SIM卡操作系统(COS)的安全分析

宋麦玲，陈云亮
（中国地质大学 计算机学院，湖北 武汉 430074）

摘要：本文深入的分析了SIM卡中的COS系统的体系结构，从安全操作系统的角度剖析了COS中的安全体系。

关键词：COS；安全体系
中图分类号：TP316　　文献标识码：A　　文章编号：1009-3044(2007)03-10708-01

An Image Retrieval Technology Based on HSV Color Space

SONG Mai-ling,CHEN Yun-liang
(School of Computer,China Univercity of Geosciences,Wuhan 430074,China)

Abstract: In this paper, we analaze the system structure of COS in SIM deeply,and analize the safety system of COS in the way of the safe OS.

Key words: COS;safety system

1 引言

SIM卡是Subscriber Identity Module的缩写，即用户识别模块，用来标识一个特定移动用户的网络连接。SIM卡的主要功能是来存储用户数据和完成客户身份鉴权以及客户信息加密过程，此功能主要是由SIM卡内的一部具有操作系统的微处理器完成。

COS的全称是Chip Operating System(片内操作系统)，它一般是紧紧围绕着它所服务的智能卡的特点而开发的。由于不可避免地受到了智能卡内微处理器芯片的性能及内存容量的影响，因此，COS在很大程度上不同于我们通常所能见到的微机上的操作系统（例如DOS、UNIX等）。在本文中我们探讨的是SIM卡中的COS系统，主要的功能是维护SIM卡中的文件系统，处理手机下发给SIM卡的各种命令，并且提供SIM卡应用程序开发包（即STK)来实现增值服务的开发。COS的出现不仅大大地改善了智能卡的交互界面，使智能卡的管理变得容易，而且更为重要的是，使智能卡本身向着个人计算机化的方向迈出了一大步，为智能卡的发展开拓了极为广阔的道路[3]。

2 COS的基本模型

SIM卡中集成了微处理器CPU、存储器和芯片操作系统(COS)，构成一个完整的计算机系统，具有独立的数据处理能力，SIM卡的结构如图1所示。

COS系统在SIM卡的结构中处于中间层，介于底层硬件与上层应用之间，它向下组织、协调系统硬件，实现I/O，存储管理等功能，向上为应用提供服务。在SIM卡中的COS系统主要是为了实现移动通信的服务。我们参考网络ISO模型，如图2所示把COS系统的结构分为以下四个层次。

图1　SIM卡结构图

图2　COS层次结构

这样的层次划分的主要原则是，将应用代码从COS主体中独立出来，提供一个统一的接口进行管理；将和底层SIM卡硬件相关的操作提取出来，便于和上层代码的复用和移植；整个系统通过统一的调度管理。各个层次间提供一个接口以服务的方式进行调用，下层的内部实现对上层来说是透明的。

3 COS的安全体系

根据接触式IC卡国际标准ISO/IEC7816-4，COS安全体系包括三部分：安全状态，安全属性，安全机制。

安全状态是指SIM卡当前所处的安全级别，即当前安全状态寄存器的值，这种状态在SIM进行完复位应答后初始化或者在处理完某种命令后得到的。

安全属性，它定义了执行某个命令需要的一些条件，即在进行某种操作时要求安全状态寄存器的值是什么。

安全机制从广义上说是SIM卡支持的各种安全模式，从狭义上说是安全状态实现转移所采用的方法和手段。

一种安全状态通过上述安全机制转移到另一种状态，把该安全状态与某个安全属性相比较，如果一致，则表明能够执行该属性对应的命令；如果不一致，则相关命令不能被执行，从而达到了安全控制的目的，这就是COS安全体系的基本工作原理，如图3所示。

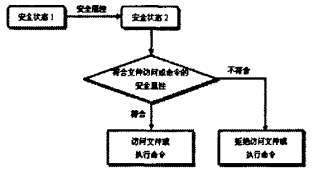

图3　安全状态转移

4 COS的应用安全

4.1 应用脚本的安全

SIM卡对下载的应用脚本必须具备保证完整性和安全性的功能，由于应用脚本的下载实现是以短信的方式来实现的，而在现有短信传输机制中，是进行的明文数据传输，在用户通过无线网络来进行菜单和新业务的定制过程中，有些消息是经过了有线网络，这就给攻击者提供了对空中下载服务系统进行篡改、假造、重传等攻击的机会，因此为了提供一个安全可靠的数据传输通道，在下载过程中要对下载的应用脚本数据提供身份认证和同步处理机制。

