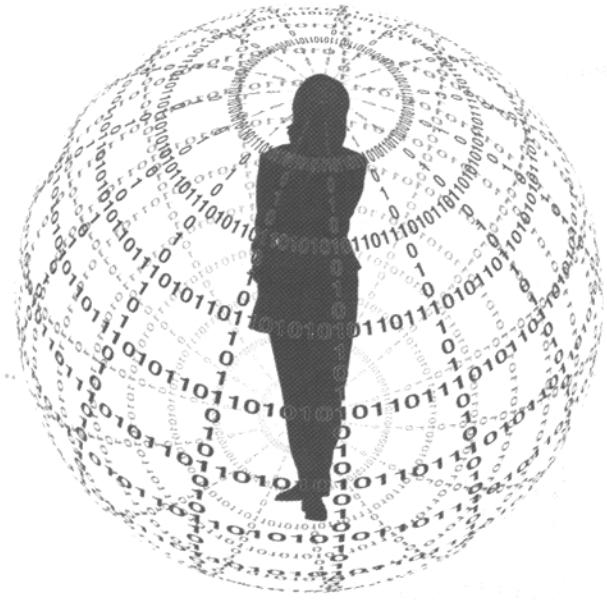

CMPP协议中费用分担认证机制的不

——简析国内Internet短消息计费机制的一个缺陷

王江春

(上海交通大学计算机系CIT实验室 200030)

摘要：国内Internet上发送手机短消息日益受到广大用户的喜爱，其基础协议CMPP是中国移动结合SMPP和网络特点推出的一种Internet手机短消息协议。本文简单分析CMPP的特点，指出其在计费机制上存在的漏洞，同时提供一种便捷的解决方案。

关键词：CMPP 短消息

1 简介

随着通信技术的发展，各种各样的通信方式层出不穷。手机短消息（又称短信）以其迅速、准确、费用低廉日益受到广大手机用户的宠爱，特别在年青人中间颇受青睐。但是，用手机输入中文相对局促，信息有限；同时Internet在国内日益普及，广大的网上用户对此有着迫切的需求。针对于此，中国移动通信集团公司推出了"中国移动通信信息资源站实体与互联网短消息网关接口协议"[1]，实现了通过PC在Internet上发送短消息，大大丰富了短消息资源，从手机短消息、铃声、屏幕保护、背景图片等多方面满足用户的个性化需求。

该协议中的核心协议CMPP（China Mobile Peer to Peer）中国移动点对点协议，是基于SMPP协议而制定的适应在Internet上发送手机短消息协议，2000年11月29日推出1.1版本，在2001年6月12日更新为1.2，其稳定性和准确性是值得信赖的。但是由于为了方便Internet用户使用，其协议在认证机制上适当放宽了条件，特别在费用分担的确认机制上，使用一种较为简单的方式，给手机用户带来了潜在损失的风险。

2 CMPP协议

CMPP是China Mobile Peer to Peer的缩写，代表中国移动点对点协议"。CMPP用以建立短消息中心和ICP之间的通路，业务和信息的提供由ICP完成。可以为实现移动数据增值业务提供服务，例如以下业务：Email通知、语音信箱通知、Internet发短消息、移动台发Email、催费通知、自动综合业务信息台（信息点播业务，主要有：天气预报、股票信息、航班信息等）。

以下以Email通知业务为例，讲述信息的流程：

- 某因特网的用户向SP(Service Provider)的Email Server发送一封Email。
- SP的POP3 SERVER激活过滤进程，如果该用户申请了Email通知业务，则过滤进程将用户登记的手机号码取出，将Email的标题取出，绑定在CMPP-SUBMIT消息中，发送给ISMG。
- ISMG将检查CMPP-SUBMIT消息中"接

