ISSN 1009-3044
Computer Knowledge and Technology 电脑知识与技术
Vol.17, No.13 May 2021
E-mail: jslt@dnzs.net.cn
http://www.dnzs.net.cn
Tel:+86-551-65690963 65690964

可信计算技术在网络信息安全中的应用与研究

冯德尹,吴明念

(贵州工程应用技术学院,贵州 毕节 551700)

摘要:在目前网络技术应用越来越广泛的背景下,各种网络信息也越来越多,这些网络信息在人们的日常生活及工作中有着较高的价值,也就需要确保这些网络信息的安全性。在当前的网络信息安全中,要想使信息安全性真正实现有效提升,需要对各种相关的科学技术进行应用,而可信计算技术就是比较重要的一种,因而相关技术人员需要合理应用可信计算技术确保网络信息安全,以实现网络信息的更好应用。

关键词:网络信息安全;可信计算机技术;应用

中图分类号:TP393 文献标识码:A

文章编号:1009-3044(2021)13-0053-02

DOI:10.14004/j.cnki.ckt.2021.1345

开放科学(资源服务)标识码(OSID):

在现代网络信息越来越多的情况下,网络信息的利用也越来越重要,而网络信息的有效应用需要以网络信息安全为基础,也就必须要保证网络信息安全。就目前的网络信息安全来看,可信计算技术在保证网络信息安全性方面发挥着不可替代的价值及意义,因而相关技术人员必要要对可信计算技术及网络信息安全加强重视,且需要在网络信息完全中对可视化计算技术实行有效应用,以满足实际需求。

1 可信计算技术概述

所谓可信计算机就是以可信理论及算计理论相结合而形成的一种信息安全保护技术,在目前的网络信息安全保护方面有着十分重要的应用,并且在实际应用过程中也发挥出比较满意的效果。所谓可信所指的就是对于相关实体进行描述的属性特点,具体包括两个方面的特点,分别为主观特点与客观特点,其中客观特点主要就是利用计算机硬件实行判断,而主观特点主要就是由具体人实行主观判断。而可信计算所指的就是对于特定可信组件而言,在任何一种操作条件下都能够实行有效预测,且对于不良代码具有比较理想的抵抗作用,还能够有效防治物理干扰所造成的一些损坏。在当前的计算机网络信息安全中,可信计算已经成为重要基础,以可信跟角度为出发点,可使计算机网络安全问题得到有效解决。就目前可信计算应用的实际情况而言,可信计算终端是以可信计算平台模块为基础的,而可信计算平台模块需要提供几个放满的功能,主要包括数据保护、身份证明以及完整性测量,还有完整性存储与报告等相关内容。

就目前可信计算技术的应用而言,其主要就是将安全芯片结构引入计算机硬件平台中,利用其所提供的安全特性,使终端系统可以增强自身安全性。就目前可信计算的实现而言,其具体路线包括以下几点。首先,在PC机中需要进行信任根的构建,而信任根的可信任性可以通过物理安全、技术安全以及管理安全共同进行保证。在此基础上进行信任链的构建,整个信任链的层级就是由信任根到硬件平台,再到操作系统,之后到应用,通过逐级认证、逐级信任的方式,使这种信任可以不断扩展到整体PC系统。对于可信任链传递及可信任环境,其属于可信任链有计算机开始启动到整个操作系统完成内核装载前整体过程,具体来说就是计算机停电后开始启动,整个系统运行就会由可信BIOS传递至自检,然后向主引导区进行传递,且向可信操作系统装载器进行传递,之后就是向操作系统内核实行传递,开始系统初始化进程,在这一整个过程中,都是通过可信密码模块实现认证及处理,在经过可信任链相关传递之后,可进入可信服务及可信应用。通过以上步骤,也就可以使整个计算机操作系统的安全启动得以完成,并且利用可信平台模块对其可信性实行测量及评估,从而使网络信息安全得到更好的保证,使网络信息安全的价值更好地发挥出来。因此,在当前的网络信息安全中,对于可信计算技术实行有效应用十分必要,具有重要的价值及意义,也就需要实现可信计算技术的有效应用[1-2]。

2 可信计算技术在网络信息安全中的应用意义及价值

依据上文中对于可信计算技术的介绍,在当前的网络信息安全中对可信计算技术进行应用在确保信息安全性方面可以取得比较理想的效果,且具有重要的价值及意义,具体表现在以下方面。

首先,就安全技术方面来看,通过可信计算技术的应用对于信息控制中心的保护具有重要的作用及价值,可使信息数据的保护得以更好山西爱你,在对各种信息数据进行处理以及网络信息系统的实际运行操作过程中,可使网络信息系统的安全性及完整性得到更好地保证,在此基础上也就可以实现网络信息的更好利用,使网络信息的价值更好发挥,满足网络信息的应用需求及要求。其次,就管理措施层面而言,由于目前很多

收稿日期:2020-06-27

作者简介:冯德尹(1977—),女,贵州黔西县人、硕士,高级实验师,主要研究方向为计算机应用;吴明念(1975—),男,贵州大方县人、本科,高级工程师,主要研究方向为计算机应用、计算机网络及安全。

的网络信息安全管理中选择白名单机制安全系统，在对可信计算技术中的逐级测量及逐级信任的准入制度进行有效应用的基础上，对于信息安全管理可以实行更有效控制，在此基础上也就可以使网络信息的安全性得到更好的保证，为各种网络信息的更好利用提供更好的支持。再次，就技术价值层面而言。由于目前的很多网络信息中都包含一定的机密信息，这些机密信息涉及企业及单位的重要机密，一旦泄露，将会导致十分严重的后果及经济损失，而可信计算技术的应用可使信息安全得到更好保证，也就可以更有效地避免信息泄露情况出现，有效避免经济损失，因而具有十分重要的价值及意义[2-3]。

