

无驱智能卡加密锁的妙用



1. 引言

ROCKEY6是北京飞天诚信科技有限公司推出的全球首款32位无驱智能卡加密锁，作为一款高性价比的软件保护产品，ROCKEY6本身并不提供PIN管理的功能。因为对于软件保护而言，锁就是唯一的认证因子。锁存在，软件可以运行；锁不存在，则软件不能正常运行。但是ROCKEY6的设计凝结了飞天诚信在软件保护和身份认证领域十几年的经验和心得，其安全机制和开发模式都独具匠心，本文将介绍利用ROCKEY6提供的强大功能，如何实现智能卡的PIN管理。

2. PIN管理

PIN即Personal Identification Number的缩写，就是常说的个人密码，通常用于卡片对其持有者身份进行认证。

PIN管理主要有以下几个方面（参考《中国金融集成电路卡规范》即PBOC1.0规范）

* 校验PIN：验证用户PIN，如果PIN正确，则可以获得某些权限。

* 修改PIN：将旧的PIN，换成新的PIN。

* 解锁PIN：将锁定的PIN进行解锁。下面会介绍PIN锁定的概念。

* 重装PIN：在不知道旧PIN的情况下，产生一个新的PIN（可以与原PIN相同）

前两个功能是一般用户使用的，后两个功能是卡管理者使用的。

那什么是PIN锁定？PIN的锁定指得是PIN码错误重试次数已经为0的状态。在此状态下PIN码不能再进行VERIFY操作，也不能进行CHANGE操作，只能解锁PIN或重装PIN。设置PIN锁定状态的目的是为了防止“尝试PIN攻击”，即穷举PIN的所有情况，不断尝试。一般设置PIN码错误重试次数为3，PIN码错误一次，该次数减1，减到0则表示锁定。一旦认证成功，重试次数又恢复到3。

明确了PIN管理的内容，下面来看ROCKEY6的安全机制和开发模式。

3. ROCKEY6的安全机制和开发模式

3.1 几个相关概念：

要了解ROCKEY6的安全机制，需要先弄清楚几个概念：

3.1.1 系统安全级别：

系统本身的安全级别，分为16个不同的级别，其中0是最低级，15是最高级。

3.1.2 文件类别：

文件类别（FCLA），是文件的分类标志。类别编码相同的文件一般会被假定为同一应用的文件。文件类别是以一个字节来标志，可以取值为（0x00-0xFF）。

关于类别有如下的规定：

1) 0xFF表示“无类别”，这个类别的数据文件可以被任何类别的可执行文件访问，而这个类别的可执行文件只能访问类别为0xFF的数据文件。

2) 系统根目录的类别是“无类别”。

3) 在加密锁中，相同类别的文件构成一个相对独立的子系统，“无类别”数据文件是公共数据，“无类别”可执行文件是公共处理程序。

3.1.3 文件安全级别：

文件安全级别用来限制相同类别文件的访问控制，即安全级别是针对相同类别文件设置的。分为16个不同的级别，其中0是最低级，15是最高级。

3.1.4 文件属性：

文件属性有五种，分别是普通、内部使用、高于忽略、目录和可执行文件。一个文件可以有多个属性。

* “普通”属性没有任何的特殊性，如果不设置，就默认为此属性。

* “可执行”属性指出文件是否为一个能在COS

上运行的文件，这种文件必须放在加密锁的根目录下，而且只有在超级密码验证通过后才能创建和删除。

* “目录”属性表示这是一个子目录，如果这个属性被设置，其它属性位会被忽略。

* “高于忽略”属性只对加密锁内部的可执行文件有效，表示这个可执行文件只在系统安全级别低于可执行程序自身安全级别的情况下才运行，若系统安全级别已经高于或等于可执行文件自身的安全级别，这个文件就不执行。

* “内部使用”如果是数据文件，表示这个文件只能由加密锁内部的可执行文件来访问，外部操作只有在超级密码验证通过后可以删除，但不可以读写。没有超级密码验证通过的时候根本不允许外部访问。如果是可执行文件，表示这个文件有隐含的属性，在列目录时，如果没有通过超级密码验证，有隐含属性的可执行文件就不会显示出来，这也是对可执行文件的一种保护。

3.2 安全机制

ROCKEY6 安全机制的核心在于“系统安全级别”。它和文件的安全级别一样，都是 16 级。“系统安全级别”与“文件安全级别”相配合以提供整个卡片的完全控制。具体来说，我们如果需要操作卡内的某些文件，就必须让“系统安全级别”高于或等于“文件安全级别”。而改变“系统安全级别”的方法只有三个：

- * 一是校验“超级密码”，
- * 二是通过在虚拟机上运行的可执行程序。
- * 三是通过选择文件，造成类别切换。

在 COS 的实现中安全机制分成三个部分分散在系统中，下面加以简介：

3.2.1 全局的安全

ROCKEY6 使用一个 8 字节的“超级密码”作为全局的安全策略。超级密码是由 ROCKEY6 生产厂家提供给软件开发商，且可以由软件开发商自己修改或废除的一个口令字。当正确的超级密码送入卡内验证后，“系统安全级别”会设为最大值，卡内所有普通数据文件（不包括内部使用的）都可以读出到卡外或由卡外予以更新，而可执行文件只能被“选择/删除”。另外，如果想在卡内建立可执行文件，也必须先验证超级密码。当开发商把超级密码修改为全 0 以后，超级密码

