



(12)发明专利申请

(10)申请公布号 CN 106507349 A

(43)申请公布日 2017. 03. 15

(21)申请号 201610892459.6

(22)申请日 2016.10.13

(71)申请人 山东康威通信技术股份有限公司
地址 250101 山东省济南市高新技术开
发区舜华路1号齐鲁软件园F-1座A203

(72)发明人 孔得朋 杨震威

(74)专利代理机构 济南圣达知识产权代理有限
公司 37221

代理人 黄海丽

(51) Int. Cl.

H04W 12/06(2009.01)

H04L 9/32(2006.01)

H04L 9/06(2006.01)

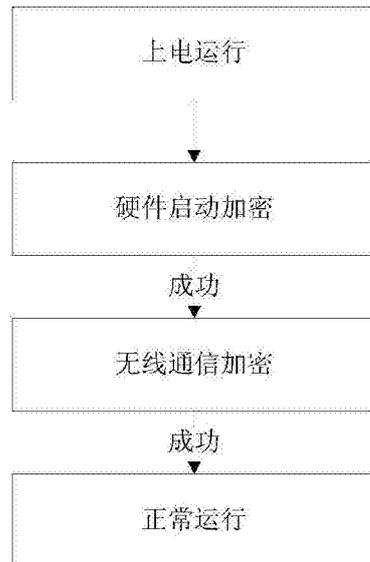
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种软硬件结合的嵌入式终端加密系统及加密方法

(57)摘要

本发明公开了一种软硬件结合的嵌入式终端加密系统及加密方法;包括:嵌入式终端,嵌入式终端与服务器或者移动终端通信;嵌入式终端包括MCU,MCU分别与FLASH存储单元和加密芯片连接;进行数据和命令信息的传输;FLASH存储单元受控于MCU;所述加密芯片用于加密运算,根据MCU的控制指令来选择加密方式;嵌入式终端工作时,首先通过硬件启动加密验证,然后通过无线通信加密验证,最后才能正常运行。通过硬件启动加密和无线通信加密两部分结合,一起实现嵌入式终端的加密,双重加密,双重保障,保障了嵌入式终端运行的安全可靠,同时也有效的防止了那些恶意破解硬件设备及其嵌入式程序的竞争对手,有效的保障了技术的不泄露。



1. 一种软硬件结合的嵌入式终端加密系统,其特征是,包括:
嵌入式终端,所述嵌入式终端与服务器或者移动终端通信;
所述嵌入式终端包括MCU,所述MCU为主控单元,所述MCU分别与FLASH存储单元和加密芯片连接;进行数据和命令信息的传输;所述FLASH存储单元受控于MCU;所述加密芯片用于加密运算,根据MCU的控制指令来选择加密方式;
嵌入式终端工作时,首先通过硬件启动加密验证,然后通过无线通信加密验证,最后才能正常运行;通过硬件启动加密和无线通信加密两部分结合,实现嵌入式终端的加密。
2. 一种软硬件结合的嵌入式终端加密方法,其特征是,包括如下步骤:
步骤(1):上电运行;
步骤(2):硬件启动加密;验证硬件启动加密是否成功,若成功进入步骤(3);若失败就重新进行验证,若超过设定次数仍然验证失败,则返回步骤(1);
步骤(3):无线通信加密;验证无线通信加密是否成功,若成功就进入步骤(4);若失败就重新进行验证,若超过设定次数仍然验证失败,则返回步骤(3);
步骤(4):正常运行。
3. 如权利要求2所述的方法,其特征是,所述步骤(3)与步骤(4)之间还设有:
步骤(30):密钥更改,通过服务器或者移动终端实现密钥更改,验证密钥更改是否成功;若成功就进入步骤(4);若失败就重新验证,若超过设定次数仍然验证失败,则返回步骤(1)重新上电。
4. 如权利要求3所述的方法,其特征是,所述密钥更改包括硬件启动加密密钥更改和无线通信加密密钥更改。
5. 如权利要求2所述的方法,其特征是,所述步骤(2)下步骤:
步骤(21):嵌入式终端的MCU生成随机数,MCU将随机数交于加密芯片,加密芯片采用SHA1算法进行运算;加密芯片生成第一信息验证码;
步骤(22):MCU采用SHA1算法进行运算,MCU生成第二信息验证码;
步骤(23):密码验证:将第一信息验证码与第二信息验证码进行比较,若第一信息验证码与第二信息验证码一致,则嵌入式终端的MCU进入步骤(3);若第一信息验证码与第二信息验证码不一致,则返回步骤(21);若查过设定次数仍验证不一致,则返回步骤(1)。
6. 如权利要求5所述的方法,其特征是,所述步骤(21)之前还包括:
步骤(201):MCU接收密钥,同时Flash存储单元接收密钥;Flash存储单元中对接收的密钥采用密文的方式进行存储;
步骤(202):Flash存储单元接收外界写入的正常运行的程序;
步骤(203):MCU通过解密读取Flash存储单元中的密钥,得到明文密钥。
7. 如权利要求2所述的方法,其特征是,所述步骤(3)的步骤如下:
步骤(31):选择无线通信加密方式;
步骤(32):约定无线通信加密范围;
步骤(33):信息加密;
步骤(34):加密验证。
8. 如权利要求7所述的方法,其特征是,
所述步骤(31):嵌入式终端与服务器或者移动终端,首先进行第一轮明文传输,服务器

