动网络正在迅速发展. 然而,全球移动性增加了网络遭受安全攻击的可能性并引起许多安全问题,显然全球移动网络需要比现有网络安全技术更强健高效的新技术. 所以在移动网络中引入可靠的认证技术是非常必要的.

由于现有数字蜂窝系统的安全技术(例如 GSM 的认证技术[1]和 IS-41 的认证技术[2])采用 VLR[3](visitor location register)网络体系,所以并不适宜于全球移动环境[4]. 因此,文献[4~6]提出一些新的认证技术和协议. 由于应用私钥体制,这些协议需要大量的认证密钥,这使得密钥的管理及分发工作变得很复杂. 文献[7]和[8]采用公钥体制和数字签名技术,需要的密钥少,但是用户端及网络的计算量很大[9].

为此,我们提出一种新的安全管理系统模型,该模型采用数字代理签名技术[10],对全球移动网络中的移动用户进行认证. 由于访问网络能够独立地对漫游用户进行认证,所以称该系统为独立式安全管理(ISM). 相对于其它安全管理系统,ISM 的突出优点是安全责任划分清晰、认证效率高.

收稿日期:2001-08-06;修回日期:2001-12-20
基金项目:国家 863 重大课题基金(No. 863-300-01-03-99)

2 概念

为研究清楚安全性能,必须对网络的各个实体进行安全性划分[11,12]. 简明起见,本文假设移动网络由移动用户、用户的归属网络和访问网络 3 个基本部分组成,这里仅研究移动用户漫游时移动用户与访问网络的相互认证. 以下对本文的重要概念进行阐述.

2.1 独立式安全管理(ISM)

GSM 和 TIA/EIA IS-41 可被看作是集中式安全管理系统,归属网络的安全管理器通过集中方式来管理整个全球网络的安全[4]. 文献[4,5]提出分布式安全管理的模型,在此模型中,归属网络的安全管理器仅在服务建立阶段参与对整个网络的安全管理. 然而,由于用户在全球移动,所以归属网络根本不可能对世界上所有访问网络的安全性进行管理. 这就要求归属网络和访问网络的关系尽可能松弛,它们应该独立的去管理移动用户. 独立式安全管理能够满足全球移动性的要求. 独立式安全管理中,在任何服务阶段归属网络和访问网络都能够独立地对所有用户(包括本地用户及漫游用户)的安全性进行管理. 当用户在本地网接受服务时,归属网络将管理其安全;一旦用户漫游超出归属网络的服务范围,并开始接受访问网络的服务,访问网络应该全权负责此漫游用户的安全. 由于

把漫游用户的安全管理划分给访问网络,因而加强了安全管理的难度.实际上,任何网络既是归属网络又是访问网络(对它的本地用户而言,它是归属网络;对漫游用户来说,它又是访问网络).从这个角度看,所有网络的负荷都是一样的.为提高安全管理的效率,访问网络管理器需要一个安全管理代理,它可以专门用来管理漫游用户.代理的问题将另文详述.

2.2 归属网络证明

漫游期间访问网络对用户进行认证时,用户需要表明:

①他(她)归属于某合法网络;

②他(她)是合法用户.

为了满足要求①,我们在认证协议中采用归属网络证明 HNC(Home Network Certification).当移动用户在归属网络注册时,归属网络向该用户分发 HNC,HNC 含有移动用户的公钥和归属网络的私钥,显然,HNC 仅能由归属网络生成,而且仅适用于特定的用户.另外,鉴于对私钥的保密,HNC 的生成算法要保证任何别的实体不可能由 HNC 获知归属网络的私钥.

2.3 漫游认证密钥

与访问网络进行相互认证前,移动用户利用归属网络分发的 HNC 及自己的私钥生成漫游认证密钥 RAK(Roaming Authentication Key).与 HNC 类似,RAK 仅能由该用户生成,同时 RAK 的生成算法要保证任何别的实体不可能由 RAK 获知用户的私钥.移动用户用 RAK 对其发送的信息进行代理签名,访问网络通过对代理签名的验证可以同时认证用户和他(她)的归属网络.由此可见,RAK 能同时支持①和②两条要求.