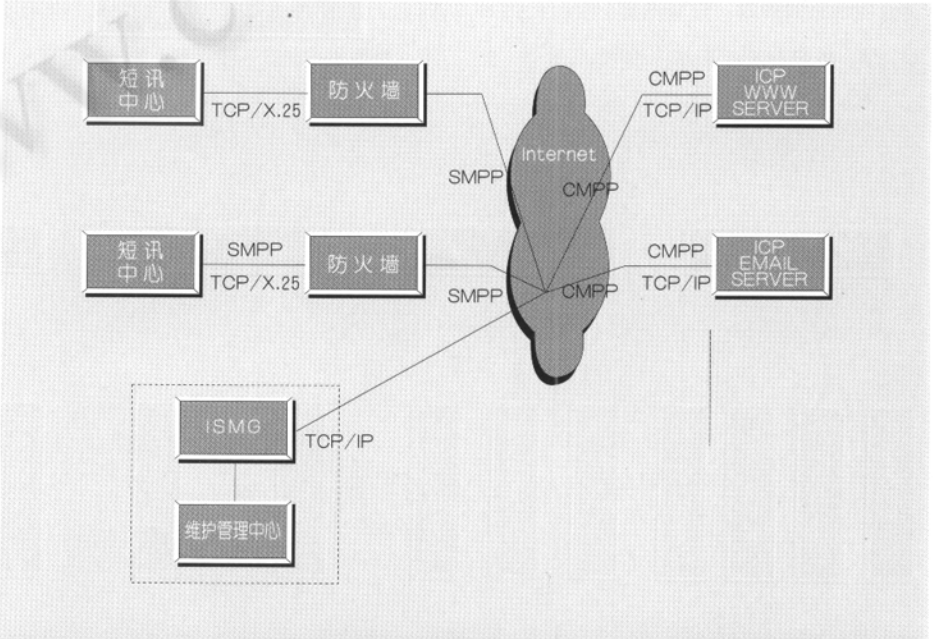

图1 网上发送短消息网络结构图

The Deficiency of Shared Cost Authentication System in CMPP

-----simply analysis a limitation of domestic internet short message charge system

收业务的手机号码" 字段，则在ISMG中查询该手机用户归属的SMC的地址，然后发送给SMC。

• ISMG得到确认消息后，将消息转换成CMPP-SUBMIT-REP，发回给SP。

• SMC收到该消息后，对该消息进行处理，发送给用户，

• SMC向ISMG回送状态报告。

由上述流程可见，对于SP来讲，要做的工作主要集中在第二步，即在EMAIL SERVER中做一个过滤程序，实现上述功能即可。从协议上说，SP只要具备CMPP中实现的接口，就可以实现对应于控制层的功能，至于对于具体的SP功能实体，比如Email Server、Web Server等，尚需做一些应用层的工作。网上发送短消息网络结构如图1，

其中，

ISMG Internet Short Message Gateway 互联网短消息网关

SMPP Short Message Peer to Peer 短消息点对点协议

SMC Short Message Center 短消息中心

3 CMPP付费认证机制中的问题

CMPP的原型为SMPP，SMPP协议是爱尔兰的逻捷克公司开发的技术，已列为业界标准的SMSC（Short Message Service Center）应用协议，其通信认证方式有着严格的界定，而CMPP为了顾及Internet用户发送短消息的便捷，安全方面做出一定的妥协，最突出的一点是发送短消息方不一定是付费方，其费用由网站指定的某个手机号码的拥有者承担，手机号码作为相对公开的信息，在当前现实情况下，很难确保这种计费方式下的每笔费用都是用户认可的。在安全性要求极高的银行系统就曾出现内部人员利用软件中四舍五入的漏洞而截留下大笔资金。当前CMPP协议的漏洞，对广大手机用户来说无疑是巨大威胁，其潜在问题如下：

