

基于增强型智能网的接入控制及协议

朱于军,王 柏,廖建新,陈俊亮

(北京邮电大学 187 信箱程控交换技术与通信网国家重点实验室,北京 100876)

摘 要: 本文针对个人通信系统的需求,给出一种基于公钥体系的认证和密钥约定协议的实现方案.在智能网体系结构中引入相应的接入控制实体,给出其实现结构、功能、协议和操作,描述了基于增强型智能网系统的安全接入.

关键词: 智能网;接入控制;认证协议;安全管理;通用个人通信

中图分类号: TN916.2 **文献标识码:** A **文章编号:** 0372-2112 (2000) 05-0075-05

Access Control Mechanism and Protocols Based on Enhanced IN Architecture

ZHU Yu-jun, WANG Bai, LIAO Jian-xin, CHEN Jun-liang

(Beijing University of Posts and Telecommunications, P. O. Box 187, Beijing 100876, China)

Abstract: In connection with the requirements on personal communications, an implementation of an authentication and key agreement protocol based on public-key cryptosystem is given. We propose an enhanced intelligent network architecture with the access control entity, of which the conceptual structure model, functionality, protocol and operation are also discussed. Finally, the secure access based on the enhanced intelligent network is described.

Key words: intelligent network; access control; authentication protocol; security management; UPT

1 引言

众所周知,智能网(IN)和电信管理网(TMN)是现有电信网络的支撑技术.但是在设计IN体系结构时,却没有很好地结合TMN的原理,只是简单地定义了一个业务管理功能(SMS)作为IN网管的集中控制机构,并且CS-1^[1]中也没有定义SMS的操作和协议.ITU-T虽然在CS-2^[2]中对网管部分作了相应的增强,但是这种弥补受到已有结构框架的限制,作用相当有限.实践证明,这种先天缺陷导致了现有IN在网管的许多方面(例如安全管理)存在着问题.

本文着重讨论的安全管理基本上位于业务管理层,恰是目前网管研究尚不够深入的方面.因此,如何在智能网结构上实现用户的安全接入是一个相当棘手的问题.现有的智能网业务普遍采用基于简单口令(PIN)的认证机制,但是这种静态弱认证方式存在着相当大的安全缺陷,例如PIN容易被攻击者猜出或窃取;认证数据以明文形式传输,易于泄漏;无法抵御重放攻击等等.

目前智能网发展的一个方向是作为核心网来实现业务控制,而接入网既可以是传统的公用电话网PSTN,也可以是移动通信网PLMN,甚至是数据网,因而IN与PLMN和Internet的综合成为相当热门的研究课题.另一方面,业务的多样化、个人化、智能化的需求也不断增长.因此,将来的个人通信业务

(例如阶段2以后的UPT^[3])必然要求IN系统提供多层次的灵活、方便而又充分的安全措施来保护用户^[4].

本文旨在通过增强智能网体系结构,并结合有效的接入协议,灵活地实现个人通信系统用户的安全接入.

2 基于公钥体系的认证和密钥约定协议

公钥体系给个人通信系统的安全带来了新的希望.随着处理器性能价格比的不断提升,以及宽带通信的逐步实现,公钥体系在电信系统中的大规模应用已可能成为现实. DAN BROWN在文献[5]中给出了一种个人通信系统的公钥体系方案.该文提出,用户和网络可以分别向证书发放机构(CA)提供证明信息,而由CA分别发放以其秘密密钥签名的证书,而后任何用户设备和个人通信系统之间都能够利用CA公钥检查彼此证书的合法性.

显然,DAN BROWN方案中不需要占用网络资源传送和存储安全相关数据,用户标识不以明文形式出现,并且能有效地防御内部攻击,所以其安全性较现有系统有大幅度提高.但是,该方案中尚有以下问题未予澄清:

- ① 网络 and 用户接入设备在申请证书时如何表明自己的合法身份?
- ② 如何保证证书分发过程的安全?