下面对身份认证进行一下简单的介绍，空中下载系统采用了双向认证的技术。用户在提出下载请求时，空中下载系统会对用户进行合法性的验证，这样确保了只有合法用户发出的下载请求才能被响应；同时SIM卡还要对空中下载系统的合法性进行验证，这样避免了恶意代码对用户SIM卡的入侵。同时双向认证机也保证了交互信息的完整性和正确性。空中下载系统在收到用户的请求信息后，马上计算此信息的MAC码，并与请求信息中的MAC码匹配，若相同则说明发送此信息的用户是合法的，且在数据的传送中未被修改。SIM卡收到下载数据后，同样计算该下载数据的MAC码，并与下载的数据中的MAC码进行匹配。相同则证明该下载数据是合法的，且是完整有效的，否则丢弃该下载数据。

(下转第803页)

收稿日期：2006-11-29

作者简介：宋麦玲(1975-)，女，山西运城人，中国地质大学(武汉)计算机学院讲师，主要研究方向为多媒体技术和图像处理；陈云亮(1979-)，江苏南通人，中国地质大学(武汉)计算机学院讲师，主要研究方向为网络技术。

```
bool Import3DS(t3DModel *pModel, char *strFileName);
// 装入 3ds 文件到模型结构中
void CreateTexture(UINT textureArray[], LPSTR strFileName,
int textureID);//从文件中创建纹理
int GetString(char *); // 读一个字符串
void ReadChunk(tChunk *);// 读下一个块
void ReadNextChunk(t3DModel *pModel, tChunk *);      // 读
下一个块
void ReadNextObjChunk (t3DModel *pModel,t3DObject *pOb-
ject,tChunk *);//读下一个对象块
void ReadNextMatChunk(t3DModel *pModel, tChunk *); // 读
下一个材质块
void ReadColor(tMatInfo *pMaterial, tChunk *pChunk);// 读对
象颜色的 RGB 值
void ReadVertices(t3DObject *pObject, tChunk *); // 读对象
的顶点
void ReadVertexIndices(t3DObject *pObject,tChunk *);// 读对
象的面信息
void ReadUVCoordinates (t3DObject *pObject,tChunk *);// 读
对象的纹理坐标
void ReadObjMat (t3DModel *pModel,t3DObject *pObject,
tChunk *pPreChunk);// 读赋予对象的材质名称
void ComputeNormals(t3DModel *pModel);   // 计算对象顶
点的法向量
void CleanUp(); // 关闭文件，释放内存空间
FILE *m_FilePointer; // 文件指针
tChunk    *m_CurrentChunk;
tChunk    *m_TempChunk;};
```

3.3 模型属性设置

为了能在 OpenGL 正确显示三维模型，应该将模型的坐标、纹理贴图、光源作相应的设置，本文将坐标中心设置在车厢底板平面中心上，以便于装载计算，贴图统一采用位图格式，光源为默认光源。图 2 为 3DS 文件中的模型，图 3 为 OpenGL 绘制的模型。

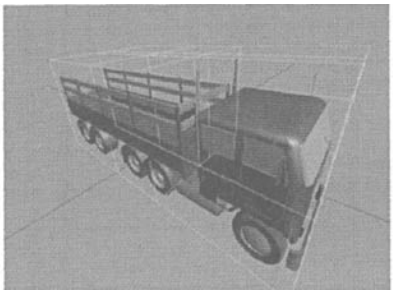

图 2　3DS 文件中的模型

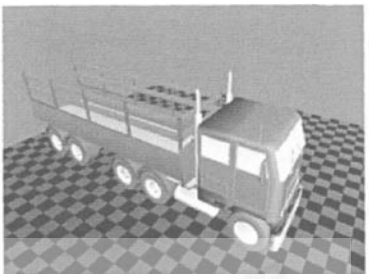

图 3　OpenGL 环境中绘制的模型

4 系统仿真过程实现

目前军事物流单位通常拥有不同型号的运输车辆，而且所需运输的货物种类也非常多，货物的尺寸、重量等特性也各不相同。其中常见的决策问题就是：在车辆最大载重量的前提下，如何最大限度利用车辆装载货物，从而使运输成本降低的同时客户服务也得到改善。系统仿真过程如图 4 所示。