2.4 用户登记阶段

在该阶段,用户开始从归属网络漫游到访问网络,并向访问网络发出漫游服务的请求.这时访问网络与漫游用户进行信令交换,从而访问网络可以独立的认证用户及其归属网络,并且用户也认证访问网络.认证结束后,访问网络认可该用户为合法漫游用户,并为他建立起漫游服务的环境.移动用户离开归属网络漫游到访问网络,在访问网络为用户建立起漫游服务之前,用户利用已生成的 RAK 对所传送的信息进行签名,然后与访问网络进行信息交互.在此交互过程中完成访问网络对移动用户及其归属网络的认证,以及用户对访问网络的认证,并且建立起后续呼叫阶段的双方共享的认证密钥(TAK_0).该阶段的认证过程仅在移动用户与访问网络之间发生,无第三实体参与.

2.5 后续呼叫阶段

用户登记阶段完成以后,访问网络可以直接向漫游用户提供漫游服务.在每次访问网络向用户提供漫游服务之前,访问网络与用户利用前-后续呼叫阶段生成的认证密钥 TAK_i 完成相互认证,并建立起下一阶段的认证密钥 TAK_{i+1}.该阶段的认证过程也仅在用户和访问网络之间发生.

3 ISM 的功能结构

ISM 的功能体系结构如图 1 所示.该体系中,归属网络管理 HNC,用户将利用 HNC 生成 RAK.访问网络管理 TAK,它是访问网络和漫游用户的共享认证密钥.任何阶段用户都应该负责管理他的 RAK,它将用来进行代理数字签名以验证用户自己和他的归属网络.在本地网络时,用户的安全由归属网络管理;当漫游出本地网络时,访问网络应该全权负责对漫游用户的安全管理.在漫游期间,漫游用户及访问网络都不应该与归属网络发生联系,也就是说,归属网络和访问网络的安全管理是独立实现的.

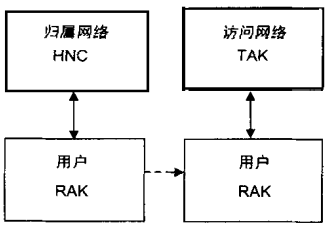

图 1 ISM 的功能结构体系

4 基于 ISM 的认证协议

为进一步阐述 ISM 的原理,我们基于 ISM 设计了一种漫游用户的认证协议.为了便于对协议的描述,首先对有关的参数和符号等作如下说明:

系统中的公开参数:p, g.其中 p 是一个素数模且 $2^{511} < p < 2^{512}$; g 是 $GF(p)$ 中阶为 $p-1$ 的一个生成元.各实体的密钥:归属网络 HN 具有两对密钥:私钥 s_{HN},公钥 R_{HN}及另一私钥 k_{HN},公钥 L_{HN};访问网络 VN 具有一对密钥:私钥 s_{VN},公钥 R_{VN};移动用户具有一对密钥:私钥 s_u,公钥 R_u.所有实体的公钥 R 与私钥 s 满足以下关系:

$$R = g^s \bmod p \qquad (1)$$

HNC:归属网络证明.RAK:漫游认证密钥.R_{RAK}:RAK 所对应的公钥,用来验证 RAK 生成的代理签名.AS_{VN}:访问网络 VN 中的认证服务器.ID_{VN}:AS_{VN} 的标识.ID_u:移动用户的标识.(a)访问网络在协议执行过程中所产生的一次性随机数(nonce).(b)移动用户在协议执行过程中所产生的一次性随机数.TAK_0:用户登记阶段中访问网络生成的一随机数,作为后续呼叫阶段用户与访问网络共享的认证密钥.TAK_i:前一次后续呼叫阶段中移动用户生成的一随机数,作为本次阶段用户与访问网络共享的认证密钥.TAK_{i+1}:本次后续呼叫阶段中移动用户生成的一随机数,作为下一阶段用户与访问网络共享的认证密钥.‖:连接操作(concatenation)符,例如:1011 ‖ 0010 = 10110010.$Sig_K(M)$:利用密钥 K 对信息 M 进行签名.$H(M)$:求信息 M 的 hash 值,其中 H 为系统中公开的单向 hash 函数.$K(M)$:利用密钥 K 对明文 M 进行加密.