或者移动终端接收到嵌入式终端的信息,根据通信协议的约定,选择一种加密方式。

9. 如权利要求7所述的方法,其特征是,

所述步骤(32):根据步骤(31)中通信协议的约定,选择后续通信内容是全部加密,还是只进行首轮通信的加密。

10. 如权利要求7所述的方法,其特征是,所述步骤(34)的步骤为:

步骤(341):在第一轮明文传输结束以后,嵌入式终端的加密芯片生成随机码,将随机码发送给服务器或者移动终端,服务器或者移动终端根据步骤(31)确定的加密方式生成第一密文,将第一密文反馈给嵌入式终端;

步骤(342):同时嵌入式终端根据步骤(31)确定的加密方式将随机码加密后生成第二密文,将第二密文与服务器或者移动终端反馈回的第一密文对比,如果内容一致,进入后续通信,如果校验失败,断开嵌入式终端与服务器或者移动终端的连接,重新启动连接;

步骤(343):进入重新启动连接以后,重复步骤(341)到步骤(343),连续三次校验失败以后,延时设定时间后再进入步骤(341)。

一种软硬件结合的嵌入式终端加密系统及加密方法

技术领域

[0001] 本发明涉及一种加密方法,尤其涉及一种软硬件结合的嵌入式终端加密系统及加密方法。

背景技术

[0002] 目前硬件产品的研发成本很高,为了其稳定性和可靠性的研究更是费时费力,有一些竞争对手,为了省力,会对同行业的硬件产品进行破解,这往往给生产厂家造成很大的损失,针对这种想象,很多厂家都采用了加密计数来防止产品被破解。

[0003] 目前,大对数的厂家采用的是使用软件方法加密,方法主要有,用软件的方法把产品中使用的部分程序代码隐藏或者掩盖起来,使用混淆的办法把部分程序代码和数据混同起来,使用乱跳的方法使程序跳来跳去,在程序中设置大量的荣誉指针和荣誉数据等单元。

[0004] 少数厂家采用比较简单的硬件加密,方法主要是:交换总线(总线乱置)、使用替代RAM、使用GAL器件对器件外EPROM中的软件加密。这样做也确实在一定程度上增大了破解产品的难度,但是总体来看产品仍有较大可能被破解,加密效果不理想。

发明内容

[0005] 本发明的目的就是为了解决上述问题,提供一种软硬件结合的嵌入式终端加密系统及加密方法,通过硬件启动加密和无线通信加密两部分结合,一起实现嵌入式终端的加密,双重加密,双重保障,保障了嵌入式终端运行的安全可靠,同时也有效的防止了那些恶意破解硬件设备及其嵌入式程序的竞争对手,有效的保障了技术的不泄露。

[0006] 为了实现上述目的,本发明采用如下技术方案:

[0007] 一种软硬件结合的嵌入式终端加密系统,包括:

[0008] 嵌入式终端,所述嵌入式终端与服务器或者移动终端通信;

[0009] 所述嵌入式终端包括MCU,所述MCU为主控单元,所述MCU分别与FLASH存储单元和加密芯片连接;进行数据和命令信息的传输;所述FLASH存储单元受控于MCU;所述加密芯片用于加密运算,根据MCU的控制指令来选择加密方式;

[0010] 嵌入式终端工作时,首先通过硬件启动加密验证,然后通过无线通信加密验证,最后才能正常运行;通过硬件启动加密和无线通信加密两部分结合,实现嵌入式终端的加密。

[0011] 所述嵌入式终端与服务器或者移动终端之间通过WIFI或者蓝牙进行通信。

[0012] 所述服务器或者移动终端,与嵌入式终端进行通信,用于实现加密信息的验证,保障系统的安全性。

[0013] 一种软硬件结合的嵌入式终端加密方法,包括如下步骤:

[0014] 步骤(1):上电运行;

[0015] 步骤(2):硬件启动加密;验证硬件启动加密是否成功,若成功进入步骤(3);若失败就重新进行验证,若超过设定次数仍然验证失败,则返回步骤(1);

- [0016] 步骤(3):无线通信加密;验证无线通信加密是否成功,若成功就进入步骤(4);若失败就重新进行验证,若超过设定次数仍然验证失败,则返回步骤(3);
- [0017] 步骤(4):正常运行。
- [0018] 所述步骤(3)与步骤(4)之间还设有:
- [0019] 步骤(30):密钥更改,通过服务器或者移动终端实现密钥更改,验证密钥更改是否成功;若成功就进入步骤(4);若失败就重新验证,若超过设定次数仍然验证失败,则返回步骤(1)重新上电。
- [0020] 所述密钥更改包括硬件启动加密密钥更改和无线通信加密密钥更改。
- [0021] 所述步骤(2)下步骤:
- [0022] 步骤(21):嵌入式终端的MCU生成随机数,MCU将随机数交于加密芯片,加密芯片采用SHA1算法进行运算;加密芯片生成第一信息验证码;
- [0023] 步骤(22):MCU采用SHA1算法进行运算,MCU生成第二信息验证码;
- [0024] 步骤(23):密码验证:将第一信息验证码与第二信息验证码进行比较,若第一信息验证码与第二信息验证码一致,则嵌入式终端的MCU进入步骤(3);若第一信息验证码与第二信息验证码不一致,则返回步骤(21);若查过设定次数仍验证不一致,则返回步骤(1)。
- [0025] 所述步骤(21)之前还包括:
- [0026] 步骤(201):MCU接收密钥,同时Flash存储单元接收密钥;Flash存储单元中对接收的密钥采用密文的方式进行存储;
- [0027] 步骤(202):Flash存储单元接收外界写入的正常运行的程序;
- [0028] 步骤(203):MCU通过解密读取Flash存储单元中的密钥,得到明文密钥。
- [0029] 所述步骤(3)的步骤如下:
- [0030] 步骤(31):选择无线通信加密方式;
- [0031] 步骤(32):约定无线通信加密范围;
- [0032] 步骤(33):信息加密;
- [0033] 步骤(34):加密验证。
- [0034] 所述步骤(31):嵌入式终端与服务器或者移动终端,首先进行第一轮明文传输,服务器或者移动终端接收到嵌入式终端的信息,根据通信协议的约定,选择一种加密方式。
- [0035] 所述加密方式包括:AES、DES、TEA和SHA1。
- [0036] 所述步骤(32):根据步骤(31)中通信协议的约定,选择后续通信内容是全部加密,还是只进行首轮通信的加密。
- [0037] 所述步骤(34)的步骤为:
- [0038] 步骤(341):在第一轮明文传输结束以后,嵌入式终端的加密芯片生成随机码,将随机码发送给服务器或者移动终端,服务器或者移动终端根据步骤(31)确定的加密方式生成第一密文,将第一密文反馈给嵌入式终端;
- [0039] 步骤(342):同时嵌入式终端根据步骤(31)确定的加密方式将随机码加密后生成第二密文,将第二密文与服务器或者移动终端反馈回的第一密文对比,如果内容一致,进入后续通信,如果校验失败,断开嵌入式终端与服务器或者移动终端的连接,重新启动连接;
- [0040] 步骤(343):进入重新启动连接以后,重复步骤(341)到步骤(343),连续三次校验失败以后,延时设定时间后再进入步骤(341)。

[0041] 本发明的有益效果:

[0042] 通过本发明的实施,通过硬件启动加密和无线通信加密两部分结合,一起实现嵌入式终端的加密,双重加密,双重保障,保障了嵌入式终端运行的安全可靠,同时也有有效的防止了那些恶意破解硬件设备及其嵌入式程序的竞争对手,有效的保障了技术的不泄露。

[0043] 同时,本发明加密成本低,双重加密可靠性高,保障性强。

附图说明

[0044] 图1为本发明的系统组成框图;

[0045] 图2为本发明的整体工作流程图实施例一;

[0046] 图3为本发明的整体工作流程图实施例二;

[0047] 图4为本发明的硬件启动加密流程图;

