

ROCKEY6 SMART 的加密方案

互联网对软件业的影响

中国人的四大发明改变了人类的世界，改变了人类的生活方式——是每一个中国人的骄傲。今天互联网在默默的改变着人类的世界，改变着人类的生活方式，改变着各个行业的运行模式，首当其冲的就是软件业。JAVA的辉煌，Google的崛起，微软的互联网转型，不都暗暗的道出了软件业发展的方向了么？

在互联网的影响下，软件的授权模式也开始了翻天覆地的变化，金山毒霸2005的销售模式历史性的从以往的付费模式转变为按服务收费，从而随即很快赢得了市场，这不得不说是互联网的力量。而那些跟不上这股浪潮的企业将慢慢的退出历史舞台，尘封在人们的记忆中。

互联网环境下新型销售模式的安全性

新的事物总是有新的挑战，新的软件销售模式也将有新的挑战。无论销售模式如何改变其最终目的都是为企业赢利，最终都要由代码转换为金钱。但是在互联网的影响下，将代码转换为金钱的最后一步却异常艰难。软件的销售模式改变了，承载软件的介质也改变了，从最常用的光盘介质已经慢慢的改变为网络介质（从互联网直接下载软件），这虽然降低了成本，但同时也方便盗版的传播。各种知名的软件的盗版可以在互联网上轻易的找到，而且相应的破解补丁也是随处可见。投入了大量人力物力的软件成为了“开源软件”，投入与回报不成比例是造成中国软件业疲软的罪魁祸首之一。互联网环境下软件销售的安全性是摆在所有软件开发商面前的一堵无法跨越的高墙，所以在满心欢喜的迎接互联网的春天的时候，你是否已经戴好了安全帽？

飞天诚信是拥有10年经验的加密锁供应商，其产品遍布全世界40多个国家，在全球加密锁领域同阿拉丁、彩虹天地（现已被收购）势为三足鼎立，并且首次将智能卡技术应用到加密锁中。针对互联网环境下软件销售安全性问题，飞天诚信推出了最新一代的高

速无驱智能卡加密锁——ROCKEY6SMART，并提供了相应的解决方案。这种产品可以根据软件的销售模式而制定不同的加密方案，可以实现远程升级，从而节省了升级硬件的资金。由于是无驱设计，可以轻松的实现跨平台，更重要的是采用的高速智能卡芯片，无论在安全性还是性能方面都非常优秀。

新型软件销售模式加密方案

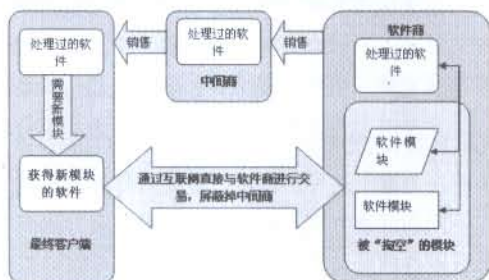
经过飞天诚信对中国软件的销售模式研究，发现中国软件业仍然以传统的分销、渠道销售等方式为主。由于分销方式可以降低成本，提高市场占有率，所以很多软件企业采用这种方式，但是这种方式有一个严重的安全性问题——盗版。盗版一套软件需要很高的费用，对于一般用户来说是难以承担的，但是在利益的驱使下，某些软件中间商会去盗版。这对软件厂商来说无疑是致命的，因为软件厂商不仅无法收回资金，而且还要为那些“正版”用户提供服务。

随着互联网的发展，出现了一种新的销售模式——网络直销，厂商通过互联网直接进行销售。这种销售模式屏蔽掉了软件中间商，但是这种模式也有它的弊端，在拓展外地业务时由于人为、地利环境的制约，难以打入当地市场。所以网络直销的销售方式很少被软件企业采用。难道没有一种鱼与熊掌兼得的销售模式么？

经过飞天诚信不懈的努力，在ROCKEY6SMART的基础上提出了相应的解决方案。其基本思路是：在软件开发初期分别设计软件的**构架**和相应的**功能模块**，在程序构架和功能模块的接口处用ROCKEY6SMART进行“掏空处理”（具体实现在后续章节会介绍），然后将处理后的软件发布给经销商，经销商再将软件卖给客户，此时的软件只是一个空的软件构架。在用户需要用到相应的模块时，需要同软件开发商联系，申请获得模块。再通过互联网远程更新ROCKEY6SMART，从

而获得新的软件模块。

具体实现流程可以参照下图:



如图所示,在软件销售过程中,中间商只是销售了空的软件构架,其内部的功能模块需要与软件商进行交易才可以获得。此时软件开发商是通过销售模块来收回资金。由于ROCKEY6SMART本身的特点(内部程序无法取出及其他安全规则),从而保证了开发商的利益。在此基础上,软件开发商还可以开拓多种软件销售模式。

软件租赁: 最终用户通过租赁的方式来为软件模块付费,可以用限次或者限时的方式实现。只需要用对ROCKEY6SMART进行简单的模块化处理就可以实现,这样做比较容易让用户接受,因为用户已经习惯为电、水、天然气付费,这样可以将软件高额的购买费用分散为租赁方式。

软件试用: 最终用户在正式使用软件之前可以免费使用若干次软件,比较符合最终用户的心里,实现方法和软件租赁类似,此处不再赘述。

软件模块授权: 当用户获得一个空的软件架构时,只有很少一部分的模块可以用。如果要使用扩展的功能,就需要向软件开发商购买。这里需要付费的软件模块是被“掏空”的,就是在软件开发过程中,主程序和模块之间的接口被移植为C语言。但是在销售软件时没有将该模块加入到ROCKEY6SMART中,需要用远程升级来将新的模块放入ROCKEY6SMART中,所以这和以往的“软件授权”是不同的。