假定本认证协议执行 ITU-T 的 X.509 公钥认证机制,因而每个实体都能够安全地获得其它实体的公钥;本协议不特别指明加解密、数字签名及验证签名的算法,移动通信系统可根据具体需要选取适当的算法.另外,为简便起见本文省略对数学公式的推导和证明.

下面是对认证协议的详细描述,该协议分为三个子协议.

4.1 RAK 的生成协议(P_1 子协议)

该子协议中用户生成 RAK,为漫游期间的认证做好准备.

® 当用户在其归属网络注册时,归属网络通过下式为用户生成 HNC.

$$HNC = s_{HN} + k_{HN} R_u \bmod (p-1) \qquad (2)$$

® 归属网络向用户发送信息 R_u(HNC ‖ H(HNC)).

® 用户用自己的私钥 s_u 解密信息,得到 HNC ‖ H(HNC);

用户计算出 HNC 的 hash 值,可以对 HNC 的完整性进行鉴别:如果计算出的 hash 值与归属网络所给的 hash 值不等,则拒绝接受该信息,终止该协议;若相等,则表明该信息是完整的,而且可通过下式来验证信息来源的合法性.

$$g^{HNC} = R_{HN} L_{HN}^{Ru} \bmod p \quad (3)$$

如果上式成立,则确认 HNC 的发送者是归属网络;如果不成立,则终止协议.

® 移动用户通过下式生成 RAK.

$$RAK = HNC + s_u \bmod (p - 1) \quad (4)$$

4.2 用户登记的认证协议(P_2 子协议)

该子协议对应于用户登记阶段.

® 当移动用户漫游到访问网络的服务区域时,移动用户收到访问网络广播的区域标识信息,其中包括 AS_{VN} 的标识 ID_{VN}. 通过比较标识信息 ID_{VN} 和存储在用户终端的信息,移动用户判断出漫游服务状态. 并且,用户利用 ID_{VN} 可获得访问网络的公钥 R_{VN}.

® 移动用户向访问网络发出漫游服务请求,其中包括用户的标识 ID_u.

® 访问网络收到移动用户发出的漫游服务请求,通过比较标识信息 ID_u 和存储在网络终端的信息,访问网络判断出漫游服务状态. 利用 ID_u 访问网络可获得移动用户的公钥 R_u 和其归属网络的公钥 R_{HN} 及 L_{HN}.

® 访问网络生成一随机数 a,并且向移动用户发送 a.

® 收到 a 后,移动用户生成一随机数 b,并且用 RAK 对 a、b 进行签名得到 $Sig_{RAK}(a, b)$.

® 移动用户向访问网络发送代理签名 $Sig_{RAK}(a, b)$ 作为响应信号.

® 访问网络通过下式生成用来验证代理签名的公钥 R_{RAK},然后访问网络用 R_{RAK} 对代理签名进行验证,如果验证成功,则可以认证该用户及其归属网络,并接受 b;否则,终止协议.

$$R_{RAK} = R_{HN} L_{HN}^{R_u} R_u \bmod p \quad (5)$$

® 访问网络生成一随机数 TAK_0 作为后续呼叫阶段的认证密钥,求出它的 hash 值 $H(TAK_0)$,然后用自己的私钥对 TAK_0 和 $H(TAK_0)$ 进行签名,最后访问网络向用户发送信息 $R_u(TAK_i \| Sig_{Svn}(H(TAK_0), b))$.

