(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295259 A
(43)申请公布日 2017.01.04

(21)申请号 201610638410.8

(22)申请日 2016.08.03

(71)申请人 杭州晟元数据安全技术股份有限公司

地址 311121 浙江省杭州市余杭区五常街道文一西路998号9幢东楼

(72)发明人 苗欣 夏军虎 钱志恒 洪竞志

(74)专利代理机构 杭州千克知识产权代理有限公司 33246

代理人 赵芳 张瑜

(51)Int.Cl.

G06F 21/12(2013.01)

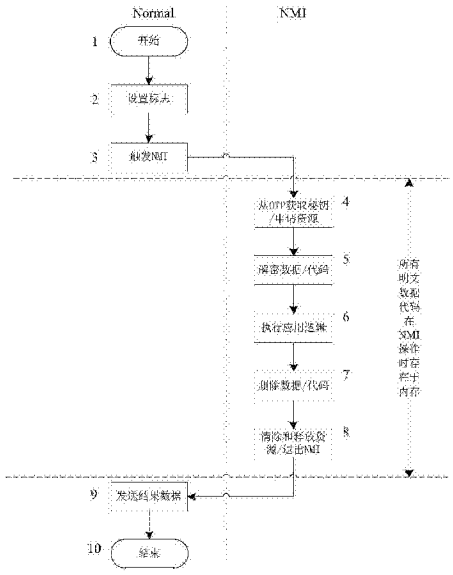
权利要求书1页 说明书4页 附图3页

(54)发明名称

一种利用不可执行中断提高物联网产品安全性的方法

(57)摘要

一种利用不可执行中断提高物联网产品安全性的方法，所有安全应用/操作在NMI中执行，步骤如下：(1)系统调用安全应用/操作N；(2)配置安全应用/操作N的调用标志；(3)触发NMI，NMI处理函数判断步骤(2)中设置的标志获知被调用的安全应用/操作以及获取参数；(4)从OTP中获取安全应用/操作N所需的各类秘钥，存放于申请到的资源中；(5)使用秘钥解密获得明文数据和代码；(6)执行安全应用/操作N的逻辑，包括数据的处理以及结果的加密和签名；(7)删除解密得到的数据和代码明文；(8)清除和释放申请到的资源，退出NMI；(9)发送安全应用/操作N的结果数据；(10)结束安全应用/操作N的调用。



CN 106295259 A

1.一种利用不可执行中断提高物联网产品安全性的方法,包括一般应用/操作和安全应用/操作,其特征在于:所有安全应用/操作在NMI中执行,具体步骤如下:

(1)系统调用安全应用/操作N;

(2)配置安全应用/操作N的调用标志;

(3)触发NMI,NMI处理函数判断步骤(2)中设置的标志获知被调用的安全应用/操作以及获取参数;

(4)从OTP中获取安全应用/操作N所需的各类秘钥,存放于申请到的资源中;

(5)使用秘钥解密获得明文数据和代码;

(6)执行安全应用/操作N的逻辑,包括数据的处理以及结果的加密和签名;

(7)删除解密得到的数据和代码明文;

(8)清除和释放申请到的资源,退出NMI;

(9)发送安全应用/操作N的结果数据;

(10)结束安全应用/操作N的调用。

2.根据权1所述的一种利用不可执行中断提高物联网产品安全性的方法,其特征在于:所述NMI初步解析和调度函数能以只执行方式存在于OTP中。

3.根据权1或2所述的一种利用不可执行中断提高物联网产品安全性的方法,其特征在于:所述安全应用/操作能调用一般外设驱动。

4.根据权3所述的一种利用不可执行中断提高物联网产品安全性的方法,其特征在于:所述一般应用能使用安全操作控制敏感外设。

一种利用不可执行中断提高物联网产品安全性的方法

技术领域

[0001] 本发明涉及一种利用不可执行中断提高物联网产品安全性的方法。

背景技术

[0002] 物联网将是下一个推动世界高速发展的“重要生产力”，是继通信网之后的另一个万亿级市场。业内专家认为，物联网一方面可以提高经济效益，大大节约成本；另一方面可以为全球经济的复苏提供技术动力。美国、欧盟等都在投入巨资深入研究探索物联网。我国也正在高度关注、重视物联网的研究，工业和信息化部会同有关部门，在新一代信息技术方面正在开展研究，以形成支持新一代信息技术发展的政策措施。