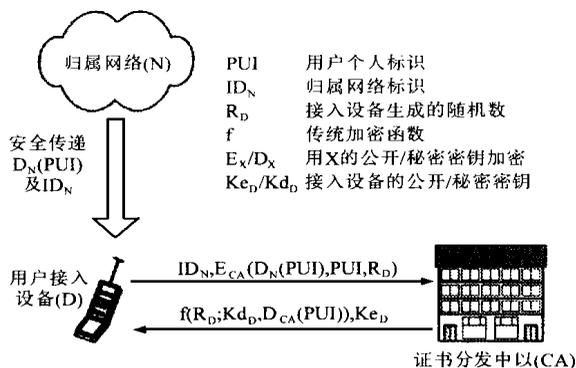


图1 证书的安全分发过程

本文中提出了一种解决方案,如图1所示.假设网络运营商通过离线的合同关系从CA处得到了网络证书,并且CA维护所有登记的网络运营商的公钥.用户接入设备在从归属网络安全获得网络对其个人标识PUI签名 $D_N(PUI)$ (其方式可以类似于现行GSM或CDMA系统)之后,生成一个随机数 R_D 作为会话密钥,与该签名一起用CA的公钥加密后发送给CA.CA验证归属网络的签名之后,以加密形式返回设备通用证书 $D_{CA}(PUI)$.此过程中, R_D 的使用保证了用户接入设备证书的安全获取.

在移动通信系统中,上述用户证书的获取过程可以发生在用户入网后第一次打开手机,用户接入设备(例如UPT卡)通过专用信令经基站子系统向CA申请,并将得到的证书一次性写入自己的永久存储器.而在固定网中,情况就比较复杂,这在后文第3节中讨论.

此外,还需要考虑的问题是:

- ⑧ 认证过程中如何保证双方证书的安全性?
- ⑨ 如何提高公钥系统的效率?
- ⑩ 如何防止内部攻击?

为了实现对等双方都不受损失的认证过程,可以考虑采用零知识认证技术,但其计算的复杂会给网络性能带来不必要的负荷.作者认为,用户的证书可以通过网络公开密钥加密得到保护,而网络证书在不影响系统整体安全性的前提下可以公开,但是为了防止攻击者仿冒合法网络与用户交互,需要

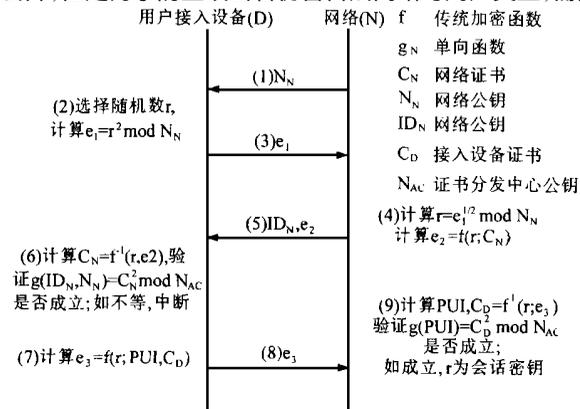


图2 基于平方剩余的用户认证和密钥约定协议

在认证协议中引入动态因子.本文提出的呼叫建立阶段的认证和密钥约定协议如图2所示.为了解决公钥系统的计算效率问题,协议中采用了平方剩余技术,旨在减少对用户接入设备的计算需求,从而降低其成本.

假定网络本身是安全且可信任的,即网络之间不会相互欺骗.由于网络公钥 N_N 、标识 ID_N 和证书 C_N 之间的关系,使得仿冒网络虽能够通过一个它自己知道其分解因子的 N_N 来欺骗用户,并解密得到用户会话密钥 r ,但却无法提供对应的 ID_N 和 C_N ,通过步骤(6)中用户接入设备的后续检测.而如果采用合法网络公钥 N_N ,则因为步骤(2)中生成的随机数的不确定性,使得仿冒网络无法在步骤(4)中解密获知该随机数,并产生正确的加密形式的网络证书以通过步骤(6)中的检测.因此,只有提供一组匹配的 N_N 、 ID_N 和 C_N ,且能够分解 N_N 的网络才能获取用户信任.事实上,只有合法网络才能做到这一点,而我们已经假定合法网络是不会为仿冒者开绿灯的.

对文献[6]提出的MSR+DH协议以及文献[7]中DMSR协议稍加改进,即可应用于图2协议的后半部分,使之能够更好地抵御内部攻击,但其代价是增加了协议的复杂性和计算量,可以根据系统的实际需要决定是否采纳这两种协议.一旦认证和会话密钥约定过程完成,则后续保密通信可以通过传统密钥加密算法实现.

3 智能网系统中的业务接入控制

当结合智能网系统考虑具体安全问题时,必须面对如何利用现存的PSTN网络的巨大投资的问题.为此,下面将讨论以下问题:

- ⑧ 如何将公钥系统有效地引入智能网系统?
- ⑨ 固定终端用户如何获得服务网络的公钥?
- ⑩ 如何处理可能的多点和层次化的CA结构?

