基于 SSX20-D 安全芯片的加密存储安全模型①

宋福刚, 魏广博, 管文强, 张卫芬

(解放军 72850 部队, 济南 250031)

摘 要: 针对特殊领域对大容量移动存储设备安全性的特殊要求, 本文在 SSX20-D 安全芯片的基础上设计了存储数据安全保护、U 盘密钥参数保护和 U 盘使用控制管理三层次的安全模型. 采用了数据加密、U 盘参数保护、加密密钥保护、口令硬件使用控制、U 盘抗攻击等安全机制, 将 KEY 的安全性拓展到大容量存储芯片中. 特别是针对密钥参数保护这一安全薄弱环节设计了三级密钥保护方式, 综合运用 SM1 算法、SHA-256 算法和自定义函数确保密钥绝对安全.

关键词: 安全芯片; 安全模型; SM1; SSX20-D

Encryption Storage Safety Model Based on SSX20-D Security Chip

SONG Fu-Gang, WEI Guang-Bo, GUAN Wen-Qiang, ZHANG Wei-Fen

(72850 Unit of PLA, Jinnan 250031, China)

Abstract: Aiming at the special requriement of the mobile hing-capacity storage device's safety in the special field, based on SSX20-D security chip, we designed the security model with three levels: data storage security protection, usb flash disk key parameter protection and usb flash disk using management. The security chip uses many security mechanisms, including data encryption, usb flash disk parameter protection, encryption key protection, password-hardware using control, and the usb flash disk anti-attack ability. The mechanism expended the Key's safety to the hing-capacity storage chip. Especially it designed three-level key-protection method which can solve the safety weakness of the key parameter protection. We are using SM1, SHA-256 and self-defined function to make sure absolute security of the key.

Key words: security chip; safety model; SM1; SSX20-D

U 盘作为信息化条件下移动载体被广泛使用, 在带来便利的同时, 也给信息资料的安全性带来严重隐患, 市面上各类安全 U 盘, 在硬件和安全模型方面还无法保证信息的绝对安全, 在特殊保密领域, 研发一款高安全性和健壮性, 能够保存高涉密信息的安全 U 盘成为一项紧迫工作. SSX20-D 安全芯片是采用 Acra2S 内核的多功能安全处理平台, 多应用于银行、电子商务的 USB KEY 和加密机中, 通过 USB KEY 协议、U 盘协议分析和硬件集成改造, 将 KEY 安全芯片的安全体系拓展到大容量FLASH芯片中, 实现移动加密存储的高安全性, 对于信息安全保密具有重大意义.

1 安全模型概述

安全模型最终的保护对象是存储的数据, 以数据的整体安全为中心, 从纵深来解决加密、控制、认证问题. 设计了存储数据安全保护、U 盘密钥参数保护和 U 盘使用控制管理三层次的安全模型. 采用了数据加密、U 盘参数保护、加密密钥保护、口令硬件使用控制、U 盘抗攻击等安全机制, 如图 1 所示.

安全模型特点为 SSX20-D 芯片内置高强度 SM1 算法与真随机数发生器, 支持数据流硬件加密及加密密钥随机生成; 密码算法运算及身份认证等所有安全性相关操作都在设备内完成, 独立于主机, 可以较好的

① 基金项目:山东省科技支撑计划基金(2013GZ0017)
收稿时间:2014-05-02;收到修改稿时间:2014-05-26

保护敏感数据; 支持多级基于硬件的代码保护机制与最大为四级的用户权限管理.

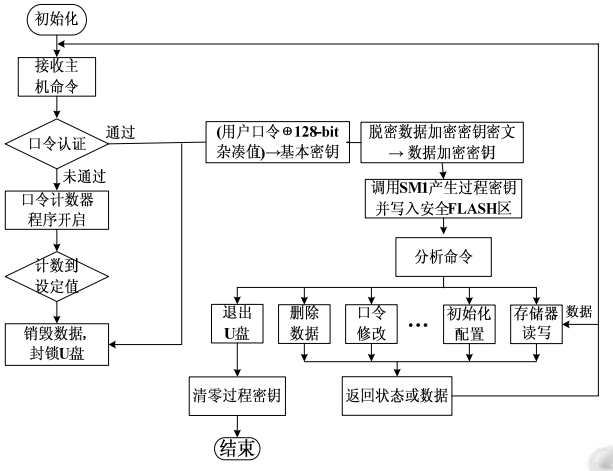

图 1　安全模型

1)数据安全保护层

数据保护是安全模型的核心, 确保数据安全是安全 U 盘设计的最根本目的. 数据加密是保护信息的核心技术, 是任何其它手段都无法替代的. 安全 U 盘使用 SM1 密码算法, 对用户存储数据实施加密, 保证存储在 U 盘中的数据始终是密文, 防止非法用户直接读取, 获得有用信息.

