基于证书的移动通信认证模型

朱 斌[1], 张琳峰[1], 朱海云[2]
(1. 华南理工大学计算机系, 广东广州 510640; 2. 广东省电信科学技术研究院, 广东广州 510630)

摘 要: 本文针对 GSM 移动通信系统的安全缺陷, 提出了一种基于证书的安全认证模型, 并设计了基于证书的移动通信安全协议. 该模型将 IP 网络的 CA 认证技术引入到无线网络, 并对经典 PKI 进行了改进, 将身份认证和访问授权进行了区分, 实现了密钥和持有人的 1∶n 关系, 并支持匿名访问. 通过实验证明了证书模型解决移动通信安全性的可行性.

关键词: 移动通信; 认证中心; 身份证书; 授权证书
中图分类号: TN929.5 文献标识码: A 文章编号: 0372-2112 (2002) 06-0868-04

An Authentication Model in Mobile Communication System Based on Certificates

ZHU Bin[1], ZHANG Lin-feng[1], ZHU Hai-yun[2]
(1. *Dept. Computer Science and Engineering, South China University of Technology, Guangzhou, Guangdong 510630, China;*
2. *Guangdong Telecommunication Academy of Science and Technology, Guangzhou, Guangdong 510630, China*)

Abstract: In order to overcome the security weakness of the GSM system, this paper presents an authentication model and security protocols based on certificates. The new model introduces the CA technology of IP network into the mobile communication systems. It improves on classical PKI, distinguishes access authentication from identification, implements the 1∶n relationship between keyholder and keypair, also it supports anonymous access. In addition, the feasibility of using certificate model in the mobile communication system is verified by some tests.

Key words: mobile communication system; certification authority; identification certificate; authorization certificate

1 移动通信系统的安全缺陷与改进思路

在移动通信中, 在归属域注册的用户经常出现在另一个域申请服务, 这样就出现了涉及三方的身份认证过程: 移动用户、访问域、归属域. GSM (Global System for Mobile Communication) 的认证思路是, 通过移动用户向访问域的 VLR (Visitor Location Register) 发出申请, 然后由 VLR 把移动用户的身份以及其它信息传递给归属域 HLR (Home Location Register), 最后由 HLR 确定移动用户的身份后, 把确定的信息和与之相关用户的现在状态传递给 VLR, 完成认证过程. 总体上说, 现有的 GSM 移动通信系统采用的是传统对称密码体制, 由 PIN (Personal Identity Number) 码与 SIM (Subscriber Identification Module) 卡相结合产生鉴权应答的方式作为安全管理方案[1]. 这种方案因算法简单而被大多数移动通信系统所采用, 但是, 它存在以下一些安全方面的不足:

第一, 它只能提供 MS (Mobile Station) 与 MSC (Mobile-service Switching Center) 之间线路的保密, 而用户信息对于通信网却是暴露的;

第二, AUC (Authentication Center) 向 MSC/VLR 传送有关用户鉴权数据时可能受到安全攻击, 同时 MSC/VLR 必须存储所有访问它的用户鉴权数据, 增加了数据库安全管理的困难;

第三, 移动台无法对 MSC 的身份进行鉴别, 使非法盗用者窃取移动台的用户密钥成为可能;

第四, 存储用户数据的拜访局 (VLR) 和归属局 (HLR) 也可能遭到网络内部攻击者的侵入, 窃取合法用户的身份信息和密钥, 从而假冒合法用户身份, 而且, 不同网络经营者之间可能出于竞争目的, 假冒对方合法用户身份, 破坏对方网络的正常运营. 漫游网络之间由于利益冲突, 也可能否认对方提供的服务.

总之, 现有的基于对称密钥技术的 GSM 系统无法解决 GSM 内部的不安全因素. 那么, 如何实现端到端身份鉴权和会话密钥交换功能, 同时要保证两个移动用户之间的保密通信不被包括通信网络操作员在内的其它人窃听? 仅仅采用对称密钥技技术是不够的, 笔者认为有必要引入非对称密钥技术, 而手机终端和 SIM 卡等硬件设备的功能日益增强, 使得这一改进思路成为可能. 目前 PKI (Public Key Infrastructure)[2] 在 Internet 的成功应用已经显示出公钥密码体制的生命力, 但是

收稿日期: 2001-04-09; 修回日期: 2001-08-18

PKI 所采用的 X. 509 证书格式以及 PKI 信任模型都暴露出一定的局限性,因此我们不能简单地将 PKI 照搬到移动通信系统. 随着移动通信网络的 IP 化,以及移动数据业务的兴起,移动通信系统的安全性涉及到认证、保密、防抵赖等多个方面,其中认证和访问授权是首要的问题,同时要考虑用户的隐私保护.