[0048] 图5为本发明的无线通信加密流程图。

具体实施方式

[0049] 下面结合附图与实施例对本发明作进一步说明。

[0050] 如图1所示,一种嵌入式加密系统包括嵌入式终端和服务器或者移动终端,二者通过WIFI或者蓝牙进行通信。

[0051] 嵌入式终端包括MCU,FLASH存储单元,加密芯片。MCU为主控单元,与FLASH存储单元,加密芯片连接,进行数据和命令信息的传输;FLASH存储单元用来存储需要保存的有效信息,受控于MCU。加密芯片负责加密运算,通过MCU的控制来选择加密方式。

[0052] 服务器或者移动终端,与嵌入式终端进行通信,实现二者之间加密信息的验证,保障系统的安全性。

[0053] 如图2所示,一种嵌入式加密系统的加密方法,通过以下步骤来完成:

[0054] 系统启动:嵌入式终上电,准备运行。

[0055] 硬件启动加密:进入硬件启动加密验证过程,进行如图4所示的验证过程中。

[0056] 无线通信加密:当硬件启动加密成功以后,进入如图5所示的验证过程中。

[0057] 正常运行:系统进入正常运行阶段,通过双重的加密保障了系统的安全可靠运行。

[0058] 如图3所示,一种嵌入式加密系统的加密方法,通过以下步骤来完成:

[0059] 系统启动:嵌入式终上电,准备运行。

[0060] 硬件启动加密:进入硬件启动加密验证过程,进行如图4所示的验证过程中。

[0061] 无线通信加密:当硬件启动加密成功以后,进入如图5所示的验证过程中。

[0062] 密钥更改:当无线通信加密完成以后,可以通过服务器或者移动终端实现密钥更改,密钥更改包括启动硬件启动加密密钥更改和无线通信密钥更改。

[0063] 正常运行:当密钥更改成功以后,系统进入正常运行阶段,通过双重的加密以及加密验证以后的密钥更改,保障了系统的安全可靠运行。

[0064] 如图4所示,硬件启动加密通过如下流程实现:

[0065] 上电运行:嵌入式硬件终端上电,准备运行

[0066] 读取密钥:MCU首先读取硬件终端的FLASH中的密文的密钥

[0067] 解密:MCU将密钥解密得到明文密钥,然后生成随机数

[0068] 加密芯片生成验证码:将MCU生成的随机数,写入到加密芯片中,加密芯片采用SHA1算法,将随机数计算为信息验证码。

[0069] MCU生成信息验证码:MCU将随机数也通过SHA1算法,生成信息验证码。

[0070] 密码验证:将加密芯片计算出的信息验证码与MCU计算出的结果对比。

[0071] 正常运行或者重新启动:如果结果一致,程序进入正常运行流程,如果结果不一致,程序进入复位流程,重新启动。

[0072] 如图5所示,无线通信加密通过如下流程实现:

[0073] 加密方式选择:在通信的开始,嵌入式终端与服务器或者移动终端,首先进行一轮明文传输,服务器或者移动终端接收到嵌入式终端的信息,根据通信协议的约定,选择一种加密方式。在嵌入式终端已经实现的加密方式有AES、DES、TEA、SHA1。

[0074] 加密范围的选择:根据第一轮明文通信协议的内容约定,同时服务器或者移动终端确定后续通信内容全部加密,还是只进行首轮通信的加密验证。

[0075] 信息加密:在第一轮明文通信结束以后,嵌入式终端的加密芯片生成随机码,将随机码发送给服务器或者移动终端,服务器或者移动终端根据步骤1确定的加密方式生成密文,将密文反馈给嵌入式终端。

[0076] 加密验证:同时嵌入式终端根据选定的加密方式将随机码加密后生成密文,与服务器或者移动终端反馈回的密文对比验证。

[0077] 验证结果:如果内容一致,进入后续通信,如果校验失败,断开与服务器或者移动终端的连接,重新启动连接。进入重新启动连接以后,重复以上步骤,连续三次校验失败以后,系统自动延时三分钟再进入验证程序,防止暴力破解。

[0078] 上述虽然结合附图对本发明的具体实施方式进行了描述,但并非对本发明保护范围的限制,所属领域技术人员应该明白,在本发明的技术方案的基础上,本领域技术人员不需要付出创造性劳动即可做出的各种修改或变形仍在本发明的保护范围以内。