(1) 如何确认SP所发短消息是用户认可的；

(2) 用户如何取消在SP上已经申请的发短消息的服务，即SP已经知道用户的手机号码，如何限制其用这个号码发送短消息。

3.1 从CMPP协议包来分析该问题

SP与ISMG之间进行信息交互时，可以采用长连接方式，也可以采用短连接方式，所谓长连接，指在一个连接上可以连续发送多个数据包，

字段名	字节数	属性	描述
Msg-id	8	Integer	信息标识（略）
Pk-total	1	Integer	相同Msg-id的消息总条数，从1开始
Pk-number	1	Integer	相同Msg-id的消息序号，从1开始
Registered-Delivery	1	Integer	是否要求返回状态确认报告（略）
Msg-level	1	Integer	信息级别
Service-id	1	Integer	业务类型
Fee-UserType	1	Integer	计费用户类型字段，0：对目的终端MSISDN计费；1：对源终端MSISDN计费；2：对SP计费；3：表示本字段无效，对谁计费参见Fee-terminal-id字段。
Fee-terminal_id	21	Integer	被计费用户的号码（如本字节填空，则表示本字段无效，对谁计费参见Fee-UserType字段，本字段与Fee-UserType字段互斥）
TP-pid	1	Integer	GSM协议类型。
TP-udhi	1	Integer	GSM协议类型。
Msg-Fmt	1	Integer	信息格式
Msg-src	6	Octet String	信息内容来源(SP-ID)
FeeType	2	Octet String	资费类别
FeeCode	6	Octet String	资费代码（以分为单位）
Valid-Time	17	Octet String	存活有效期，格式遵循SMPP3.3协议
At-Time	17	Octet String	定时发送时间，格式遵循SMPP3.3协议
Src-terminal_id	21	Octet String	源终端MSISDN号码(没有可以为空)
DestUsr-tl	1	Integer	接收消息的用户数量(小于100个用户)
Dest-terminal-id	21*DestUsr-tl	Octet String	接收业务的MSISDN号码
Msg-Length	1	Integer	消息长度(略)
Msg-Content	Msg-length	Octet String	消息内容
Reserve	8	Octet String	保留

图1 网上发送短消息网络结构图

然后断开连接，在连接保持期间，如果没有数据包发送，需要双方发链路检测包。短连接是指通信双方有数据交互时，就建立一个连接，数据发送完成后，则断开此连接，即每次连接只完成一项业务的发送。

SP向ISMG发送的消息类型包括：

(1) CMPP-Connect请求应用层连接；

(2) CMPP-Terminate终止应用层连接；

(3) CMPP-Terminate-REP终止应用层连接应答；

(4) CMPP-Deliver-REP下发短消息应答；

(5) CMPP-Submit提交短消息；

(6) CMPP-Query发送短消息状态查询；

(7) CMPP-Cancel删除短消息；

(8) CMPP-Active-Test激活测试；

(9) CMPP-Active-Test-REP激活测试应答。

ISMG向SP发送的消息类型包括：

(1) CMPP-Connect-REP请求连接应答；

(2) CMPP-Deliver短消息下发；

(3) CMPP-Submit-REP提交短消息应答；

(4) CMPP-Query-REP短消息状态查询结果

(5) CMPP-Cancel-REP删除短消息应答；

(6) CMPP-Active-Test-REP激活测试应答；

(7) CMPP-Active-Test激活测试；

(8) CMPP-Terminate终止应用层连接；

(9) CMPP-Terminate-Rep终止应用层连接应答。

在这些消息定义中，SP向ISMG发送的CMPP-Submit消息是费用计算的关键。其信息包结构如下：

协议中计费关键项目为Fee-UserType和Fee-terminal-id，只要设置Fee-UserType=3，Fee-terminal-id所代表的手机号码就成为付费方。经过实际测试（测试环境NT4.0和DELPHI5），我们确认这里计费的决定权在SP，发送短消息方不一定是付费方，费用由网站指定的某个手机号码的拥有者承担。也就是说，根据CMPP协议，每个SP自动成为所有移动手机用户的短消息代理商，无论是否得到用户认可。在该协议的1.1版本中是不存在这几个数据项[3]，不言而喻，费用不由手机用户承担。但是，在1.2版本后，不仅要用户承担，而且协议中对网站没有约束，使用户承担极大风险，因此有必要进行适当修正。

