(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 109951276 B
(45)授权公告日 2021.12.03

(21)申请号 201910159069.1

(22)申请日 2019.03.04

(65)同一申请的已公布的文献号
申请公布号 CN 109951276 A

(43)申请公布日 2019.06.28

(73)专利权人 北京工业大学
地址 100124 北京市朝阳区平乐园100号

(72)发明人 王冠 陈憨 陈健中 周珺

(74)专利代理机构 北京思海天达知识产权代理有限公司 11203
代理人 刘萍

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 29/06(2006.01)

(56)对比文件
US 2011167503 A1,2011.07.07
CN 104580250 A,2015.04.29
池亚军.基于USBkey 的可信平台模块的研究与仿真设计.《北京电子科技学院学报》.2007,第15卷(第4期),
RUCHIKA GUPTA等.SECURITY 301: QORIQ TRUST ARCHITECTURE AS SOFT TRUSTED PLATFORM MODULE (TPM).《FTF 2016》.2016,
Iliano Cervesato.Trusted Computing Technology and Client-Side Access Control Architecture.《ISA 767》.2006,

审查员 万林青

权利要求书2页 说明书4页 附图1页

(54)发明名称

基于TPM的嵌入式设备远程身份认证方法

(57)摘要

基于TPM的嵌入式设备远程身份认证方法属于信息安全领域，利用的是可信计算技术，它是信息安全领域的一门新技术，具有自主免疫、全程可控可测等优点。本发明旨在利用可信计算完整性度量、密钥管理和平台绑定等优势，设计一种远程身份认证的方法。先对平台配置做可信度量，然后将度量值扩展到平台配置寄存器，把此度量值作为认证信息中的一项。TPM芯片内的背书密钥(EK)与平台身份绑定，由背书密钥(EK)产生身份认证密钥(AIK)，然后再由身份认证密钥(AIK)签名平台配置度量值，这样不但可以验证平台身份，还可以认证平台完整性。这相较于传统的远程身份认证优势明显。

CN 109951276 B

1.基于TPM的嵌入式设备远程认证方法,其特征在于包括以下步骤:

(1).生成平台完整性信息并存储:

1.1在加载任一模块之前,通过可信平台模块TPM采用SHA1算法计算其二进制代码的散列值,并将其扩展到PCR中;

(2).生成验证信息并打包发送:

2.1用可信平台模块TPM生成一对AIK公私钥对;

AIK公私钥对用RSA算法产生,步骤如下:

1)随机产生两个大奇素数p和q;

2)计算n,n=p*q;

3)随机选取一个数e,e是小于$\varphi(n)=(p-1)(q-1)$且与它互素的正整数;

4)计算d,使得$ed \equiv 1 \bmod \varphi(n)$;

5)公钥为{e,n},私钥为{d,p,q};

2.2把生成AIK的公钥、配置日志、平台完整性信息、哈希算法类型、背书证书和平台证书一起打包;

2.3将包做MD5转换,生成摘要m

2.4使用AIK(Attestation Identity Key)的私钥部分对产生的包摘要m进行签名,产生签名s;

$s=m^d \bmod n$

2.5将签名值和包一起发送给一个可信第三方Privacy CA;

(3).第三方验证配置信息:

3.1可信第三方Privacy CA接收到申请请求信息之后,首先使用AIK的公钥检验签名信息是否正确;

1)获得公钥{n,e};

2)计算$m'=s^e \bmod n$

3)验证m是否等于m',如果相等,则签名通过;

3.2读取包中的哈希算法类型;

3.3对配置日志用SHA-1取哈希值;

3.4与请求者上传的日志哈希值对比,看是否正确;

(4).第三方颁发证书:

4.1若签名和哈希值都正确,则根据其中的AIK公钥部分生成一个身份密钥证书;

4.2可信第三方Privacy CA产生一个对称密钥作为会话密钥;

4.3使用会话密钥对新生成的AIK证书进行加密,产生一个对称加密密文;

4.4可信第三方Privacy CA使用发送申请请求的可信平台模块的EK公钥对该会话密钥加密,产生一个非对称密文结构;应答信息包括被加密的会话密钥,被加密的证书,以及加密算法参数;

1)首先将明文比特串分组,使得每个分组对应的十进制数小于n,即分组长度小于$\log_2 n$;n=p*q.