当前的智能网规范很大程度上忽略了用户应用和信息方面.为了在各种通信网络上灵活安全地使用智能网所提供的各种业务,有必要在两方面作出努力.在用户侧,需要提供个人接入设备并增强现有的固定终端能力(例如安装智能卡读卡设备).而作为本文讨论重点的网络侧,则需要引入相应功能实体,并对电信用户接入协议和INAP协议进行增强.

3.1 业务接入功能的引入

在体系结构上需要将智能网的业务控制与业务接入进一步分离,在现有智能网中引入业务接入控制功能SACF和业务接入数据功能SADF的概念,主要负责完成业务用户的认证、授权以及实施安全接入策略.将业务接入与业务控制分离的主要理由如下:

- ⑧ 不同系统采用的接入协议和实现机制由接入提供者决定,其差别显而易见.业务接入与业务控制的分离使系统的功能划分更加清晰,功能实体与物理实体的映射也更加灵活,有助于在竞争的社会环境中分开接入提供者和业务提供者.
- ⑨ 不同用户对不同呼叫的业务接入安全性也会有不同的要求.因此,业务提供者需要方便灵活地提供因人而异的客户化接入方案,而不会影响具体的业务控制逻辑.

- ⑩ 通过分离/重用(采用面向对象技术)通用的接入逻辑,简化

了业务控制逻辑的设计,使其集中于灵活路由选择和计费,有助于智能业务的快速提供。

® 功能的专一性使得业务接入功能能够很简洁高效地实现其自身的控制逻辑,并在性能上分担了业务控制功能 SCF 的负

图 3 给出了增强后的智能网分布功能平面图,新增的实体和关系以加粗形式示出,管理关系以虚线表示。图中的 CCAF/ SCUAF(传统话机或增强型终端)与网络之间的通信可以仍采用 DTMF 信令,也可以是双向数字信令;SACF 与 SADF 之间为内部专用协议,在智能网的物理层这两个功能实体通常映射成单个物理实体 SACP(业务接入控制点);SACF-SSF、SACF-CUSF 和 SACF-SRF 之间的协议基本上可以沿用现有 SCF 与这些功能实体的 INAP,只有 SACF-SCF 之间的协议为 INAP+,需要对现有 INAP 协议进行扩充,增加类似 InitialDP 的消息,用以在业务接入成功后触发 SCF 中相应的业务逻辑,以及 Auth. req 和 Auth. res 两条信息流,SCF 用以要求 SACF 对指定用户接入信息进行核实;其它功能实体之间的协议保持不变。业务提供者可以通过 SMF 加/卸载 SACF 中的业务接入逻辑(例如认证协议的实现),对 SADF 中的用户业务接入数据(例如认证数据)进行修改。

3.2 SACF 和 SADF 的结构模型

结合现有智能网功能实体的概念模型,图 4 和图 5 分别给出了 SACF 和 SADF 的结构模型。SACF 平台提供了一个业务接入逻辑的执行环境,与业务相关的接入逻辑实例 SALI 在其中运行,实现特定业务接入。SACF 平台还管理多个 SALI 的同时激活和执行。