2　基于证书的移动通信认证模型

以公共密钥体制为基础,针对移动通信的特点,笔者提出了一种基于证书的移动通信认证模型(如图 1 所示). 该模型借鉴了经典 PKI 的优秀思想[3,4] 但克服了 PKI 的局限性,将身份认证和访问控制分离,不仅可以实现用户认证和保密通信,而且可以支持匿名访问和不可否认业务,并有利于数据增值业务的快速开发和应用.

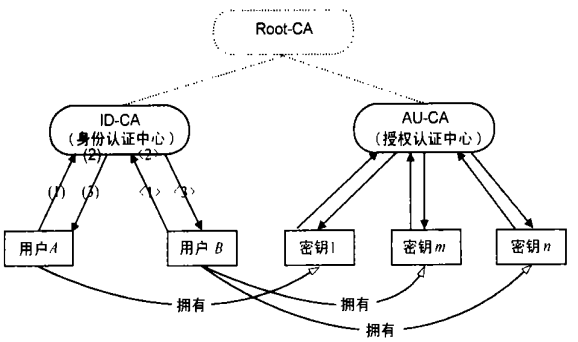

图 1　移动通信证书认证模型

其中 ID-CA(Identification CA) 指身份鉴别中心,负责签发和管理身份证书; AU-CA(Authorization CA) 指访问授权中心,负责签发和管理授权证书.

2.1　身份认证模型:ID-CA

在基于 ID-CA 认证的移动通信系统中,假设每个用户拥有 ID-CA 签发的数字身份证书. 证书中应包含用户身份(ID)、公开密钥、有效日期、以及证书机构的签名等内容,定义用户 A 的证书形式如下:

$$ID\text{-}Cert_A = \{ ID_A, pub_A, period_A, others, [hash(ID_A, pub_A, period_A, others)]Sign_{ID\text{-}CA}\};$$

其中,ID_A 指移动用户 A 的有效身份,如可以用身份证标识; pub_A 指用户 A 的公开密钥; hash() 是一个单向散列函数,如可以采用 MD5 或者 SHA1; $period_A$ 指证书的有效期限,包括生效和失效时间; $[\cdots\cdots]Sign_{CA}$ 指用 CA 私钥对 [……] 内容签名后的结果,其有效性可以使用 CA 公钥进行验证,而 CA 的公钥算法可以采用经过实践证明的 RSA 算法或者具有较低运算量的椭圆曲线算法 ECDSA(参见 X9.62); others 指证书中包含的其它信息,如发行者、所用算法的标识、证书版本号、证书内部标识、以及一些证书扩展域等.

考虑到 RSA 是迄今为止理论上最为成功的公开密钥密码体制,以 RSA 为例, CA 的初始化过程如下[5]: 根据 RSA 公钥密码算法,选择两个大素数 p 和 q,计算 $N = pq$ 和 $\varphi(N) = (p-1)(q-1)$,再选取一个与 $\varphi(N)$ 互素的数 e,计算 d,使 $ed \equiv 1 \bmod \varphi(N)$,将 (N, e) 作为公开钥,将 $(p, q, d, \varphi(N))$ 作为秘密钥. 用公开钥加密消息 m 如下: $c = m^e \bmod N$,解密密文 c 如下: $m = c^d \bmod N$.

用户的初始化过程如下:

(1)用户产生自己的 RSA 公钥、私钥对,用自己的公开钥 $P = (N, e)$ 向 CA 中心申请证书;

(2)CA 机构对用户身份进行审核(一般采用离线方式),通过后进入步骤 3,否则拒绝申请;

(3) CA 中心对 P 产生数字签名,记为 $D_d(P)$,再产生证书 $C = \{P, D_d(P)\}$ 返回给用户.

在建立 ID-CA 时,要考虑的一个重要问题就是命名空间(Naming Space). 包含在一个证书内的身份信息可以是名字、地址、城市、以及居住国家等,也可以由名字、部门、员工编号等组成,也可以用 IP、域名或者 E-mail 地址标识. 每个 CA 都要用它认为最重要的信息来对一个实体进行描述,这样在不同 PKI 域中的 CA 之间,命名空间有可能发生交叉冲突的情况. 在移动通信系统中,一个可行的方案是使用"姓名+移动电话号码"来构成命名空间. 例如:"CN=张琳峰, MP=86-20-13600006706"可以构成一个 DN(Distinguished Name).