2)然后对每个明文分组M作加密运算:$c=M^e \pmod n$;

4.5可信第三方Privacy CA将上述应答信息发送给可信平台模块；

(5).平台解密证书：

5.1平台首先使用自己的EK私钥部分解密加密证书的会话密钥；

对密文分组c作解密运算:$M=c^{d}(\mathrm{mod}\ n)$；

5.2再使用该会话密钥解密证书；

于步骤2.3具体为：

1)对消息进行填充,使其长度等于448mod 512；

2)将消息长度缩减为mod 64,然后以一个64位的数字添加到扩展后消息的尾部；

3)MD5初始输出放在四个32位寄存器A、B、C、D中,这些寄存器随后将用于保存散列函数的中间结果和最终结果;初始值为：

A＝67452301;B＝EFCDAB89;C＝98BADCFE;D＝10325476

4)MD5将以四轮方式处理每一个512位块；

5)完成所有四轮之后,ABCD的初始值加到ABCD的新值上,生成第i个消息块的输出;这个输出用作开始处理第i+1个消息块的输入;最后一个消息块处理完之后,ABCD中保存的128位内容就是所处理消息的散列值。

基于TPM的嵌入式设备远程身份认证方法

技术领域

[0001] 本专利属于信息安全领域，利用的是可信计算技术，它是信息安全领域的一门新技术，具有自主免疫、全程可控可测等优点。本发明旨在利用可信计算完整性度量、密钥管理和平台绑定等优势，设计一种远程身份认证的方法。

背景技术

[0002] 可信计算的基本思想是立足于终端，在终端构建一个信任根，以信任根为起点，通过完整性度量技术，建立信任链，实现信任由信任根扩展到硬件平台、操作系统，直至整个网络，保证整个计算环境的可信。其目的是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高整体的安全性。可信计算技术弥补了以防外为主的防御手段的缺陷。它立足于入侵源头设防，对网络上的每一个节点实施认证和控制，建立点对点的信任机制。基于这个信任系统，实施身份认证、授权访问控制和安全责任审计等防御手段，突破了传统的“堵漏洞、做高墙、防外攻”的被动方式。可信计算技术以完整性度量技术为基础，通过信息的信任传递模式，保障了信息在用户、程序与机器之间的可信传递，建立了由信任根到

[0003] 网络的信任链，从而维护了网络和信息安全。

[0004] 可信平台模块(TPM)是一种集成在可信计算平台中，用于建立和保障信任源点的硬件核心模块，为可信计算提供完整性度量、安全存储、可信报告以及密码服务等功能。可信平台模块作为信任度量的起点包括可信度量根、可信存储根和可信报告根三个信任根。以可信平台控制模块为基础，可以扩展出可信计算平台的可信度量功能、可信报告功能与可信存储功能。可信平台控制模块是可信计算平台体系结构中的信任根。可信平台模块是以密码模块的密码技术为基础，为平台自身的完整性、身份可信性和数据安全性提供密码支持。

发明内容

[0005] 本发明通过提供一系列与平台相关的证书和平台信息来证明通信的平台就是一个可信计算平台的真实身份。可信计算平台的身份是通过可信平台模块(TPM)的背书密钥证书EK(Endorsement Key Credential)来标识的，该证书可以表明安全芯片与平台之间的绑定关系。如果直接使用EK(Endorsement Key)证书来进行远程证明，可能会暴露背书密钥EK(Endorsement Key)。因此，使用可信第三方Privacy CA的方法协助可信平台模块(TPM)完成身份证明。基于Privacy CA的证明方法就是通过为可信平台模块(TPM)平台身份密钥颁发平台身份密钥证书来标识身份。证明时验证方需要向Privacy CA请求，确认平台身份密钥的正确性来完成证明。本发明在请求验证的信息中加入了平台度量信息，实现了对平台的身份认证和完整性认证。

[0006] 具体步骤为：

[0007] 1.可信平台模块(TPM)生成一对AIK(Attestation Identity Key)公私钥对，把生

成的AIK(Attestation Identity Key)的公钥部分以及请求产生AIK(Attestation Identity Key)证书的可信平台模块(TPM)的一些标识信息(其中包括设备度量信息),包括背书证书和平台证书打包;

[0008] 2.使用AIK(Attestation Identity Key)的私钥部分对刚产生的包进行签名;

[0009] 3.将签名值和包一起发送给一个可信第三方Privacy CA,等待Privacy CA接收请求后生成证言身份证书;