[0003] 此外，普及以后，用于动物、植物和机器、物品的传感器与电子标签及配套的接口装置的数量将大大超过手机的数量。物联网的推广将会成为推进经济发展的又一个驱动器，为产业开拓了又一个潜力无穷的发展机会。按照对物联网的需求，需要按亿计的传感器和电子标签，这将大大推进信息技术元件的生产。

[0004] 然而随着物联网的高速发展，物联网产品的安全问题也越来越受到重视。根据物联网自身的特点，物联网除了面对移动通信网络的传统网络安全问题之外，还存在着一些与已有移动网络安全不同的特殊安全问题。这是由于物联网是由大量的机器构成，缺少人对设备的有效监控，并且数量庞大，设备集群等相关特点造成的，这些特殊的安全问题主要有以下几个方面。

[0005] 物联网机器/感知节点的本地安全问题。由于物联网的应用可以取代人来完成一些复杂、危险和机械的工作。所以物联网机器/感知节点多数部署在无人监控的场景中。那么攻击者就可以轻易地接触到这些设备，从而对他们造成破坏，甚至通过本地操作更换机器的软硬件。

[0006] 物联网业务的安全问题。由于物联网设备可能是先部署后连接网络，而物联网节点又无人看守，所以如何对物联网设备进行远程签约信息和业务信息配置就成了难题。另外，庞大且多样化的物联网平台必然需要一个强大而统一的安全管理平台，否则独立的平台会被各式各样的物联网应用所淹没，但如此一来，如何对物联网机器的日志等安全信息进行管理成为新的问题，并且可能割裂网络与业务平台之间的信任关系，导致新一轮安全问题的产生。

[0007] 普通的物联网机器/感知节点的结构如图1所示，其系统调用应用/操作N的流程图如图2所示，具体步骤如下：

1、系统调用应用/操作N；

2、从OTP(One Time Programable，是MCU的一种存储器类型，意思是一次性可编程：程序烧入IC后，将不可再次更改和清除)中获取应用/操作N所需的各类秘钥，存放于申请到的资源(堆/栈)中；

3、使用秘钥解密获得明文数据和代码；

4、执行应用/操作N的逻辑，包括数据的处理以及结果的加密和签名；

5、删除解密得到的数据和代码明文；

6、发送应用/操作N的结果数据；

7、结束应用/操作N的调用。

[0008] 其中，步骤2到步骤7之间，内存中存在明文操作代码；步骤3到步骤6之间，内存中存在明文秘钥、明文敏感数据；因此，攻击者通过操作系统漏洞或者其他方式突破应用之间的隔离后，可以在A1-A5这5个攻击点获取应用/操作N的明文代码，可以在A2-A4这3个攻击点获取明文秘钥和敏感信息。当攻击者从A2-A4间获取明文秘钥后，一切防护手段都形同虚设，而即使没有获得秘钥，攻击者也可以在A1-A5之间获取操作/应用的明文代码，从而侵害开发者的知识产权。由于操作系统的漏洞是普遍存在的，因此目前方案的安全性无法得到保障。

[0009] 目前大多数的物联网产品方案，安全性上已经做了一定的设计，其方法的主要是对数据的交互进行加密，端上仍然以明文存在，设备的安全性依然存在不小的缺陷。具体如下：

