空中下载(OTA)系统安全性的研究

陶鸿飞[1)] 赵正德[1)] 王 文[2)]

[1)](上海大学计算机工程与科学学院,上海 200072) [2)](上海大学计算中心,上海 200436)

摘 要 随着互联网和移动增值业务的迅猛发展,用户规模与市场规模不断扩大,以及国内 3G 时代的到来,移动增值业务必将成为拉动整个通信行业的新亮点。考虑到消息在空中传输的安全性,设计并实现了空中下载技术(OTA)系统的密钥管理,加入 MAC(消息验证码)保证数据的安全性,从而保证了数据在服务器端和 USIM 卡端传输的安全性和完整性,为开展移动增值业务提供了安全保障。

关键词 空中下载技术 3G 全球用户身份模块 密钥管理 传输安全性

中图法分类号:TP39 **文献标识码**:A **文章编号**:1006-8961(2008)10-1930-04

Security Research of OTA(Over the Air) System

TAO Hong-fei[1)], ZHAO Zheng-de[1)], WANG Wen[2)]

[1)](*School of Computer Engineering and Science, Shanghai University, Shanghai* 200072)

[2)](*Computer Center, Shanghai University, Shanghai* 200436)

Abstract With the rapid development of the Internet and the mobile value-added services, the increasingly expansion of users and markets and the coming of China's 3G-Time, the mobile value-added services will be a bright spot to uplift the mobile communication industry. In this paper, the writer studied the security issue of transferring messages with mobile devices, and planned and realized the key management of OTA system by adding MAC (message authentication code) to ensure data security. It ensures the safety and completeness of the data transformation between the server and the USIM card; therefore it provides the guarantee to the launch of the mobile value-added services.

Keywords OTA, 3G, USIM, key management, security of transferring

1 引 言

空中下载技术(OTA)传输消息通过短信通道在空中传播,其间有可能被恶意窃听或者修改消息,导致运营商的经济损失,用户的个人信息也可能会被泄露造成严重后果。因此本文研究 OTA 系统的安全机制,以保证传输消息在空中传输的安全性。

2 相关技术

2.1 OTA 技术

OTA 技术最早出现在日本,OTA 技术通过移动通信全球行动通讯系统标准(GSM)或码分多址标准(CDMA)的空中接口对用户识别卡(SIM 卡)数据及应用进行远程管理。空中接口可以采用移动协议标准(WAP)、通用分组无线业务(GPRS)、CDMA1X 以及最为普及的短消息技术[1]。OTA 技术的应用,使移动通信不但提供了移动化的语音和数据服务,还能提供移动化的新业务下载[2]。这样,应用及内容服务商可不受平台的局限,不断开发出更具个性化的贴近用户需求的服务,如信息点播、互动娱乐以及银行交易等[3]。通过 OTA 技术,手机用户只要进行简单操作,就可以按照个人喜好把网络所提供的各种业务菜单利用短消息

基金项目:上海市重点学科建设基金项目(J50103)

收稿日期:2008-07-11;**改回日期**:2008-08-01

第一作者简介:陶鸿飞(1983~),男。上海大学计算机工程与科学学院计算机科学与技术专业在读硕士研究生。主要研究方向为计算机支持的协同工作,计算机网络。E-mail:thf0917@163.com

机制下载到手机(U)SIM 卡中,并且还可根据自己意愿定制具体业务[4]。

2.2　MAC(消息验证码)认证机制

在信息安全领域,常见的信息保护手段大致可以分为保密和认证两大类。其中消息认证就是验证收到的消息确实是来自真正的发送者且未被修改过。也可以验证信息的顺序和及时性。消息认证实际上是对信息产生一个冗余的信息——MAC 利用密钥对认证的消息产生新的数据块并对数据块加密生成,可以有效地保护信息的完整性。以及实现发送方信息的不可抵赖性和不能伪造。

3　系统安全性设计

3.1　双向认证技术流程

OTA 业务系统采用健全的双向认证技术。

上行 MAC 认证:OTA 应用下载服务器收到上行数据后,计算该上行数据的 MAC,并与上行数据中的 MAC 进行比较。若两者相同,证明该上行数据的发送者是合法用户,且数据在传送过程中未被修改、删除或者重组,该上行数据有效;否则,丢弃该上行数据,如图 1 所示。

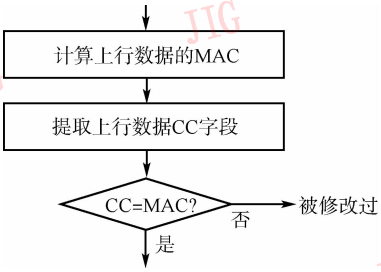

图 1　上行 MAC 认证过程

Fig. 1　Upward MAC authentication process

CC 为 Third Generation Partnership Project (3GPP)组织制定的最基本的通信过程命令包中安全应用数据段。

下行 MAC 认证:收到下行数据后,计算该下行数据的 MAC,并与下行数据中的 MAC 进行比较。若两者相同,证明该下行数据来自合法的 OTA 应用下载服务器,且数据在传送过程中未被修改、删除或者重组,该下行数据有效;否则,丢弃该下行数据。下行 MAC 认证过程类同于上行 MAC 认证过程。