® 移动用户用自己的私钥解密所收到的信息,再利用访问网络的公钥 R_{VN} 验证签名 $Sig_{Svn}(H(TAK_0), b)$:如果验证成功,则可以认证访问网络;否则,终止协议. 此外,用户还应计算出 TAK_0 的 hash 值,利用计算出的 hash 值与签名中的 $H(TAK_0)$ 作比较:如果它们相等,则可以证明 TAK_0 的完整性,并且用户接受 TAK_0 作为认证密钥;否则,用户拒绝接受该信息.

至此,用户登记阶段的认证协议已完成.

4.3 后续呼叫认证协议(P_3 子协议)

该子协议对应于后续呼叫阶段. 该子协议中的相互认证是通过用户与访问网络共享的认证密钥 TAK_i 来实现的. 访问网络判断出漫游服务状态后,

® 访问网络生成一次性随机数 a,并向移动用户发送 a.

® 移动用户生成随机数 TAK_{i+1} 作为下一次阶段的认证密钥,并向访问网络发送 $TAK_i(a, TAK_{i+1} \| H(TAK_{i+1}))$ 作为响应.

® 访问网络解密 $TAK_i(a, TAK_{i+1} \| H(TAK_{i+1}))$. 通过 a 访问网络可认证用户;通过比较计算 TAK_{i+1} 的 hash 值与信息中的 hash 值可完成 TAK_{i+1} 的完整性验证.

® 访问网络向移动用户发送 $TAK_i(TAK_{i+1})$.

® 移动用户通过解密 $TAK_i(TAK_{i+1})$ 得到 TAK_{i+1} 可认证访问网络.

至此,后续呼叫认证协议已完成,移动用户与访问网络之间成功进行了双向认证,建立起下一阶段的认证密钥.

5 协议的性能分析

5.1 安全性分析

下面对本文提出的认证协议的安全性进行分析.

(1) 安全责任:在子协议 P_2 和 P_3 中,用户仅与访问网络发生联系,即用户漫游期间的安全管理只由访问网络负责,在此期间发生的安全事故仅由访问网络承担. 在 P_2 中,访问网络通过验证用户在 P_1 中生成的代理签名可直接认证用户及其归属网络,不必与归属网络接触;在 P_3 中,用户与访问网络利用 P_2 中生成的认证密钥可直接相互认证. 从而子协议 P_2 和 P_3 对安全责任区域作出清楚的划分.

(2) 双向认证:移动通信中,双向认证的目的是鉴别认证实体身份,防止假冒实体的攻击. 假冒实体的通用攻击手段包括:(a) 获取合法实体的私钥或认证密钥. (b) 重放攻击,即利用合法实体以前使用过的信息进行非法访问.

本协议传输的密文中包含密钥(如 TAK). 假冒实体可能对传输的密文进行分析,解出密钥,这种可能性取决于加密算法的安全性. 本文假定协议所采用的加密算法具有足够高的安全性. 协议中的一次性随机数 a、b 及随机数 TAK 用于抵抗重放攻击.

(3) 不可抵赖性:当用户否认访问网络向他(她)提供过漫游服务,访问网络可将代理签名 $Sig_{RAK}(a, b)$ 作为证据交由共同信赖的第三方进行仲裁,因为用于签名的密钥 RAK 含有用户的私钥 s_u,只有用户才能生成 RAK,别的实体甚至包括归属网络都不能够伪造出 RAK,所以用户无法抵赖曾接受过访问网络的服务.

(4) 信息完整性:本协议采用 hash 函数来保证信息的完整性.

5.2 运行效率分析

如表 1 所示,为分析本协议的运行效率,我们把它与一些具有代表性的认证协议(文献[4][5])作比较. 其中,文献[4]采用私钥体制,而文献[5]采用私钥/公钥混合体制. 表 1 中,s 与 p 分别代表用户登记阶段和后继呼叫阶段,U、H、V 分别代表用户、归属网络和访问网络;随机数包括认证过程中生成的随机密钥.