[0010] 4.可信第三方Privacy CA接收到申请请求信息之后,首先使用AIK(Attestation Identity Key)的公钥检验签名信息是否正确,若正确则根据其中的AIK(Attestation Identity Key)公钥部分生成一个身份密钥证书;

[0011] 5.随后,可信第三方Privacy CA产生一个对称密钥作为会话密钥,并使用这个密钥对新生成的AIK(Attestation Identity Key)证书进行加密,产生一个对称加密密文;

[0012] 6.可信第三方Privacy CA使用发送申请请求的可信平台模块(TPM)的EK(Endorsement Key)公钥对该会话密钥加密,产生一个非对称密文结构。应答信息包括被加密的会话密钥,被加密的证书,以及一些加密算法参数等。最后可信第三方Privacy CA将应答信息发送给可信平台模块(TPM);

[0013] 7.可信平台模块(TPM)接收到该结构之后进行解密:首先使用自己的EK(Endorsement Key Credential)私钥部分解密加密证书的会话密钥,然后再使用该会话密钥解密证书。

附图说明

[0014] 图1是TPM芯片体系结构图

[0015] 图2是嵌入式平台的信任链构建过程

[0016] 图3是远程身份认证流程图

具体实施方式

[0017] 1.生成平台完整性信息并存储:

[0018] 1.1在加载任一模块D之前,通过TPM采用SHA1算法计算其二进制代码的散列值,并将其扩展到PCR中,扩展操作为:

[0019] PCR[i]=SHA1(PCR[i]||SHA1(D)。

[0020] 2.生成验证信息并打包发送:

[0021] 2.1用可信平台模块(TPM)生成一对AIK(Attestation Identity Key)公私钥对;

[0022] AIK公私钥对用RSA算法产生,步骤如下:

[0023] 1)随机产生两个大奇素数p和q;

[0024] 2)计算n,n=p*q;

[0025] 3)随机选取一个数e,e是小于$\varphi(n)=(p-1)(q-1)$且与它互素的正整数;

[0026] 4)计算d,使得$ed\equiv 1 \bmod \varphi(n)$;

[0027] 5)公钥为{e,n},私钥为{d,p,q}。

[0028] 2.2把生成AIK(Attestation Identity Key)的公钥、配置日志、平台完整性信息、哈希算法类型、背书证书和平台证书一起打包;

[0029] 2.3将包做MD5转换,生成摘要m

[0030] 1)对消息进行填充,使其长度等于448mod 512;

[0031] 2)将消息长度缩减为mod 64,然后以一个64位的数字添加到扩展后消息的尾部;

[0032] 3)MD5初始输出放在四个32位寄存器A、B、C、D中,这些寄存器随后将用于保存散列函数的中间结果和最终结果。初始值为(十六进制形式):

[0033] A＝67452301;B＝EFCDAB89;C＝98BADCFE;D＝10325476

[0034] 4)MD5将以四轮方式处理每一个512位块;

[0035] 5)完成所有四轮之后,ABCD的初始值加到ABCD的新值上,生成第i个消息块的输出。这个输出用作开始处理第i+1个消息块的输入。最后一个消息块处理完之后,ABCD中保存的128位内容就是所处理消息的散列值。

[0036] 2.4使用AIK(Attestation Identity Key)的私钥部分对产生的包摘要m进行签名,产生签名s;

[0037] $s＝m^{d} \bmod n$

[0038] 2.5将签名值和包一起发送给一个可信第三方Privacy CA;

[0039] 3.第三方验证配置信息:

[0040] 3.1可信第三方Privacy CA接收到申请请求信息之后,首先使用AIK(Attestation Identity Key)的公钥检验签名信息是否正确;

[0041] 1)获得公钥{n,e};

[0042] 2)计算$m'＝s^{e} \bmod n$

[0043] 3)验证m是否等于m',如果相等,则签名通过。

[0044] 3.2读取包中的哈希算法类型;

[0045] 3.3对配置日志用SHA-1取哈希值;

[0046] 3.4与请求者上传的日志哈希值对比,看是否正确;

[0047] 4.第三方颁发证书:

[0048] 4.1若签名和哈希值都正确,则根据其中的AIK(Attestation Identity Key)公钥部分生成一个身份密钥证书;

[0049]

Version	2
Serial Number	10035
Signature Algorithm	SHA-1,RSA
Issuer DN	cu=US,o=VF
Validity Period	04/01/2016 08:00:00 04/01/2018 05:00:00
Subject DN	c=US,o=gov cn=John Smith
Subject Public Key	RSA,5503 3997…
Issuer UID	Usually omitted
Subject UID	Usually omitted
Signature	6A21 3E9F…