3.2　MAC 算法

MAC 算法采用标准的密码块链接数据加密标准(DES-CBC)算法,计算 MAC 时应包含以下数据:

上行数据:卡商代码及协议版本号 1 位、ICCID 8 位、KeySet 1 位、同步计数器 5 位、CC 8 位,命令类型 1 位、命令长度 1 位、命令参数若干位。

下行数据:命令包长度、命令包头长度、保密数据指示、KIC(加密数据密钥)、KIC(认证消息密钥)、应用类型、同步计数器、PCNTR、命令类型、命令长度、命令参数、加密所需填充数据。若数据不是 8 的倍数,则以 0x00 填充。计算结果为 8 位。

算法过程:将所有原始数据按照每 8 个字节一组进行分组,计算 MAC 所需填充的数据不包含在上、下行消息数据中,由 USIM 卡/OTA 应用下载服务器在计算 MAC 时根据上行/下行数据长度自行填充。

以 KID 作为 DES 算法的密钥,初始数据为 8 字节的“0x00”,对第 1 分组数据与初始数据异或后的数据进行运算,DES 算法的输出数据与第 2 分组数据异或后,继续以 KEY 为密钥进行 DES 运算,依次进行下去直至最后一个分组处理完毕。MAC 取最后一次 DES-CBC 运算的 8 字节输出数据。

MAC 算法流程如图 2 所示。

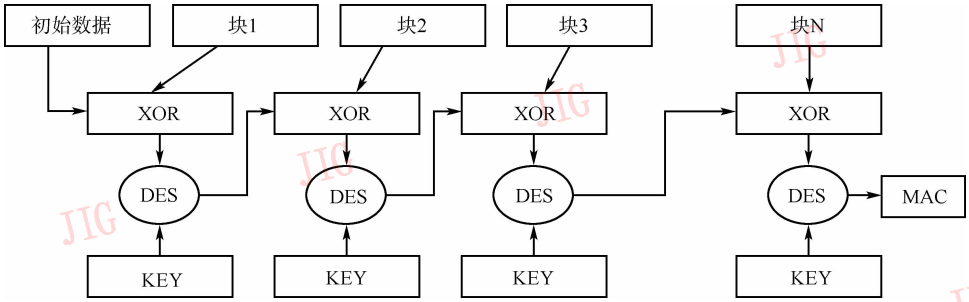

图 2　MAC 算法流程

Fig. 2　MAC algorithm folw

3.3 密钥管理

密钥管理在整个系统的安全机制中至关重要，如果密钥被破解将会导致传输消息在传输过程中被第三方窃听，如远程文件更新操作在更新过程中被窃听到，窃听者就可以任意更新用户 USIM 卡上的文件，这是非常严重的后果。这里设计的 OTA 系统的密钥管理如下：

OTA 服务器和 USIM 卡各存放 3 组密钥，主密钥由运营商生产并下发给各卡商。下面 key1 ~ key6 是 6 组系统使用的主密钥。

key 1	0x1111111111111111
key 2	0x2222222222222222
key 3	0x3333333333333333
key 4	0x44444444444444444444444444444444（远程文件更新使用）
key 5	0x55555555555555555555555555555555
key 6	0x66666666666666666666666666666666

其中，OTA 服务器存放下行密钥，USIM 卡存放上行密钥，上行密钥的编号是 key 1 ~ 3，下行密钥使用 key 4 ~ 6。上行密钥由卡片循环选择使用哪组密钥，下行密钥由服务器根据下行数据命令选择使用哪组密钥。上行密钥组中只包括 KID（Key and algorithm Iaentifer for RC/CC/DS）8 个字节。下行密钥组中包括 KIC 和 KID，KIC 为 16 个字节，KID 为 8 个字节，OTA 命令只需要 KID，远程文件更新需要 KIC 和 KID。上行密钥 KID 是发行卡片的时候由上行主密钥（8 个字节）跟主帐号 IMSI 前 8 个字节加密计算出来并直接写入卡中，加密算法是 DES-CBC。计算 OTA 命令校验值时直接使用。

下行密钥 KIC 是发行卡片的时候由下行主密钥（16 个字节）跟主帐号 IMSI 后 8 个字节（不包括长度字节）加密计算出来并直接写入卡中，加密算法是 DES-CBC，KIC 用于 3DES CBC 的运算；KID 为 KIC 的前 8 个字节。计算 OTA 命令校验值或加密数据时直接使用，无需进一步分散。