表 1 运行效率的比较

		认证步骤		随机数个数		公钥加/解密		私钥加/解密		HASH 函数		保存密钥
		s	*p*	*s*	*p*	*s*	*p*	*s*	*p*	*s*	*p*	
文献[4]	*U*	7	4	0	0	0	0	5	3	不提供信息完整性		1
	V			4	1	0		7	3			2
	H			1	0	0		5	0			1
文献[5]	*U*	6	4	1	1	0	0	0	2	3	2	1
	V			2	1	1		0	2	2	2	2
	H			1	0	0		0	0	5	0	1
本文	*U*	4	4	1	1	3	0	0	2	1	1	0
	V			2	1	3		0	2	1	1	0
	H	0										

由表 1 可知,我们的协议在认证步骤、随机数生成、加/解密以及事先保存密钥等方面都比其它两个协议优越,具有较高的运行效率.

6 结论

本文提出一种适合全球移动网络的新型安全管理模型 ISM. 这种系统模型基于公钥体制实现用户认证. 该系统通过两个步骤进行安全管理:登记阶段和后继呼叫阶段. 在 ISM 中,访问网络能够独立地对漫游用户进行认证. 相对于其它安全管理,ISM 的突出优点是安全责任划分更加清晰、认证效率更高. 当然,支持这种新认证技术(如公钥的管理和分发机制)还需要进一步研究.

参考文献:

[1] D Brown. Techniques for privacy and authentication personal communication systems [J]. IEEE Personal Commun,1995.

[2] TIA/ EIA IS-41. Cellular Radio Telecommunications Intersystem Operations [S]. 1991.

[3] TTC JJ-70.10. Personal Digital Cellular Digital Mobile Communication Networks Inter-Node Interface-Mobile Application Par [S]. 1995.

[4] Shigefusa Suzuki, Kazuhiko Nakada. An authentication technique based on distributed security management for the global mobility network [J]. IEEE Journal on select, 1997:1608 - 1617.

[5] 刘建伟,等. 基于 Krypto Kinght 的移动用户认证协议 [J]. 电子学报,1998,26(1):93 - 97.

[6] Liu Jian-wei, Wang Yu-min. A user authentication protocol for digital mobile communication network [A]. Seventh IEEE International Symposium on Personal, Indoor and Mobile Radio Communications [C]. 1996.

[7] M J Beller, et al. Privacy and authentication on portable communication system [J]. IEEE J. on SAC, August 1993, 11(6):821 - 829.

[8] A Aziz, W Diffie. Privacy and authentication for wireless local area networks [J]. IEEE Personal commun, First Quarter 1994:25 - 31.

[9] 王育民,刘建伟. 通信网的安全 - 理论与技术 [M]. 西安市:西安电子科技大学出版社,1999. 487 - 494.

[10] Kim S, et al. Proxy signatures, Revisited [A]. ICICS '97 [C]. 1997. 223 - 232.

[11] ITU-T, Draft Recommendation Q. ASEC. Security Mechanisms and Protocols for Protecting the Access to Network Services [S]. 1997.

[12] ITU-T, Draft Recommendation Q. NSEC. Network Security [S]. 1997.

作者简介:

董雨果 男,1976 年 7 月生于四川雅安,1998 年、2001 年于空军工程大学分别获工学学士、工学硕士学位,现为国家数字交换系统工程技术研究中心博士生,已发表论文数十篇,主要研究方向为通信网络安全、路由技术. E-mail: dyg@mail.ndsc.com.cn

刘勤让 男,1975 年 11 月生于河南睢县,国家数字交换系统工程技术研究中心博士生,主要研究方向为无线通信,移动 IP 技术.

赵昭灵 1976 年生,国家数字交换系统工程技术研究中心博士生,主要研究方向为主动网络.

邬江兴 1953 年生,教授,博士生导师,国家数字交换系统工程技术研究中心主任,国家超级 863 计划软课题研究组成员,国家级有突出贡献专家,全国优秀科技工作者.