2.2　授权认证模型:AU-CA

ID-Cert 证书的实质只是名字与密钥的绑定,只能申明谁是密钥持有者,但是在实际的应用中,还需要知道,该密钥持有者得到了什么样的授权,即可以使用该密钥干什么,有时甚至不需要知道密钥持有者是谁. 使用 AU-Cert 就可以解决这个问题. 在 AU-CA 模型中, AU-CA 的职能是授权认证中心,负责签发授权证书 AU-Cert,当然二者可以使用统一的私钥签发证书(即 ID-CA 和 AU-CA 属于同一个 Root CA).

AU-CA 签发和管理 ID-Cert 的流程与 ID-CA 类似,主要区别在于是否需要审核、以及证书格式. AU-Cert 授权证书的目的是对密钥持有者授权一个动作,批准一个许可权,或者仅仅是为了证明密钥持有者的一种能力. 即它是密钥和授权的绑定,而不是名字与密钥的绑定,其主要用途是访问控制(Access Control). 从技术上看,授权证书的思路是将 key 与 keyholder 身份分离开,所有 key 都是平等的,而不管该 key 被授予什么权利. AU-Cert 证书的格式也不同于 ID-Cert(X.509 格式)证书,具体定义如下:

$$AU\text{-}Cert = \{ issuer, subject, authorization, period, [hash(issuer, subject, authorization, period)]Sign_{AU\text{-}CA}\};$$

其中, issuer 指证书签发者的公钥或者公钥 hash 值, subject 指证书主体的公钥(或者是一个 DN 名字), period 定义了证书的有效期限, authorization 指具体的访问权限,不同的应用可以任意定义所需的权限内容,在 GSM 中,可以根据业务细分为主叫号码显示、语音信箱、短消息、遇忙前转、无应答前转、无条件前转、不可及前转、呼叫等待、呼叫保持、三方通话、数据传真、信息点播、手机银行、WAP(Wireless Application Protocol)上网、移动 IP 等等,在同一张证书中可以列出一个或者多个访问权限. 类似于 SPKI 证书的"5-tuple",证书内容采用 S-expression 表达式来描述,而不是 X.509 证书使用的 ASN.1/BER 编码,因为 S-expression 更适合于内存容量和处理器能力都有限的微小设备.

由此可见, AU-Cert 证书中的主体是对公钥的唯一标识, AU-CA 的职能不仅是证书认证中心, 而且可以作为授权服务器, 提供集中的访问控制服务. 因此, 该模型的目的主要是将密钥与持有人分离开, 实现持有人与密钥对的 1: n 关系, 即, 每个用户可以拥有一张身份证书以及多张授权证书. 一般, 身份证书的周期较长(如: 1~ 3 年), 而授权证书的周期较短(如: 1 小时~ 3 个月). 这样, 移动用户可以使用身份证书或者授权证书来进入移动网络, 不同内容的授权证书可以区分不同的访问业务权限.

2.3 模型讨论

在以上的证书模型中, ID-CA 可以充当第三方可信任 CA, 而 AU-CA 则属于移动通信网络专用的"Service CA", 与前者的意义和作用是不同的. 对于运营商来说, 建设统一根的 ID-CA 和 AU-CA, 可以实现较好的互操作特性. 现有的 GSM 入网用户, 其实已经进行了用户审核, 因此可以适用于 ID-CA 模型, 具体权限并不需要作为证书内容, 因为 AUC 数据库中已经静态登记了用户所需的业务种类. 对于一些增值数据业务, 如移动商务中不可否认的交易, 可以将 ID-Cert 证书用作签名证书.

而 AU-CA 模型则可以较好地支持另外一些增值业务, 如预付费业务(中国移动通信的"神州行"与中国联通的"如意通"都是手机预付费卡). 采用该模型, 不用审核用户的身份(即不用颁发 ID 证书), 仅仅颁发一个周期比较短(如: 限制用户在 3 个月内用完)的授权证书, 直接写在预付费卡中发放给用户, 用户只需要将预付费卡插入数字移动电话裸机内, 就可以访问移动网络. 这些增值服务吸引用户的主要原因除了计费因素之外, 主要是提供了匿名访问方式, 不需要验证身份, 保护了用户隐私, 而且使用非常便利.