1、加解密操作本身暴露在攻击者面前，攻击者可以很轻易的侵入加解密操作；

2、当攻击者侵入加解密操作时，敏感信息和代码可以被很轻易的获取；

3、应用和应用之间采用软件或操作系统隔离，由于操作系统的漏洞普遍存在，因此攻击者很容易突破隔离，获取或控制应用。

发明内容

[0010] 本发明提供了一种提高数据和代码安全性、通用性高、不易被入侵的利用不可执行中断提高物联网产品安全性的方法，其中不可执行中断简称NMI。

[0011] 本发明采用的技术方案是：

一种利用不可执行中断提高物联网产品安全性的方法，包括一般应用/操作和安全应用/操作，其特征在于：所有安全应用/操作在NMI中执行，具体步骤如下：

(1)系统调用安全应用/操作N；

(2)配置安全应用/操作N的调用标志；

(3)触发NMI，NMI处理函数判断步骤(2)中设置的标志获知被调用的安全应用/操作以及获取参数；

(4)从OTP中获取安全应用/操作N所需的各类秘钥，存放于申请到的资源(堆/栈)中；

(5)使用秘钥解密获得明文数据和代码；

(6)执行安全应用/操作N的逻辑，包括数据的处理以及结果的加密和签名；

(7)删除解密得到的数据和代码明文；

(8)清除和释放申请到的资源，退出NMI；

(9)发送安全应用/操作N的结果数据；

(10)结束安全应用/操作N的调用。

[0012] 本发明所有安全应用/操作所需的敏感数据/秘钥/代码都只在步骤(4)到步骤(8)之间存在于内存中，在其余步骤中只以密文形式存在；同时，由于步骤(4)到步骤(8)不可被中断、嵌套、屏蔽，因此可以视作一个原子操作，攻击者无法通过任何软件或漏洞来攻击，而其余步骤，虽然攻击者能够攻击，但并不存在任何明文敏感数据/代码，因此攻击者无法获

取任何有意义的敏感数据/代码。此外，攻击者在一般状态下虽然可以通过攻击来修改NMI响应函数指针，但由于攻击者无法获得敏感信息/操作/代码因此无法操作敏感外设或获取敏感信息，只能操作一般外设或者获取一般信息，从而提高数据和代码的安全性。

[0013] 进一步，所述NMI初步解析和调度函数能以只执行方式存在于OTP中，保证NMI响应无法被修改和获取。

[0014] 进一步，所述安全应用/操作能调用一般外设驱动，此时一般外设驱动的行为也享有高安全性，但由于本身代码存在于非安全区，外设行为本身可能事先被攻击者篡改。

[0015] 进一步，所述一般应用能使用安全操作控制敏感外设，改操作本身享有高安全性。

[0016] 本发明的有益效果：

1、通用性很高，基本上使用任何MCU设计的产品都能实现；

2、能大幅提高安全性，基本杜绝任何非硬件方式的攻击；

3、不需要修改现有产品的任何硬件设计，方便目前设备的安全升级；

4、可以以操作为单元而并非以应用为单元进行保护，从而实现保持高性能下系统的安全；

5、可以实现软件层面的定制，高度灵活，可以按照实际需求实现性能和安全的协调；

6、保护数据安全的同时可以保护开发者代码安全，防止抄袭，复制等知识产权侵权；

7、在物联网产品等应用处理相对简单，对实时性要求相对较低，因此采用本发明完全可以按需优化和满足其对实时性的需求。

附图说明

[0017] 图1是现有物联网机器/感知节点的结构示意图。

[0018] 图2是现有物联网机器/感知节点的系统调用应用/操作N的流程示意图。

[0019] 图3是本发明物联网机器/感知节点的结构示意图。

[0020] 图4是本发明物联网机器/感知节点的系统调用应用/操作N的流程示意图。

具体实施方式

[0021] 下面结合具体实施例来对本发明进行进一步说明，但并不将本发明局限于这些具体实施方式。本领域技术人员应该认识到，本发明涵盖了权利要求书范围内所可能包括的所有备选方案、改进方案和等效方案。

[0022] 参照图3、图4，一种利用不可执行中断提高物联网产品安全性的方法，包括一般应用/操作和安全应用/操作，其特征在于：所有安全应用/操作在NMI中执行，具体步骤如下：

(1)系统调用安全应用/操作N；

(2)配置安全应用/操作N的调用标志；

(3)触发NMI，NMI处理函数判断步骤(2)中设置的标志获知被调用的安全应用/操作以及获取参数；

(4)从OTP中获取安全应用/操作N所需的各类秘钥，存放于申请到的资源(堆/栈)中；

(5)使用秘钥解密获得明文数据和代码；

(6)执行安全应用/操作N的逻辑，包括数据的处理以及结果的加密和签名；

(7)删除解密得到的数据和代码明文；

(8)清除和释放申请到的资源,退出NMI;