2)密钥参数保护层

密钥是密码算法的最关键参数, 密钥的保护至关重要. 安全模型采用三级密钥保护方式, 将 SSX20-D 安全芯片的安全 FLASH 区进行分割并设置不同访问权限. SM1 算法代码存放于固定保护区域, 在存储空间上, 与口令、密钥及固件控制程序完全隔离. 算法区域具有本地可执行的属性, 只有固件控制程序可通过调用算法程序入口执行该区域内程序代码, 而上层应用程序无任何访问权限; 密钥存储区仅对于固件控制程序而言是可读可写的, 外部应用程序无访问权限.

口令以杂凑值形式存储, 其存储区域只有固件控制程序可以进行读写访问; 基本密钥在每次使用时由口令和口令杂凑值通过特殊函数运算得出, 不进行存储; 加密密钥由基本密钥通过 SM1 算法加密成密文存放于设计人员指定的 FLASH 安全区; 过程密钥由加密密钥随机产生, 保证一次一密.

3)安全 U 盘使用控制管理层

采用硬件实现口令认证方式, 即通过硬件实现用户对 U 盘访问操作口令认证, 当口令不正确时, 用户将无法访问 U 盘数据及参数, 当口令输入错误累计次数达到安全策略定义的阈值时, 硬件实现 U 盘锁定.

2　安全模型设计与实现

2.1 存储加密设计

2.1.1 系统整体存储密码结构

安全模型采用了两级密钥结构, 口令密钥 KA, 数据加密密钥密文 KF. 当大容量 FLASH 数据要进行加/脱密处理时, 首先, 口令密钥通过 SM1 算法脱密数据加密密钥密文得加密密钥明文, 用加密密钥明文通过 SM1 算法生成过程密钥, 将过程密钥暂存于 SSX20-D 安全芯片内, 用过程密钥加/脱密,进/出大容量 FLASH 的数据流.

整个加/脱密过程都由固件控制程序独立管理. KF 在设备掉电不会丢失、U 盘每次初始化或修改口令, KF 更新一次, 外部程序不能从安全 U 盘将其读出、修改或删除, 只能由固件控制程序的加密操作调用.

数据加密密钥并不直接用作安全 U 盘存储数据的加密密钥, 而在 SM1 算法过程密钥生成函数的调度下生成的过程密钥, 过程密钥才用作存储数据的加密密钥.

2.1.2 FLASH 存储加密

为防止非法用户利用其他手段直接读取 FLASH 存储芯片, 单纯的 U 盘访问控制机制并不能从根本上解决安全 U 盘的安全隐患, 存储数据还需要进行加密处理. 数据加密是该安全 U 盘的核心, 安全 U 盘按照功能设计要求, 采用 SM1 分组加密算法, 分组长度 128-bit, 算法主密钥长度为 128-bit; U 盘数据加密密钥密文、用户口令的杂凑值存储在 SSX20-D 安全芯片安全存储区内, 当向 FLASH 芯片内写入数据时, 首先调用 SM1 算法, 对数据流进行加密后, 然后调用底层写函数(物理地址对底层 FLASH 的写函数 udisk_write_2k), 将数据写入 FLASH; 当由 FLASH 芯片内读出数据时, 首先调用底层读函数(物理地址对底层 FLASH 的读函数 udisk_read_2k), 然后调用 SM1 算法, 将读出数据流进行脱密后, 送入到主机.

2.2 控制模块设计

对于此安全模型来说, 安全管理模块, 也即固件控制程序的设计是关键.

1) 固件工作原理

安全 U 盘初始化完成后, 首先需要对用户进行身

份认证. 验证通过, 启动安全管理模块, 实现对 U 盘的安全访问. 再继续接受主机命令, 并进行相关操作.

如果口令验证不正确, 则启动口令计数器计数, 继续进行口令验证. 当计数累计达到预定的阈值时, 则锁定安全 U 盘, 使用户不能进行任何操作. 只有返回生产厂商重新进行复位设备操作, 且同时销毁 U 盘加密密钥与数据.

数据的加密存储采用分组密码 SM1 算法加密. 其主密钥长度为 128-bit, 分组长度为 128-bit. 采用 128-bit 的数据加密密钥调度产生的 160 个字节过程密钥为对大容量 FLASH 存储器上的存储数据加密.

安全 U 盘根据上层传输的用户命令, 执行相应的处理, 比如数据分组的加/解密运算、修改认证口令、初始化 U 盘分区等操作.