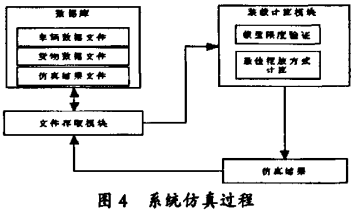

图 4　系统仿真过程

5 结束语

本文给出了一种应用 OpenGL 技术进行军用物资仿真软件设计的过程和部分代码，应用 3DMAX 建立基于了 OpenGL 的几何模型，找出了一种复杂物体建模的有效途径，降低 OpenGL 了建模的难度。经过实际验证，本软件可实用性较好，同时可利用代码移植性好的特点，将本软件集成到大型物流管理软件中。

参考文献：

[1]朱长德，叶钦媚.一种基于 OpenGL 的三维模型转化方法[J].金卡工程.2005,(7):47-49.

[2]杨春金.刘敏.基于 OpenGL 地形地物三维可视化研究[J].武汉理工大学学报.2005,(6):400-403.

[3]郭成操.基于 OpenGL 的仿真加工系统的研究[J].成都电子机械高等专科学校学报.2005,(6):29-32.

[4][美]Richard S.Wright,Jr.Benjamin Lipchak 著，徐波译.OpenGL 超级宝典[M].第三版.北京：人民邮电出版社.2005.22-23.

(上接第 708 页)

4.2 GSM 网络的安全机制

GSM 网络对用户身份标识的认证是通过一种挑战应答的机制来实现的。GSM 系统中的安全认证参数三元组包括一个 128bit 长的伪随机数 RAND，32bit 长的认证响应 SRES 和一个 64bit 长的临时加密密钥 KC，移动用户的身份认证过程描述如下：

(a) 移动用户把 TMSI 和访问网络服务请求发给移动基站，基站将 TMSI 和请求发给拜访局。

(b) 拜访局根据 TMSI 从数据库中调出移动用户的认证参数(RAND,RES,KC)，并传送 RAND 给移动用户。

(c) 移动电话中的 SIM 卡利用移动用户的秘密密钥和 RAND 通过身份认证算法和密钥生成算法生成认证响应 RES′ 何 KC，并将 RES′ 经过基站发给拜访局。

(d)拜访局比较 RES???′ 和 RES；如果相同则拜访局为该移动用户重新分配一个新的 TMSI′ ，并且利用加密密钥 KC 加密 TMSI′ 后发给移动用户，并确认登记成功。

上述移动用户身份认证过程不仅可以实现移动用户的身份认证性，也可以实现移动用户身份保密性。GSM 网络采用了临时身份号的方法，在一定程度上可以保护移动用户的真实身份 IMSI。但是当移动电话第一次使用时，它传其 IMSI 和其他数据给网络端的拜访局进行登记。

5 结束语

移动通信的发展给用户带了方便和自由，然而信息在空中的无线传播也给移动通信带了潜在的威胁，通信的内容可能会被窃听、通信对方的身份可能被假冒。SIM 卡作为用户身份的安全载体，采用了加密和身份认证技术来保护用户的通话内容，防止非法用户访问移动网络，在很大程度上提高了移动通信的安全性。本文对 SIM 卡的安全基础——COS 系统，做了十分详尽的分析，为今后电子商务的应用开发打下了坚实的基础。

参考文献：

[1]田敏,黄翊.等.译.移动应用开发—短消息业务和 SIM 卡开发包[M].第 1 版.北京:人民邮电出版社,2003.

[2]王爱英.智能卡技术[M].第 2 版.北京:清华大学出版社,2000.

[3]王卓人.IC 卡的技术与应用[M].第 1 版.北京:电子工业出版社,1999.