(9)发送安全应用/操作N的结果数据;

(10)结束安全应用/操作N的调用。

[0023] 本发明所有安全应用/操作所需的敏感数据/秘钥/代码都只在步骤(4)到步骤(8)之间存在于内存中,在其余步骤中只以密文形式存在;同时,由于步骤(4)到步骤(8)不可被中断、嵌套、屏蔽,因此可以视作一个原子操作,攻击者无法通过任何软件或漏洞来攻击,而其余步骤,虽然攻击者能够攻击,但并不存在任何明文敏感数据/代码,因此攻击者无法获取任何有意义的敏感数据/代码。此外,攻击者在一般状态下虽然可以通过攻击来修改NMI响应函数指针,但由于攻击者无法获得敏感信息/操作/代码因此无法操作敏感外设或获取敏感信息,只能操作一般外设或者获取一般信息,从而提高数据和代码的安全性。本发明一般操作安全要求不高,可以存在明文信息/代码/配置等。

[0024] 本实施例所述NMI初步解析和调度函数能以只执行方式存在于OTP中,保证NMI响应无法被修改和获取。

[0025] 本实施例所述安全应用/操作能调用一般外设驱动,此时一般外设驱动的行为也享有高安全性,但由于本身代码存在于非安全区,外设行为本身可能事先被攻击者篡改。

[0026] 本实施例所述一般应用能使用安全操作控制敏感外设,改操作本身享有高安全性。

[0027] 本发明在普通状态下,系统本身不存在任何敏感的代码/数据/秘钥,因此攻击者没有数据可以探测;在真正敏感操作执行的流程中,通过NMI的特性保证攻击者无法采取中断/嵌套/注入应用实现攻击,无法获取任何信息;从而实现通用芯片中开发物联网应用的数据和代码安全性大幅提高。由于完全利用绝大部分内核普遍存在的特性,不需要修改硬件或影响芯片选型,不需要选用带有自带安全单元的MCU或外挂SE芯片,不提高生产和设计成本;可以很好的和硬件保护方案形成互补;同时能很好的保护开发者代码的安全,保护代码知识产权;能够按照需求实现以操作为单位的保护,根据实际应用场景,开发者可以实现性能和安全之间的平衡,从而灵活的调整安全和性能间的平衡,以适应各种应用。