2)固件的基本工作流程

安全 U 盘的工作流程如图 5 所示. 安全 U 盘初始化完成后, 固件控制程序开始接受主机命令, 完成相应操作并返回状态和数据. 使用安全 U 盘时, 首先要进行用户口令验证, 完成用户身份认证. 当验证通过后, 用户口令与其低 128-bit 的杂凑值异或(异或运算时, 口令不足 128-bit 的高位用“0x00”补齐, 多于 128-bit 的则裁减其高位), 将所得结果调用 SM1 算法脱密数据加密密钥密文, 然后将得到的数据加密密钥进行 SM1 算法密钥调度, 生成 160 字节的过程密钥暂存于 SSX20-D 安全芯片的安全 FLASH 区内; 安全 U 盘继续接受主机命令, 并进行相应操作, 如 FLASH 内数据的删除或读写、安全 U 盘内口令设置、重新初始化等. 命令执行完成后, 安全 U 盘根据命令向主机(或存储器)返回状态或数据, 然后继续等待主机命令.

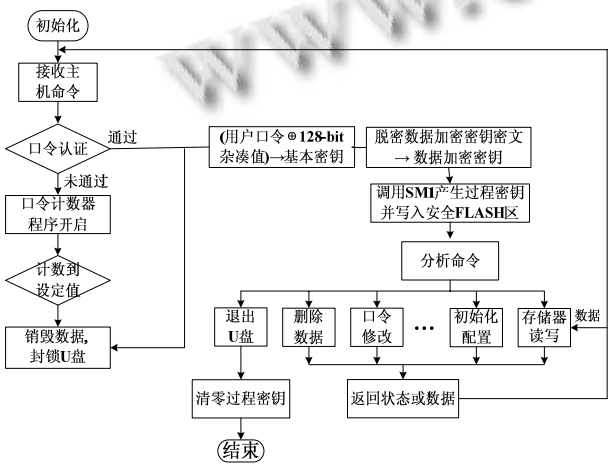

图 2 固件工作流程

若口令验证不正确, 则进入审计过程, 启动口令计数器计数, 继续进行口令验证. 当输入口令次数达到内部预先设定值时, 则锁定安全 U 盘, 使非法用户不能再进行任何操作, 而只有生产厂商才可以对安全 U 盘进行重新配置.

当接收到用户退出安全 U 盘命令时, 固件控制程序将安全区内的 160 字节的过程密钥清零.

2.3 密钥管理设计

安全模型采用三级密钥方式. 一级密钥为口令密钥, 二级密钥为基本密钥, 三级密钥为数据加密密钥. 用户口令经 SSX20-D 安全芯片的 SHA-256 算法模块处理后, 得到 256-bit 杂凑值, 存储于 SSX20-D 安全芯片的安全 FLASH 区; 当安全 U 盘启用时, 验证登录口令杂凑值与安全 FLASH 区的杂凑值一致时,判断为合法用户, 固件控制程序取口令杂凑值的低 128-bit 与用户口令(128bit 补 0x00,高于 128-bit 取其低 128-bit)相异或得到的密钥为口令密钥. 数据加密密钥由随机发生器产生, 而将口令密钥调用 SM1 算法加密数据加密密钥, 得到 128-bit 的数据加密密钥密文并存储于安全 FLASH 区内. 安全 FLASH 区具有读写可控制的特性, 非法使用者难以获得其内部有效数据; 在合法用户通过认证后, 在固件控制程序调度下, 提供给 SM1 密码算法, 生成 160 个字节的过程密钥, 将过程密密钥临时存储在 SSX20-D 安全芯片内, 用以正确的实施数据加/脱密.

3 模型安全性分析与验证

3.1 安全策略分析

研究 Flash 的数据流程, 我们会发现在缓冲区的处理上, 移动存储介质是比较特别的. 当我们从介质中读数据时直接从 Flash 存储芯片中读就行了, 数据并不需要经过缓冲区, 而写数据时由于 Flash 擦除机制的原因, 必须先将数据块复制到缓冲区中, 修改好了再写入 Flash. 为此我们设计的安全 U 盘存储数据加密方案为: 在主控制器修改缓冲区中数据的时候加密, 在主控制器向 PC 机送数据即从控制器管道读的时候对数据进行脱密. 密钥由安全芯片存储, 长度固定, 由应用程序向加密 U 盘发送的命令流控制字通知密钥的读取与修改. 结合安全 U 盘的实际情况, 本方案采用 SM1 分组密码算法对存储数据进行加密, 分组长度为 128-bit.

3.2 密钥安全分析

在系统设计中, 用 SSX20-D 安全芯片中 SHA-256

算法对用户口令进行杂凑运算后存储,要使用安全 U 盘, 首先要进行口令认证. 产品采用二级密钥来进行管理, 口令密钥长度固定为 128-bit, 与用户口令密切相关, 口令长度为 8 个字符至 64 个字符之间, 口令的修改会使口令密钥发生变化, 口令密钥在安全 U 盘合法用户认证通过后在 SSX20-D 安全芯片内合成, 密钥分量以密文的形式存储于 SSX20-D 安全专用 FLASH 区内, 非法用户难以获得.