就不能够再被修改或验证。这相当于废除了超级密码，任何人再也无法获得超级用户的权限，请慎用。

3.2.2 文件系统的安全

文件系统的安全包括两点内容，一是文件类别的应用，这主要为了将文件归于不同组，不同类别的文件其安全级别互相独立。另外文件类别也用于限制在虚拟机上运行的程序不能访问与其分属不同类别的数据文件。二是当可执行程序操作其它数据文件时，COS 会检查可执行程序的安全级别是否高于或等于待操作的数据文件的安全级别。

3.2.3 COS 的安全限制

当运行中的可执行程序如果需要改变“系统安全级别”时，COS 会限制应用程序设置的安全级别不会超过它本身设定的安全级别。

3.3 开发模式

ROCKEY6 很重要的一个特性就是在 COS 内实现了虚拟机，允许用户编写程序在 ROCKEY6 内部执行。从某种意义上讲，可以认为 ROCKEY6 是一台安装有操作系统的专用小电脑。

通过 3.1 的介绍，我们知道 ROCKEY6 内部的文件可以是数据文件，也可以是可执行文件。数据文件又可以分为普通数据文件和内部数据文件。这些文件都可以通过开发包中提供的集成开发环境 IDE 进行创建，对可执行文件，也可通过 VC 插件创建。

4. PIN 管理方案

4.1 文件结构

文件类别主要用来区分一类应用，我们的示例方案只有一个应用，所以都使用 FF 类别，以下不再特别说明。

4.1.1 USERPIN 文件

安全级别为 0，属性为内部数据文件，长度为 PIN 最大长度+2，结构为：错误重试次数（1 字节）| PIN 长度（1 字节）| PIN（PIN 长度字节）。用于存储用户 PIN。其中错误重试次数字节分为高 4 比特和低 4 比特，高 4 比特表示设定的最大错误重试次数；低 4 比特表示当前剩余的错误重试次数。

4.1.2 SOPIN 文件

安全级别为 0，属性与结构同上，用于存储解锁

和重装PIN的超级用户PIN。

4.1.3 校验PIN文件：

可执行文件，安全级别为4，功能是验证PIN后，提升系统的安全等级。执行逻辑后面详述。

4.1.4 修改PIN文件：

可执行文件，安全级别为0，功能是在参数提供的旧PIN正确时，将用户PIN改为参数提供的新PIN。

4.1.5 解锁PIN文件：

可执行文件，安全级别为0，功能是在参数提供的超级用户PIN正确时，将错误重试次数置为设置的最大值，用户PIN并不会改变。

4.1.6 重装PIN文件：

可执行文件，安全级别为0，功能是在参数提供的超级用户PIN正确时，将用户PIN改为参数提供的新的PIN。如果用户PIN处于锁定状态，要同时解锁。

4.1.7 LOGOFF文件：

可执行文件，安全级别为0，功能是将系统安全级别置为0。

4.1.8 用户数据文件：

普通数据文件，安全级别为4，用于存储用户数据。

4.2 程序逻辑

4.2.1 校验PIN：

参数：

BYTE *Pin; // 存放PIN的地址

BYTE PinLen; // PIN的长度

逻辑：

- 1) 读USERPIN文件，
- 2) 如果当前剩余的错误重试次数为0，则返回被锁定。
- 3) 如果USERPIN文件中的PIN长度与参数PinLen不相等，则当前剩余的错误重试次数-1，写回USERPIN文件，并返回当前剩余的错误重试次数。
- 4) 如果USERPIN文件中的PIN与参数Pin前PinLen个字节有不同，则当前剩余的错误重试次数-1，写回USERPIN文件，并返回当前剩余的错误重试次数。
- 5) 提升系统安全级别为校验PIN文件本身的安全级别。

6) 将当前剩余的错误重试次数改为设定的最大错误重试次数，写回USERPIN文件。

7) 返回成功

4.2.2 修改PIN

参数：

BYTE *OldPin; // 存放旧PIN的地址

BYTE OldPinLen; // 旧PIN的长度

BYTE *NewPin; // 存放新PIN的地址

BYTE NewPinLen; // 新PIN的长度

逻辑：

- 1) 读USERPIN文件，
- 2) 如果当前剩余的错误重试次数为0，则返回被锁定。
- 3) 如果USERPIN文件中的PIN长度与参数PinLen不相等，则当前剩余的错误重试次数-1，写回USERPIN文件，并返回当前剩余的错误重试次数。
- 4) 如果USERPIN文件中的PIN与参数Pin前PinLen个字节有不同，则当前剩余的错误重试次数-1，写回USERPIN文件，并返回当前剩余的错误重试次数。