2.4 与经典 PKI 模型的对比

在经典 PKI(基于 X.509v3)的模型中, 没有授权证书的概念, 它通过隐含的办法实现授权(如 SSL 证书隐含的授权就是建立安全 WEB 服务器), 另外, 也可以在扩展域中定义授权内容, 但是这样做限制了灵活性和可扩展性. 因为:

第一, 身份认证可以使用公共 CA 签发的数字证书来证明, 但是授权是与应用相关的. 不同的应用领域, 授权的颗粒度也不同, 对于权限划分细致的授权活动, 如何定义证书扩展域成为一个问题, 对于授权内容的修改更是无能为力. 另外, 访问授权应该由网络运营商或者服务提供商控制, 公共 CA 怎么有权力提供授权业务呢?

第二, 在现实生活中, 存在很多匿名访问的需求, 即使在电子商务方面, 用户往往希望能够确认商家的身份, 同时却并不愿意暴露自己的身份. 将授权认证与身份认证结合在一起, 显然不能满足这一类的需求.

第三, 无线网络中的资源非常宝贵, 移动终端的处理能力和内存容量都受到较大的限制. 在身份证书中扩展多种域是不合适的, 将身份内容和授权内容分离后, 身份证书中只含有身份 ID, 不用任何扩展域; 而在授权证书中, 可以用字节位定义具体内容, 因此节省了存储空间. 用户进入移动网络, 既可以使用身份证书, 也可以使用授权证书, 前者是隐式授权, 后者是显式授权.

因此, 我们可以看出, 在现实生活中, 认证和授权的模型应该是可以分开的, 这样既可以支持单独的授权活动, 又可以将认证作为授权的前提, 本文所提出的证书认证模型即可以支持匿名访问, 又可以支持交易的不可否认业务, 更加适合移动互联网络的需求.

3 基于证书的移动通信安全协议

3.1 移动用户与基站系统之间的双向鉴别和密钥协商

假定移动台 MS 拥有用户端证书, 其中私钥是利用 SIM 卡产生并存储在卡中的受保护区, 而基站系统拥有身份证书, 系统建立的用户证书数据库可以根据 IMSI 号索引. 那么在用户和系统间实现双向鉴别和密钥协商的协议如图 2 所示:

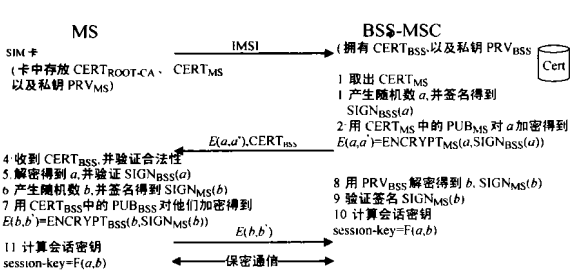

图 2 MS-BSS 安全协议

该协议的主要特点是, 系统集中管理用户证书库, 便于进行证书验证; 随机参数 a 和 b 用来建立会话用的对称密钥, 函数 F 可以使用简单的加或者乘运算, 这样产生的密钥对会话双方都是公平的; 另外, 对随机参数的签名是为了确认对方的公钥和私钥是匹配的, 以防止可能的欺骗.

3.2 移动用户之间的双向认证协议

根据 GSM 漫游呼叫的特点, 可以利用证书实现两个移动用户的双向身份认证和安全通信. 具体协议设计如下: 先假定两个属于不同网络的 MSA 和 MSB 需要进行安全通信, 但位置

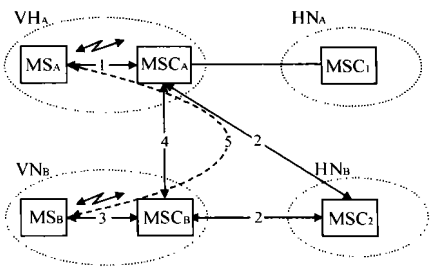

图 3 漫游用户安全会话的建立

都不在各自的归属网络(HNA、HNB)中, 且分别漫游到拜访网络 VNA 和 VNB 中. 则协议内容如下:

(1) MS_A 和 MSC_A 实现基于证书的双向鉴别;

(2) MSC_A 通过"网络寻呼"找到 MSC_B 和 MS_B;

(3) MSC_B 和 MS_B 之间实现基于证书的双向鉴别;

(4) MSC_A 和 MSC_B 交换用户 A、B 的证书, 并分别传递给 MS_A 和 MS_B;

(5) MS_A 和 MS_B 直接利用证书建立会话密钥;

该协议的主要特点是: 移动用户之间的鉴别是间接进行

的,通过系统对用户的分别鉴定实现,减少了用户端的计算量;而密钥协商是直接进行的,并可以由软件自动实现,系统操作员无法破译,实现了真正的保密通信;另外,在 MSC 之间的 7 号信令网中传送的是用户公钥证书,不需要加密.