3.4 密钥分散算法

密钥分散用于对 USIM 卡与 OTA 应用下载服务器共享的主密钥进行分散，以产生计算 MAC 时所需要的会话密钥，并保持会话密钥的动态性和随机性。

上行密钥选择：图 3 为上行密钥的分散策略。

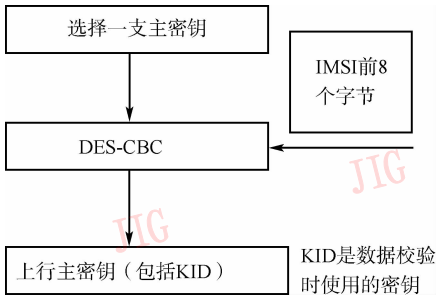

图 3 上行主密钥形成策略

Fig. 3 Upward main secret key formation strategy

下行密钥选择：图 4 为下行密钥的分散策略。

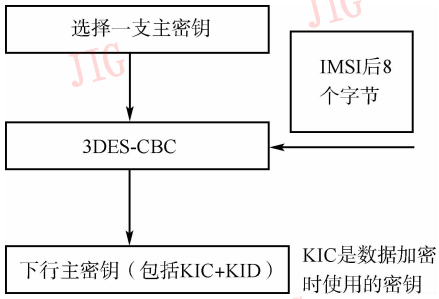

图 4 下行主密钥形成策略

Fig. 4 Downward main secret key formation strategy

4 系统实例

系统在中国电信上海研究院的 3G 实验室开发与试验，承载网络是 WCDMA 网络，OTA 服务器的配置，在验证 OTA 的安全性保证方面，以动态下载一个业务“天气预报”为实例，其中，上行消息数据为

0x102222222222221111130000000059cbf00a01e650db60206310100004fa7，其各个字段完全符合上行消息的各个细节字段的设计，其分解如下：10 为卡商代码、2222222222221111 为 ICCID、13 为密钥编号、0000000005 为同步计数器、9cbf00a01e650db6 为 CC、02 为命令类型、06 为命令长度、310100004fa7 为命令参数。

其中，MAC 为 9cbf00a01e650db6，可以看到上行消息使用的编号为 3 的密钥（KID 为 0x13），服务器端根据 MAC 算法计算得到的 MAC 值是完全一致的，因此得到了服务器的认证。

另外，此条消息中得到 KID 为 0x13：表明是使用第 3 组密钥：

key 3……0x3333333333333333

key3 和卡片的 ISMI 文件中后 8 个字节分散得到的加密数据 Result:

IMSI:　49 06 60 00 00 00 00 94

key3:　33 33 33 33 33 33 33 33

Result: 4A 94 7B 45 74 54 A9 17

再通过 Result 来加密 CC 字段,其中,每张不同 USIM 卡内的 IMSI 文件内容是唯一的,而且其读写权限受 USIM 卡内部安全机制管理,符合安全标准,从而保证了分散后得到的密钥 Result 数据的保密性,体现了本文密钥管理机制的设计思想。

下行消息数据为

0x027000005515122140 41c000100000000005007a4175eb2ebf1112023d3101000301010000320000310100003209805929 6C14988462A572002105048144551 4062B50544B5451052B5150544B0481445550082B44 42545159422073000076000 0A419008F0A01806C148 C618BA252368F0A02806309676170B964AD0002A41 1008F0601808BA252368F06028090008BA20184A317 00008D11088BF78F93516557CE5E02533A53F7FF1A 030401067003160021930800000406200D01000000930 A00000406230D0224000000

其中,MAC 为 07a4175eb2ebf111,同样,卡片通过 MAC 算法得到的 MAC 值也是 07a4175eb2ebf111,因此得到了卡片的认证。

因此证明运用消息认证码的健全的双向认证机制是可行性的,加上密钥管理机制,更加保证了系统的安全性。

5　结　论

主要分析了系统存在的安全风险,引入了 MAC 认证机制,保证数据在服务器端和卡端传输的安全性和完整性。同时也引入了密钥管理保证了系统保密性。

文中两种安全机制极大地提高了系统的安全性和可靠性,为系统开展移动增值业务提供了安全保障。

参考文献(References)

1　You Xiao-hu, Cao Shu-min, Li Jian-dong. A Perspective of the Third Generation Mobile Communications System [J]. Acta Electronica Sinica, 1999, **27**(11A): 3 ~ 8. [尤肖虎,曹淑敏,李建东. 第三代移动通信系统发展现状与展望[J]. 电子学报,1999, **27**(11A): 3 ~ 8.]

2　Chen Gu-jie. The application of OTA in the mobile internet[J]. Communications Today, 2002, (6): 43 ~ 46. [陈固杰. 空中下载技术在移动互联网中的应用[J]. 现代通信,2002,(6):43 ~ 46.]

3　Hou Xiao-xia, Yang Long-xiang. Study and application of the OTA in the mobile internet[J]. Communications Today, 2003, (12): 25 ~ 39. [候晓霞,杨龙祥. 空中下载技术及其在移动互联网中的应用[J]. 电信快报, 2003,(12):25 ~ 39.]

4　Wang Qi. Study of the standard and development of 3G technology [J]. Scienfic & Technical Information of Gansu, 2007, **36**(2): 46 ~ 47. [王琪. 3G 技术标准及其发展研究[J]. 甘肃科技纵横,2007, **36**(2):46 ~ 47.]