USIM 卡的补丁下载机制的研究

赵正德 陶鸿飞 陈霞萍
(上海大学计算机工程与科学学院,上海 200072)

摘 要 提出了基于 USIM(全球用户身份模块)卡的补丁下载机制,采用鉴权技术实现空中下载系统与动态链接库之间互相鉴权认证,保证两者间的相互信任;提出采用动态链接库技术实现补丁下载机制,并通过定义底层 API 来提供对补丁下载进行控制与管理,实现空中下载系统对 USIM 卡上的应用可以通过该机制下载修复或者升级的功能。

关键词 全球用户身份模块 补丁下载 传输协议 鉴权
中图法分类号:TP39 **文献标识码**:A **文章编号**:1006-8961(2008)10-1971-04

The Patch Download Mechanism Studied on USIM Card

ZHAO Zheng-de, TAO Hong-fei, CHEN Xia-ping
(*School of Computer Engineering and Science, Shanghai University, Shanghai* 200072)

Abstract The mechanism of patch downloading based on USIM card is proposed in this paper. This mechanism adopts authentication technology to enable the co-authentication between OTA (over the air) and dynamic linking library (DLL), ensuring the mutual trust. In the paper, DLL is also suggested to practise the patch-download mechanism. In this approach the application on USIM card can be updated by OTA through the control and management of patch downloading provided by the definition of lower level API.

Keywords universal subscriber identity module (USIM), patch download, transport protocol, authentication

1 引 言

第 3 代移动通信网络使用的 USIM(全球用户身份模块)卡片发卡后,卡片的系统不可能是最完整的,就像 Window 操作系统一样,操作系统会有各种各样漏洞,需要提供补丁下载机制来完善其功能[1]。对于卡片,可能存在卡片操作系统(COS)的漏洞,卡片上存在的应用也可能因为应用平台的更新而有所更新。程序补丁下载机制实现对卡片操作系统以及程序和应用下载功能平台进行功能升级和错误修正。

2 相关技术

2.1 USIM 卡相关技术

众所周知,SIM 在 2G 时代的主要应用是语音业务和用户鉴权,但随着 3G 时代的到来,国际标准化组织 3GPP(第三代合作伙伴计划)制定了适合 3 G 网络的 USIM 卡相应规范。USIM 卡最根本的创新是通过引入 UICC(universal integrated circuit card)多应用 IC 卡平台的概念,突破了 SIM 卡等同于 GSM(全球行动通讯系统标准)的单应用框架,实现了多个应用同时运行的多通道机制。USIM 卡是一个真正意义上的多应用卡[2]。卡上不但可以存放多个应用,并且可以同

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**:2008-07-31

第一作者简介:赵正德(1956~),男。副教授。原上海科学技术大学计算机应用技术专业硕士研究生。主要研究方向为计算机支持的协同工作,计算机网络与分布式计算。E-mail:zhdzhao@163.com

时运行多达 4 个不同应用,例如用户可以在打电话的同时进行数据下载和网上支付等[3]。

2.2 动态链接库技术及优点

Visual C + + 支持 3 种 DLL,它们分别是 Non-MFCDll(非 MFC 动态链接库)、RegularDll(常规 DLL)、EXtensionDll(扩展 DLL)。Non-MFCDLL 指的是不用 MFC 的类库结构,直接用 C 语言写的 DLL,其导出的函数是标准的 C 接口,能被非 MFC 或 MFC 编写的应用程序所调用。本文对 USIM 卡的补丁下载机制中所设计的底层 API 都采用 DLL 设计。动态链接库具有以下优点:

(1)多个应用程序、甚至是不同语言编写的应用程序可以共享一个动态链接库文件,真正实现了资源"共享",大大缩小了应用程序的执行代码,更加有效地利用了内存。

(2)动态链接库文件作为一个单独的程序模块,封装性、独立性好,在软件需要升级的时候,开发人员只需要修改相应的动态链接库文件就可以了,而且,当动态链接库中的函数改变后,只要不是参数的改变,程序代码并不需要重新编译。这在编程时十分有用,大大提高了软件开发和维护的效率。

3 程序补丁的管理和实现

补丁下载通过指定的下行消息执行,服务器运行由卡商提供的个性化补丁管理模块,该模块每次组织一条消息发给卡片,每条消息都需要卡片的回馈,回馈消息中说明卡片对于上一条补丁解释和执行的情况,该结果会原封不动地发给补丁管理模块,由补丁管理模块决定下一条补丁是什么,是否继续发送新的消息。

服务器对补丁内容的管理要提供统一的数据存储结构,卡商的补丁管理模块从统一的数据接口中提取补丁内容,然后下发给卡片。

程序补丁可以分为两种:应用相关补丁与应用无关补丁。对于应用相关的程序补丁,服务器应在应用数据表中关联出其对应补丁 ID。与应用相关的补丁 ID 由服务器统一确定。补丁 ID 总共不超过 20 个字节。对于应用无关的补丁,服务器应维护每个卡商所提供的一个补丁 ID 的列表及对每个补丁用途的详细描述。