3 网络信息安全中可信计算技术的具体应用

依据上文所述，可信计算技术在网络信息安全中发挥着十分重要的作用，也就需要对可信计算技术实行有效应用，具体需要从以下几个方面入手，以可信计算技术为基础，对网络信息安全机制进行构建。

3.1 基于可信计算技术构建信息安全密钥管理机制

在网络信息安全方面，其关键就是信息安全存储，而安全存储属于可信计算平台所具备的各个功能中比较重要的一种，在信息安全存储方面的关键及核心技术就是密钥管理技术，对于密钥管理技术进行深入研究及合理应用在保证网络安全存储方面有着重要的价值及意义。在目前的可信计算平台中，依据可信计算技术标准，对于密钥管理机制进行有效构建，在该管理机制中所包含的内容主要就是密钥分类、密钥对象数据结构以及密钥对象存储机制等，还要密钥具体用途。对于可信计算平台中的密钥，依据其应用范围可以分为两种，即可迁移密钥与非迁移密钥，而依据不同功能，可以将其划分为存储密钥与签名密钥。对于密钥管理机制中每个密钥，其均具备固定数据结构，主要包含三个部分内容，即密钥特性、密钥通用信息及密钥专门信息等。其中，密钥特性所包含的内容就是主要就是对密钥对象的可迁特性进行描述，同时填充PCR值中的数据项；而密钥通用信息主要包括对密钥对象描述的相关密码算法、密钥类型及有关密钥授权信息；而密钥专门信息所包含的内容主要就是密钥长度、密钥标识付及密钥数据等。就当前的密钥对象存储而言，所包含的内容主要就是外部密钥存储与内部密钥存储，其中内部密钥存储主要就是以明文形式实行存储，而外部密钥存储主要就是通过密文方式实行存储。在当前的密钥对象中，只有两种密钥对象在可信计算平台内部永久性存储，即背书密钥与密钥根。其中，背书根密钥可以表明可信计算平台模块中的属主身份，在可以在申请身份证书时进行应用，无法直接提供身份证明，每个可信计算平台所对应的密钥根都是唯一的。

3.2 基于可信计算技术的信息安全远程报告机制

在当前的计算机网络维护过程中，在对系统补丁实行安装过程中，需要确定在PC操作系统中是不是已经安装了正确补丁；在实际的网络交易过程中，需要确定交易软件的安全性以及是否被病毒入侵；在将个人信息提交到网络系统的过程中，需确定个人信息安全性以及是否被窃取及篡改。在计算机网络信息系统的运行中，为能够使上述问题得到有效解决，在可信计算平台中以可信计算技术为基础构建远程完整性报告机制，从而对远程实体软件状态进行确定，这也是可信计算技术平台的重要功能之一。对于基于可信计算技术的远程完整性报告而言，穷属于各平台之间实现网络可信的重要依据，具有重要的价值。在计算机中接入可信网络的情况下，不但需要对网络自身身份可信度进行鉴定，并且需要对对象网络服务器实行鉴定，主要就是鉴定其运行环境及相关程序可信度，也就是网络安全性。在对这种方式进行有效应用的基础上，可有效避免不法程序的恶意感染，方式与恶意网络实现连接，从而使整个网络系统的安全性得到较好的保证，使计算机网络更加具有可信度，也就可以使网络信息安全得到保证，避免网络信息出现问题。

3.3 基于可信计算技术的信息安全匿名认证机制

随着目前科学技术的不断科学技术的不断快速发展，笔记本电脑及智能手机在人们的日常生活及工作中越来越普及，而这些设备中均配备可信计算平台模块。就这些设备的最初应用而言，可信计算平台模块的配备，不但未能够使终端设备可信度实现，反而致使人们在对这些设备实行营养过程中泄露自身隐私，致使一些不必要损失出现。为能够使这一问题得以有效解决，并且使可信计算平台模块实现更广泛应用及推广，在可信计算平台中构建Privacy方案，在这一方案中，对于可信计算平台模块，通过方案中的AIK证书实行验证，但是这一方案在实际应用中仍旧存在一定的问题，在此基础上又再次提出直接匿名认证机制。对于这一机制而言，其主要就是通过知识证明方式向远程实体实现身份证明，这样一来，也就可以在远程平台认证的过程中对于用户隐私进行有效保护，这样一来，也就可以使用户信息安全得到更好的保证，使网络信息安全性得以有效提升，为网络信息的更好利用提供基础与支持[3-4]。

4 结语

在当前的计算机网络运行过程中，保证网络信息的安全性已经成为重要的任务及需求，也是实现网络信息有效应用的重要基础，因而需要在这一方面更充分投入，而可信计算技术的应用对于该目标的实现十分有利。因此，相关研究人员及技术人员需要注重可信计算技术，并且以可信计算技术为基础，实行网络信息安全机制的有效构建，促使网络信息安全性得以有效提升，使网络信息的更好应用需求得到满足。

参考文献：

[1] 陈韶华.试论移动互联网时代信息安全新技术的展望[J].网络安全技术与应用,2019(11):2-3.
[2] 汪晓睿,张学超.云计算安全中可信计算技术的应用[J].卫星电视与宽带多媒体,2019(17):40-41.
[3] 许庆光,罗云锋,熊伟.嵌入式可信计算平台构建技术研究[J].网络安全技术与应用,2017(11):20-21.
[4] 安宁钰,徐志博,周峰.可信计算技术在全球能源互联网信息安全中的应用[J].电力信息与通信技术,2016,14(3):84-88.

【通联编辑：光文玲】