[0050] X.509证书格式

[0051] 4.2可信第三方Privacy CA产生一个对称密钥作为会话密钥；

[0052] 4.3使用会话密钥对新生成的AIK(Attestation Identity Key)证书进行加密,产生一个对称加密密文；

[0053] 4.4可信第三方Privacy CA使用发送申请请求的可信平台模块(TPM)的EK(Endorsement Key)公钥对该会话密钥加密,产生一个非对称密文结构。应答信息包括被加密的会话密钥,被加密的证书,以及加密算法参数。

[0054] 1)首先将明文比特串分组,使得每个分组对应的十进制数小于n,即分组长度小于$\log_2 n$。n＝p*q.

[0055] 2)然后对每个明文分组M作加密运算:$c = M^e \pmod n$。

[0056] 4.5可信第三方Privacy CA将上述应答信息发送给可信平台模块(TPM)；

[0057] 5.平台解密证书：

[0058] 5.1平台首先使用自己的EK(Endorsement Key Credential)私钥部分解密加密证书的会话密钥；

[0059] 对密文分组c作解密运算:$M = c^d \pmod n$。

[0060] 5.2再使用该会话密钥解密证书。


密码
协处理器
HMAC
引擎
SHA-1
引擎
配置选择
非易失性
存储器
I/O 部件
密钥产生
部件
随机数
发生器
电源检测
部件
执行引擎
易失性
存储器

图1

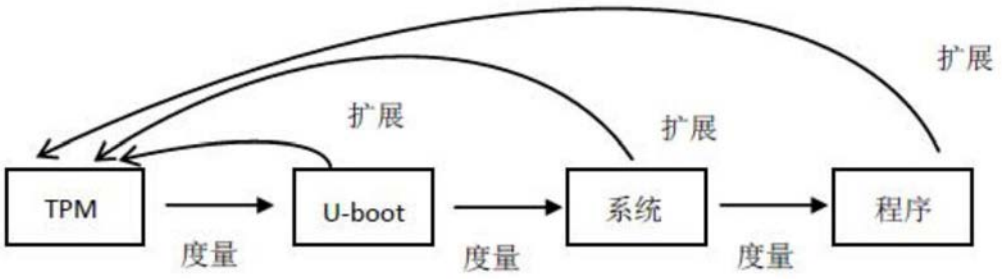
扩展
扩展
扩展
TPM
U-boot
系统
程序
度量
度量
度量

图2

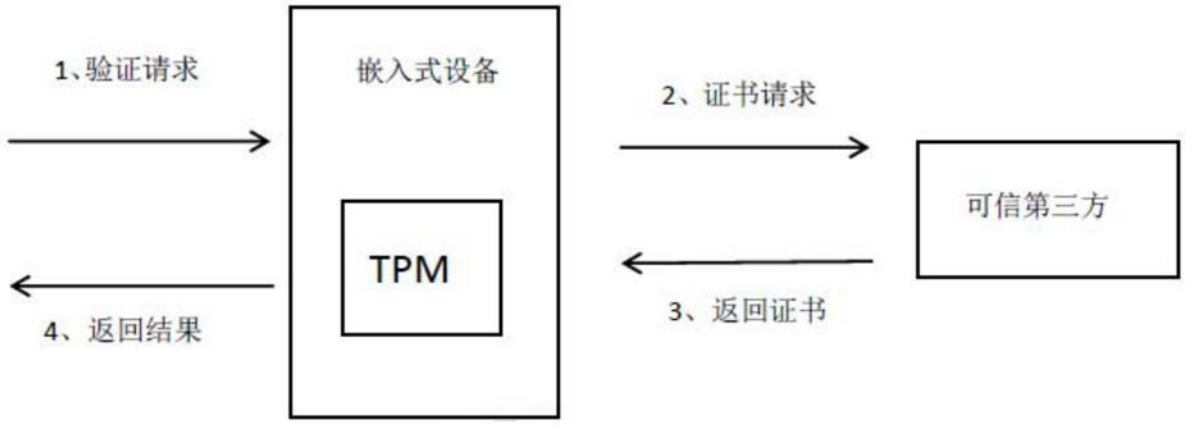
1、验证请求
嵌入式设备
2、证书请求
可信第三方
TPM
4、返回结果
3、返回证书

图3