本文设计的程序补丁下载机制包括鉴权流程和补丁下载管理流程,由动态链接库统一封装,使用动态链接库模块化特点,使服务器独立于动态链接库。动态链接库通过定义一系列 API 实现了对 USIM 卡的补丁下载进行控制和管理。

4 动态链接库 API 定义

动态链接库(DLL)的接口是采用 C 语言描述的。

4.1 获取补丁数据长度

该函数必须在服务器鉴权后方可执行。

函数结构:

```
Int CheckPatchSize(
[in] char * AuthRes, //参见 4.5 节"进行服务器鉴权"
[in] char * CardOSversion,   //卡片发行批号
[in] char * PatchID   //补丁程序 ID
)
```

函数描述:检查某补丁程序 ID 在某卡片发行批号(COS)上是否需要下载,如需要下载则返回需要下载的数据长度

函数返回:

-1:服务器未完成鉴权

0:不需要下载补丁

其他:补丁程序的数据长度

4.2 获取补丁数据

该函数必须在服务器鉴权后方可执行。

函数结构:

```
Int GetPatch(
[in] char * AuthRes, //参见 4.5 节"进行服务器鉴权"
[in] char * CardOSVersion, //卡片发行批号
[in] char * PatchID, //补丁程序 ID
[in] char * LastSeq, //上次执行指令的序列号
[in] char * LastResponseCode, //上次执行指令返回的状态字(由"补丁下载确认"返回)
[in] DWORD MAXPDUSIZE, //最大允许的 PDU 的长度,以字节为单位。
[in] DWORD operationType, //操作类型,0 - 下载,1 - 删除,其他保留。
[out] char * NextSeq, //下一条需要执行的指令的序列号
[out] char * NextExeCode, //需要下发到(U)SIM 卡的指令,指令以 16 进制字符串的方式存放,要求
```

动态链接库每次只生成一条补丁消息数据,等待卡片返回接收确认后,才允许生成下一条补丁消息数据。

[out] char * CardOSVersionUpdated) //Patch 执行成功之后卡片应有的卡片发行批号)

函数描述:

获取需要执行的补丁程序管理指令,动态链接库应能够跟据最大允许 PDU 长度自动拆分补丁程序数据,然后返回给服务器。此一组数据必须能够触发卡片上发"补丁下载确认"命令。服务器无需解释从卡端上发的 response,而是通过 getPatch 方法直接传给动态链接库,之后的动作由动态链接库来确定。

函数返回:

-1: 服务器未完成鉴权

0: 成功结束,服务器需要获取 CardOSVersionUpdated 值

1:继续获取指令序列号 NextSeq 以及指令 NextExeCode

2:处理失败,该 Patch 下载失败

其他:保留

4.3　获取动态链接库版本

函数结构:

Int GetDllVersion([out] DWORD * DllVersion //动态链接库版本号)

函数描述:

服务器获取动态链接库的版本,服务器根据版本管理策略管理个卡商的动态链接库。

函数返回:

0:成功获得动态链接库版本

其他:无法获得动态链接库版本

4.4　动态链接库鉴权

函数结构:

Int AuthDll(

[in] char * Rand,　//动态链接库鉴权随机数

[out] char * AuthRes2　//动态链接库鉴权运算返回结果

)

函数描述:

服务器向动态链接库传入一个 16 位的十六进制随机数 Rand 参数,动态链接库使用 3DES-ECB(一种密码块链接数据加密标准)算法加密运算,将随机数与动态链接库内封装的 16 位十六进制动态链接库密钥(DK1)进行计算,将运算结果作为 AuthRes 参数传出。

运算示例:

Rand = 1234567890ABCDEF

Key = 00000000000000000000000000000000

AuthRes = 516AE556C8F4C96F

函数返回:

0:成功进行动态链接库鉴权运算

其他:进行动态链接库鉴权失败

4.5　获取服务器鉴权随机数

函数结构:

Int GetAuthServerRnd(

[out] char * Rand　//服务器鉴权随机数)

函数描述:

服务器从动态链接库中获得服务器鉴权流程中需要用的 16 位十六进制随机数,动态链接库需要在自己的内存空间内保留此数值供下一步鉴权运算使用。

函数返回:

0:成功生成服务器鉴权随机数

其他:无法生成服务器鉴权随机数

进行服务器鉴权:

函数结构:

Int AuthServer(

[in] char * AuthRes　//服务器鉴权运算结果)

函数描述:

服务器使用获得的服务器鉴权流程中的随机数与自有的 16 位十六进制服务器密钥进行 3DES-ECB 算法加密运算,将获得运算结果作为 AuthRes 参数传入动态链接库内,动态链接库使用服务器鉴权流程随机数与动态链接库内封装的 16 位十六进制服务器密钥(DK2)进行 3DES-ECB 算法加密运算,将运算结果 AuthRes2 与服务器传入的 AuthRes 进行比较,如比较结果相同,则鉴权通过,反之鉴权失败,动态链接库通过函数返回值返回鉴权结果。