上图只是一个简单的软件销售方案模型,具体实施时可以根据实际情况进行修改。所有的销售方案都是建立在ROCKEY6SMART的远程升级和智能卡的基础上的。上面所提出的几种销售模式只是例子模式,具体

情况中可以根据实际情况进行扩充。并且飞天诚信很愿意为广大软件商提供技术支持和解决方案。下面将详细介绍远程升级和智能卡加密的具体实现方法。

针对安全性问题的解决方案

一、知道你在用什么

在使用ROCKEY6SMART之前先要了解一下ROCKEY6SMART的特点

1. 该加密锁内嵌智能卡芯片——可以执行标准C程序(算法隐藏)。
2. ROCKEY6SMART是无驱型的——可以很方便的实现跨平台(良好的适应性)
3. 高速-32位CPU——可以提高信息处理的速率(解决程序瓶颈问题)
4. 内嵌DES/3DES/RSA和许多数学算法库——可以实现数据加密(极大提高加密安全性)

二、知道你要干什么

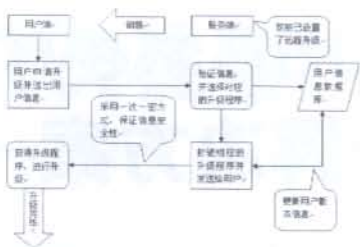
在了解了ROCKEY6SMART的产品特性之后,就可以和软件有机的结合起来了。在此要纠正一个误区:很多人认为对软件进行加密就是在软件开发完之后,再用工具对开发好的软件进行处理。而真正的使用方法是,根据硬件产品(加密锁)的特性,让硬件产品实现一定的功能,从而实现深度的加密。这样作的好处是:不仅不会因为“强行”加密,而造成水土不服,还可以提高安全性。所以在软件设计阶段就应当考虑好整个项目的各个部分的设计,并有机的将加密机制糅合进设计中,其中最让人感到困难的就是软件的升级/维护策略。下面将以一个现实中的实例来进行分析。

三、怎么做?

远程升级方案

在软件的设计初期应该考虑到软件的升级/维护策略,如果没有处理好该问题,在软件开发完毕后单单是对软件的售后服务就足以拖跨一个小型公司。而且远程升级也是实现新型销售方式的基础。飞天诚信为此提供了相应的远程升级方案。该方案可以通过互联网进行安全、稳定的远程升级。

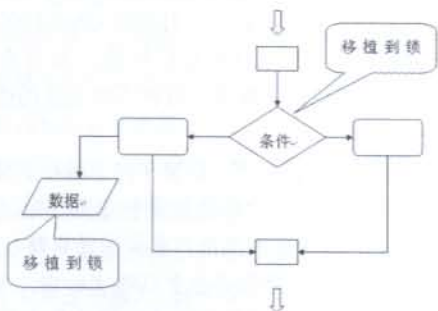
下面将用一个图例来描述远程升级的解决方案



飞天诚信已经将远程升级解决方案集成到ROCKEY6SMART中,对软件的远程升级只需要在发布软件前对ROCKEY6SMART进行相应的设置即可以实现远程升级。详细信息可以查阅 <http://www.FTsafe.com.cn>

“掏空”处理

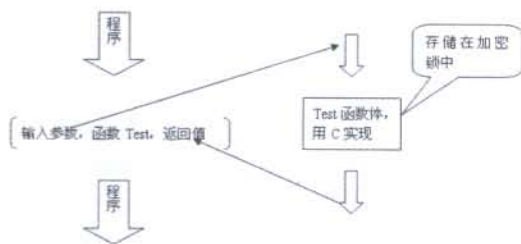
下面将讲述如何用ROCKEY6SMART实现“掏空处理”。在初期设计好您的软件,让ROCKEY6SMART承担一部分功能。将软件中最重要的部分代码提取出来,并用C语言改写(不能是调用系统API或者其他函数库的代码)。这部分工作是在软件设计初期完成的。



此图主要介绍ROCKEY6SMART的加密原理,这种算法隐藏不同于普通的数据隐藏,因为数据隐藏在多次测试的情况下是可以猜测出来的,但是ROCKEY6SMART

是将整个算法移植到智能卡中运行,运行中的数据不会出现在内存中。这为那些对代码保护能力较差的语言提供了很高的加密解决方案(例如JAVA和C#)。这也是ROCKEY6SMART的优越性之一。但是如何实现呢?

对ROCKEY6SMART的所有操作都是由我们提供的标准的API函数来实现的,对运行嵌入到ROCKEY6SMART的函数也是一样的,基本格式是:(锁参数 + 相应的输入参数 + 要运行的函数的名字 + 相应的输出参数)看看是不是就好像用DOS一样简单?也许这里用一个图表来表示更加清晰。



由于这个Test函数存储在加密锁中,从而实现了函数/算法隐藏,即使程序本身被反编译了,TEST函数仍然是不可见的。从根本(跟踪内存,反编译等)上去除了破解的可能。

这个Test函数是由特殊的编译器(KEIL)来编译生成的,运行方式跟编译普通的C程序没有区别。这样在程序设计初期就已经将加密糅合进去,可以防止强行加密的水土不服,并且可以极大的提高加密安全性。至此,ROCKEY6 SMART的加密方案已经介绍完了,如果希望获得更多技术资料请访问飞天诚信的网站主页: <http://www.FTsafe.com.cn>