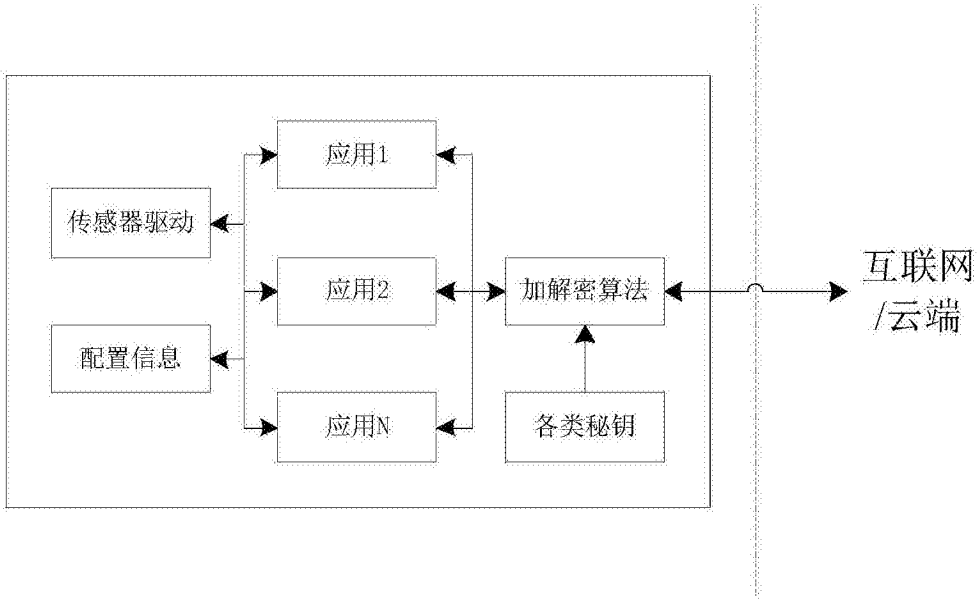


图1

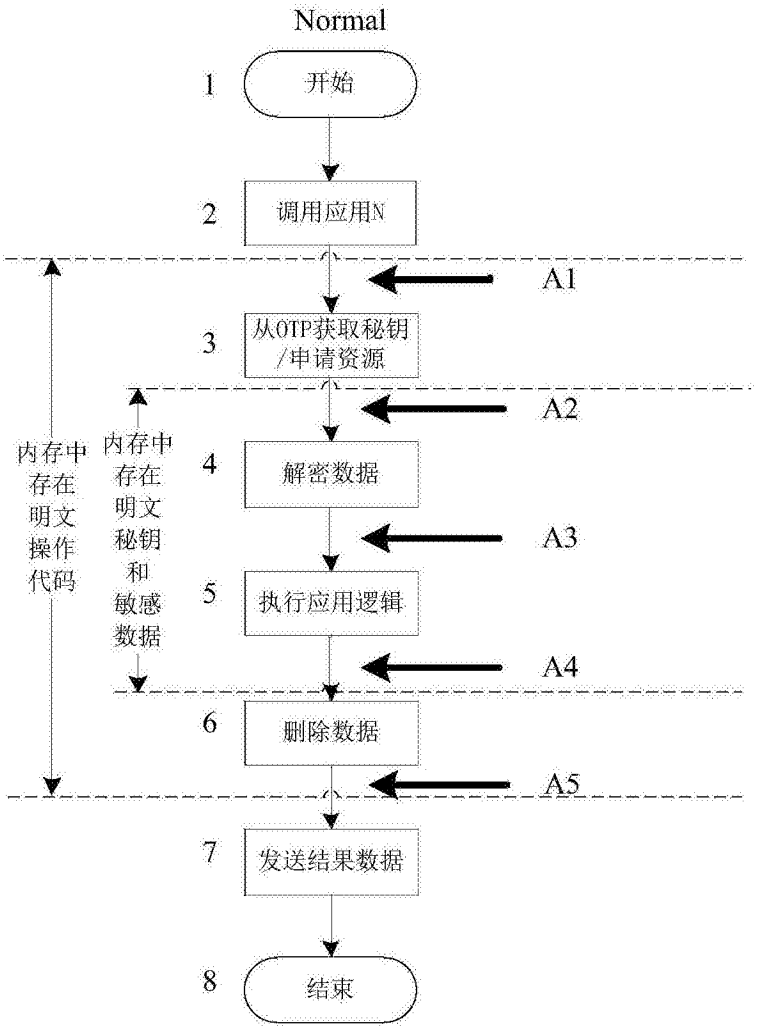

Normal
1
开始
2
调用应用N
A1
3
从OTP获取秘钥/申请资源
A2
内存中存在明文操作代码
内存中存在明文秘钥和敏感数据
4
解密数据
A3
5
执行应用逻辑
A4
6
删除数据
A5
7
发送结果数据
8
结束