5) 将当前剩余的错误重试次数改为设定的最大错误重试次数，写回USERPIN文件。

6) 将新的PIN有PIN长度，写入USERPIN文件

7) 返回成功

4.2.3 解锁PIN

参数：

BYTE *Pin; // 存放PIN的地址

BYTE PinLen; // PIN的长度

逻辑：

- 1) 读SOPIN文件，
- 2) 如果当前剩余的错误重试次数为0，则返回被锁定。
- 3) 如果SOPIN文件中的PIN长度与参数PinLen不相等，则当前剩余的错误重试次数-1，写回SOPIN文件，并返回当前剩余的错误重试次数。
- 4) 如果SOPIN文件中的PIN与参数Pin前PinLen个字节有不同，则当前剩余的错误重试次数-1，写回SOPIN文件，并返回当前剩余的错误重试次数。
- 5) 将当前剩余的错误重试次数改为设定的最大错误重试次数，写回SOPIN文件。

6) 将USERPIN文件中的当前剩余的错误重试次数改为设定的最大错误重试次数, 写入USERPIN文件

7) 返回成功

4.2.4 重装 PIN

参数:

BYTE *SOPin; // 存放 SOPIN 的地址

BYTE SOPinLen; // SOPIN 的长度

BYTE *NewPin; // 存放新 PIN 的地址

BYTE NewPinLen; // 新 PIN 的长度

逻辑:

1) 读 SOPIN 文件,
2) 如果当前剩余的错误重试次数为 0, 则返回被锁定。

3) 如果 SOPIN 文件中的 PIN 长度与参数 SOPinLen 不相等, 则当前剩余的错误重试次数 - 1, 写回 SOPIN 文件, 并返回当前剩余的错误重试次数。

4) 如果 SOPIN 文件中的 PIN 与参数 SOPin 前 SOPinLen 个字节存在不同, 则当前剩余的错误重试次数 - 1, 写回 SOPIN 文件, 并返回当前剩余的错误重试次数。

5) 将当前剩余的错误重试次数改为设定的最大错误重试次数, 写回 SOPIN 文件。

6) 将 USERPIN 文件中的当前剩余的错误重试次数改为设定的最大错误重试次数, 写入 USERPIN 文件

7) 将参数 NewPinLen 和 NewPin 写入 USERPIN 文件

8) 返回成功

4.2.5 LOGOFF

参数:

无

逻辑:

将系统安全级别置为 0, 无返回。

4.3 方案说明

* 由于 ROCKEY6 的强大和灵活, 该方案并不是唯一的, 只是可行方案中的一个。

* 文件系统的创建, 只有在验证了“超级密码”后, 才可以, 这个过程相当于智能卡的个人化。

* 在上面的方案中, USERPIN 和 SOPIN 文件设计为内部文件, 由 ROCKEY6 的安全机制保证了它们不可能被外部读出或修改, 只能通过内部的可执行文件访问。

* ROCKEY6 加电时, 系统安全级别为 0, 系统当前文件类别为 FF。

* 当校验 PIN 成功后, 系统安全级别提升为 4。

* 由于用户数据文件安全级别是 4, 所以只有校验 PIN 成功后, 才可以对文件读写。

4.4 更进一步

ROCKEY6 的 COS 被设计为可以接收并处理用户传入的 APDU, 实际上 APDU 是 COS 的唯一命令接口, 但为了给用户提供最大的方便, 我们将大部份的 APDU 都封装成简单的 API 调用, 只对用户开放了 8 条 APDU (详见《ROCKEY6 高级指南》), 这 8 条 APDU 也完全可以用 API 代替。但如果用户是智能卡应用开发的高手, 已经习惯了用 APDU 控制卡片, 那能不能只通过 APDU 实现 PIN 管理呢? 答案是肯定的。因为在 ROCKEY6 设计之初, 我们就考虑到用户可能有扩展 APDU 或修改 APDU 功能的需求, 所以 ROCKEY6 中提供了一个很强大的功能, 就是“过滤 APDU”。简单说就是 COS 在处理 APDU 之前, 先看有没有相应的过滤文件存在, 如果有, 则将 APDU 交给过滤文件处理 (详见《ROCKEY6 高级指南》)。过滤文件也是一种可执行文件, 也就是说, 我们只要将方案中的可执行文件命名为相应的过滤文件, 则用户就可以只通过 APDU 实现 PIN 管理。

5. 结论

通过本文的讲解, 我们可以看到, ROCKEY6 给用户提供的是一个强大的、灵活的开发平台, 在这个平台中, 已经具备了完善的安全机制和灵活的开发模式。利用 ROCKEY6, 不仅可以轻松实现不可破解的软件保护方案, 而且, 还可以方便地构建出大多数的标准智能卡应用。ROCKEY6 巨大的应用潜力, 还有待用户来挖掘。

6. 参考文献

- 1) 《中国金融集成电路卡规范》即 PBOC1.0 规范
- 2) 《ROCKEY6 用户手册》
- 3) 《ROCKEY6 高级指南》