数据加密密钥由SSX20-D安全芯片的真随机数发生器产生, 安全 U 盘每初始化一次数据加密密钥更换一次; 数据加密密钥由口令密钥保护, 口令的修改影响数据加密密钥文的变化; 数据加密密钥只有在合法用户认证通过后才能产生; 数据加密密钥密文存储在 SSX20-D 安全芯片专用 FLASH 区内; 对安全 U 盘的使用, 在验证口令时, 错误次数超过 8 次, 固件控制程序将清除所有密钥信息并自动死锁, 这样安全 U 盘内部的数据都将无法读出, 有效地保证了用户口令及密钥的安全. 密钥的产生、存贮都保证了不出 SSX20-D 安全芯片, 保证了其物理安全性.

3.3 数据安全性分析

安全U盘中的数据均由SSX20-D安全芯片加密后存储, 即使将存储芯片拆离安全 U 盘, 也不能读出其中的数据; 用于其加密的数据加密密钥采取二级密钥保护的方式进行, 且密钥的整个生命过程均在SSX20-D安全芯片内进行; 安全U盘利用SSX20-D安全芯片, 在 SSX20-D 安全芯片内部实现基于硬件的加、脱密全过程, 不会出现数据泄露问题.

3.4 整体安全性分析

安全模型整体设计从以下几个方面保证了密钥、算法及数据的安全:

1)口令密钥的密文主要分量存储于 SSX20-D 安全芯片安全 FLASH 区内, SSX20-D 安全芯片本身设计了防止外部非法攻击者访问机制; 而非法攻击者即便获取了口令密钥分量也难以得出用户有效的登录口令.

2)数据加密密钥由 SSX20-D 安全芯片内部真随机数发生器产生, 且经过严格的随机性检测并与口令密钥通过 SM1 加密后得到的数据加密密钥的密文存储在安全专用 FLASH 区中.

3)真正用于数据加密的密钥为基于数据加密密钥生成过程密钥, 临时存储于安全芯片 SSX20-D 的安全 FLASH 区, 安全 U 盘使用完成一次操作退出时, 随即将过程密钥清零. 这样部分密钥参数信息泄露, 也不会对加密数据构成威胁.

4)算法属于独立的程序和数据代码, 配置于安全芯片 SSX20-D 的独立算法区内, 与固件控制程序完全隔离, 固件控制程序仅能对其通过预留程序入口调用, 不可做任何形式修改, 这样就确保了算法自身的安全.

5)存储在 U 盘里的数据都是密文, 防止非法用户直接读取大容量闪存, 获得有用信息.

6)安全U盘的使用必须经过硬件口令认证, 且口令的长度最多可达64个字节, 连续8次口令认证错误, 固件控制程序将清零安全U盘的密钥、配置数据等参数, 彻底使安全U盘死锁.

4 实验测试

测试内容: 功能测试(略)、性能测试(略)、算法正确性测试.

测试方法: 当向 FLASH 芯片内写入文件数据时, 通过调用 SM1 算法, 对数据流进行加密后, 然后调用底层写函数, 将数据写入 FLASH; 当由 FLASH 芯片内读出数据时, 调用底层读函数, 然后调用 SM1 算法, 将读出数据流进行脱密后, 送入到主机, 可以看出数据正确脱密.

当由FLASH芯片内读出数据时, 首先调用底层读函数, 然后修改固件将调用 SM1 算法操作屏蔽, 此时读入到主机的数据为文件数据密文, 用户可以观察到此数据无法解读.

测试结果: 通过在 WindowsXP 和 win7 平台进行功能测试、性能测试和算法正确性测试, 安全 U 盘功能可用, 性能稳定, 算法安全可靠, 达到了设计要求.

5 结语

安全模型采用存储数据安全保护、U 盘密钥参数保护和 U 盘使用控制管理三层次的安全模型. 通过对安全芯片的Flash区划分并进行权限设定, 采用固件程序访问机制, 防止外部程序读写, 从硬件层实现 U 盘安全, 满足了高涉密领域对移动存储设备的安全需求.

参考文献

1 徐远航.USB Key 身份认证产品的产生与发展.计算机安全, 2011, 8: 44−45.

2 姜雪莲,司徒忠.基于单片机的嵌入式 U 盘控制器的设计与实现.机电工程技术,2009,34(4):79−81.

3 严波,郭莉,潘强宗.基于 USB KEY 的身份鉴别技术研究与应用.高性能计算机技术,2009,174:36−38.

4 陈纬,周培源,童敏.智能卡数据安全技术的研究.信息安全与通讯保密,2008,3:44−47.

5 范晓红,吴今培,张其善.智能卡文件系统的安全访问机制.微计算机应用,2009,25(l):37−39.