图2

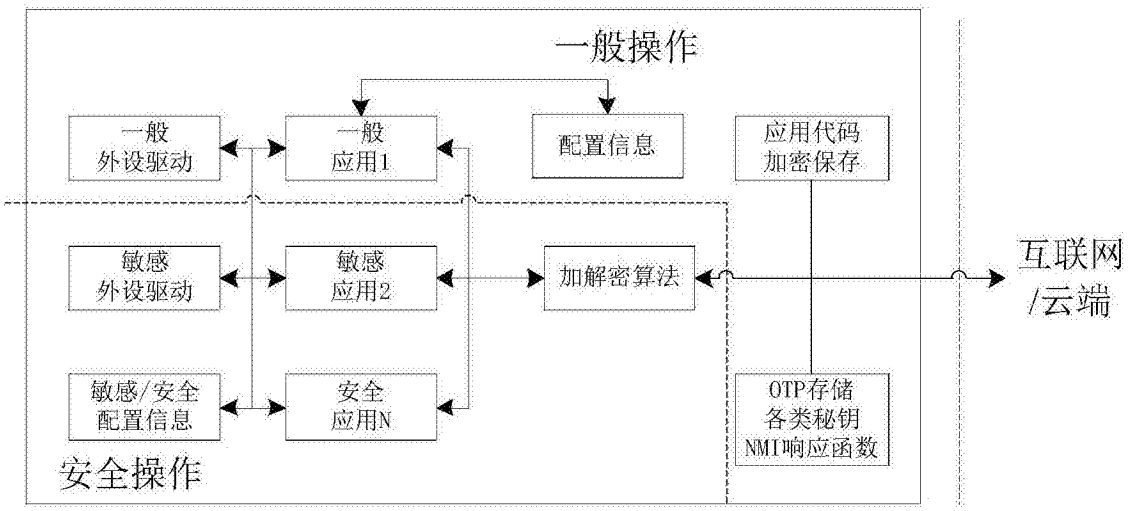

一般操作
一般外设驱动
一般应用1
配置信息
应用代码加密保存
敏感外设驱动
敏感应用2
加解密算法
互联网/云端
敏感/安全配置信息
安全应用N
OTP存储各类秘钥NMI响应函数
安全操作

图3

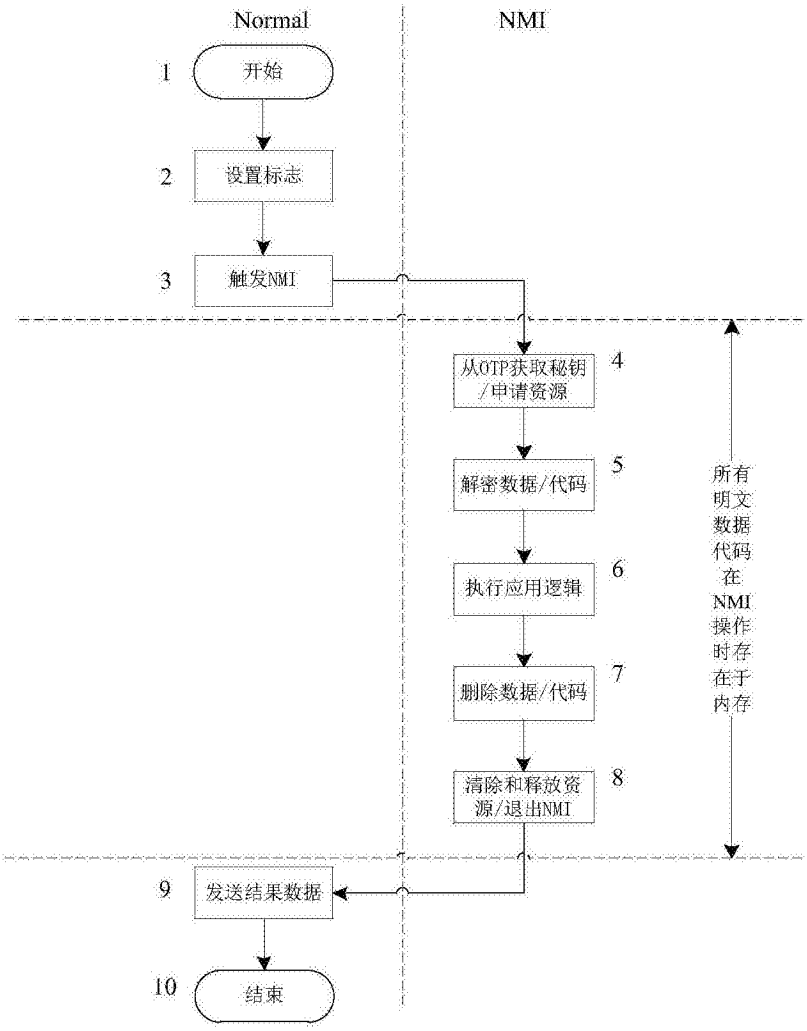

Normal
NMI
1
开始
2
设置标志
3
触发NMI
从OTP获取秘钥/申请资源
4
解密数据/代码
5
执行应用逻辑
6
删除数据/代码
7
清除和释放资源/退出NMI
8
所有明文数据代码在NMI操作时存在于内存
9
发送结果数据
10
结束

图4