函数返回:

0:服务器鉴权通过

其他:服务器鉴权失败

5　服务器与动态链接库的交互

服务器与动态链接库的交互是通过鉴权控制来进行的。服务器与动态链接库直接的鉴权需经过两个流程,流程如图 1 所示。

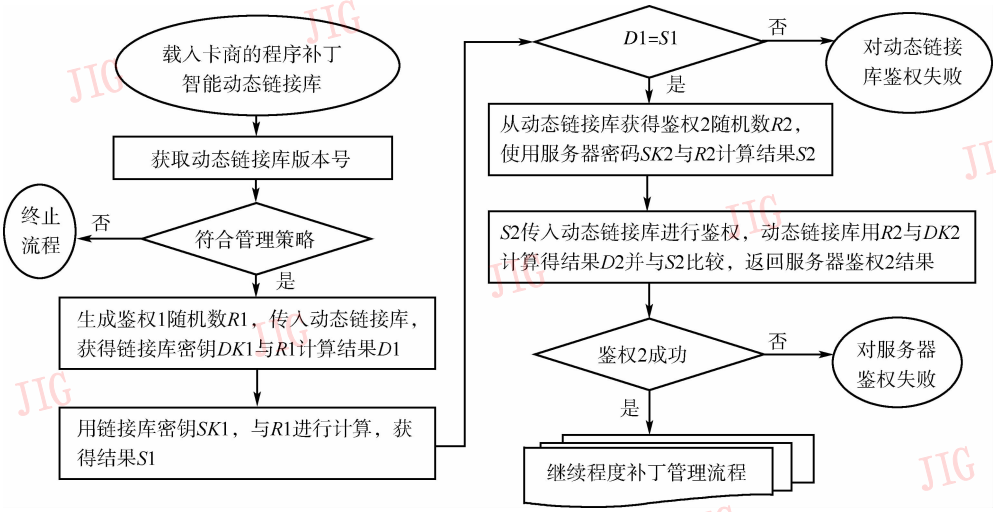

图 1 鉴权控制流程

Fig. 1 The control flow of authentication

鉴权流程 1 为服务器对动态链接库进行鉴权，每个动态链接库有唯一的 32 位密钥，封装在动态链接库内的该密钥称 *DK*1，随动态链接库上传至服务器的该密钥称 *SK*1，只有在 *SK*1 和 *DK*1 相同情况下，才能通过服务器对动态链接库的鉴权；鉴权流程 2 为动态链接库对服务器进行鉴权，每个服务器有唯一的 16 位密钥，封装在动态链接库内的该密钥称 *DK*2，存储在服务器上的该密钥称 *SK*2，只有在 *DK*2 和 *SK*2 相同情况下，才能通过动态链接库对服务器的鉴权。只有在通过鉴权 1 和鉴权 2 的情况下，服务器和动态链接库才能进入下一步的程序补丁管理流程，以保证机密数据不被窃取。

版本管理策略一般由服务器规划与实现。服务器可根据实际需求和场景增加版本管理策略规则。一般情况下，卡片提供商在提供新的动态链接库时需提供该链接库鉴权密钥（即 *SK*1，*SK*1 应与封装在链接库内的 *DK*1 相同）；服务器将 *SK*1 存储在数据库内，将链接库存储在服务器磁盘的安全区域内。补丁的管理逻辑完全由动态链接库来实现，服务器通过调用动态链接库所提供的接口，完成补丁的下载与删除。

6 系统实例

系统在中国电信上海研究院的 3G 实验室开发与实验，承载网络是 WCDMA 网络，此条补丁的功能是在 USIM 卡的电话簿号码加前缀“ + 86”，体现卡片升级效果，通过实验如图 2 所得到了预期的效果，验证了补丁下载机制不仅正确并且是可行性的。

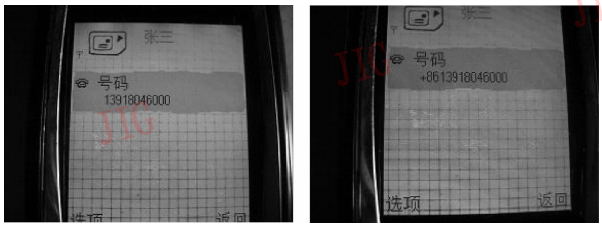

图 2 实验效果

Fig. 2 The effect of experimentation

7 结 论

基于 USIM 卡的补丁的特点，及其下载和删除的流程，提出了基于 USIM 卡的补丁下载机制，设计了补丁的鉴权流程，并通过定义底层 API，运用动态链接库实现对 USIM 卡补丁下载的控制与管理。

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 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.]