3.2 解决方案

在SMPP协议中手机用户身份认证主要通过SIM卡号与手机号码匹配，即私有信息与共有信息对照，共同确认用户。参考SMPP协议，在CMPP协议费用确认过程中，增加个人短消息服务许可权限码认证信息，通过号码和个人短消息服务许可权限码共同确认承担费用用户。发送短消息需要提供手机号码和个人短消息服务许可权限码。个人短消息服务许可权限码由用户通过电话方式向电信运营商（例如中国移动）根据移动电话号码和密码获取，同时可以修改。为了兼容以前没有申请此权限码的用户，在默认情况下，设置为000000，网站可以给原来的用户服务。当用户修改个人短消息服务许可权限码，网站发送短消息对用户计费就必须获得该个人短消息服务许可权限码。具体见图2。对于信誉良好的网站是不难从用户中获取这种个人信息。但是，由此从协议角度电信运营商对短消息SP就有了一定约束，对广大手机用户也是一种负责的态度。用户也就有了适当的权利，决定在某个SP上注册后是否继续使用对方提供的服务。当然，我们在CMPP中可以适当加入第三方认证机制，但是，其复杂性会大大增加，同时也会更多的增加运营成本。对广大用户来说，也可能得不偿失。

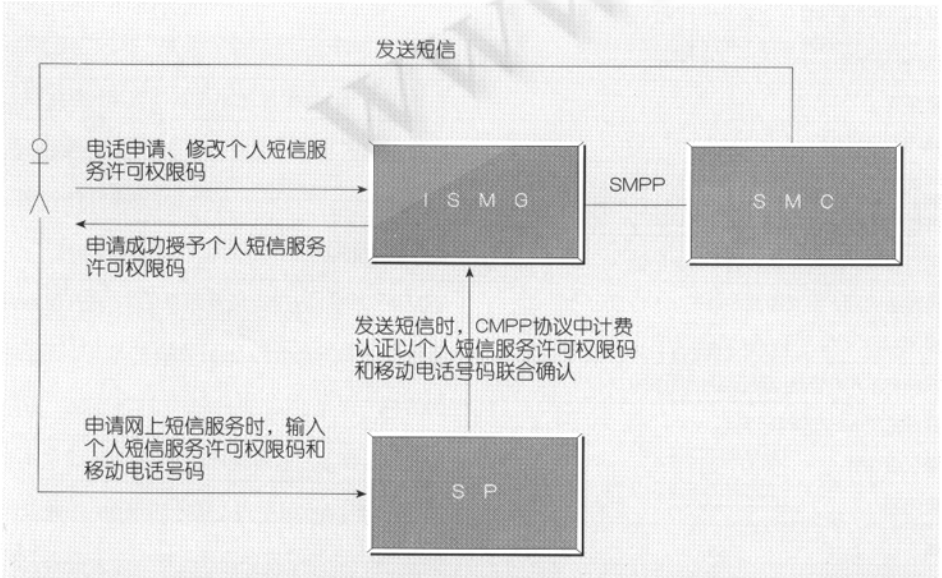

图2 网上短消息计费认证方式修改流程示意图

4 总结

利用手机号码和个人短消息服务许可权限码作为付费方身份认证机制，可以大大降低用户风险，完善了CMPP在付费机制上的一个缺陷。同时，由上述论述可知，在订立通信协议，需要进行多方面权衡，从性能、易用性、安全性、经济性等方面考虑，特别在当前公众对电信资费较为敏感时期显得尤其重要。

参考资料

1 《中国移动通信信息资源站实体与互联网短消息网关接口协议》1.2。

2 http://www.chinabyte.com/20010718/1411401.shtml。

3 http://www.simpleteam.com 关于CMPP1.1的说明文档。