4　实验结果

为了验证在移动通信系统中采用证书认证技术的可行性,作者开发了一个小型的 CA 试验系统,该系统包括证书签发系统和证书申请系统[6]. 其中,证书签发系统以 CDSA 平台为基础,在 Windows 环境下实现,证书申请系统采用 IIS 4.0 作为 Web Server,使用 CryptoAPI 实现. 由于移动话音通信的测试受到条件的限制,作者用 C 语言开发了一个基于 Linux 平台的小型 WAP 网关系统,重点测试了 WAP 网关证书在移动数据通信中的应用过程.

测试一: 系统签发的 X.509 格式的数字证书(在 IE5.0 中的显示)

图 4　IE5.0 中看到的 X.509 证书

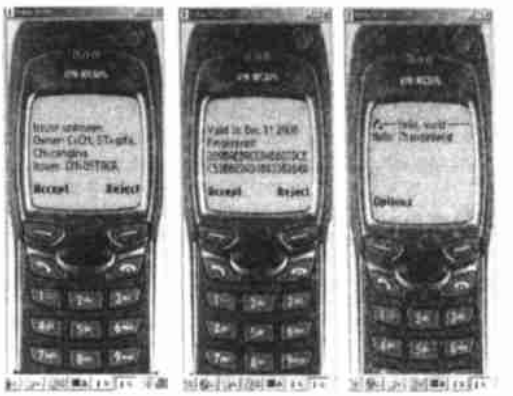

图 5　Nokie7110 模拟器中看到的网关证书和安全页面

测试二: WAP 上网的安全流程(图 5 中手机屏幕左上方的锁表示浏览的是安全页面)

注: WTLS(Wireless Transport Layer Security) 协议测试中所用的算法是 1024bit RSA 和 128bit RC5,另外,Nokie7110 还支持 DH 密钥交换算法.

5　结论

本文研究的是将 IP 网络的 CA 认证技术经改造后引入到无线通信网络,从而提出了基于证书的移动通信认证模型,并在此基础上设计了基于证书的移动通信安全协议. 实验结果表明了该证书模型的可行性. 考虑到未来发展中,移动通信网络的核心逐渐向 IP 演进,以及数据业务将占据主导,移动通信网络的安全问题日益突出,在考虑安全性的同时,要充分重视用户隐私的保护问题,本文提出的证书模型能够同时满足移动话音通信和数据通信的安全性,显示出广阔的发展前景,在未来的第三代移动通信系统(3G) 中,该模型的应用会有所不同,但是在现阶段(2G~ 2.5G) ,它可以解决 WAP 上网的安全性,从而促进移动数据业务的发展.

参考文献:

[1] Michel MOULY, Marie-Bernadette PAUTET. GSM 数字移动通信基础 [M]. 北京: 电子工业出版社. 1997.73- 95.

[2] RFC2459. Public Key Infrastructure Certificate and CRL Profile [S].

[3] RFC2692, SPKI Requirements [S].

[4] RFC2693. SPKI Certificate Theory [S].

[5] 张琳峰, 朱斌. 电子商务中 CA 的实现 [J]. 广东电脑与电讯, 1999, (2): 64- 66.

[6] 张琳峰. 基于证书的移动通信认证模型的研究 [D]. 广州: 华南理工大学. 2001: 43- 56.

作者简介:

朱　斌　男, 1940 年 3 月生于云南个旧, 教授, 研究生导师, 中国电子学会高级会员, 1963 年毕业于华南理工大学计算机专业, 毕业后至今长期在华南理工大学计算机系从事教学和科研工作, 参加和主持过国家自然科学基金、国家九五攻关、广东省等多项科研, 主要研究方向是计算机应用, 曾获国家教委、省科委科技进步奖.

张琳峰　男, 1972 年 12 月生于湖北潜江, 华南理工大学计算机系统结构硕士研究生, 1994 年 7 月获华南理工大学计算机软件专业的学士学位. 研究方向是计算机系统集成.