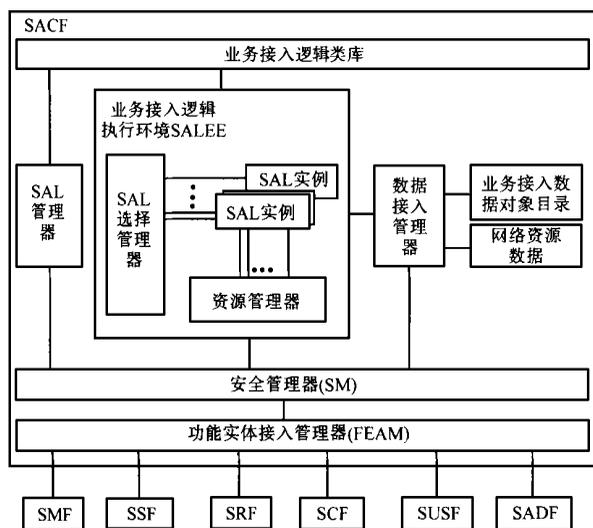


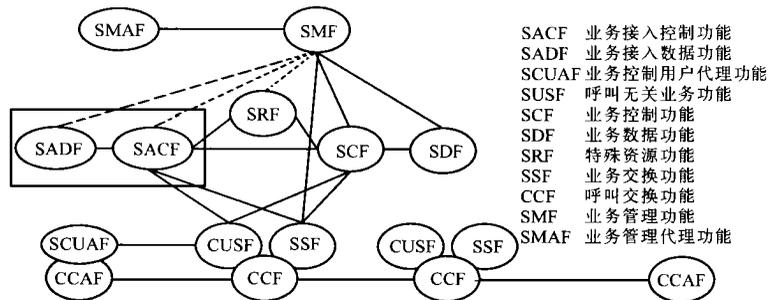
图 4 SACF 的结构模型

图 4 所示的 SACF 各实体的功能如下:

- ® 功能实体接入管理器负责与其它功能实体的交互。
- ® 安全管理器保证其它功能实体(例如 SADF、SMF)到 SACF 的安全接入。
- ® SAL 管理器负责管理 SAL 类库,加/卸载专用接入逻辑类和

荷;更为重要的是,业务接入功能屏蔽了大量的非法呼叫,减轻了作为智能网处理颈的 SCF 的处理需求。

® 安全相关数据的分离和独立处理,有利于提高系统的安全性性能。



- SACF 业务接入控制功能
- SADF 业务接入数据功能
- SCUAF 业务控制用户代理功能
- SUSF 呼叫无关业务功能
- SCF 业务控制功能
- SDF 业务数据功能
- SRF 特殊资源功能
- SSF 业务交换功能
- CCF 呼叫交换功能
- SMF 业务管理功能
- SMAF 业务管理代理功能

图 3 引入业务接入功能的增强型智能网分布功能平面图

通用接入逻辑类(例如询问应答机制实现)。

® 业务接入逻辑执行环境 SALEE 的功能是处理和控制在 SAL 类库中选择需要执行的 SAL,创建并执行业务接入逻辑实例 SALI,通过资源管理器控制本地 SACF 资源的分配,并接入相关的网络资源以支持 SALI 的执行。

® 数据接入管理器为 SACF 中信息的存取和管理提供支持,并提供接入 SADF 中信息所需的功能。业务接入数据对象目录使得接入特定数据对象所需的定位过程对 SALEE(及其 SALI)透明。网络资源数据则定位适当的功能实体(例如 SRF)以接入具有适当能力的特定资源。

图 5 所示的 SADF 的结构相对简单,其中的实体功能如下:

® 安全管理器保证其它功能实体(例如 SACF、SMF)到 SADF 的安全接入。

® SADF 数据管理器提供 SADF 中存取和管理信息所需的功能(例如需要处理 SQL 语言)。

® 业务接入数据对象代表与具体业务相关的业务接入数据(例如专用算法、用户认证数据);通用业务接入算法包含各种通用的算法(例如 DES、RSA)以供重用;操作数据则是 SADF 本身用于操作和管理目的的数据(例如对象类引用)。

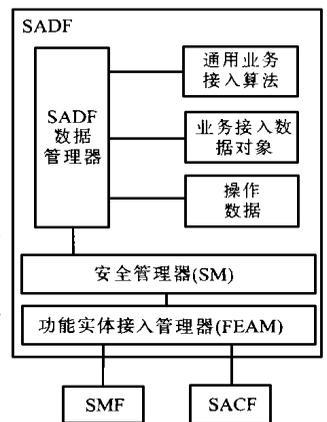


图 5 SADF 的结构模型

3.3 业务接入功能的应用

下面结合图 6 详细讨论基于上述增强型智能网系统中如何解决前述多个问题。首先给出采用公钥系统的前提:

- ® 用户需要拥有一个易于携带使用的个人接入设备(例如 UPT 卡),该接入设备存有用户的认证数据,能够与系统交互,通过复杂的计算完成认证协议,获取系统信任。
- ® CCAF/ SCUAF 应配备这种个人接入设备的接口装置(例如

叫。

6) PIM 直接将 VAC 协议参数发送给 SACF。

7) SACF 生成一个 VAC 接入逻辑实例,利用从 SADF 中检索到的单向算法和数据,计算并比较 AC 是否等于 AC,即可完成用户认证。

8) SACF 向用户提示认证结果,如果失败,则通知 SSP 释放呼叫。否则,由 SCF 完成 UPT 业务的控制逻辑(略)。

9) 在被叫接通之后,收端 SACF_r 根据安全应答的要求将收取的口令 SAPIN,通过网间互连功能回送给发端的 SCF_s。

10) SCF_s 对 SAPIN 进行核实,将结果回送给 SACF_r,从而完成业务接入。

显然,上述过程同样兼容目前普遍采用的基于 PIN 的认证形式(其中一些步骤可以略去)。需要注意几点如下:

⑧ 步骤 2 中 SACF 也可将业务请求转发给该用户的归属系统,然后在整个认证过程中充当转发者的角色,直至归属系统给出认证结果(该方案容易造成过量的网络负荷,本文不加以讨论)

⑨ 步骤 3 中,如果访问系统给出的所有接入逻辑用户接入设备都无法支持,则该次呼叫无法继续。一种解决方法是,用户接入设备中的接入逻辑程序具有可扩展性(例如采用 Java 卡^[8]),用户可以通过 Internet 从归属系统的网站上动态下载接入逻辑的新版本,或新的业务接入逻辑,以接入不同系统。

⑩ 步骤 4 中接入逻辑选通参数在用户订购业务时指定,并可以通过 UPT 用户信息文件修改流程重置,其默认值为未选通。

⑪ 步骤 7 中如果没有在本地检索到该用户的认证数据,则可以通过扩展 VAC 认证数据共享方案^[9]向该用户的归属系统发出请求。

利用增强型智能网结构,业务提供者可以应业务订购者的请求,通过 SMS 方便灵活地加/卸载 SACF 中 SAI 类库中的接入逻辑;业务订购者和业务服务用户可以在业务提供者给定的权限下,通过 WWW 浏览器或其它接入式(例如业务的个人轮廓修改过程)修改 SADF 中的个人接入轮廓文件(例如选择不同安全等级的认证方式),从而实现客户化的安全接入。

用户的接入逻辑可以重用通用接入逻辑类和 SADF 中的通用算法(实际上,大多数用户的接入逻辑都可以通过重用过程和少量的个人数据来实现),并且其本身也可以作为对象类被其它接入逻辑重用(在业务提供者认可的情况下),因而有利于接入逻辑的快速生成和改进。

5 结语

本文给出了一种增强型的智能网安全接入结构。在此基础上,结合文中给出的基于公钥体系的认证和密钥约定方案,

可以实现个人通信系统的安全接入。

但文中 SAL 类库中接入逻辑的实现和组织方式,以及是否还能以更小的粒度重用接入逻辑尚有待进一步研究。此外,如何通过 SMS 对 SACP 进行有效的管理和灵活地配置,如何组织个人接入信息文件也是需要认真研究的问题。

参考文献

- [1] ITU-T Rec. Intelligent Network Capacity Set 1 Q. 121x series, 1995
- [2] ITU-T Rec. Intelligent Network Set 2 Q. 121x series, 1997
- [3] ETSI ETS 300 391-1. Universal Personal Telecommunication (UPT); Specification of the Security Architecture for UPT Phase 1; Part 1: Specification. December 1996
- [4] Michalel Gundlach. Intelligent Security-Ways How to Deal With Threats Within Intelligent Networks. IN Asia Summit, Apr. 1997
- [5] Dan Brown. Techniques for privacy and authentication in personal communication systems. IEEE Personal Communications, August 1995
- [6] M. J. Beller, L. F. Chang, Y. Yacobi. Privacy and authentication on a portable communications system. IEEE Globecom '92 Conference Record, December 2-5, 1991, 1922 ~ 1927
- [7] 徐胜波,武传坤,王新梅. 移动通信网中的认证和密钥分配. 电子学报, 1996, 10
- [8] Rinaldo S. Di Gorgio, Zhiquan Chen. Learn the inner working of the Java Card architecture, API, and runtime environment. URL: <http://www.javaworld.com/javaworld/jw-03-1998/jw-03-javadev.html>, March 1998
- [9] 朱于军,林晓东,廖建新等. UPT 系统中的鉴权和密钥分发协议. 电子学报, 1999 年 7 月, 27(7): 51 ~ 54



朱于军 1973 年出生, 1999 年 10 月毕业于北京邮电大学, 获通信与信息工程专业博士学位。主要研究方向: 智能网、个人通信和分布式计算。



王 柏 1983 年毕业于西安交通大学, 1995 年毕业于北京邮电大学获博士学位。多年来曾从事程控交换软件、智能网系统等的设计与开发工作。研究领域涉及软件工程、形式语义、分布式面向对象技术等。现为北京邮电大学副教授。