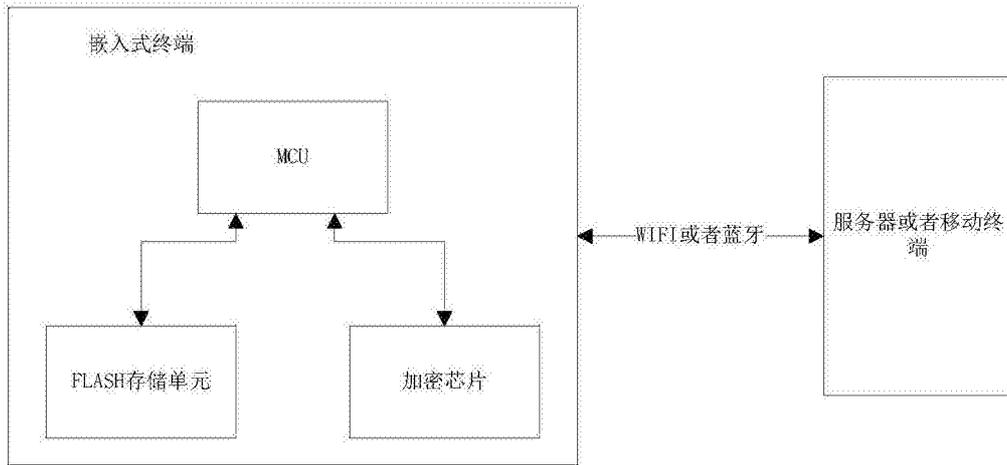


图1

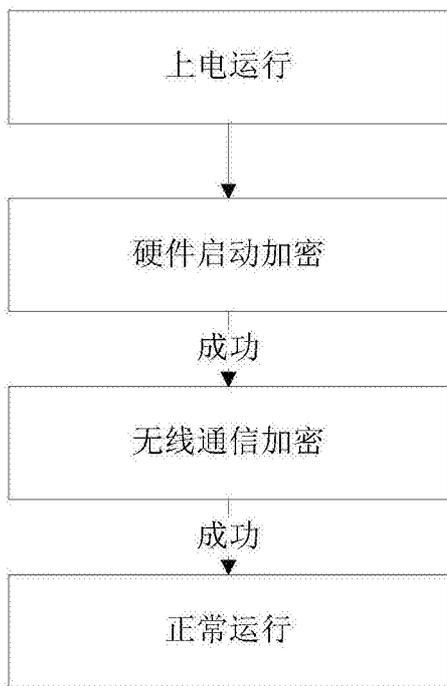


图2



图3

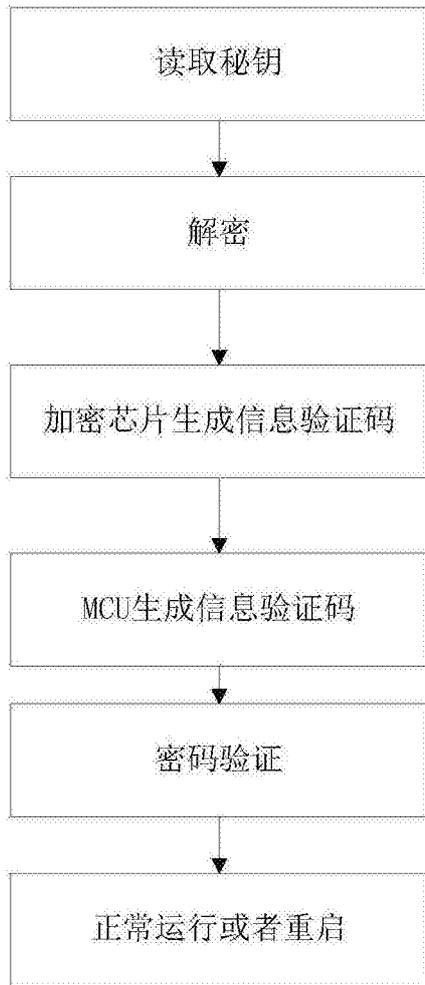


图4

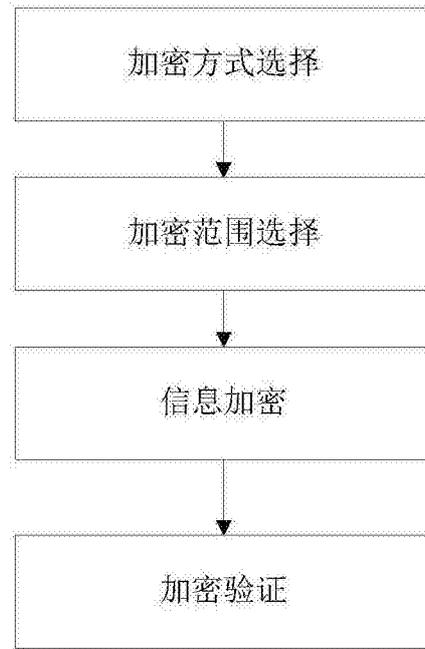


图5